

1. Upgrade Guide	2
1.1 (A) (SEC) Administration Tool Log-In Update	2
1.2 (SQL) (UP) Update Database Field Lengths	3
1.3 (AC) (COMPAT) Fix Timezone Warning Messages for PHP v5.3	4
1.4 (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3	5
1.5 (C) (SEC) Add Customer Session Token to Forms	18
1.6 (C) (BUG) Validate Removal of Customer Address	27
1.7 (AC) (BUG) Sanitize Parameters	27
1.8 (A) (UP) Add Support for Basic HTTP Authentication	36
1.9 (C) (UP) Generate a New Shopping Cart ID When Restoring Products	45
1.10 (C) (BUG) Fix Navigation History Session Content	46
1.11 (AC) (UP) Improve Validation of E-Mail Addresses	46
1.12 (AC) (UP) Code Cleanup	51
1.13 (A) (UP) Update Define Languages Page	52
1.14 (C) (BUG) Verify Shopping Cart Product Attribute Combinations	57
1.15 (AC) (UP) Remove PHP3 Compatibility Code	58
1.16 (AC) (UP) Improve IP Address Detection	66
1.17 (A) (BUG) Don't Show Empty Menu Entries	70
1.18 (AC) (UP) Add htaccess Protection to the Images Directory	70
1.19 (C) (UP) Optimize Tax Calculations	70
1.20 (AC) (UP) Improve Force Cookie Usage in Sessions	73
1.21 (A) (BUG) Fix Automatic Removal of Manufacturer Images	73
1.22 (A) (UP) Add API Version Tag to Modules	74
1.23 (C) (UP) Hide Currencies and Languages Info Boxes for Single Currencies and Languages	75
1.24 (A) (UP) Hide Language Selection if Only One Language is Installed	76
1.25 (C) (BUG) Fix Retrieval of Special Product Prices	77
1.26 (A) (BUG) Fix HTML E-Mails	78
1.27 (A) (BUG) Improve Saving of Module Parameters	79
1.28 (AC) (UP) Add Pre-Populated List of Currencies	80
1.29 (A) (SQL) (NEW) Introduce Security Directory Permissions Feature	83
1.30 (AC) (SQL) (NEW) Introduce Action Recorder Feature	85
1.31 (AC) (UP) Cleanup Language Definitions	93
1.32 (AC) (NEW) Move Installation Checks to New Security Checks Modules	96
1.33 (A) (UP) Introduce Windows Compatible is_writable() Function	102
1.34 (A) (UP) Bypass HTTP Authentication for IIS Web servers	108
1.35 (AC) (UP) Update PHP_SELF Value	109
1.36 (A) (NEW) Introduce Easy Store Logo Uploader	110
1.37 (AC) (SQL) (UP) Update Password Hashing to Phpass	111
1.38 (C) (BUG) Fix Length Check of Customer Passwords	116
1.39 (C) (BUG) Fix Notice When Products Without Attributes are Added to the Shopping Cart	117
1.40 (C) (BUG) Verify Languages Currency Exists	118
1.41 (C) (BUG) Allow Quoted Words to be Searched	118

Upgrade Guide

osCommerce Online Merchant v2.3 Upgrade Guide

This upgrade guide is based on the osCommerce Online Merchant v2.2 Release Candidate 2a release. If you have not yet updated to v2.2RC2a, please review its upgrade guide in the extras directory ([upgrade-22rc2a.html](#)) before applying these changes.



This upgrade guide only provides the minimum required changes in the form of security updates and bug fixes. These changes will not upgrade your store to a complete v2.3 version. Please continue to use v2.2 add-ons and do not install v2.3 optimized add-ons as they may not function with your installation. If you wish to upgrade to a full v2.3 version, perform only (SQL) Database Changes and use the database with a new v2.3 installation.



The following changes should be performed in the following order.

Legend: (SQL) Database Changes (A) Administration Tool (C) Catalog

Types: (SEC) Security Update (BUG) Bug Fix (COMPAT) Compatibility Update (UP) General Update (NEW) New Feature

[View Changes Online](#)

- (A) (SEC) Administration Tool Log-In Update — Importance: High | Difficulty: Easy
- (SQL) (UP) Update Database Field Lengths — Importance: High | Difficulty: Easy
- (AC) (COMPAT) Fix Timezone Warning Messages for PHP v5.3 — Importance: Medium | Difficulty: Easy
- (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3 — Importance: Medium | Difficulty: Hard
- (C) (SEC) Add Customer Session Token to Forms — Importance: Medium | Difficulty: Medium
- (C) (BUG) Validate Removal of Customer Address — Importance: High | Difficulty: Easy
- (AC) (BUG) Sanitize Parameters — Importance: High | Difficulty: Medium
- (A) (UP) Add Support for Basic HTTP Authentication — Importance: High | Difficulty: Medium
- (C) (UP) Generate a New Shopping Cart ID When Restoring Products — Importance: Medium | Difficulty: Easy
- (C) (BUG) Fix Navigation History Session Content — Importance: High | Difficulty: Easy
- (AC) (UP) Improve Validation of E-Mail Addresses — Importance: Medium | Difficulty: Medium
- (AC) (UP) Code Cleanup — Importance: High | Difficulty: Easy
- (A) (UP) Update Define Languages Page — Importance: Medium | Difficulty: Medium
- (C) (BUG) Verify Shopping Cart Product Attribute Combinations — Importance: High | Difficulty: Easy
- (AC) (UP) Remove PHP3 Compatibility Code — Importance: Low | Difficulty: Easy
- (AC) (UP) Improve IP Address Detection — Importance: Medium | Difficulty: Easy
- (A) (BUG) Don't Show Empty Menu Entries — Importance: Low | Difficulty: Easy
- (AC) (UP) Add htaccess Protection to the Images Directory — Importance: Medium | Difficulty: Easy
- (C) (UP) Optimize Tax Calculations — Importance: Medium | Difficulty: Easy
- (AC) (UP) Improve Force Cookie Usage in Sessions — Importance: Medium | Difficulty: Easy
- (A) (BUG) Fix Automatic Removal of Manufacturer Images — Importance: High | Difficulty: Easy
- (A) (UP) Add API Version Tag to Modules — Importance: Low | Difficulty: Easy
- (C) (UP) Hide Currencies and Languages Info Boxes for Single Currencies and Languages — Importance: Low | Difficulty: Easy
- (A) (UP) Hide Language Selection if Only One Language is Installed — Importance: Low | Difficulty: Easy
- (C) (BUG) Fix Retrieval of Special Product Prices — Importance: Low | Difficulty: Easy
- (A) (BUG) Fix HTML E-Mails — Importance: Low | Difficulty: Easy
- (A) (BUG) Improve Saving of Module Parameters — Importance: Low | Difficulty: Easy
- (AC) (UP) Add Pre-Populated List of Currencies — Importance: Low | Difficulty: Easy
- (A) (SQL) (NEW) Introduce Security Directory Permissions Feature — Importance: Medium | Difficulty: Easy
- (AC) (SQL) (NEW) Introduce Action Recorder Feature — Importance: Medium | Difficulty: Hard
- (AC) (UP) Cleanup Language Definitions — Importance: Low | Difficulty: Easy
- (AC) (NEW) Move Installation Checks to New Security Checks Modules — Importance: Medium | Difficulty: Easy
- (A) (UP) Introduce Windows Compatible is_writable() Function — Importance: Low | Difficulty: Easy
- (A) (UP) Bypass HTTP Authentication for IIS Web servers — Importance: Low | Difficulty: Easy
- (AC) (UP) Update PHP_SELF Value — Importance: Low | Difficulty: Easy
- (A) (NEW) Introduce Easy Store Logo Uploader — Importance: Low | Difficulty: Easy
- (AC) (SQL) (UP) Update Password Hashing to Phpass — Importance: High | Difficulty: Easy
- (C) (BUG) Fix Length Check of Customer Passwords — Importance: Low | Difficulty: Easy
- (C) (BUG) Fix Notice When Products Without Attributes are Added to the Shopping Cart — Importance: Low | Difficulty: Easy
- (C) (BUG) Verify Languages Currency Exists — Importance: Low | Difficulty: Easy
- (C) (BUG) Allow Quoted Words to be Searched — Importance: Low | Difficulty: Easy

(A) (SEC) Administration Tool Log-In Update

(A) (SEC) Administration Tool Log-In Update

Importance: High | Difficulty: Easy

The Administration Tool log-in feature introduced in v2.2RC2 can be bypassed on Apache web servers with AcceptPathInfo enabled by manipulating the URL.

The fix involves setting a local `$login_request` variable in the `login.php` page and is checked for in `application_top.php` when no administrator session exists.

Affected Files

- `catalog/admin/includes/application_top.php`
- `catalog/admin/login.php`

[View Changes Online](#)

catalog/admin/includes/application_top.php

```
@@ -146,6 +146,10 @@
    $redirect = true;
}

+   if (!isset($login_request) || isset($_GET['login_request']) ||
isset($_POST['login_request']) || isset($_COOKIE['login_request']) ||
isset($_SESSION['login_request']) || isset($_POST_FILES['login_request']) ||
isset($_SERVER['login_request'])) {
+       $redirect = true;
+   }
+
+   if ($redirect == true) {
+       tep_redirect(tep_href_link(FILENAME_LOGIN));
+   }
```

catalog/admin/login.php

```
@@ -10,6 +10,8 @@
Released under the GNU General Public License
*/

+ $login_request = true;
+
+ require('includes/application_top.php');
+ require('includes/functions/password_funcs.php');
```

(SQL) (UP) Update Database Field Lengths

(SQL) (UP) Update Database Field Lengths

Importance: High | Difficulty: Easy

Update database table column field lengths.

[View Changes Online](#)

SQL Queries

```

alter table address_book modify entry_gender char(1);
alter table address_book modify entry_company varchar(255);
alter table address_book modify entry_firstname varchar(255) NOT NULL;
alter table address_book modify entry_lastname varchar(255) NOT NULL;
alter table address_book modify entry_street_address varchar(255) NOT NULL;
alter table address_book modify entry_suburb varchar(255);
alter table address_book modify entry_postcode varchar(255) NOT NULL;
alter table address_book modify entry_city varchar(255) NOT NULL;
alter table address_book modify entry_state varchar(255);

alter table administrators modify user_name varchar(255) binary NOT NULL;

alter table configuration modify configuration_value text NOT NULL;

alter table countries modify countries_name varchar(255) NOT NULL;

alter table customers modify customers_gender char(1);
alter table customers modify customers_firstname varchar(255) NOT NULL;
alter table customers modify customers_lastname varchar(255) NOT NULL;
alter table customers modify customers_email_address varchar(255) NOT NULL;
alter table customers modify customers_telephone varchar(255) NOT NULL;
alter table customers modify customers_fax varchar(255);

alter table orders modify customers_name varchar(255) NOT NULL;
alter table orders modify customers_company varchar(255);
alter table orders modify customers_street_address varchar(255) NOT NULL;
alter table orders modify customers_suburb varchar(255);
alter table orders modify customers_city varchar(255) NOT NULL;
alter table orders modify customers_postcode varchar(255) NOT NULL;
alter table orders modify customers_state varchar(255);
alter table orders modify customers_country varchar(255) NOT NULL;
alter table orders modify customers_telephone varchar(255) NOT NULL;
alter table orders modify customers_email_address varchar(255) NOT NULL;
alter table orders modify delivery_name varchar(255) NOT NULL;
alter table orders modify delivery_company varchar(255);
alter table orders modify delivery_street_address varchar(255) NOT NULL;
alter table orders modify delivery_suburb varchar(255);
alter table orders modify delivery_city varchar(255) NOT NULL;
alter table orders modify delivery_postcode varchar(255) NOT NULL;
alter table orders modify delivery_state varchar(255);
alter table orders modify delivery_country varchar(255) NOT NULL;
alter table orders modify billing_name varchar(255) NOT NULL;
alter table orders modify billing_company varchar(255);
alter table orders modify billing_street_address varchar(255) NOT NULL;
alter table orders modify billing_suburb varchar(255);
alter table orders modify billing_city varchar(255) NOT NULL;
alter table orders modify billing_postcode varchar(255) NOT NULL;
alter table orders modify billing_state varchar(255);
alter table orders modify billing_country varchar(255) NOT NULL;
alter table orders modify cc_owner varchar(255);

alter table reviews modify customers_name varchar(255) NOT NULL;

alter table whos_online modify full_name varchar(255) NOT NULL;

alter table zones modify zone_name varchar(255) NOT NULL;

```

(AC) (COMPAT) Fix Timezone Warning Messages for PHP v5.3

(AC) (COMPAT) Fix Timezone Warning Messages for PHP v5.3

Importance: Medium | Difficulty: Easy

PHP v5.3 displays a warning message if a default timezone has not been defined in its php.ini configuration file.

This fix checks if a default timezone has been defined and if not, defines a default timezone with the `date_default_timezone_get()` PHP function.

Affected Files

- catalog/admin/includes/functions/compatibility.php
- catalog/includes/functions/compatibility.php

[View Changes Online](#)

catalog/admin/includes/functions/compatibility.php

```
@@ -49,6 +49,11 @@
    do_magic_quotes_gpc($HTTP_COOKIE_VARS);
}

+// set default timezone if none exists (PHP 5.3 throws an E_WARNING)
+ if ((strlen(ini_get('date.timezone')) < 1) && function_exists('date_default_timezone_set')) {
+     date_default_timezone_set(@date_default_timezone_get());
+ }
+
+ if (!function_exists('is_numeric')) {
+     function is_numeric($param) {
+         return ereg("[0-9]{1,50}.?[0-9]{0,50}$", $param);
```

catalog/includes/functions/compatibility.php

```
@@ -49,6 +49,11 @@
    do_magic_quotes_gpc($HTTP_COOKIE_VARS);
}

+// set default timezone if none exists (PHP 5.3 throws an E_WARNING)
+ if ((strlen(ini_get('date.timezone')) < 1) && function_exists('date_default_timezone_set')) {
+     date_default_timezone_set(@date_default_timezone_get());
+ }
+
+ if (!function_exists('array_splice')) {
+     function array_splice(&$array, $maximum) {
+         if (sizeof($array) >= $maximum) {
```

(AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3

(AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3

Importance: Medium | Difficulty: Hard

The POSIX Regular Expressions (ereg) functions have been deprecated in PHP v5.3 which displays warning messages when the functions are used.

The fix is to replace all ereg related functions with preg functions.

Affected Files

- catalog/admin/backup.php
- catalog/admin/cache.php
- catalog/admin/configuration.php
- catalog/admin/includes/classes/language.php
- catalog/admin/includes/classes/phplot.php
- catalog/admin/includes/classes/sessions.php
- catalog/admin/includes/functions/compatibility.php
- catalog/admin/includes/functions/general.php
- catalog/admin/includes/functions/html_graphs.php
- catalog/admin/includes/functions/validations.php
- catalog/admin/modules.php
- catalog/admin/server_info.php
- catalog/admin/whos_online.php
- catalog/advanced_search_result.php
- catalog/includes/application_top.php
- catalog/includes/classes/cc_validation.php

- [catalog/includes/classes/http_client.php](#)
- [catalog/includes/classes/language.php](#)
- [catalog/includes/classes/sessions.php](#)
- [catalog/includes/functions/compatibility.php](#)
- [catalog/includes/functions/general.php](#)
- [catalog/includes/functions/validations.php](#)
- [catalog/index.php](#)

[View Changes Online](#)

catalog/admin/backup.php

```

@@ -63,7 +63,7 @@
        $schema .= ',' . "\n";
    }

-        $schema = ereg_replace(",\n$", '', $schema);
+        $schema = preg_replace("/,\n$/", '', $schema);

    // add the keys
    $index = array();
@@ -111,7 +111,7 @@
        $schema .= 'NULL, ';
    } elseif (tep_not_null($rows[$i])) {
        $row = addslashes($rows[$i]);
-        $row = ereg_replace("\n#", "\n".'\'#', $row);
+        $row = preg_replace("/\n#/ ", "\n".'\'#', $row);

        $schema .= '\'. ' . $row . '\', ';
    } else {
@@ -119,7 +119,7 @@
    }
}

-        $schema = ereg_replace(', $', ', ', $schema) . ');' . "\n";
+        $schema = preg_replace('/, $/', ', ', $schema) . ');' . "\n";
+        fputs($fp, $schema);
    }
}

@@ -239,7 +239,7 @@
        if ($next == '') { // get the last insert query
$next = 'insert';
        }
-        if ( (ereg('create', $next)) || (ereg('insert', $next)) || (ereg('drop t',
$next)) ) {
+        if ( (preg_match('/create/i', $next)) || (preg_match('/insert/i', $next)) ||
(preg_match('/drop t/i', $next)) ) {
            $query = substr($restore_query, 0, $i);

            $next = '';
@@ -248,7 +248,7 @@
        $sql_length = strlen($restore_query);
        $i = strpos($restore_query, ';')-1;

-        if (ereg('^create*', $query)) {
+        if (preg_match('/^create*/i', $query)) {
            $table_name = trim(substr($query, strpos($query, 'table ')+6));
            $table_name = substr($table_name, 0, strpos($table_name, ' '));

```

catalog/admin/cache.php

```

@@ -80,7 +80,7 @@
    }

    for ($i=0, $n=sizeof($cache_blocks); $i<$n; $i++) {
-       $cached_file = ereg_replace('-language', '-' . $language, $cache_blocks[$i]['file']);
+       $cached_file = preg_replace('/-language/', '-' . $language, $cache_blocks[$i]['file']);

        if (file_exists(DIR_FS_CACHE . $cached_file)) {
            $cache_mtime = strftime(DATE_TIME_FORMAT, filemtime(DIR_FS_CACHE . $cached_file));
@@ -89,9 +89,9 @@
            $dir = dir(DIR_FS_CACHE);

            while ($cache_file = $dir->read()) {
-               $cached_file = ereg_replace('-language', '-' . $language, $cache_blocks[$i]['file']);
+               $cached_file = preg_replace('/-language/', '-' . $language, $cache_blocks[$i]['file']);

-               if (ereg('^' . $cached_file, $cache_file)) {
+               if (preg_match('/^' . $cached_file . '/', $cache_file)) {
                    $cache_mtime = strftime(DATE_TIME_FORMAT, filemtime(DIR_FS_CACHE . $cache_file));
                    break;
                }
            }
        }
    }
}

```

catalog/admin/configuration.php

```

@@ -77,7 +77,7 @@
    while ($configuration = tep_db_fetch_array($configuration_query)) {
        if (tep_not_null($configuration['use_function'])) {
            $use_function = $configuration['use_function'];
-           if (ereg('->', $use_function)) {
+           if (preg_match('/->/', $use_function)) {
                $class_method = explode('->', $use_function);
                if (!is_object(${$class_method[0]})) {
                    include(DIR_WS_CLASSES . $class_method[0] . '.php');
                }
            }
        }
    }
}

```

catalog/admin/includes/classes/language.php

```

@@ -84,7 +84,7 @@
    for ($i=0, $n=sizeof($this->browser_languages); $i<$n; $i++) {
        reset($this->languages);
        while (list($key, $value) = each($this->languages)) {
-           if (ereg('^(' . $value . ')(;q=[0-9]\\.[0-9])?$', $this->browser_languages[$i]) &&
isset($this->catalog_languages[$key])) {
+           if (preg_match('/^(' . $value . ')(;q=[0-9]\\.[0-9])?$/i', $this->browser_languages[$i]) && isset($this->catalog_languages[$key])) {
                $this->language = $this->catalog_languages[$key];
                break 2;
            }
        }
    }
}

```

catalog/admin/includes/classes/phplot.php

```

@@ -674,8 +674,8 @@ class PHPlot{
    if ($which_valign == 'top') {
        $which_ypos = $which_ypos - ImageFontHeight($which_font);
    }
-   $which_text = ereg_replace("\r","", $which_text);
-   $sstr = split("\n", $which_text); //multiple lines submitted by Remi Ricard
+   $which_text = preg_replace("/\r/", "", $which_text);
+   $sstr = explode("\n", $which_text); //multiple lines submitted by Remi Ricard
$height = ImageFontHeight($which_font);
$width = ImageFontWidth($which_font);
    if ($which_angle == 90) { //Vertical Code Submitted by Marlin Viss
@@ -779,7 +779,7 @@ class PHPlot{
    function SetPlotType($which_pt) {
        $accepted = "bars,lines,linepoints,area,points,pie,thinbarline";
        $asked = trim($which_pt);
-       if (eregi($asked, $accepted)) {
+       if (preg_match('/' . $asked . '/i', $accepted)) {
            $this->plot_type = $which_pt;
            return true;
        } else {
@@ -936,7 +936,7 @@ class PHPlot{
    // It thus depends on the current character size, set by SetCharacterHeight().
    //////////////////////////////////////

-   $sstr = split("\n", $this->title_txt);
+   $sstr = explode("\n", $this->title_txt);
    $nbLines = count($sstr);

    if ($this->use_ttf == 1) {

```

catalog/admin/includes/classes/sessions.php

```

@@ -379,7 +379,7 @@
    // '<session-name>=<session-id>' to allow URLs of the form
    // http://yoursite/<session-name>=<session-id>/script.php
    if (empty($session->id)) {
-       eregi($session->name . '=[(AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP
v5.3^/]+)', $GLOBALS['REQUEST_URI'], $regs);
+       preg_match('/' . $session->name . '=[(AC) (COMPAT) Use Perl-Compatible Regular Expressions
for PHP v5.3^/]+/i', $GLOBALS['REQUEST_URI'], $regs);
        $regs[1] = trim($regs[1]);
        if (!empty($regs[1])) {
            $session->id = $regs[1];

```

catalog/admin/includes/functions/compatibility.php

```

@@ -56,7 +56,7 @@

    if (!function_exists('is_numeric')) {
        function is_numeric($param) {
-           return ereg("[0-9]{1,50}.?[0-9]{0,50}$", $param);
+           return preg_match("/^[0-9]{1,50}.?[0-9]{0,50}$/", $param);
        }
    }

@@ -87,7 +87,7 @@
    if(tep_not_null($host) && tep_not_null($type)) {
        @exec("nslookup -type=$type $host", $output);
        while(list($k, $line) = each($output)) {
-           if(ereg("^$host", $line)) {
+           if(preg_match("/^$host/i", $line)) {
                return true;
            }
        }
    }

```

catalog/admin/includes/functions/general.php


```

@@ -52,9 +52,9 @@
    }

    function tep_sanitiz_string($string) {
-       $string = ereg_replace(' +', ' ', $string);
-
-       return preg_replace("/[<>]/", '_', $string);
+       $patterns = array ('/ +/', '/[<>]/');
+       $replace = array (' ', '_');
+       return preg_replace($patterns, $replace, trim($string));
    }

    function tep_customers_name($customers_id) {
@@ -146,7 +146,7 @@
        if (@date('Y', mktime($hour, $minute, $second, $month, $day, $year)) == $year) {
            return date(DATE_FORMAT, mktime($hour, $minute, $second, $month, $day, $year));
        } else {
-            return ereg_replace('2037' . '$', $year, date(DATE_FORMAT, mktime($hour, $minute, $second,
$month, $day, 2037)));
+            return preg_replace('/2037$/', $year, date(DATE_FORMAT, mktime($hour, $minute, $second,
$month, $day, 2037)));
        }
    }
}

@@ -938,8 +938,8 @@
        $cached_file = $cache_blocks[$i]['file'];
        $languages = tep_get_languages();
        for ($j=0, $k=sizeof($languages); $j<$k; $j++) {
-            $cached_file_unlink = ereg_replace('-language', '-' .
$languages[$j]['directory'], $cached_file);
-            if (ereg('^' . $cached_file_unlink, $cache_file)) {
+            $cached_file_unlink = preg_replace('/-language/', '-' .
$languages[$j]['directory'], $cached_file);
+            if (preg_match('/^' . $cached_file_unlink . '/', $cache_file)) {
                @unlink(DIR_FS_CACHE . $cache_file);
            }
        }
    }

@@ -950,7 +950,7 @@
        $cached_file = $cache_blocks[$i]['file'];
        $languages = tep_get_languages();
        for ($i=0, $n=sizeof($languages); $i<$n; $i++) {
-            $cached_file = ereg_replace('-language', '-' . $languages[$i]['directory'],
$cached_file);
+            $cached_file = preg_replace('/-language/', '-' . $languages[$i]['directory'],
$cached_file);
            @unlink(DIR_FS_CACHE . $cached_file);
        }
    }
}

@@ -1276,7 +1276,7 @@
// nl2br() prior PHP 4.2.0 did not convert linefeeds on all OSs (it only converted \n)
function tep_convert_linefeeds($from, $to, $string) {
    if ((PHP_VERSION < "4.0.5") && is_array($from)) {
-        return ereg_replace('(' . implode('|', $from) . ')', $to, $string);
+        return preg_replace('/(' . implode('|', $from) . ')/', $to, $string);
    } else {
        return str_replace($from, $to, $string);
    }
}

```

catalog/admin/includes/functions/html_graphs.php

```

@@ -160,7 +160,7 @@
    $horizontal_graph_string .= '>';

    // decide if the value in bar is a color code or image.
-    if (ereg('^#', $bars[$i])) {
+    if (preg_match('/^#/', $bars[$i])) {
        $horizontal_graph_string .= '<table cellpadding="0" cellspacing="0" bgcolor="' .
$bars[$i] . '" width="' . ($values[$i] * $vals['scale']) . '">' . "\n" .
            ' <tr>' . "\n" .
            ' <td>&nbsp;</td>' . "\n" .

@@ -251,7 +251,7 @@
            ' <td>'

    // set background to a color if it starts with # or an image otherwise.
-    if (ereg('^#', $dbars[$i])) {
+    if (preg_match('/^#/', $dbars[$i])) {
        $double_horizontal_graph_string .= ' bgcolor="' . $dbars[$i] . '">';
    } else {
        $double_horizontal_graph_string .= ' background="' . $dbars[$i] . '">';
@@ -260,7 +260,7 @@
    $double_horizontal_graph_string .= '<nowrap>';

    // decide if the value in bar is a color code or image.
-    if (ereg('^#', $bars[$i])) {
+    if (preg_match('/^#/', $bars[$i])) {
        $double_horizontal_graph_string .= '<table align="left" cellpadding="0" cellspacing="0"
bgcolor="' . $bars[$i] . '" width="' . ($values[$i] * $vals['scale']) . '">' . "\n" .
            ' <tr>' . "\n" .
            ' <td>&nbsp;</td>' . "\n" .

```

catalog/admin/includes/functions/validations.php

```

@@ -43,22 +43,22 @@
function tep_validate_email($email) {
    $valid_address = true;

-    $mail_pat = '^(.+)(.+)$';
+    $mail_pat = '/^(.+)(.+)$/i';
    $valid_chars = "[ (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3^]
\\(<>@,;:\.\\\\"[[]";
    $atom = "$valid_chars+";
    $quoted_user='\"[ (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3^\"
]*\\\"';
    $word = "($atom|$quoted_user)";
-    $user_pat = "$word\\. $word)*$";
-    $ip_domain_pat='^\\([([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\)$';
-    $domain_pat = "^$atom\\. $atom)*$";
+    $user_pat = "/^$word\\. $word)*$/i";
+    $ip_domain_pat='/^\\([([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\)$$/i';
+    $domain_pat = "/^$atom\\. $atom)*$/i";

-    if (ereg($mail_pat, $email, $components)) {
+    if (preg_match($mail_pat, $email, $components)) {
        $user = $components[1];
        $domain = $components[2];
        // validate user
-        if (ereg($user_pat, $user)) {
+        if (preg_match($user_pat, $user)) {
            // validate domain
-            if (ereg($ip_domain_pat, $domain, $ip_components)) {
+            if (preg_match($ip_domain_pat, $domain, $ip_components)) {
                // this is an IP address
                for ($i=1;$i<=4;$i++) {
                    if ($ip_components[$i] > 255) {
@@ -69,7 +69,7 @@
                }
            } else {
                // Domain is a name, not an IP
-                if (ereg($domain_pat, $domain)) {
+                if (preg_match($domain_pat, $domain)) {
                    /* domain name seems valid, but now make sure that it ends in a valid TLD or ccTLD
                    and that there's a hostname preceding the domain or country. */
                    $domain_components = explode(".", $domain);
@@ -79,7 +79,7 @@
                } else {
                    $stop_level_domain = strtolower($domain_components[sizeof($domain_components)-1]);
                    // Allow all 2-letter TLDs (ccTLDs)
-                    if (ereg('^[a-z][a-z]$', $stop_level_domain) != 1) {
+                    if (preg_match('/^[a-z][a-z]$/i', $stop_level_domain) != 1) {
                        $tld_pattern = '';
                        // Get authorized TLDs from text file
                        $tlds = file(DIR_WS_INCLUDES . 'tld.txt');
@@ -88,13 +88,13 @@
                        $words = explode('#', $line);
                        $tld = trim($words[0]);
                        // TLDs should be 3 letters or more
-                        if (ereg('^[a-z]{3,}$', $tld) == 1) {
+                        if (preg_match('/^[a-z]{3,}$/i', $tld) == 1) {
                            $tld_pattern .= '^' . $tld . '$|';
                        }
                    }
                    // Remove last '|'
                    $tld_pattern = substr($tld_pattern, 0, -1);
-                    if (ereg("$tld_pattern", $stop_level_domain) == 0) {
+                    if (preg_match("/$tld_pattern/i", $stop_level_domain) == 0) {
                        $valid_address = false;
                    }
                }
            }
        }
    }
}

```

```

@@ -234,7 +234,7 @@
    $keys .= '<b>' . $value['title'] . '</b><br>';
    if ($value['use_function']) {
        $use_function = $value['use_function'];
-       if (ereg('->', $use_function)) {
+       if (preg_match('/->/', $use_function)) {
            $class_method = explode('->', $use_function);
            if (!is_object(${ $class_method[0]})) {
                include(DIR_WS_CLASSES . $class_method[0] . '.php');

```

catalog/admin/server_info.php

```

@@ -109,7 +109,7 @@ hr {display: none;}
    ob_end_clean();

    $phpinfo = str_replace('border: 1px', '', $phpinfo);
-   ereg('<body>(.*?)</body>', $phpinfo, $regs);
+   preg_match('/<body>(.*?)</body>/is', $phpinfo, $regs);
    echo '<table border="1" cellpadding="3" width="600" style="border: 0px; border-color:
#000000;">' .
        ' <tr><td><a href="http://www.oscommerce.com"><img border="0" src=
"images/oscommerce.png" title="' . PROJECT_VERSION . '" /></a><h1 class="p"> ' . PROJECT_VERSION .
'</h1></td>' .
        ' </tr>' .

```

catalog/admin/whos_online.php

```

@@ -84,7 +84,7 @@
        <td class="dataTableContent" align="center"><?php echo
$whos_online['ip_address']; ?></td>
        <td class="dataTableContent"><?php echo date('H:i:s',
$whos_online['time_entry']); ?></td>
        <td class="dataTableContent" align="center"><?php echo date('H:i:s',
$whos_online['time_last_click']); ?></td>
-       <td class="dataTableContent"><?php if (ereg('^(.*)' . tep_session_name() .
'=[a-f,0-9]+[&]*(.*)', $whos_online['last_page_url'], $array)) { echo $array[1] . $array[2]; }
else { echo $whos_online['last_page_url']; } ?>&nbsp;</td>
+       <td class="dataTableContent"><?php if (preg_match('/^(.*)' . tep_session_name() .
'=[a-f,0-9]+[&]*(.*)/i', $whos_online['last_page_url'], $array)) { echo $array[1] . $array[2]; }
else { echo $whos_online['last_page_url']; } ?>&nbsp;</td>
        </tr>
    </tr>
</tr>
<?php
}

```

catalog/advanced_search_result.php

```

@@ -300,7 +300,7 @@
    $where_str .= " group by p.products_id, tr.tax_priority";
}

-   if ( (!isset($HTTP_GET_VARS['sort'])) || (!ereg('[1-8][ad]', $HTTP_GET_VARS['sort'])) ||
(substr($HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
+   if ( (!isset($HTTP_GET_VARS['sort'])) || (!preg_match('/[1-8][ad]/i', $HTTP_GET_VARS['sort']))
|| (substr($HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
        for ($i=0, $n=sizeof($column_list); $i<$n; $i++) {
            if ($column_list[$i] == 'PRODUCT_LIST_NAME') {
                $HTTP_GET_VARS['sort'] = $i+1 . 'a';

```

catalog/includes/application_top.php


```

@@ -84,7 +84,7 @@
    for ($i=0, $n=sizeof($this->browser_languages); $i<$n; $i++) {
        reset($this->languages);
        while (list($key, $value) = each($this->languages)) {
-         if (ereg('^((' . $value . ')(;q=[0-9]\\.[0-9])?'$, $this->browser_languages[$i]) &&
isset($this->catalog_languages[$key])) {
+         if (preg_match('/^((' . $value . ')(;q=[0-9]\\.[0-9])?$/i', $this
->browser_languages[$i]) && isset($this->catalog_languages[$key])) {
            $this->language = $this->catalog_languages[$key];
            break 2;
        }
    }
}

```

catalog/includes/classes/sessions.php

```

@@ -388,7 +388,7 @@
// '<session-name>=<session-id>' to allow URLs of the form
// http://yoursite/<session-name>=<session-id>/script.php
if (empty($session->id)) {
-     eregi($session->name . '=[(AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP
v5.3^/]+)', $GLOBALS['REQUEST_URI'], $regs);
+     preg_match('/' . $session->name . '=[(AC) (COMPAT) Use Perl-Compatible Regular Expressions
for PHP v5.3^/]+/i', $GLOBALS['REQUEST_URI'], $regs);
    $regs[1] = trim($regs[1]);
    if (!empty($regs[1])) {
        $session->id = $regs[1];
    }
}

```

catalog/includes/functions/compatibility.php

```

@@ -123,7 +123,7 @@

if (!function_exists('is_numeric')) {
    function is_numeric($param) {
-     return ereg('^[0-9]{1,50}.?[0-9]{0,50}$', $param);
+     return preg_match('/^[0-9]{1,50}.?[0-9]{0,50}$/i', $param);
    }
}

@@ -173,7 +173,7 @@
if (tep_not_null($host) && tep_not_null($type)) {
    @exec("nslookup -type=$type $host", $output);
    while(list($k, $line) = each($output)) {
-     if(ereg("^$host", $line)) {
+     if(preg_match("/^$host/i", $line)) {
        return true;
    }
}
}

```

catalog/includes/functions/general.php

```

@@ -58,9 +58,9 @@
}

function tep_sanitize_string($string) {
-     $string = ereg_replace(' +', ' ', trim($string));
-
-     return preg_replace("/[<>]/", '_', $string);
+     $patterns = array ('/ +/', '/[<>]/');
+     $replace = array (' ', '_');
+     return preg_replace($patterns, $replace, trim($string));
}

////
@@ -584,7 +584,7 @@
if (@date('Y', mktime($hour, $minute, $second, $month, $day, $year)) == $year) {

```

```

        return date(DATE_FORMAT, mktime($hour, $minute, $second, $month, $day, $year));
    } else {
-       return ereg_replace('2037' . '$', $year, date(DATE_FORMAT, mktime($hour, $minute, $second,
$month, $day, 2037)));
+       return preg_replace('/2037$/', $year, date(DATE_FORMAT, mktime($hour, $minute, $second,
$month, $day, 2037)));
    }
}

@@ -594,7 +594,7 @@
    $search_str = trim(strtolower($search_str));

    // Break up $search_str on whitespace; quoted string will be reconstructed later
-    $pieces = split('[:space:]]+', $search_str);
+    $pieces = preg_split('[:space:]]+/', $search_str);
    $objects = array();
    $tmpstring = '';
    $flag = '';
@@ -635,7 +635,7 @@
    */

    // Add this word to the $tmpstring, starting the $tmpstring
-    $tmpstring = trim(ereg_replace('"', ' ', $pieces[$k]));
+    $tmpstring = trim(preg_replace('/"/', ' ', $pieces[$k]));

    // Check for one possible exception to the rule. That there is a single quoted word.
if (substr($pieces[$k], -1) == '"') {
@@ -685,7 +685,7 @@
    $piece onto the tail of the string, push the $tmpstring onto the $haves,
    kill the $tmpstring, turn the $flag "off", and return.
    */
-    $tmpstring .= ' '. trim(ereg_replace('"', ' ', $pieces[$k]));
+    $tmpstring .= ' '. trim(preg_replace('/"/', ' ', $pieces[$k]));

    // Push the $tmpstring onto the array of stuff to search for
$objects[] = trim($tmpstring);
@@ -1043,7 +1043,7 @@
    ///
    // Get the number of times a word/character is present in a string
function tep_word_count($string, $needle) {
-    $temp_array = split($needle, $string);
+    $temp_array = preg_split('/' . $needle . '/', $string);

    return sizeof($temp_array);
}
@@ -1053,7 +1053,7 @@

    if (empty($modules)) return $count;

-    $modules_array = split(';', $modules);
+    $modules_array = explode(';', $modules);

    for ($i=0, $n=sizeof($modules_array); $i<$n; $i++) {
        $class = substr($modules_array[$i], 0, strrpos($modules_array[$i], '.'));
@@ -1087,11 +1087,11 @@
        $char = chr(tep_rand(0,255));
    }
    if ($type == 'mixed') {
-        if (ereg('^[a-z0-9]$', $char)) $rand_value .= $char;
+        if (preg_match('/^[a-z0-9]$/i', $char)) $rand_value .= $char;
+        if (preg_match('/^[a-z0-9]$/i', $char)) $rand_value .= $char;
    } elseif ($type == 'chars') {
-        if (ereg('^[a-z]$', $char)) $rand_value .= $char;
+        if (preg_match('/^[a-z]$/i', $char)) $rand_value .= $char;
+        if (preg_match('/^[a-z]$/i', $char)) $rand_value .= $char;
    } elseif ($type == 'digits') {
-        if (ereg('^[0-9]$', $char)) $rand_value .= $char;
+        if (preg_match('/^[0-9]$/i', $char)) $rand_value .= $char;
+        if (preg_match('/^[0-9]$/i', $char)) $rand_value .= $char;
    }
}

@@ -1300,7 +1300,7 @@
    // nl2br() prior PHP 4.2.0 did not convert linefeeds on all OSs (it only converted \n)
function tep_convert_linefeeds($from, $to, $string) {
    if ((PHP_VERSION < "4.0.5") && is_array($from)) {
-        return ereg_replace('(' . implode('|', $from) . ')', $to, $string);
+        return preg_replace('/(' . implode('|', $from) . ')/', $to, $string);
    }
}

```

```
} else {
```



```

    return str_replace($from, $to, $string);
}

```

catalog/includes/functions/validations.php

```

@@ -43,22 +43,22 @@
function tep_validate_email($email) {
    $valid_address = true;

-    $mail_pat = '^(.+)(.+)$.';
+    $mail_pat = '/^(.+)(.+)$/i';
    $valid_chars = "[ (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3^]
    \(\)<>@,;:\.\\\"'";
    $atom = "$valid_chars+";
    $quoted_user='\"[ (AC) (COMPAT) Use Perl-Compatible Regular Expressions for PHP v5.3^\"
    ]*\\"';
    $word = "($atom|$quoted_user)";
-    $user_pat = "^$word(\.$word)*$";
-    $ip_domain_pat='^\[([0-9]{1,3})\]\.([0-9]{1,3})\]\.([0-9]{1,3})\]\.([0-9]{1,3})\]$';
-    $domain_pat = "^$atom(\.$atom)*$";
+    $user_pat = "/^$word(\.$word)*$/i";
+    $ip_domain_pat='/^\[([0-9]{1,3})\]\.([0-9]{1,3})\]\.([0-9]{1,3})\]\.([0-9]{1,3})\]$'/i';
+    $domain_pat = "/^$atom(\.$atom)*$/i";

-    if (ereg($mail_pat, $email, $components)) {
+    if (preg_match($mail_pat, $email, $components)) {
        $user = $components[1];
        $domain = $components[2];
        // validate user
-        if (ereg($user_pat, $user)) {
+        if (preg_match($user_pat, $user)) {
            // validate domain
-            if (ereg($ip_domain_pat, $domain, $ip_components)) {
+            if (preg_match($ip_domain_pat, $domain, $ip_components)) {
                // this is an IP address
                for ($i=1;$i<=4;$i++) {
                    if ($ip_components[$i] > 255) {
@@ -69,7 +69,7 @@
            }
        } else {
            // Domain is a name, not an IP
-            if (ereg($domain_pat, $domain)) {
+            if (preg_match($domain_pat, $domain)) {
                /* domain name seems valid, but now make sure that it ends in a valid TLD or ccTLD
                and that there's a hostname preceding the domain or country. */
                $domain_components = explode(".", $domain);
@@ -79,7 +79,7 @@
        } else {
            $stop_level_domain = strtolower($domain_components[sizeof($domain_components)-1]);
            // Allow all 2-letter TLDs (ccTLDs)
-            if (ereg('^[a-z][a-z]$', $stop_level_domain) != 1) {
+            if (preg_match('^[a-z][a-z]$/i', $stop_level_domain) != 1) {
                $tld_pattern = '';
                // Get authorized TLDs from text file
                $tlds = file(DIR_WS_INCLUDES . 'tld.txt');
@@ -88,13 +88,13 @@
                $words = explode('#', $line);
                $tld = trim($words[0]);
                // TLDs should be 3 letters or more
-                if (ereg('^[a-z]{3,}$', $tld) == 1) {
+                if (preg_match('^[a-z]{3,}$/i', $tld) == 1) {
                    $tld_pattern .= '^' . $tld . '$|';
                }
            }
            // Remove last '|'
            $tld_pattern = substr($tld_pattern, 0, -1);
-            if (ereg("$tld_pattern", $stop_level_domain) == 0) {
+            if (preg_match("/$tld_pattern/i", $stop_level_domain) == 0) {
                $valid_address = false;
            }
        }
    }
}

```

catalog/index.php

```
@@ -188,7 +188,7 @@
    }
}

-   if ( (!isset($_HTTP_GET_VARS['sort'])) || (!ereg('^[1-8][ad]$', $_HTTP_GET_VARS['sort'])) ||
(substr($_HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
+   if ( (!isset($_HTTP_GET_VARS['sort'])) || (!preg_match('/^[1-8][ad]$/',
$_HTTP_GET_VARS['sort'])) || (substr($_HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
        for ($i=0, $n=sizeof($column_list); $i<$n; $i++) {
            if ($column_list[$i] == 'PRODUCT_LIST_NAME') {
                $_HTTP_GET_VARS['sort'] = $i+1 . 'a';
            }
        }
    }
}
```

(C) (SEC) Add Customer Session Token to Forms

(C) (SEC) Add Customer Session Token to Forms

Importance: Medium | Difficulty: Medium

Add a customer session token to forms to protect against Cross-Site Request Forgeries (CSRF).

Affected Files

- catalog/account_edit.php
- catalog/account_newsletters.php
- catalog/account_notifications.php
- catalog/account_password.php
- catalog/address_book_process.php
- catalog/checkout_payment.php
- catalog/checkout_payment_address.php
- catalog/checkout_shipping.php
- catalog/checkout_shipping_address.php
- catalog/create_account.php
- catalog/includes/application_top.php
- catalog/includes/functions/html_output.php
- catalog/login.php
- catalog/password_forgotten.php
- catalog/product_reviews_write.php
- catalog/tell_a_friend.php

[View Changes Online](#)

catalog/account_edit.php

```

@@ -20,7 +20,7 @@
// needs to be included earlier to set the success message in the messageStack
require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_ACCOUNT_EDIT);

- if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process')) {
+ if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    if (ACCOUNT_GENDER == 'true') $gender = tep_db_prepare_input($HTTP_POST_VARS['gender']);
    $firstname = tep_db_prepare_input($HTTP_POST_VARS['firstname']);
    $lastname = tep_db_prepare_input($HTTP_POST_VARS['lastname']);
@@ -142,7 +142,7 @@
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php echo tep_draw_form('account_edit',
tep_href_link(FILENAME_ACCOUNT_EDIT, '', 'SSL'), 'post', 'onSubmit="return
check_form(account_edit);"') . tep_draw_hidden_field('action', 'process'); ?><table border="0"
width="100%" cellpadding="0" cellspacing="0">
+ <td width="100%" valign="top"><?php echo tep_draw_form('account_edit',
tep_href_link(FILENAME_ACCOUNT_EDIT, '', 'SSL'), 'post', 'onSubmit="return
check_form(account_edit);"', true) . tep_draw_hidden_field('action', 'process'); ?><table border=
"0" width="100%" cellpadding="0" cellspacing="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>

```

catalog/account_newsletters.php

```

@@ -23,7 +23,7 @@
$newsletter_query = tep_db_query("select customers_newsletter from " . TABLE_CUSTOMERS . "
where customers_id = " . (int)$customer_id . " ");
$newsletter = tep_db_fetch_array($newsletter_query);

- if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process')) {
+ if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    if (isset($HTTP_POST_VARS['newsletter_general']) &&
is_numeric($HTTP_POST_VARS['newsletter_general'])) {
        $newsletter_general = tep_db_prepare_input($HTTP_POST_VARS['newsletter_general']);
    } else {
@@ -79,7 +79,7 @@ function checkBox(object) {
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php echo tep_draw_form('account_newsletter',
tep_href_link(FILENAME_ACCOUNT_NEWSLETTERS, '', 'SSL')) . tep_draw_hidden_field('action',
'process'); ?><table border="0" width="100%" cellpadding="0" cellspacing="0">
+ <td width="100%" valign="top"><?php echo tep_draw_form('account_newsletter',
tep_href_link(FILENAME_ACCOUNT_NEWSLETTERS, '', 'SSL'), 'post', '', true) .
tep_draw_hidden_field('action', 'process'); ?><table border="0" width="100%" cellpadding="0"
cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>

```

catalog/account_notifications.php

```

@@ -23,7 +23,7 @@
    $global_query = tep_db_query("select global_product_notifications from " . TABLE_CUSTOMERS_INFO
    . " where customers_info_id = '" . (int)$customer_id . "'");
    $global = tep_db_fetch_array($global_query);

-   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process')) {
+   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
    isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
        if (isset($HTTP_POST_VARS['product_global']) &&
        is_numeric($HTTP_POST_VARS['product_global'])) {
            $product_global = tep_db_prepare_input($HTTP_POST_VARS['product_global']);
        } else {
@@ -105,7 +105,7 @@ function checkBox(object) {
    <!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('account_notifications',
    tep_href_link(FILENAME_ACCOUNT_NOTIFICATIONS, '', 'SSL')) . tep_draw_hidden_field('action',
    'process'); ?><table border="0" width="100%" cellspacing="0" cellpadding="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('account_notifications',
    tep_href_link(FILENAME_ACCOUNT_NOTIFICATIONS, '', 'SSL'), 'post', '', true) .
    tep_draw_hidden_field('action', 'process'); ?><table border="0" width="100%" cellspacing="0"
    cellpadding="0">
        <tr>
            <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
                <tr>

```

catalog/account_password.php

```

@@ -20,7 +20,7 @@
    // needs to be included earlier to set the success message in the messageStack
    require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_ACCOUNT_PASSWORD);

-   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process')) {
+   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
    isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
        $password_current = tep_db_prepare_input($HTTP_POST_VARS['password_current']);
        $password_new = tep_db_prepare_input($HTTP_POST_VARS['password_new']);
        $password_confirmation = tep_db_prepare_input($HTTP_POST_VARS['password_confirmation']);
@@ -87,7 +87,7 @@
    <!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('account_password',
    tep_href_link(FILENAME_ACCOUNT_PASSWORD, '', 'SSL'), 'post', 'onSubmit="return
    check_form(account_password);"') . tep_draw_hidden_field('action', 'process'); ?><table border="0"
    width="100%" cellspacing="0" cellpadding="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('account_password',
    tep_href_link(FILENAME_ACCOUNT_PASSWORD, '', 'SSL'), 'post', 'onSubmit="return
    check_form(account_password);"', true) . tep_draw_hidden_field('action', 'process'); ?><table
    border="0" width="100%" cellspacing="0" cellpadding="0">
        <tr>
            <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
                <tr>

```

catalog/address_book_process.php

```

@@ -20,7 +20,7 @@
// needs to be included earlier to set the success message in the messageStack
require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_ADDRESS_BOOK_PROCESS);

- if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'deleteconfirm') &&
isset($HTTP_GET_VARS['delete']) && is_numeric($HTTP_GET_VARS['delete'])) {
+ if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'deleteconfirm') &&
isset($HTTP_GET_VARS['delete']) && is_numeric($HTTP_GET_VARS['delete']) &&
isset($HTTP_GET_VARS['formid']) && ($HTTP_GET_VARS['formid'] == md5($sessiontoken))) {
    tep_db_query("delete from " . TABLE_ADDRESS_BOOK . " where address_book_id = '" . (int)
($HTTP_GET_VARS['delete']) . "' and customers_id = '" . (int)$customer_id . "'");

    $messageStack->add_session('addressbook', SUCCESS_ADDRESS_BOOK_ENTRY_DELETED, 'success');
@@ -30,7 +30,7 @@

// error checking when updating or adding an entry
$process = false;
- if (isset($HTTP_POST_VARS['action']) && (($HTTP_POST_VARS['action'] == 'process') ||
($HTTP_POST_VARS['action'] == 'update')) {
+ if (isset($HTTP_POST_VARS['action']) && (($HTTP_POST_VARS['action'] == 'process') ||
($HTTP_POST_VARS['action'] == 'update')) && isset($HTTP_POST_VARS['formid']) &&
($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    $process = true;
    $error = false;

@@ -270,7 +270,7 @@
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php if (!isset($HTTP_GET_VARS['delete'])) echo
tep_draw_form('addressbook', tep_href_link(FILENAME_ADDRESS_BOOK_PROCESS,
(isset($HTTP_GET_VARS['edit']) ? 'edit=' . $HTTP_GET_VARS['edit'] : ''), 'SSL'), 'post',
'onSubmit="return check_form(addressbook);"); ?><table border="0" width="100%" cellpadding="0"
cellpadding="0">
+ <td width="100%" valign="top"><?php if (!isset($HTTP_GET_VARS['delete'])) echo
tep_draw_form('addressbook', tep_href_link(FILENAME_ADDRESS_BOOK_PROCESS,
(isset($HTTP_GET_VARS['edit']) ? 'edit=' . $HTTP_GET_VARS['edit'] : ''), 'SSL'), 'post',
'onSubmit="return check_form(addressbook);", true); ?><table border="0" width="100%" cellpadding="0"
cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>
@@ -329,7 +329,7 @@
        <tr>
            <td width="10"><?php echo tep_draw_separator('pixel_trans.gif', '10', '1');
?></td>
            <td><?php echo '<a href="' . tep_href_link(FILENAME_ADDRESS_BOOK, '', 'SSL') . "'
>' . tep_image_button('button_back.gif', IMAGE_BUTTON_BACK) . '</a>'; ?></td>
-            <td align="right"><?php echo '<a href="' .
tep_href_link(FILENAME_ADDRESS_BOOK_PROCESS, 'delete=' . $HTTP_GET_VARS['delete'] .
'&action=deleteconfirm', 'SSL') . '>' . tep_image_button('button_delete.gif',
IMAGE_BUTTON_DELETE) . '</a>'; ?></td>
+            <td align="right"><?php echo '<a href="' .
tep_href_link(FILENAME_ADDRESS_BOOK_PROCESS, 'delete=' . $HTTP_GET_VARS['delete'] .
'&action=deleteconfirm&formid=' . md5($sessiontoken), 'SSL') . '>' .
tep_image_button('button_delete.gif', IMAGE_BUTTON_DELETE) . '</a>'; ?></td>
            <td width="10"><?php echo tep_draw_separator('pixel_trans.gif', '10', '1');
?></td>
        </tr>
    </table></td>

```

```

@@ -138,7 +138,7 @@ function rowOutEffect(object) {
    <!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
-    <td width="100%" valign="top"><?php echo tep_draw_form('checkout_payment',
tep_href_link(FILENAME_CHECKOUT_CONFIRMATION, '', 'SSL'), 'post', 'onsubmit="return check_form();"
'); ?><table border="0" width="100%" cellspacing="0" cellpadding="0">
+    <td width="100%" valign="top"><?php echo tep_draw_form('checkout_payment',
tep_href_link(FILENAME_CHECKOUT_CONFIRMATION, '', 'SSL'), 'post', 'onsubmit="return check_form();"
', true); ?><table border="0" width="100%" cellspacing="0" cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
            <tr>

```

catalog/checkout_payment_address.php

```

@@ -28,7 +28,7 @@

$error = false;
$process = false;
- if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'submit')) {
+ if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'submit') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    // process a new billing address
    if (tep_not_null($HTTP_POST_VARS['firstname']) && tep_not_null($HTTP_POST_VARS['lastname']) &&
tep_not_null($HTTP_POST_VARS['street_address'])) {
        $process = true;
@@ -263,7 +263,7 @@ function check_form_optional(form_name) {
    <!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
-    <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_PAYMENT_ADDRESS, '', 'SSL'), 'post', 'onSubmit="return
check_form_optional(checkout_address);"'); ?><table border="0" width="100%" cellspacing="0"
cellpadding="0">
+    <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_PAYMENT_ADDRESS, '', 'SSL'), 'post', 'onSubmit="return
check_form_optional(checkout_address);"', true); ?><table border="0" width="100%" cellspacing="0"
cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
            <tr>

```

catalog/checkout_shipping.php

```

@@ -95,7 +95,7 @@
    }

    // process the selected shipping method
-   if ( isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') ) {
+   if ( isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken) ) {
        if (!tep_session_is_registered('comments')) tep_session_register('comments');
        if (tep_not_null($HTTP_POST_VARS['comments'])) {
            $comments = tep_db_prepare_input($HTTP_POST_VARS['comments']);
@@ -205,7 +205,7 @@ function rowOutEffect(object) {
    <!-- left_navigation_eof //-->
</table></td>
    <!-- body_text //-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_SHIPPING, '', 'SSL')) . tep_draw_hidden_field('action',
'process'); ?><table border="0" width="100%" cellpadding="0" cellspacing="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_SHIPPING, '', 'SSL'), 'post', '', true) .
tep_draw_hidden_field('action', 'process'); ?><table border="0" width="100%" cellpadding="0" cellspacing="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>

```

catalog/checkout_shipping_address.php

```

@@ -41,7 +41,7 @@

    $error = false;
    $process = false;
-   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'submit')) {
+   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'submit') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    // process a new shipping address
    if (tep_not_null($HTTP_POST_VARS['firstname']) && tep_not_null($HTTP_POST_VARS['lastname']) &&
tep_not_null($HTTP_POST_VARS['street_address'])) {
        $process = true;
@@ -275,7 +275,7 @@ function check_form_optional(form_name) {
    <!-- left_navigation_eof //-->
</table></td>
    <!-- body_text //-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_SHIPPING_ADDRESS, '', 'SSL'), 'post', 'onSubmit="return
check_form_optional(checkout_address);"'); ?><table border="0" width="100%" cellpadding="0" cellspacing="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('checkout_address',
tep_href_link(FILENAME_CHECKOUT_SHIPPING_ADDRESS, '', 'SSL'), 'post', 'onSubmit="return
check_form_optional(checkout_address);"', true); ?><table border="0" width="100%" cellpadding="0" cellspacing="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>

```

catalog/create_account.php

```

@@ -16,7 +16,7 @@
    require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_CREATE_ACCOUNT);

    $process = false;
-   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process')) {
+   if (isset($HTTP_POST_VARS['action']) && ($HTTP_POST_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
        $process = true;

        if (ACCOUNT_GENDER == 'true') {
@@ -226,6 +226,9 @@
            tep_session_register('customer_country_id');
            tep_session_register('customer_zone_id');

// reset session token
+   $sessiontoken = md5(tep_rand() . tep_rand() . tep_rand() . tep_rand());
+
    // restore cart contents
    $cart->restore_contents();

@@ -274,7 +277,7 @@
    <!-- left_navigation_eof //-->
</table></td>
    <!-- body_text //-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('create_account',
tep_href_link(FILENAME_CREATE_ACCOUNT, '', 'SSL'), 'post', 'onSubmit="return
check_form(create_account);"' . tep_draw_hidden_field('action', 'process'); ?><table border="0"
width="100%" cellpadding="0" cellspacing="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('create_account',
tep_href_link(FILENAME_CREATE_ACCOUNT, '', 'SSL'), 'post', 'onSubmit="return
check_form(create_account);"' . true) . tep_draw_hidden_field('action', 'process'); ?><table
border="0" width="100%" cellpadding="0" cellspacing="0">
    <tr>
        <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
            <tr>

```

catalog/includes/application_top.php

```

@@ -199,6 +199,12 @@
    extract($_SESSION, EXTR_OVERWRITE+EXTR_REFS);
}

// initialize a session token
+   if (!tep_session_is_registered('sessiontoken')) {
+   $sessiontoken = md5(tep_rand() . tep_rand() . tep_rand());
+   tep_session_register('sessiontoken');
+   }
+
    // set SID once, even if empty
    $SID = (defined('SID') ? SID : '');

```

catalog/includes/functions/html_output.php


```

@@ -145,13 +145,19 @@

    ///
    // Output a form
-   function tep_draw_form($name, $action, $method = 'post', $parameters = '') {
+   function tep_draw_form($name, $action, $method = 'post', $parameters = '', $tokenize = false) {
+   global $sessiontoken;
+
    $form = '<form name="' . tep_output_string($name) . '" action="' . tep_output_string($action)
    . '" method="' . tep_output_string($method) . '"';

    if (tep_not_null($parameters)) $form .= ' ' . $parameters;

    $form .= '>';

+   if ( ($tokenize == true) && isset($sessiontoken) ) {
+       $form .= '<input type="hidden" name="formid" value="' . tep_output_string($sessiontoken) .
    '>';
+   }
+
    return $form;
    }

```

catalog/login.php

```

@@ -20,7 +20,7 @@
    require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_LOGIN);

    $error = false;
-   if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process')) {
+   if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process') &&
    isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
        $email_address = tep_db_prepare_input($HTTP_POST_VARS['email_address']);
        $password = tep_db_prepare_input($HTTP_POST_VARS['password']);

@@ -54,6 +54,9 @@

        tep_db_query("update " . TABLE_CUSTOMERS_INFO . " set customers_info_date_of_last_logon =
    now(), customers_info_number_of_logons = customers_info_number_of_logons+1 where customers_info_id
    = " . (int)$customer_id . " ");

    // reset session token
+   $sessiontoken = md5(tep_rand() . tep_rand() . tep_rand() . tep_rand());
+
    // restore cart contents
    $cart->restore_contents();

@@ -101,7 +104,7 @@ function session_win() {
    <!-- left_navigation_eof /-->
</table></td>
    <!-- body_text /-->
-   <td width="100%" valign="top"><?php echo tep_draw_form('login', tep_href_link(FILENAME_LOGIN,
    'action=process', 'SSL')); ?><table border="0" width="100%" cellpadding="0">
+   <td width="100%" valign="top"><?php echo tep_draw_form('login', tep_href_link(FILENAME_LOGIN,
    'action=process', 'SSL'), 'post', '', true); ?><table border="0" width="100%" cellpadding="0">
        <tr>
            <td><table border="0" width="100%" cellpadding="0">
                <tr>

```

catalog/password_forgotten.php

```

@@ -14,7 +14,7 @@

require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_PASSWORD_FORGOTTEN);

- if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process')) {
+ if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    $email_address = tep_db_prepare_input($HTTP_POST_VARS['email_address']);

    $check_customer_query = tep_db_query("select customers_firstname, customers_lastname,
customers_password, customers_id from " . TABLE_CUSTOMERS . " where customers_email_address = '" .
tep_db_input($email_address) . "'");
@@ -61,7 +61,7 @@
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php echo tep_draw_form('password_forgotten',
tep_href_link(FILENAME_PASSWORD_FORGOTTEN, 'action=process', 'SSL')); ?><table border="0" width=
"100%" cellspacing="0" cellpadding="0">
+ <td width="100%" valign="top"><?php echo tep_draw_form('password_forgotten',
tep_href_link(FILENAME_PASSWORD_FORGOTTEN, 'action=process', 'SSL'), 'post', '', true); ?><table
border="0" width="100%" cellspacing="0" cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
            <tr>

```

catalog/product_reviews_write.php

```

@@ -27,7 +27,7 @@
$customer_query = tep_db_query("select customers_firstname, customers_lastname from " .
TABLE_CUSTOMERS . " where customers_id = '" . (int)$customer_id . "'");
$customer = tep_db_fetch_array($customer_query);

- if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process')) {
+ if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    $rating = tep_db_prepare_input($HTTP_POST_VARS['rating']);
    $review = tep_db_prepare_input($HTTP_POST_VARS['review']);

@@ -122,7 +122,7 @@ function popupWindow(url) {
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php echo tep_draw_form('product_reviews_write',
tep_href_link(FILENAME_PRODUCT_REVIEWS_WRITE, 'action=process&products_id=' .
$HTTP_GET_VARS['products_id']), 'post', 'onSubmit="return checkForm();"'); ?><table border="0"
width="100%" cellspacing="0" cellpadding="0">
+ <td width="100%" valign="top"><?php echo tep_draw_form('product_reviews_write',
tep_href_link(FILENAME_PRODUCT_REVIEWS_WRITE, 'action=process&products_id=' .
$HTTP_GET_VARS['products_id']), 'post', 'onSubmit="return checkForm();"'); ?><table border=
"0" width="100%" cellspacing="0" cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
            <tr>

```

catalog/tell_a_friend.php

```

@@ -33,7 +33,7 @@

require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_TELL_A_FRIEND);

- if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process')) {
+ if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'process') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
    $error = false;

    $to_email_address = tep_db_prepare_input($HTTP_POST_VARS['to_email_address']);
@@ -115,7 +115,7 @@
<!-- left_navigation_eof //-->
</table></td>
<!-- body_text //-->
- <td width="100%" valign="top"><?php echo tep_draw_form('email_friend',
tep_href_link(FILENAME_TELL_A_FRIEND, 'action=process&products_id=' .
$HTTP_GET_VARS['products_id'])); ?><table border="0" width="100%" cellspacing="0" cellpadding="0">
+ <td width="100%" valign="top"><?php echo tep_draw_form('email_friend',
tep_href_link(FILENAME_TELL_A_FRIEND, 'action=process&products_id=' .
$HTTP_GET_VARS['products_id']), 'post', '', true); ?><table border="0" width="100%" cellspacing=
"0" cellpadding="0">
    <tr>
        <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
            <tr>

```

(C) (BUG) Validate Removal of Customer Address

(C) (BUG) Validate Removal of Customer Address

Importance: High | Difficulty: Easy

Validate the address being deleted is not assigned as the customers default address.

Affected Files

- [catalog/address_book_process.php](#)

[View Changes Online](#)

catalog/address_book_process.php

```

@@ -21,9 +21,13 @@
require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_ADDRESS_BOOK_PROCESS);

if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'deleteconfirm') &&
isset($HTTP_GET_VARS['delete']) && is_numeric($HTTP_GET_VARS['delete']) &&
isset($HTTP_GET_VARS['formid']) && ($HTTP_GET_VARS['formid'] == md5($sessiontoken))) {
- tep_db_query("delete from " . TABLE_ADDRESS_BOOK . " where address_book_id = " . (int)
$HTTP_GET_VARS['delete'] . " and customers_id = " . (int)$customer_id . "");
+ if ($HTTP_GET_VARS['delete'] == $customer_default_address_id) {
+     $messageStack->add_session('addressbook', WARNING_PRIMARY_ADDRESS_DELETION, 'warning');
+ } else {
+     tep_db_query("delete from " . TABLE_ADDRESS_BOOK . " where address_book_id = " . (int)
$HTTP_GET_VARS['delete'] . " and customers_id = " . (int)$customer_id . "");

-     $messageStack->add_session('addressbook', SUCCESS_ADDRESS_BOOK_ENTRY_DELETED, 'success');
+     $messageStack->add_session('addressbook', SUCCESS_ADDRESS_BOOK_ENTRY_DELETED, 'success');
+ }

    tep_redirect(tep_href_link(FILENAME_ADDRESS_BOOK, '', 'SSL'));
}

```

(AC) (BUG) Sanitize Parameters

(AC) (BUG) Sanitize Parameters

Importance: High | Difficulty: Medium

Sanitize parameters.

Affected Files

- catalog/account_edit.php
- catalog/address_book_process.php
- catalog/admin/includes/classes/phplot.php
- catalog/admin/includes/functions/compatibility.php
- catalog/admin/includes/functions/html_output.php
- catalog/admin/login.php
- catalog/checkout_confirmation.php
- catalog/checkout_payment_address.php
- catalog/checkout_process.php
- catalog/create_account.php
- catalog/includes/application_top.php
- catalog/includes/boxes/currencies.php
- catalog/includes/boxes/tell_a_friend.php
- catalog/includes/functions/compatibility.php
- catalog/includes/functions/general.php
- catalog/includes/functions/html_output.php
- catalog/product_info.php
- catalog/tell_a_friend.php

[View Changes Online](#)

catalog/account_edit.php

```
@@ -52,7 +52,7 @@
    }

    if (ACCOUNT_DOB == 'true') {
-       if (!checkdate(substr(tep_date_raw($dob), 4, 2), substr(tep_date_raw($dob), 6, 2),
substr(tep_date_raw($dob), 0, 4))) {
+       if ((is_numeric(tep_date_raw($dob)) == false) || (@checkdate(substr(tep_date_raw($dob), 4,
2), substr(tep_date_raw($dob), 6, 2), substr(tep_date_raw($dob), 0, 4)) == false)) {
            $error = true;

        $messageStack->add('account_edit', ENTRY_DATE_OF_BIRTH_ERROR);
    }
```

catalog/address_book_process.php

```
@@ -21,7 +21,7 @@
    require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_ADDRESS_BOOK_PROCESS);

    if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'deleteconfirm') &&
isset($HTTP_GET_VARS['delete']) && is_numeric($HTTP_GET_VARS['delete']) &&
isset($HTTP_GET_VARS['formid']) && ($HTTP_GET_VARS['formid'] == md5($sessiontoken))) {
-       if ($HTTP_GET_VARS['delete'] == $customer_default_address_id) {
+       if ((int)$HTTP_GET_VARS['delete'] == $customer_default_address_id) {
            $messageStack->add_session('addressbook', WARNING_PRIMARY_ADDRESS_DELETION, 'warning');
        } else {
            tep_db_query("delete from " . TABLE_ADDRESS_BOOK . " where address_book_id = " . (int)
($HTTP_GET_VARS['delete']) . " and customers_id = " . (int)$customer_id . "");
        }
    }
```

catalog/admin/includes/classes/phplot.php

```

@@ -672,12 +672,12 @@
    $which_xpos, $which_ypos, $which_color, $which_font, $which_text);
} else {
    if ($which_valign == 'top') {
-       $which_ypos = $which_ypos - ImageFontHeight($which_font);
+       $which_ypos = $which_ypos - ImageFontHeight((int)$which_font);
    }
    $which_text = preg_replace("/\r/", "", $which_text);
    $str = explode("\n", $which_text); //multiple lines submitted by Remi Ricard
-   $height = ImageFontHeight($which_font);
-   $width = ImageFontWidth($which_font);
+   $height = ImageFontHeight((int)$which_font);
+   $width = ImageFontWidth((int)$which_font);
    if ($which_angle == 90) { //Vertical Code Submitted by Marlin Viss
for($i=0;$i<count($str);$i++) {
    ImageStringUp($this->img, $which_font, ($i*$height + $which_xpos), $which_ypos, $str[$i],
$which_color);
@@ -686,9 +686,9 @@
    for($i=0;$i<count($str);$i++) {
        if ($which_halign == 'center') {
            $xpos = $which_xpos - strlen($str[$i]) * $width/2;
-            ImageString($this->img, $which_font, $xpos, ($i*$height + $which_ypos), $str[$i],
$which_color);
+            ImageString($this->img, (int)$which_font, $xpos, ($i*$height + $which_ypos), $str[$i],
$which_color);
        } else {
-            ImageString($this->img, $which_font, $which_xpos, ($i*$height + $which_ypos), $str[$i],
$which_color);
+            ImageString($this->img, (int)$which_font, $which_xpos, ($i*$height + $which_ypos),
$str[$i], $which_color);
        }
    }
}
}

```

catalog/admin/includes/functions/compatibility.php

```

@@ -85,7 +85,7 @@
    if (!function_exists('checkdnsrr')) {
        function checkdnsrr($host, $type) {
            if (tep_not_null($host) && tep_not_null($type)) {
-                @exec("nslookup -type=$type $host", $output);
+                @exec("nslookup -type=" . escapeshellarg($type) . " " . escapeshellarg($host), $output);
                while(list($k, $line) = each($output)) {
                    if(preg_match("/^$host/i", $line)) {
                        return true;
                    }
                }
            }
        }
    }
}

```

catalog/admin/includes/functions/html_output.php

```

@@ -13,6 +13,8 @@
    ///
    // The HTML href link wrapper function
    function tep_href_link($page = '', $parameters = '', $connection = 'NONSSL') {
+       $page = tep_output_string($page);
+
        if ($page == '') {
            die('</td></tr></table></td></tr></table><br><br><font color="#ff0000"
><b>Error!</b></font><br><br><b>Unable to determine the page link!<br><br>Function
used:<br><br>tep_href_link(\'\' . $page . \'\' , \'\' . $parameters . \'\' , \'\' . $connection .
\'\' )</b>');
        }
    }
@@ -30,7 +32,7 @@
    if ($parameters == '') {
        $link = $link . $page . '?' . SID;
    } else {
-       $link = $link . $page . '?' . $parameters . '&' . SID;
+       $link = $link . $page . '?' . tep_output_string($parameters) . '&' . SID;
    }

    while ( (substr($link, -1) == '&') || (substr($link, -1) == '?') ) $link = substr($link, 0,
-1);

```

catalog/admin/login.php

```

@@ -69,7 +69,7 @@
    $username = tep_db_prepare_input($HTTP_POST_VARS['username']);
    $password = tep_db_prepare_input($HTTP_POST_VARS['password']);

-       tep_db_query('insert into ' . TABLE_ADMINISTRATORS . ' (user_name, user_password)
values ('' . $username . '", '' . tep_encrypt_password($password) . "')');
+       tep_db_query("insert into " . TABLE_ADMINISTRATORS . " (user_name, user_password)
values ('" . tep_db_input($username) . '", '" . tep_db_input(tep_encrypt_password($password)) .
"')");
    }

    tep_redirect(tep_href_link(FILENAME_LOGIN));

```

catalog/checkout_confirmation.php

```

@@ -52,7 +52,7 @@

    $payment_modules->update_status();

-   if ( ( is_array($payment_modules->modules) && (sizeof($payment_modules->modules) > 1) &&
!is_object($payment) ) || (is_object($payment) && ($payment->enabled == false)) ) {
+   if ( ($payment_modules->selected_module != $payment) || ( is_array($payment_modules->modules)
&& (sizeof($payment_modules->modules) > 1) && !is_object($payment) ) || (is_object($payment) &&
($payment->enabled == false)) ) {
        tep_redirect(tep_href_link(FILENAME_CHECKOUT_PAYMENT, 'error_message=' .
urlencode(ERROR_NO_PAYMENT_MODULE_SELECTED), 'SSL'));
    }

```

catalog/checkout_payment_address.php

```

@@ -166,7 +166,7 @@

    $billto = $HTTP_POST_VARS['address'];

-    $check_address_query = tep_db_query("select count(*) as total from " . TABLE_ADDRESS_BOOK .
+    $check_address_query = tep_db_query("select count(*) as total from " . TABLE_ADDRESS_BOOK .
" where customers_id = '" . $customer_id . "' and address_book_id = '" . $billto . "'");
+    $check_address_query = tep_db_query("select count(*) as total from " . TABLE_ADDRESS_BOOK .
" where customers_id = '" . (int)$customer_id . "' and address_book_id = '" . (int)$billto . "'");
    $check_address = tep_db_fetch_array($check_address_query);

    if ($check_address['total'] == '1') {

```

catalog/checkout_process.php

```

@@ -68,7 +68,7 @@

    $payment_modules->update_status();

-    if ( ( is_array($payment_modules->modules) && (sizeof($payment_modules->modules) > 1) &&
+    if ( ( is_array($payment_modules->modules) && (sizeof($payment_modules->modules) > 1) &&
!is_object($payment) ) || (is_object($payment) && ($payment->enabled == false)) ) {
+    if ( ($payment_modules->selected_module != $payment) || ( is_array($payment_modules->modules)
&& (sizeof($payment_modules->modules) > 1) && !is_object($payment) ) || (is_object($payment) &&
($payment->enabled == false)) ) {
        tep_redirect(tep_href_link(FILENAME_CHECKOUT_PAYMENT, 'error_message=' .
urlencode(ERROR_NO_PAYMENT_MODULE_SELECTED), 'SSL'));
    }

```

catalog/create_account.php

```

@@ -77,7 +77,7 @@
    }

    if (ACCOUNT_DOB == 'true') {
-    if (checkdate(substr(tep_date_raw($dob), 4, 2), substr(tep_date_raw($dob), 6, 2),
+    if (checkdate(substr(tep_date_raw($dob), 4, 2), substr(tep_date_raw($dob), 6, 2),
substr(tep_date_raw($dob), 0, 4)) == false) {
+    if ((is_numeric(tep_date_raw($dob)) == false) || (@checkdate(substr(tep_date_raw($dob), 4,
2), substr(tep_date_raw($dob), 6, 2), substr(tep_date_raw($dob), 0, 4)) == false)) {
        $error = true;

    $messageStack->add('create_account', ENTRY_DATE_OF_BIRTH_ERROR);

```

catalog/includes/application_top.php

```

@@ -93,6 +93,7 @@
    $GET_array = array();
    $PHP_SELF = str_replace(getenv('PATH_INFO'), '', $PHP_SELF);
    $vars = explode('/', substr(getenv('PATH_INFO'), 1));
+    do_magic_quotes_gpc($vars);
    for ($i=0, $n=sizeof($vars); $i<$n; $i++) {
        if (strpos($vars[$i], '[')) {
            $GET_array[substr($vars[$i], 0, -2)][] = $vars[$i+1];

```

catalog/includes/boxes/currencies.php

```

@@ -30,7 +30,7 @@
    $hidden_get_variables = '';
    reset($HTTP_GET_VARS);
    while (list($key, $value) = each($HTTP_GET_VARS)) {
-       if ( ($key != 'currency') && ($key != tep_session_name()) && ($key != 'x') && ($key != 'y'))
+       if ( ($key != 'currency') && ($key != tep_session_name()) && ($key != 'x') && ($key != 'y'))
    ) {
+       if ( is_string($value) && ($key != 'currency') && ($key != tep_session_name()) && ($key != 'x') && ($key != 'y')) {
            $hidden_get_variables .= tep_draw_hidden_field($key, $value);
        }
    }
}

```

catalog/includes/boxes/tell_a_friend.php

```

@@ -22,7 +22,7 @@
    $info_box_contents = array();
    $info_box_contents[] = array('form' => tep_draw_form('tell_a_friend',
    tep_href_link(FILENAME_TELL_A_FRIEND, '', 'NONSSL', false), 'get'),
                                'align' => 'center',
-                               'text' => tep_draw_input_field('to_email_address', '', 'size="10"
+                               'text' => tep_draw_input_field('to_email_address', '', 'size="10"
    ') . '&nbsp;' . tep_image_submit('button_tell_a_friend.gif', BOX_HEADING_TELL_A_FRIEND) .
    tep_draw_hidden_field('products_id', $HTTP_GET_VARS['products_id']) . tep_hide_session_id() .
    '<br>' . BOX_TELL_A_FRIEND_TEXT);
+                               'text' => tep_draw_input_field('to_email_address', '', 'size="10"
+                               'text' => tep_draw_input_field('to_email_address', '', 'size="10"
    ') . '&nbsp;' . tep_image_submit('button_tell_a_friend.gif', BOX_HEADING_TELL_A_FRIEND) .
    tep_draw_hidden_field('products_id', (int)$HTTP_GET_VARS['products_id']) . tep_hide_session_id() .
    '<br>' . BOX_TELL_A_FRIEND_TEXT);

    new infoBox($info_box_contents);
?>

```

catalog/includes/functions/compatibility.php

```

@@ -171,7 +171,7 @@
    if (!function_exists('checkdnsrr')) {
        function checkdnsrr($host, $type) {
            if (tep_not_null($host) && tep_not_null($type)) {
-                @exec("nslookup -type=$type $host", $output);
+                @exec("nslookup -type=" . escapeshellarg($type) . " " . escapeshellarg($host), $output);
            while(list($k, $line) = each($output)) {
                if(preg_match("/^$host/i", $line)) {
                    return true;
                }
            }
        }
    }
}

```

catalog/includes/functions/general.php


```

@@ -160,7 +160,7 @@
    if (is_array($HTTP_GET_VARS) && (sizeof($HTTP_GET_VARS) > 0)) {
        reset($HTTP_GET_VARS);
        while (list($key, $value) = each($HTTP_GET_VARS)) {
-         if ( (strlen($value) > 0) && ($key != tep_session_name()) && ($key != 'error') &&
(!in_array($key, $exclude_array)) && ($key != 'x') && ($key != 'y') ) {
+         if ( is_string($value) && (strlen($value) > 0) && ($key != tep_session_name()) && ($key
!= 'error') && (!in_array($key, $exclude_array)) && ($key != 'x') && ($key != 'y') ) {
            $get_url .= $key . '=' . rawurlencode(stripslashes($value)) . '&';
        }
    }
}
@@ -914,7 +914,7 @@
// Return a product ID with attributes
function tep_get_uprid($prid, $params) {
    if (is_numeric($prid)) {
-     $uprid = $prid;
+     $uprid = (int)$prid;

        if (is_array($params) && (sizeof($params) > 0)) {
            $attributes_check = true;
@@ -974,7 +974,7 @@
        $pieces = explode('{', $uprid);

        if (is_numeric($pieces[0])) {
-         return $pieces[0];
+         return (int)$pieces[0];
        } else {
            return false;
        }
    }
}

```

catalog/includes/functions/html_output.php

```

@@ -15,6 +15,8 @@
function tep_href_link($page = '', $parameters = '', $connection = 'NONSSL', $add_session_id =
true, $search_engine_safe = true) {
    global $request_type, $session_started, $SID;

+    $page = tep_output_string($page);
+
    if (!tep_not_null($page)) {
        die('</td></tr></table></td></tr></table><br><br><font color="#ff0000"
><b>Error!</b></font><br><br><b>Unable to determine the page link!<br><br>');
    }
}

```

catalog/product_info.php

```

@@ -139,7 +139,7 @@
    }
}

-     if
(isset($cart->contents[$HTTP_GET_VARS['products_id']]['attributes'][$products_options_name['products_
{
+         if (is_string($HTTP_GET_VARS['products_id']) &&
isset($cart->contents[$HTTP_GET_VARS['products_id']]['attributes'][$products_options_name['products_o
{
            $selected_attribute =
$cart->contents[$HTTP_GET_VARS['products_id']]['attributes'][$products_options_name['products_options
} else {
    $selected_attribute = false;
}

```

catalog/tell_a_friend.php

```

@@ -28,7 +28,7 @@

```

```

    }

    if ($valid_product == false) {
-       tep_redirect(tep_href_link(FILENAME_PRODUCT_INFO, 'products_id=' .
$HTTP_GET_VARS['products_id']));
+       tep_redirect(tep_href_link(FILENAME_PRODUCT_INFO, 'products_id=' . (int
)$HTTP_GET_VARS['products_id']));
    }

    require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_TELL_A_FRIEND);
@@ -74,14 +74,14 @@
        $email_body .= $message . "\n\n";
    }

-       $email_body .= sprintf(TEXT_EMAIL_LINK, tep_href_link(FILENAME_PRODUCT_INFO, 'products_id='
. $HTTP_GET_VARS['products_id'], 'NONSSL', false)) . "\n\n" .
+       $email_body .= sprintf(TEXT_EMAIL_LINK, tep_href_link(FILENAME_PRODUCT_INFO, 'products_id='
. (int)$HTTP_GET_VARS['products_id'], 'NONSSL', false)) . "\n\n" .
        sprintf(TEXT_EMAIL_SIGNATURE, STORE_NAME . "\n" . HTTP_SERVER .
DIR_WS_CATALOG . "\n");

    tep_mail($to_name, $to_email_address, $email_subject, $email_body, $from_name,
$from_email_address);

    $messageStack->add_session('header', sprintf(TEXT_EMAIL_SUCCESSFUL_SENT,
$product_info['products_name'], tep_output_string_protected($to_name)), 'success');

-       tep_redirect(tep_href_link(FILENAME_PRODUCT_INFO, 'products_id=' .
$HTTP_GET_VARS['products_id']));
+       tep_redirect(tep_href_link(FILENAME_PRODUCT_INFO, 'products_id=' . (int
)$HTTP_GET_VARS['products_id']));
    }
    } elseif (tep_session_is_registered('customer_id')) {
        $account_query = tep_db_query("select customers_firstname, customers_lastname,
customers_email_address from " . TABLE_CUSTOMERS . " where customers_id = " . (int)$customer_id .
"");
@@ -91,7 +91,7 @@
        $from_email_address = $account['customers_email_address'];
    }

-       $breadcrumb->add(NAVBAR_TITLE, tep_href_link(FILENAME_TELL_A_FRIEND, 'products_id=' .
$HTTP_GET_VARS['products_id']));
+       $breadcrumb->add(NAVBAR_TITLE, tep_href_link(FILENAME_TELL_A_FRIEND, 'products_id=' . (int
)$HTTP_GET_VARS['products_id']));
    }
    ?>
    <!doctype html public "-//W3C//DTD HTML 4.01 Transitional//EN">
    <html <?php echo HTML_PARAMS; ?>>
    @@ -115,7 +115,7 @@
    <!-- left_navigation_eof //-->
    </table></td>
    <!-- body_text //-->
-       <td width="100%" valign="top"><?php echo tep_draw_form('email_friend',
tep_href_link(FILENAME_TELL_A_FRIEND, 'action=process&products_id=' .
$HTTP_GET_VARS['products_id']), 'post', '', true); ?><table border="0" width="100%" cellpadding=
"0" cellspacing="0">
+       <td width="100%" valign="top"><?php echo tep_draw_form('email_friend',
tep_href_link(FILENAME_TELL_A_FRIEND, 'action=process&products_id=' . (int
)$HTTP_GET_VARS['products_id']), 'post', '', true); ?><table border="0" width="100%" cellpadding=
"0" cellspacing="0">
        <tr>
            <td><table border="0" width="100%" cellpadding="0" cellspacing="0">
                <tr>
    @@ -211,7 +211,7 @@
            <td><table border="0" width="100%" cellpadding="0" cellspacing="2">
                <tr>
                    <td width="10"><?php echo tep_draw_separator('pixel_trans.gif', '10', '1');
?></td>
-                   <td><?php echo '<a href="' . tep_href_link(FILENAME_PRODUCT_INFO, 'products_id='
. $HTTP_GET_VARS['products_id']) . '">' . tep_image_button('button_back.gif', IMAGE_BUTTON_BACK) .
'</a>'; ?></td>
+                   <td><?php echo '<a href="' . tep_href_link(FILENAME_PRODUCT_INFO, 'products_id='
. (int)$HTTP_GET_VARS['products_id']) . '">' . tep_image_button('button_back.gif',
IMAGE_BUTTON_BACK) . ' </a>'; ?></td>
                    <td align="right"><?php echo tep_image_submit('button_continue.gif',
IMAGE_BUTTON_CONTINUE); ?></td>

```

```
<td width="10"><?php echo tep_draw_separator('pixel_trans.gif', '10', '1');
```

?></td>

</tr>

(A) (UP) Add Support for Basic HTTP Authentication

(A) (UP) Add Support for Basic HTTP Authentication

Importance: High | Difficulty: Medium

Add support for Basic HTTP Authentication to the Administration Tool login routine. Administrator accounts can be saved in htpasswd files using the Apache APR-MD5 algorithm. Upon successful Basic HTTP Authentication, an automatic login occurs if the authentication password matches the administrator password stored in the database.

Affected Files

- catalog/admin/.htpasswd_oscommerce --- (new file)
- catalog/admin/administrators.php
- catalog/admin/includes/application_top.php
- catalog/admin/includes/functions/password_funcs.php
- catalog/admin/includes/languages/english/administrators.php
- catalog/admin/login.php

[View Changes Online](#)



This changeset includes an update to an English language definition file. Please perform similar changes to other languages that are also installed.

catalog/admin/.htpasswd_oscommerce --- (new file)



This is a new empty file. ([Download File](#))

catalog/admin/administrators.php

```
@@ -12,6 +12,37 @@

    require('includes/application_top.php');

+   $htaccess_array = null;
+   $htpasswd_array = null;
+
+   $authuserfile_array = array('##### OSCOMMERCE ADMIN PROTECTION - BEGIN #####',
+                               'AuthType Basic',
+                               'AuthName "osCommerce Online Merchant Administration Tool"',
+                               'AuthUserFile ' . DIR_FS_ADMIN . '.htpasswd_oscommerce',
+                               'Require valid-user',
+                               '##### OSCOMMERCE ADMIN PROTECTION - END #####');
+
+   if (file_exists(DIR_FS_ADMIN . '.htpasswd_oscommerce') && is_writable(DIR_FS_ADMIN .
'.htpasswd_oscommerce') && file_exists(DIR_FS_ADMIN . '.htaccess') && is_writable(DIR_FS_ADMIN .
'.htaccess')) {
+       $htaccess_array = array();
+       $htpasswd_array = array();
+
+       if (filesize(DIR_FS_ADMIN . '.htaccess') > 0) {
+           $fg = fopen(DIR_FS_ADMIN . '.htaccess', 'rb');
+           $data = fread($fg, filesize(DIR_FS_ADMIN . '.htaccess'));
+           fclose($fg);
+
+           $htaccess_array = explode("\n", $data);
+       }
+
+       if (filesize(DIR_FS_ADMIN . '.htpasswd_oscommerce') > 0) {
+           $fg = fopen(DIR_FS_ADMIN . '.htpasswd_oscommerce', 'rb');
+           $data = fread($fg, filesize(DIR_FS_ADMIN . '.htpasswd_oscommerce'));
```

```

+         fclose($fg);
+
+         $htpasswd_array = explode("\n", $data);
+     }
+ }
+
+ $action = (isset($HTTP_GET_VARS['action']) ? $HTTP_GET_VARS['action'] : '');
+
+ if (tep_not_null($action)) {
@@ -26,6 +57,38 @@
+
+     if (tep_db_num_rows($check_query) < 1) {
+         tep_db_query("insert into " . TABLE_ADMINISTRATORS . " (user_name, user_password)
+ values ('" . tep_db_input($username) . "', '" . tep_db_input(tep_encrypt_password($password)) .
+ "')");
+
+         if (is_array($htpasswd_array)) {
+             for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
+                 list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);
+
+                 if ($ht_username == $username) {
+                     unset($htpasswd_array[$i]);
+                 }
+             }
+
+             if (isset($HTTP_POST_VARS['htaccess']) && ($HTTP_POST_VARS['htaccess'] == 'true')) {
+                 $htpasswd_array[] = $username . ':' . tep_crypt_apr_md5($password);
+             }
+
+             $fp = fopen(DIR_FS_ADMIN . '.htpasswd_oscommerce', 'w');
+             fwrite($fp, implode("\n", $htpasswd_array));
+             fclose($fp);
+
+             if (!in_array('AuthUserFile ' . DIR_FS_ADMIN . '.htpasswd_oscommerce',
+ $htaccess_array) && !empty($htpasswd_array)) {
+                 array_splice($htaccess_array, sizeof($htaccess_array), 0, $authuserfile_array);
+             } elseif (empty($htpasswd_array)) {
+                 for ($i=0, $n=sizeof($htaccess_array); $i<$n; $i++) {
+                     if (in_array($htaccess_array[$i], $authuserfile_array)) {
+                         unset($htaccess_array[$i]);
+                     }
+                 }
+             }
+
+             $fp = fopen(DIR_FS_ADMIN . '.htaccess', 'w');
+             fwrite($fp, implode("\n", $htaccess_array));
+             fclose($fp);
+         }
+     } else {
+         $messageStack->add_session(ERROR_ADMINISTRATOR_EXISTS, 'error');
+     }
@@ -38,17 +101,75 @@
+     $username = tep_db_prepare_input($HTTP_POST_VARS['username']);
+     $password = tep_db_prepare_input($HTTP_POST_VARS['password']);
+
+     -     $check_query = tep_db_query("select id from " . TABLE_ADMINISTRATORS . " where user_name
+ = '" . tep_db_input($admin['username']) . "'");
+     +     $check_query = tep_db_query("select id, user_name from " . TABLE_ADMINISTRATORS . " where
+ id = '" . (int)$HTTP_GET_VARS['aID'] . "'");
+     $check = tep_db_fetch_array($check_query);
+
+     -     if ($admin['id'] == $check['id']) {
+ // update username in current session if changed
+     +     if ( ($check['id'] == $admin['id']) && ($check['user_name'] != $admin['username']) ) {
+         $admin['username'] = $username;
+     }
+
+ // update username in htpasswd if changed
+     +     if (is_array($htpasswd_array)) {
+         for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
+             list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);
+
+             if ( ($check['user_name'] == $ht_username) && ($check['user_name'] != $username) ) {
+                 $htpasswd_array[$i] = $username . ':' . $ht_password;
+             }
+         }
+     }

```

```

+     }
+ }
+
+     tep_db_query("update " . TABLE_ADMINISTRATORS . " set user_name = '" .
tep_db_input($username) . "' where id = '" . (int)$HTTP_GET_VARS['aID'] . "'");

+     if (tep_not_null($password)) {
+// update password in httpasswd
+         if (is_array($httpasswd_array)) {
+             for ($i=0, $n=sizeof($httpasswd_array); $i<$n; $i++) {
+                 list($ht_username, $ht_password) = explode(':', $httpasswd_array[$i], 2);
+
+                 if ($ht_username == $username) {
+                     unset($httpasswd_array[$i]);
+                 }
+             }
+
+             if (isset($HTTP_POST_VARS['htaccess']) && ($HTTP_POST_VARS['htaccess'] == 'true')) {
+                 $httpasswd_array[] = $username . ':' . tep_crypt_apr_md5($password);
+             }
+         }
+
+         tep_db_query("update " . TABLE_ADMINISTRATORS . " set user_password = '" .
tep_db_input(tep_encrypt_password($password)) . "' where id = '" . (int)$HTTP_GET_VARS['aID'] .
'"");
+     } elseif (!isset($HTTP_POST_VARS['htaccess']) || ($HTTP_POST_VARS['htaccess'] != 'true'))
+     {
+         if (is_array($httpasswd_array)) {
+             for ($i=0, $n=sizeof($httpasswd_array); $i<$n; $i++) {
+                 list($ht_username, $ht_password) = explode(':', $httpasswd_array[$i], 2);
+
+                 if ($ht_username == $username) {
+                     unset($httpasswd_array[$i]);
+                 }
+             }
+         }
+     }
+
+// write new httpasswd file
+     if (is_array($httpasswd_array)) {
+         $fp = fopen(DIR_FS_ADMIN . '.httpasswd_oscommerce', 'w');
+         fwrite($fp, implode("\n", $httpasswd_array));
+         fclose($fp);
+
+         if (!in_array('AuthUserFile ' . DIR_FS_ADMIN . '.httpasswd_oscommerce', $htaccess_array)
&& !empty($httpasswd_array)) {
+             array_splice($htaccess_array, sizeof($htaccess_array), 0, $authuserfile_array);
+         } elseif (empty($httpasswd_array)) {
+             for ($i=0, $n=sizeof($htaccess_array); $i<$n; $i++) {
+                 if (in_array($htaccess_array[$i], $authuserfile_array)) {
+                     unset($htaccess_array[$i]);
+                 }
+             }
+         }
+
+         $fp = fopen(DIR_FS_ADMIN . '.htaccess', 'w');
+         fwrite($fp, implode("\n", $htaccess_array));
+         fclose($fp);
+     }

+     tep_redirect(tep_href_link(FILENAME_ADMINISTRATORS, 'aID=' . (int)
)$HTTP_GET_VARS['aID']));
@@ -56,19 +177,57 @@
+     case 'deleteconfirm':
+         $id = tep_db_prepare_input($HTTP_GET_VARS['aID']);

-         $check_query = tep_db_query("select id from " . TABLE_ADMINISTRATORS . " where user_name
= '" . tep_db_input($admin['username']) . "'");
+         $check_query = tep_db_query("select id, user_name from " . TABLE_ADMINISTRATORS . " where
id = '" . (int)$id . "'");
+         $check = tep_db_fetch_array($check_query);

-         if ($id == $check['id']) {
+         if ($admin['id'] == $check['id']) {
+             tep_session_unregister('admin');

```

```

    }

    tep_db_query("delete from " . TABLE_ADMINISTRATORS . " where id = '" . (int)$id . "'");

+   if (is_array($htpasswd_array)) {
+       for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
+           list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);
+
+           if ($ht_username == $check['user_name']) {
+               unset($htpasswd_array[$i]);
+           }
+       }
+
+       $fp = fopen(DIR_FS_ADMIN . '.htpasswd_oscommerce', 'w');
+       fwrite($fp, implode("\n", $htpasswd_array));
+       fclose($fp);
+
+       if (empty($htpasswd_array)) {
+           for ($i=0, $n=sizeof($htaccess_array); $i<$n; $i++) {
+               if (in_array($htaccess_array[$i], $authuserfile_array)) {
+                   unset($htaccess_array[$i]);
+               }
+           }
+
+           $fp = fopen(DIR_FS_ADMIN . '.htaccess', 'w');
+           fwrite($fp, implode("\n", $htaccess_array));
+           fclose($fp);
+       }
+   }

    tep_redirect(tep_href_link(FILENAME_ADMINISTRATORS));
    break;
}
}

+ $secMessageStack = new messageStack();
+
+ if (is_array($htpasswd_array)) {
+     if (empty($htpasswd_array)) {
+         $secMessageStack->add(sprintf(HTPASSWD_INFO, implode('<br />', $authuserfile_array)),
+ 'error');
+     } else {
+         $secMessageStack->add(HTPASSWD_SECURED, 'success');
+     }
+ } else {
+     $secMessageStack->add(HTPASSWD_PERMISSIONS, 'error');
+ }
+
+ ?>
+ <!doctype html public "-//W3C//DTD HTML 4.01 Transitional//EN">
+ <html <?php echo HTML_PARAMS; ?>>
+ @@ -102,11 +261,19 @@
+     </table></td>
+     </tr>
+     <tr>
+         <td>
+ <?php
+ echo $secMessageStack->output();
+ ?>
+         </td>
+     </tr>
+     <tr>
+         <td><table border="0" width="100%" cellspacing="0" cellpadding="0">
+             <tr>
+                 <td valign="top"><table border="0" width="100%" cellspacing="0" cellpadding="2">
+                     <tr class="dataTableHeadingRow">
+                         <td class="dataTableHeadingContent"><?php echo TABLE_HEADING_ADMINISTRATORS;
+ ?></td>
+                     <td class="dataTableHeadingContent" align="center"><?php echo
+ TABLE_HEADING_HTPASSWD; ?></td>
+                     <td class="dataTableHeadingContent" align="right"><?php echo
+ TABLE_HEADING_ACTION; ?>&nbsp;</td>
+                 </tr>
+             </table>
+ <?php
+ @@ -116,6 +283,19 @@
+             $aInfo = new objectInfo($admins);

```

```

    }

+   $htpasswd_secured = tep_image(DIR_WS_IMAGES . 'icon_status_red.gif', 'Not Secured', 10, 10);
+
+   if (is_array($htpasswd_array)) {
+       for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
+           list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);
+
+           if ($ht_username == $admins['user_name']) {
+               $htpasswd_secured = tep_image(DIR_WS_IMAGES . 'icon_status_green.gif', 'Secured', 10,
10);
+               break;
+           }
+       }
+   }
+
+   if ( (isset($aInfo) && is_object($aInfo)) && ($admins['id'] == $aInfo->id) ) {
+       echo '
        <tr id="defaultSelected" class="dataTableRowSelected" onmouseover="rowOverEffect(this)" onmouseout="rowOutEffect(this)" onclick="document.location.href=\'' .
tep_href_link(FILENAME_ADMINISTRATORS, 'aID=' . $aInfo->id . '&action=edit') . '\'">'. "\n";
        } else {
@@ -123,13 +303,14 @@
        }
    }

    ?>

        <td class="dataTableContent"><?php echo $admins['user_name']; ?></td>
+
        <td class="dataTableContent" align="center"><?php echo $htpasswd_secured; ?></td>
        <td class="dataTableContent" align="right"><?php if ( (isset($aInfo) &&
is_object($aInfo)) && ($admins['id'] == $aInfo->id) ) { echo tep_image(DIR_WS_IMAGES .
'icon_arrow_right.gif', ''); } else { echo '<a href="' . tep_href_link(FILENAME_ADMINISTRATORS,
'aID=' . $admins['id']) . '">' . tep_image(DIR_WS_IMAGES . 'icon_info.gif', IMAGE_ICON_INFO) .
'</a>'; } ?>&nbsp;</td>
        </tr>

    <?php
    }
    ?>

    <tr>
-
        <td colspan="2" align="right"><?php echo '<a href="' .
tep_href_link(FILENAME_ADMINISTRATORS, 'action=new') . '">' .
tep_image_button('button_insert.gif', IMAGE_INSERT) . '</a>'; ?></td>
+
        <td colspan="3" align="right"><?php echo '<a href="' .
tep_href_link(FILENAME_ADMINISTRATORS, 'action=new') . '">' .
tep_image_button('button_insert.gif', IMAGE_INSERT) . '</a>'; ?></td>
        </tr>
    </table></td>

    <?php
@@ -140,19 +321,40 @@
    case 'new':
        $heading[] = array('text' => '<b>' . TEXT_INFO_HEADING_NEW_ADMINISTRATOR . '</b>');

-
        $contents = array('form' => tep_draw_form('administrator', FILENAME_ADMINISTRATORS,
'action=insert'));
+
        $contents = array('form' => tep_draw_form('administrator', FILENAME_ADMINISTRATORS,
'action=insert', 'post', 'autocomplete="off"'));
        $contents[] = array('text' => TEXT_INFO_INSERT_INTRO);
        $contents[] = array('text' => '<br>' . TEXT_INFO_USERNAME . '<br>' .
tep_draw_input_field('username'));
        $contents[] = array('text' => '<br>' . TEXT_INFO_PASSWORD . '<br>' .
tep_draw_password_field('password'));
+
+       if (is_array($htpasswd_array)) {
+           $contents[] = array('text' => '<br>' . tep_draw_checkbox_field('htaccess', 'true') . ' '
. TEXT_INFO_PROTECT_WITH_HTTPASSWD);
+       }
+
        $contents[] = array('align' => 'center', 'text' => '<br>' .
tep_image_submit('button_save.gif', IMAGE_SAVE) . '&nbsp;<a href="' .
tep_href_link(FILENAME_ADMINISTRATORS) . '">' . tep_image_button('button_cancel.gif',
IMAGE_CANCEL) . '</a>');
        break;
    case 'edit':
        $heading[] = array('text' => '<b>' . $aInfo->user_name . '</b>');

-
        $contents = array('form' => tep_draw_form('administrator', FILENAME_ADMINISTRATORS, 'aID='
. $aInfo->id . '&action=save'));
+
        $contents = array('form' => tep_draw_form('administrator', FILENAME_ADMINISTRATORS, 'aID='

```



```

. $aInfo->id . '&action=save', 'post', 'autocomplete="off"');
$content[] = array('text' => TEXT_INFO_EDIT_INTRO);
$content[] = array('text' => '<br>' . TEXT_INFO_USERNAME . '<br>' .
tep_draw_input_field('username', $aInfo->user_name));
$content[] = array('text' => '<br>' . TEXT_INFO_NEW_PASSWORD . '<br>' .
tep_draw_password_field('password'));
+
+     if (is_array($htpasswd_array)) {
+         $default_flag = false;
+
+         for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
+             list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);
+
+             if ($ht_username == $aInfo->user_name) {
+                 $default_flag = true;
+                 break;
+             }
+         }
+
+         $content[] = array('text' => '<br>' . tep_draw_checkbox_field('htaccess', 'true',
$default_flag) . ' ' . TEXT_INFO_PROTECT_WITH_HTPASSWD);
+     }
+
+     $content[] = array('align' => 'center', 'text' => '<br>' .
tep_image_submit('button_update.gif', IMAGE_UPDATE) . '&nbsp;<a href="' .
tep_href_link(FILENAME_ADMINISTRATORS, 'aID=' . $aInfo->id) . '"' .
tep_image_button('button_cancel.gif', IMAGE_CANCEL) . '</a>');

```

```
break;
case 'delete':
```

catalog/admin/includes/application_top.php

```
@@ -135,6 +135,13 @@

    $current_page = basename($PHP_SELF);

+// if the first page request is to the login page, set the current page to the index page
+// so the redirection on a successful login is not made to the login page again
+  if ( ($current_page == FILENAME_LOGIN) && !tep_session_is_registered('redirect_origin') ) {
+    $current_page = FILENAME_DEFAULT;
+    $HTTP_GET_VARS = array();
+  }
+
+  if ($current_page != FILENAME_LOGIN) {
+    if (!tep_session_is_registered('redirect_origin')) {
+      tep_session_register('redirect_origin');
@@ -143,6 +150,14 @@
                                'get' => $HTTP_GET_VARS);
    }

+// try to automatically login with the HTTP Authentication values if it exists
+  if (!tep_session_is_registered('auth_ignore')) {
+    if (isset($HTTP_SERVER_VARS['PHP_AUTH_USER']) &&
+!empty($HTTP_SERVER_VARS['PHP_AUTH_USER']) && isset($HTTP_SERVER_VARS['PHP_AUTH_PW']) &&
+!empty($HTTP_SERVER_VARS['PHP_AUTH_PW'])) {
+      $redirect_origin['auth_user'] = $HTTP_SERVER_VARS['PHP_AUTH_USER'];
+      $redirect_origin['auth_pw'] = $HTTP_SERVER_VARS['PHP_AUTH_PW'];
+    }
+  }
+
+  $redirect = true;
+}

@@ -151,7 +166,7 @@
}

  if ($redirect == true) {
-    tep_redirect(tep_href_link(FILENAME_LOGIN));
+    tep_redirect(tep_href_link(FILENAME_LOGIN, (isset($redirect_origin['auth_user']) ?
'action=process' : '')));
  }

  unset($redirect);
```

catalog/admin/includes/functions/password_funcs.php

```

@@ -43,4 +43,67 @@

    return $password;
}
+
+////
+// This function produces a crypted string using the APR-MD5 algorithm
+// Source: http://www.php.net/crypt
+ function tep_crypt_apr_md5($password, $salt = null) {
+     if (empty($salt)) {
+         $salt_string = '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz';
+
+         $salt = '';
+
+         for ($i = 0; $i < 8; $i++) {
+             $salt .= $salt_string[rand(0, 61)];
+         }
+     }
+
+     $len = strlen($password);
+
+     $result = $password . '$apr1$' . $salt;
+
+     $bin = pack('H32', md5($password . $salt . $password));
+
+     for ($i=$len; $i>0; $i-=16) {
+         $result .= substr($bin, 0, min(16, $i));
+     }
+
+     for ($i=$len; $i>0; $i>= 1) {
+         $result .= ($i & 1) ? chr(0) : $password[0];
+     }
+
+     $bin = pack('H32', md5($result));
+
+     for ($i=0; $i<1000; $i++) {
+         $new = ($i & 1) ? $password : $bin;
+
+         if ($i % 3) {
+             $new .= $salt;
+         }
+
+         if ($i % 7) {
+             $new .= $password;
+         }
+
+         $new .= ($i & 1) ? $bin : $password;
+
+         $bin = pack('H32', md5($new));
+     }
+
+     for ($i=0; $i<5; $i++) {
+         $k = $i + 6;
+         $j = $i + 12;
+
+         if ($j == 16) {
+             $j = 5;
+         }
+
+         $tmp = $bin[$i] . $bin[$k] . $bin[$j] . $tmp;
+     }
+
+     $tmp = chr(0) . chr(0) . $bin[11] . $tmp;
+     $tmp = strtr(strrev(substr(base64_encode($tmp), 2)),
+ 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',
+ './0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz');
+
+     return '$apr1$' . $salt . '$' . $tmp;
+ }
+
+?>

```

```

@@ -13,6 +13,7 @@
define('HEADING_TITLE', 'Administrators');

define('TABLE_HEADING_ADMINISTRATORS', 'Administrators');
+define('TABLE_HEADING_HTPASSWD', 'Secured by htpasswd');
define('TABLE_HEADING_ACTION', 'Action');

define('TEXT_INFO_INSERT_INTRO', 'Please enter the new administrator with its related data');
@@ -22,6 +23,11 @@ define('TEXT_INFO_HEADING_NEW_ADMINISTRATOR', 'New Administrator');
define('TEXT_INFO_USERNAME', 'Username:');
define('TEXT_INFO_NEW_PASSWORD', 'New Password:');
define('TEXT_INFO_PASSWORD', 'Password:');
+define('TEXT_INFO_PROTECT_WITH_HTPASSWD', 'Protect With htaccess/htpasswd');

define('ERROR_ADMINISTRATOR_EXISTS', 'Error: Administrator already exists.');
```

-?>

+

```

+define('HTPASSWD_INFO', '<b>Additional Protection With htaccess/htpasswd</b><p>This osCommerce
Online Merchant Administration Tool installation is not additionally secured through
htaccess/htpasswd means.</p><p>Enabling the htaccess/htpasswd security layer will automatically
store administrator username and passwords in a htpasswd file when updating administrator password
records.</p><p><b>Please note</b>, if this additional security layer is enabled and you can no
longer access the Administration Tool, please make the following changes and consult your hosting
provider to enable htaccess/htpasswd protection:</p><p><u><b>1. Edit this file:</b></u><br /><br
/>' . DIR_FS_ADMIN . '.htaccess</p><p>Remove the following lines if they
exist:</p><p><i>%s</i></p><p><u><b>2. Delete this file:</b></u><br /><br />' . DIR_FS_ADMIN .
'.htpasswd_oscommerce</p>');
```

```

+define('HTPASSWD_SECURED', '<b>Additional Protection With htaccess/htpasswd</b><p>This osCommerce
Online Merchant Administration Tool installation is additionally secured through htaccess/htpasswd
means.</p>');
```

```

+define('HTPASSWD_PERMISSIONS', '<b>Additional Protection With htaccess/htpasswd</b><p>This
osCommerce Online Merchant Administration Tool installation is not additionally secured through
htaccess/htpasswd means.</p><p>The following files need to be writable by the web server to enable
the htaccess/htpasswd security layer:</p><ul><li>' . DIR_FS_ADMIN . '.htaccess</li><li>' .
DIR_FS_ADMIN . '.htpasswd_oscommerce</li></ul><p>Reload this page to confirm if the correct file
permissions have been set.</p>');
```

+?>

catalog/admin/login.php

```

@@ -17,11 +17,21 @@

$action = (isset($_HTTP_GET_VARS['action']) ? $_HTTP_GET_VARS['action'] : '');

+// prepare to logout an active administrator if the login page is accessed again
+ if (tep_session_is_registered('admin')) {
+     $action = 'logout';
+ }
+
+ if (tep_not_null($action)) {
+     switch ($action) {
+         case 'process':
-         $username = tep_db_prepare_input($_HTTP_POST_VARS['username']);
-         $password = tep_db_prepare_input($_HTTP_POST_VARS['password']);
+         if (tep_session_is_registered('redirect_origin') && isset($_redirect_origin['auth_user']))
+         {
+             $username = tep_db_prepare_input($_redirect_origin['auth_user']);
+             $password = tep_db_prepare_input($_redirect_origin['auth_pw']);
+         } else {
+             $username = tep_db_prepare_input($_HTTP_POST_VARS['username']);
+             $password = tep_db_prepare_input($_HTTP_POST_VARS['password']);
+         }

        $check_query = tep_db_query("select id, user_name, user_password from " .
TABLE_ADMINISTRATORS . " where user_name = '" . tep_db_input($username) . "'");

@@ -58,6 +68,12 @@
        case 'logout':
            tep_session_unregister('selected_box');
            tep_session_unregister('admin');

+
+         if (isset($_HTTP_SERVER_VARS['PHP_AUTH_USER']) &&
!empty($_HTTP_SERVER_VARS['PHP_AUTH_USER']) && isset($_HTTP_SERVER_VARS['PHP_AUTH_PW']) &&
!empty($_HTTP_SERVER_VARS['PHP_AUTH_PW'])) {
+             tep_session_register('auth_ignore');
+             $auth_ignore = true;
+         }

        tep_redirect(tep_href_link(FILENAME_DEFAULT));

        break;

```

(C) (UP) Generate a New Shopping Cart ID When Restoring Products

(C) (UP) Generate a New CartID When Restoring Products

Importance: Medium | Difficulty: Easy

Generate a new shopping cart ID (cartID) when restoring products stored in the database.

Affected Files

- [catalog/includes/classes/shopping_cart.php](#)

[View Changes Online](#)

catalog/includes/classes/shopping_cart.php

```

@@ -56,6 +56,9 @@
    }

    $this->cleanup();
+
+// assign a temporary unique ID to the order contents to prevent hack attempts during the
+checkout procedure
+    $this->cartID = $this->generate_cart_id();
+    }

function reset($reset_database = false) {

```

(C) (BUG) Fix Navigation History Session Content

(C) (BUG) Fix Navigation History Session Content

Importance: High | Difficulty: Easy

Fix a rare instance of the navigation history content being damaged in the session.

Affected Files

- [catalog/includes/application_top.php](#)

[View Changes Online](#)

catalog/includes/application_top.php

```

@@ -306,7 +306,7 @@
    }

    // navigation history
-    if (tep_session_is_registered('navigation')) {
+    if (tep_session_is_registered('navigation') && is_object($navigation)) {
        if (PHP_VERSION < 4) {
            $broken_navigation = $navigation;
            $navigation = new navigationHistory;

```

(AC) (UP) Improve Validation of E-Mail Addresses

(AC) (UP) Improve Validation of E-Mail Addresses

Importance: Medium | Difficulty: Medium

Improve validation of e-mail addresses and remove the tld.txt file.

Affected Files

- [catalog/admin/includes/functions/validations.php](#)
- [catalog/admin/includes/tld.txt](#) --- (deleted)
- [catalog/includes/functions/validations.php](#)
- [catalog/includes/tld.txt](#) --- (deleted)

[View Changes Online](#)

catalog/admin/includes/functions/validations.php

```

@@ -21,102 +21,53 @@
    //
    // Description : function for validating email address that conforms to RFC 822 specs
    //

```

```

- //      This function is converted from a JavaScript written by
- //      Sandeep V. Tamhankar (stamhankar@hotmail.com). The original JavaScript
- //      is available at http://javascript.internet.com
+ //      This function will first attempt to validate the Email address using the filter
+ //      extension for performance. If this extension is not available it will
+ //      fall back to a regex based validator which doesn't validate all RFC822
+ //      addresses but catches 99.9% of them. The regex is based on the code found at
+ //      http://www.regular-expressions.info/email.html
+ //
+ //      Optional validation for validating the domain name is also valid is supplied
+ //      and can be enabled using the administration tool.
//
// Sample Valid Addresses:
//
//      first.last@host.com
//      firstlast@host.to
- //      "first last"@host.com
- //      "first@last"@host.com
//      first-last@host.com
- //      first.last@[123.123.123.123]
+ //      first_last@host.com
//
// Invalid Addresses:
//
//      first last@host.com
- //
+ //      first@last@host.com
//
////////////////////////////////////
function tep_validate_email($email) {
-     $valid_address = true;
-
-     $mail_pat = '/^(.+)(.+)$/i';
-     $valid_chars = "[^ \(\)<>@,;:\.\\\"' \[\]";
-     $atom = "$valid_chars+";
-     $quoted_user='(\\"[^\"]*"')';
-     $word = "($atom|$quoted_user)";
-     $user_pat = "/^$word(\\. $word)*$/i";
-     $ip_domain_pat='/^([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})$/i';
-     $domain_pat = "/^$atom(\\. $atom)*$/i";
+     $email = trim($email);
+     if (strlen($email) > 255) {
+         $valid_address = false;
+     } elseif (function_exists('filter_var') && defined('FILTER_VALIDATE_EMAIL')) {

-     if (preg_match($mail_pat, $email, $components)) {
-         $user = $components[1];
-         $domain = $components[2];
-         // validate user
-         if (preg_match($user_pat, $user)) {
-             // validate domain
-             if (preg_match($ip_domain_pat, $domain, $ip_components)) {
-                 // this is an IP address
-                 for ($i=1;$i<=4;$i++) {
-                     if ($ip_components[$i] > 255) {
-                         $valid_address = false;
-                         break;
-                     }
-                 }
-             }
-             else {
-                 // Domain is a name, not an IP
-                 if (preg_match($domain_pat, $domain)) {
-                     /* domain name seems valid, but now make sure that it ends in a valid TLD or ccTLD
-                     and that there's a hostname preceding the domain or country. */
-                     $domain_components = explode(".", $domain);
-                     // Make sure there's a host name preceding the domain.
-                     if (sizeof($domain_components) < 2) {
-                         $valid_address = false;
-                     } else {
-                         $top_level_domain = strtolower($domain_components[sizeof($domain_components)-1]);
-                         // Allow all 2-letter TLDs (ccTLDs)
-                         if (preg_match('/^[a-z][a-z]$/i', $top_level_domain) != 1) {
-                             $tld_pattern = '';
-                             // Get authorized TLDs from text file

```

```
- $tlds = file(DIR_WS_INCLUDES . 'tld.txt');
- while (list(,$line) = each($tlds)) {
-     // Get rid of comments
-     $words = explode('#', $line);
-     $tld = trim($words[0]);
-     // TLDs should be 3 letters or more
-     if (preg_match('/^[a-z]{3,}$/i', $tld) == 1) {
-         $tld_pattern .= '^' . $tld . '$|';
-     }
- }
- // Remove last '|'
- $tld_pattern = substr($tld_pattern, 0, -1);
- if (preg_match("/$tld_pattern/i", $stop_level_domain) == 0) {
-     $valid_address = false;
- }
- }
- }
- else {
-     $valid_address = false;
- }
- }
+ $valid_address = (bool)filter_var($email, FILTER_VALIDATE_EMAIL);
+ } else {
+     if ( substr_count( $email, '@' ) > 1 ) {
+         $valid_address = false;
+     }
-     else {
+         if ( preg_match(
+             '/[a-z0-9!#$%&'"+\/=^?_`{|}~]+(?:\.[a-z0-9!#$%&'"+\/=^?_`{|}~]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?'
+             , $email)) {
+             $valid_address = true;
+         } else {
+             $valid_address = false;
+         }
-     }
-     else {
-         $valid_address = false;
-     }
+
+     if ($valid_address && ENTRY_EMAIL_ADDRESS_CHECK == 'true') {
-         if (!checkdnsrr($domain, "MX") && !checkdnsrr($domain, "A")) {
+             $domain = explode('@', $email);
+             if (!checkdnsrr($domain[1], "MX") && !checkdnsrr($domain[1], "A")) {
+                 $valid_address = false;
+             }

```



```
}  
?>
```

catalog/admin/includes/tld.txt --- (deleted)



This file has been deleted.

catalog/includes/functions/validations.php

```
@@ -21,102 +21,55 @@  
  //  
  // Description : function for validating email address that conforms to RFC 822 specs  
  //  
  - //          This function is converted from a JavaScript written by  
  - //          Sandeep V. Tamhankar (stamhankar@hotmail.com). The original JavaScript  
  - //          is available at http://javascript.internet.com  
  + //          This function will first attempt to validate the Email address using the filter  
  + //          extension for performance. If this extension is not available it will  
  + //          fall back to a regex based validator which doesn't validate all RFC822  
  + //          addresses but catches 99.9% of them. The regex is based on the code found at  
  + //          http://www.regular-expressions.info/email.html  
  //  
  + //          Optional validation for validating the domain name is also valid is supplied  
  + //          and can be enabled using the administration tool.  
  + //  
  // Sample Valid Addresses:  
  //  
  //      first.last@host.com  
  //      firstlast@host.to  
  - //      "first last"@host.com  
  - //      "first@last"@host.com  
  //      first-last@host.com  
  - //      first.last@[123.123.123.123]  
  + //      first_last@host.com  
  //  
  // Invalid Addresses:  
  //  
  //      first last@host.com  
  + //      first@last@host.com  
  //  
  - //  
  //////////////////////////////////////  
function tep_validate_email($email) {  
  -   $valid_address = true;  
  +   $email = trim($email);  
  
  -   $mail_pat = '/^(.+)(.+)$/i';  
  -   $valid_chars = "[(AC) (UP) Improve Validation of E-Mail Addresses^] \\(\\)<>@,;:\\.\\\"\\'\\[\\]";  
  -   $atom = "$valid_chars+";  
  -   $quoted_user='(\"[(AC) (UP) Improve Validation of E-Mail Addresses^\"]*\\')';  
  -   $word = "($atom|$quoted_user)";  
  -   $user_pat = "^$word(\\. $word)*$/i";  
  -   $ip_domain_pat='/^[([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})$/i';  
  -   $domain_pat = "^$atom(\\. $atom)*$/i";  
  -  
  -   if (preg_match($mail_pat, $email, $components)) {  
  -       $user = $components[1];  
  -       $domain = $components[2];  
  -       // validate user  
  -       if (preg_match($user_pat, $user)) {  
  -           // validate domain  
  -           if (preg_match($ip_domain_pat, $domain, $ip_components)) {  
  -               // this is an IP address  
  -               for ($i=1;$i<=4;$i++) {  
  -                   if ($ip_components[$i] > 255) {  
  -                       $valid_address = false;  
  -                       break;  
  -                   }  
  -               }  
  -           }  
  -       }  
  -   }  
  - }  
  - }
```

```

-     }
-     else {
-         // Domain is a name, not an IP
-         if (preg_match($domain_pat, $domain)) {
-             /* domain name seems valid, but now make sure that it ends in a valid TLD or ccTLD
-              and that there's a hostname preceding the domain or country. */
-             $domain_components = explode(".", $domain);
-             // Make sure there's a host name preceding the domain.
-             if (sizeof($domain_components) < 2) {
-                 $valid_address = false;
-             } else {
-                 $stop_level_domain = strtolower($domain_components[sizeof($domain_components)-1]);
-                 // Allow all 2-letter TLDs (ccTLDs)
-                 if (preg_match('/^[a-z][a-z]$/i', $stop_level_domain) != 1) {
-                     $tld_pattern = '';
-                     // Get authorized TLDs from text file
-                     $tlds = file(DIR_WS_INCLUDES . 'tld.txt');
-                     while (list(,$line) = each($tlds)) {
-                         // Get rid of comments
-                         $words = explode('#', $line);
-                         $tld = trim($words[0]);
-                         // TLDs should be 3 letters or more
-                         if (preg_match('/^[a-z]{3,}$/i', $tld) == 1) {
-                             $tld_pattern .= '^' . $tld . '$|';
-                         }
-                     }
-                     // Remove last '|'
-                     $tld_pattern = substr($tld_pattern, 0, -1);
-                     if (preg_match("/$tld_pattern/i", $stop_level_domain) == 0) {
-                         $valid_address = false;
-                     }
-                 }
-             }
-         }
-         else {
-             $valid_address = false;
-         }
-     }
+     if ( strlen($email) > 255 ) {
+         $valid_address = false;
+     } elseif ( function_exists('filter_var') && defined('FILTER_VALIDATE_EMAIL') ) {
+         $valid_address = (bool)filter_var($email, FILTER_VALIDATE_EMAIL);
+     } else {
+         if ( substr_count( $email, '@' ) > 1 ) {
+             $valid_address = false;
+         }
+         else {
+             if ( preg_match(
+                 "/[a-z0-9!#$%&'*\+/=?^_`{|}~-]+(?:\.[a-z0-9!#$%&'*\+/=?^_`{|}~-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])
+                 , $email) ) {
+                 $valid_address = true;
+             } else {
+                 $valid_address = false;
+             }
+         }
-     }
-     else {
-         $valid_address = false;
-     }
+     if ($valid_address && ENTRY_EMAIL_ADDRESS_CHECK == 'true') {
-         if (!checkdnsrr($domain, "MX") && !checkdnsrr($domain, "A")) {
+         $domain = explode('@', $email);
+
+         if ( !checkdnsrr($domain[1], "MX") && !checkdnsrr($domain[1], "A") ) {
+             $valid_address = false;
+         }
+     }
+ }
+
+ return $valid_address;

```

```
}  
?>
```

catalog/includes/tld.txt --- (deleted)



This file has been deleted.

(AC) (UP) Code Cleanup

(AC) (UP) Code Cleanup

Importance: High | Difficulty: Easy

Code cleanup and spelling error fixes.

Affected Files

- [catalog/admin/includes/graphs/banner_infobox.php](#)
- [catalog/admin/includes/languages/english/modules/index/customers.php](#)
- [catalog/admin/includes/languages/english/server_info.php](#)
- [catalog/includes/functions/general.php](#)
- [catalog/index.php](#)

[View Changes Online](#)



This changeset includes an update to an English language definition file. Please perform similar changes to other languages that are also installed.

catalog/admin/includes/graphs/banner_infobox.php

```
@@ -36,7 +36,7 @@  
    $graph->SetMarginsPixels(15,15,15,30);  
  
    $graph->SetTitleFontSize('4');  
-    $graph->SetTitle('TEXT_BANNERS_LAST_3_DAYS');  
+    $graph->SetTitle(TEXT_BANNERS_LAST_3_DAYS);  
  
    $graph->SetDataValues($stats);  
    $graph->SetDataColors(array('blue','red'),array('blue', 'red'));
```

catalog/admin/includes/languages/english/modules/index/customers.php

```
@@ -10,6 +10,6 @@  
    Released under the GNU General Public License  
    */  
  
-define(ADMIN_INDEX_CUSTOMERS_TITLE, 'Customers');  
-define(ADMIN_INDEX_CUSTOMERS_DATE, 'Date');  
+define('ADMIN_INDEX_CUSTOMERS_TITLE', 'Customers');  
+define('ADMIN_INDEX_CUSTOMERS_DATE', 'Date');  
?>
```

catalog/admin/includes/languages/english/server_info.php

```

@@ -21,5 +21,5 @@ define('TITLE_PHP_VERSION', 'PHP Version:');
define('TITLE_ZEND_VERSION', 'Zend:');
define('TITLE_DATABASE_HOST', 'Database Host:');
define('TITLE_DATABASE', 'Database:');
-define('TITLE_DATABASE_DATE', 'Database Date:');
+define('TITLE_DATABASE_DATE', 'Database Date:');
?>

```

catalog/includes/functions/general.php

```

@@ -1012,7 +1012,7 @@
    if (SEND_EMAILS != 'true') return false;

    // Instantiate a new mail object
-    $message = new email(array('X-Mailer: osCommerce Mailer'));
+    $message = new email(array('X-Mailer: osCommerce'));

    // Build the text version
    $text = strip_tags($email_text);

```

catalog/index.php

```

@@ -16,8 +16,8 @@
$category_depth = 'top';
if (isset($cPath) && tep_not_null($cPath)) {
    $categories_products_query = tep_db_query("select count(*) as total from " .
TABLE_PRODUCTS_TO_CATEGORIES . " where categories_id = " . (int)$current_category_id . "");
-    $categories_products = tep_db_fetch_array($categories_products_query);
-    if ($categories_products['total'] > 0) {
+    $categories_products = tep_db_fetch_array($categories_products_query);
+    if ($categories_products['total'] > 0) {
        $category_depth = 'products'; // display products
    } else {
        $category_parent_query = tep_db_query("select count(*) as total from " . TABLE_CATEGORIES .
" where parent_id = " . (int)$current_category_id . "");

```

(A) (UP) Update Define Languages Page

(A) (UP) Update Define Languages Page

Importance: Medium | Difficulty: Medium

The Administration Tool Define Languages page has been updated to list recursive files containing language definitions. This allows language definitions for modules to also be updated.

Affected Files

- [catalog/admin/define_language.php](#)
- [catalog/admin/includes/languages/english/define_language.php](#)

[View Changes Online](#)



This changeset includes an update to an English language definition file. Please perform similar changes to other languages that are also installed.

catalog/admin/define_language.php

```

@@ -12,38 +12,38 @@

```

```

require('includes/application_top.php');

- if (!isset($HTTP_GET_VARS['lngdir'])) $HTTP_GET_VARS['lngdir'] = $language;
+ function tep_opendir($path) {
+     $path = rtrim($path, '/') . '/';

- $action = (isset($HTTP_GET_VARS['action']) ? $HTTP_GET_VARS['action'] : '');
+     $exclude_array = array('.', '..', '.DS_Store', 'Thumbs.db');

- if (tep_not_null($action)) {
-     switch ($action) {
-         case 'save':
-             if (isset($HTTP_GET_VARS['lngdir']) && isset($HTTP_GET_VARS['filename'])) {
-                 if ($HTTP_GET_VARS['filename'] == $HTTP_GET_VARS['lngdir'] . '.php') {
-                     $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename'];
-                 } else {
-                     $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['lngdir'] . '/' .
$HTTP_GET_VARS['filename'];
-                 }
+                 $result = array();

-                 if (file_exists($file)) {
-                     if (file_exists('bak' . $file)) {
-                         @unlink('bak' . $file);
-                     }
+                     if ($handle = opendir($path)) {
+                         while (false != ($filename = readdir($handle))) {
+                             if (!in_array($filename, $exclude_array)) {
+                                 $file = array('name' => $path . $filename,
+                                             'is_dir' => is_dir($path . $filename),
+                                             'writable' => is_writable($path . $filename),
+                                             'size' => filesize($path . $filename),
+                                             'last_modified' => strftime(DATE_TIME_FORMAT, filemtime($path .
$filename)));

-                                 @rename($file, 'bak' . $file);
+                                 $result[] = $file;

-                                 $new_file = fopen($file, 'w');
-                                 $file_contents = stripslashes($HTTP_POST_VARS['file_contents']);
-                                 fwrite($new_file, $file_contents, strlen($file_contents));
-                                 fclose($new_file);
+                                 if ($file['is_dir'] == true) {
+                                     $result = array_merge($result, tep_opendir($path . $filename));
+                                 }

-                                 tep_redirect(tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' .
$HTTP_GET_VARS['lngdir']));
+                                 }
+                                 break;
+                             }
+                         }

+                     closedir($handle);
+                 }

+                 return $result;
+             }

+         if (!isset($HTTP_GET_VARS['lngdir'])) $HTTP_GET_VARS['lngdir'] = $language;
+
+         $languages_array = array();
+         $languages = tep_get_languages();
+         $lng_exists = false;
@@ -55,6 +55,35 @@
    }

    if (!$lng_exists) $HTTP_GET_VARS['lngdir'] = $language;
+
+     if (isset($HTTP_GET_VARS['filename'])) {
+         $file_edit = realpath(DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename']);
+
+         if (substr($file_edit, 0, strlen(DIR_FS_CATALOG_LANGUAGES)) != DIR_FS_CATALOG_LANGUAGES) {
+             tep_redirect(tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' .
$HTTP_GET_VARS['lngdir']));
+         }
+     }
}

```

```

+
+ $action = (isset($HTTP_GET_VARS['action']) ? $HTTP_GET_VARS['action'] : '');
+
+ if (tep_not_null($action)) {
+     switch ($action) {
+         case 'save':
+             if (isset($HTTP_GET_VARS['lngdir']) && isset($HTTP_GET_VARS['filename'])) {
+                 $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename'];
+
+                 if (file_exists($file) && is_writable($file)) {
+                     $new_file = fopen($file, 'w');
+                     $file_contents = stripslashes($HTTP_POST_VARS['file_contents']);
+                     fwrite($new_file, $file_contents, strlen($file_contents));
+                     fclose($new_file);
+                 }
+
+                 tep_redirect(tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' .
$HTTP_GET_VARS['lngdir']));
+             }
+             break;
+         }
+     }
+ }
+
+ ?>
+ <!doctype html public "-//W3C//DTD HTML 4.01 Transitional//EN">
+ <html <?php echo HTML_PARAMS; ?>>
+ @@ -62,6 +91,7 @@
+ <meta http-equiv="Content-Type" content="text/html; charset=<?php echo CHARSET; ?>">
+ <title><?php echo TITLE; ?></title>
+ <link rel="stylesheet" type="text/css" href="includes/stylesheet.css">
+ <script language="javascript" src="includes/general.js"></script>
+ </head>
+ <body marginwidth="0" marginheight="0" topmargin="0" bottommargin="0" leftmargin="0" rightmargin=
"0" bgcolor="#FFFFFF">
+ <!-- header /-->
+ @@ -91,18 +121,14 @@
+         <td><table border="0" width="100%" cellpadding="2">
+
+ <?php
+     if (isset($HTTP_GET_VARS['lngdir']) && isset($HTTP_GET_VARS['filename'])) {
+ -         if ($HTTP_GET_VARS['filename'] == $HTTP_GET_VARS['lngdir'] . '.php') {
+ -             $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename'];
+ -         } else {
+ -             $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['lngdir'] . '/' .
$HTTP_GET_VARS['filename'];
+ -         }
+ +         $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename'];
+
+         if (file_exists($file)) {
+             $file_array = file($file);
+             $contents = implode('', $file_array);
+
+             $file_writeable = true;
+ -             if (!is_writeable($file)) {
+ +             if (!is_writable($file)) {
+                 $file_writeable = false;
+                 $messageStack->reset();
+                 $messageStack->add(sprintf(ERROR_FILE_NOT_WRITEABLE, $file), 'error');
+ @@ -111,12 +137,12 @@
+
+ ?>
+
+         <tr><?php echo tep_draw_form('language', FILENAME_DEFINE_LANGUAGE, 'lngdir=' .
$HTTP_GET_VARS['lngdir'] . '&filename=' . $HTTP_GET_VARS['filename'] . '&action=save'); ?>
+ -         <td><table border="0" cellpadding="2">
+ +         <td><table border="0" width="100%" cellpadding="2">
+             <tr>
+                 <td class="main"><b><?php echo $HTTP_GET_VARS['filename']; ?></b></td>
+             </tr>
+             <tr>
+ -                 <td class="main"><?php echo tep_draw_textarea_field('file_contents', 'soft',
'80', '20', $contents, (($file_writeable) ? '' : 'readonly')); ?></td>
+ +                 <td class="main"><?php echo tep_draw_textarea_field('file_contents', 'soft',
'80', '25', $contents, (($file_writeable) ? '' : 'readonly') . ' style="width: 100%;"'); ?></td>
+             </tr>
+             <tr>
+                 <td><?php echo tep_draw_separator('pixel_trans.gif', '1', '10'); ?></td>
+ @@ -126,6 +152,12 @@

```

```

        </tr>
    </table></td>
</form></tr>
+   <tr>
+       <td><?php echo tep_draw_separator('pixel_trans.gif', '1', '10'); ?></td>
+   </tr>
+   <tr>
+       <td class="main"><?php echo TEXT_EDIT_NOTE; ?></td>
+   </tr>
<?php
    } else {
    ?>
@@ -142,26 +174,31 @@
    }
    } else {
        $filename = $HTTP_GET_VARS['lngdir'] . '.php';
+       $file_extension = substr($PHP_SELF, strrpos($PHP_SELF, '.'));
    ?>

    <tr>
        <td><table width="100%" border="0" cellspacing="0" cellpadding="0">
            <tr>
                <td class="smallText"><a href="<?php echo tep_href_link(FILENAME_DEFINE_LANGUAGE,
'lngdir=' . $HTTP_GET_VARS['lngdir'] . '&filename=' . $filename); ?>"><b><?php echo $filename;
?></b></a></td>
            <td><table border="0" width="100%" cellspacing="0" cellpadding="2">
                <tr class="dataTableHeadingRow">
                    <td class="dataTableHeadingContent"><?php echo TABLE_HEADING_FILES; ?></td>
                    <td class="dataTableHeadingContent" align="center"><?php echo
TABLE_HEADING_WRITABLE; ?></td>
                    <td class="dataTableHeadingContent" align="right"><?php echo
TABLE_HEADING_LAST_MODIFIED; ?></td>
                </tr>
                <tr class="dataTableRow" onmouseover="rowOverEffect(this)" onmouseout=
"rowOutEffect(this)">
                    <td class="dataTableContent"><a href="<?php echo
tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' . $HTTP_GET_VARS['lngdir'] . '&filename=' .
$filename); ?>"><b><?php echo $filename; ?></b></a></td>
                    <td class="dataTableContent" align="center"><?php echo tep_image(DIR_WS_IMAGES .
'icons/' . ((is_writable(DIR_FS_CATALOG_LANGUAGES . $filename) == true) ? 'tick.gif' :
'cross.gif')); ?></td>
                    <td class="dataTableContent" align="right"><?php echo strftime(DATE_TIME_FORMAT,
filemtime(DIR_FS_CATALOG_LANGUAGES . $filename)); ?></td>
                </tr>
            </table>
        </td>
    </tr>
<?php
-     $left = false;
-     if ($dir = dir(DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['lngdir'])) {
-         $file_extension = substr($PHP_SELF, strrpos($PHP_SELF, '.'));
-         while ($file = $dir->read()) {
-             if (substr($file, strrpos($file, '.')) == $file_extension) {
-                 echo '
                    <td class="smallText"><a href="
                    tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' . $HTTP_GET_VARS['lngdir'] . '&filename=' .
                    $file) . '>' . $file . '</a></td>' . "\n";
-                 if (!$left) {
-                     echo '
                        </tr>' . "\n" .
-                     '
                        <tr>' . "\n";
-                 }
-                 $left = !$left;
-             }
-         }
+         foreach (tep_opendir(DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['lngdir']) as $file) {
+             if (substr($file['name'], strrpos($file['name'], '.')) == $file_extension) {
+                 $filename = substr($file['name'], strlen(DIR_FS_CATALOG_LANGUAGES));
+
+                 echo '
                    <tr class="dataTableRow" onmouseover="rowOverEffect(this)"
onmouseout="rowOutEffect(this)">' .
+                 '
                    <td class="dataTableContent"><a href="
                    tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' . $HTTP_GET_VARS['lngdir'] . '&filename=' .
                    $filename) . '>' . substr($filename, strlen($HTTP_GET_VARS['lngdir'] . '/')) . '</a></td>' .
+                 '
                    <td class="dataTableContent" align="center">' .
                    tep_image(DIR_WS_IMAGES . 'icons/' . (($file['writable'] == true) ? 'tick.gif' : 'cross.gif')) .
                    '</td>' .
+                 '
                    <td class="dataTableContent" align="right">' .
                    $file['last_modified'] . '</td>' .
+                 '
                    </tr>';
+             }
-         $dir->close();

```


?>

</tr>

catalog/admin/includes/languages/english/define_language.php

```
@@ -10,7 +10,13 @@
    Released under the GNU General Public License
    */

-define('HEADING_TITLE', 'Define Language');
+define('HEADING_TITLE', 'Define Languages');
+
+define('TABLE_HEADING_FILES', 'Files');
+define('TABLE_HEADING_WRITABLE', 'Writable');
+define('TABLE_HEADING_LAST_MODIFIED', 'Last Modified');
+
+define('TEXT_EDIT_NOTE', '<b>Editing Definitions</b><br><br>Each language definition is set using
the PHP <a href="http://www.php.net/define" target="_blank">define()</a> function in the following
manner:<br><br><nobr>define(\'TEXT_MAIN\', \'<span style="background-color: #FFFF99;">This text
can be edited. It\\\\s really easy to do!</span>\');</nobr><br><br>The highlighted text can be
edited. As this definition is using single quotes to contain the text, any single quotes within
the text definition must be escaped with a backslash (eg, It\\\\s).');

define('TEXT_FILE_DOES_NOT_EXIST', 'File does not exist.');
```

(C) (BUG) Verify Shopping Cart Product Attribute Combinations

(C) (BUG) Verify Shopping Cart Product Attribute Combinations

Importance: High | Difficulty: Easy

Verify the combination of product attributes when adding products to the shopping cart.

Affected Files

- catalog/includes/classes/shopping_cart.php

[View Changes Online](#)

catalog/includes/classes/shopping_cart.php

```

@@ -90,14 +90,22 @@

    $attributes_pass_check = true;

-    if (is_array($attributes)) {
+    if (is_array($attributes) && !empty($attributes)) {
        reset($attributes);
        while (list($option, $value) = each($attributes)) {
            if (!is_numeric($option) || !is_numeric($value)) {
                $attributes_pass_check = false;
                break;
            } else {
+                $check_query = tep_db_query("select products_attributes_id from " .
TABLE_PRODUCTS_ATTRIBUTES . " where products_id = '" . (int)$products_id . "' and options_id = '"
. (int)$option . "' and options_values_id = '" . (int)$value . "' limit 1");
+                if (tep_db_num_rows($check_query) < 1) {
+                    $attributes_pass_check = false;
+                    break;
+                }
            }
        }
    } elseif (tep_has_product_attributes($products_id)) {
+        $attributes_pass_check = false;
    }

    if (is_numeric($products_id) && is_numeric($qty) && ($attributes_pass_check == true)) {

```

(AC) (UP) Remove PHP3 Compatibility Code

(AC) (UP) Remove PHP3 Compatibility Code

Importance: Low | Difficulty: Easy

Remove PHP3 compatibility code.

Affected Files

- catalog/admin/includes/application_top.php
- catalog/admin/includes/classes/sessions.php --- (deleted)
- catalog/admin/includes/functions/compatibility.php
- catalog/admin/includes/functions/general.php
- catalog/admin/whos_online.php
- catalog/includes/application_top.php
- catalog/includes/classes/sessions.php --- (deleted)
- catalog/includes/functions/compatibility.php

[View Changes Online](#)

catalog/admin/includes/application_top.php

```

@@ -78,15 +78,6 @@
// include shopping cart class
require(DIR_WS_CLASSES . 'shopping_cart.php');

-// check to see if php implemented session management functions - if not, include php3/php4
compatible session class
- if (!function_exists('session_start')) {
-     define('PHP_SESSION_NAME', 'osCAdminID');
-     define('PHP_SESSION_PATH', '/');
-     define('PHP_SESSION_SAVE_PATH', SESSION_WRITE_DIRECTORY);
-
-     include(DIR_WS_CLASSES . 'sessions.php');
- }
-
// define how the session functions will be used
require(DIR_WS_FUNCTIONS . 'sessions.php');

```

catalog/admin/includes/classes/sessions.php --- (deleted)



This file has been deleted.

catalog/admin/includes/functions/compatibility.php

```

@@ -54,34 +54,6 @@
    date_default_timezone_set(@date_default_timezone_get());
}

- if (!function_exists('is_numeric')) {
-     function is_numeric($param) {
-         return preg_match("/^[0-9]{1,50}?.?[0-9]{0,50}$/", $param);
-     }
- }
-
- if (!function_exists('is_uploaded_file')) {
-     function is_uploaded_file($filename) {
-         if (!$tmp_file = get_cfg_var('upload_tmp_dir')) {
-             $tmp_file = dirname(tempnam('', ''));
-         }
-
-         if (strpos($tmp_file, '/')) {
-             if (substr($tmp_file, -1) != '/') $tmp_file .= '/';
-         } elseif (strpos($tmp_file, '\\')) {
-             if (substr($tmp_file, -1) != '\\') $tmp_file .= '\\';
-         }
-
-         return file_exists($tmp_file . basename($filename));
-     }
- }
-
- if (!function_exists('move_uploaded_file')) {
-     function move_uploaded_file($file, $target) {
-         return copy($file, $target);
-     }
- }
-
- if (!function_exists('checkdnsrr')) {
-     function checkdnsrr($host, $type) {
-         if (tep_not_null($host) && tep_not_null($type)) {
@@ -96,79 +68,6 @@
        }
    }

- if (!function_exists('in_array')) {
-     function in_array($lookup_value, $lookup_array) {
-         reset($lookup_array);
-         while (list($key, $value) = each($lookup_array)) {

```

```

-         if ($value == $lookup_value) return true;
-     }
-
-     return false;
- }
- }
-
- if (!function_exists('array_merge')) {
-     function array_merge($array1, $array2, $array3 = '') {
-         if ($array3 == '') $array3 = array();
-
-         while (list($key, $val) = each($array1)) $array_merged[$key] = $val;
-         while (list($key, $val) = each($array2)) $array_merged[$key] = $val;
-
-         if (sizeof($array3) > 0) while (list($key, $val) = each($array3)) $array_merged[$key] =
$aval;
-
-         return (array)$array_merged;
-     }
- }
-
- if (!function_exists('array_shift')) {
-     function array_shift(&$array) {
-         $i = 0;
-         $shifted_array = array();
-         reset($array);
-         while (list($key, $value) = each($array)) {
-             if ($i > 0) {
-                 $shifted_array[$key] = $value;
-             } else {
-                 $return = $array[$key];
-             }
-             $i++;
-         }
-         $array = $shifted_array;
-
-         return $return;
-     }
- }
-
- if (!function_exists('array_reverse')) {
-     function array_reverse($array) {
-         $reversed_array = array();
-
-         for ($i=sizeof($array)-1; $i>=0; $i--) {
-             $reversed_array[] = $array[$i];
-         }
-
-         return $reversed_array;
-     }
- }
-
- if (!function_exists('array_slice')) {
-     function array_slice($array, $offset, $length = '0') {
-         $length = abs($length);
-
-         if ($length == 0) {
-             $high = sizeof($array);
-         } else {
-             $high = $offset+$length;
-         }
-
-         for ($i=$offset; $i<$high; $i++) {
-             $new_array[$i-$offset] = $array[$i];
-         }
-
-         return $new_array;
-     }
- }
-
- /*

```

```
* http_build_query() natively supported from PHP 5.0
* From Pear::PHP_Compat
```

catalog/admin/includes/functions/general.php

```
@@ -1123,12 +1123,7 @@
    ////
    // Wrapper function for round() for php3 compatibility
    function tep_round($value, $precision) {
-     if (PHP_VERSION < 4) {
-         $exp = pow(10, $precision);
-         return round($value * $exp) / $exp;
-     } else {
-         return round($value, $precision);
-     }
+     return round($value, $precision);
    }

    ////
@@ -1193,8 +1188,6 @@
    function tep_call_function($function, $parameter, $object = '') {
        if ($object == '') {
            return call_user_func($function, $parameter);
-        } elseif (PHP_VERSION < 4) {
-            return call_user_method($function, $object, $parameter);
-        } else {
            return call_user_func(array($object, $function), $parameter);
        }
    }
}
```

catalog/admin/whos_online.php

```

@@ -112,19 +112,11 @@
    }

    if ($length = strlen($session_data)) {
-   if (PHP_VERSION < 4) {
-       $start_id = strpos($session_data, 'customer_id[==]s');
-       $start_cart = strpos($session_data, 'cart[==]o');
-       $start_currency = strpos($session_data, 'currency[==]s');
-       $start_country = strpos($session_data, 'customer_country_id[==]s');
-       $start_zone = strpos($session_data, 'customer_zone_id[==]s');
-   } else {
-       $start_id = strpos($session_data, 'customer_id|s');
-       $start_cart = strpos($session_data, 'cart|O');
-       $start_currency = strpos($session_data, 'currency|s');
-       $start_country = strpos($session_data, 'customer_country_id|s');
-       $start_zone = strpos($session_data, 'customer_zone_id|s');
-   }
+   $start_id = strpos($session_data, 'customer_id|s');
+   $start_cart = strpos($session_data, 'cart|O');
+   $start_currency = strpos($session_data, 'currency|s');
+   $start_country = strpos($session_data, 'customer_country_id|s');
+   $start_zone = strpos($session_data, 'customer_zone_id|s');

    for ($i=$start_cart; $i<$length; $i++) {
        if ($session_data[$i] == '{') {
@@ -152,12 +144,6 @@
        session_decode($session_data_zone);
        session_decode($session_data_cart);

-   if (PHP_VERSION < 4) {
-       $broken_cart = $cart;
-       $cart = new ShoppingCart;
-       $cart->unserialize($broken_cart);
-   }

-   if (is_object($cart)) {
        $products = $cart->get_products();
        for ($i = 0, $n = sizeof($products); $i < $n; $i++) {

```

catalog/includes/application_top.php

```

@@ -128,16 +128,6 @@
    // include navigation history class
    require(DIR_WS_CLASSES . 'navigation_history.php');

-   // check if sessions are supported, otherwise use the php3 compatible session class
-   if (!function_exists('session_start')) {
-       define('PHP_SESSION_NAME', 'osCsid');
-       define('PHP_SESSION_PATH', $cookie_path);
-       define('PHP_SESSION_DOMAIN', $cookie_domain);
-       define('PHP_SESSION_SAVE_PATH', SESSION_WRITE_DIRECTORY);
-   }
-   include(DIR_WS_CLASSES . 'sessions.php');
-   }

    // define how the session functions will be used
    require(DIR_WS_FUNCTIONS . 'sessions.php');

@@ -251,14 +241,8 @@
    }
}

-   // create the shopping cart & fix the cart if necessary
-   if (tep_session_is_registered('cart') && is_object($cart)) {
-       if (PHP_VERSION < 4) {
-           $broken_cart = $cart;
-           $cart = new ShoppingCart;
-           $cart->unserialize($broken_cart);
-       }

```

```

- } else {
+// create the shopping cart
+ if (!tep_session_is_registered('cart') || !is_object($cart)) {
+     tep_session_register('cart');
+     $cart = new shoppingCart;
+ }
@@ -306,13 +290,7 @@
}

// navigation history
- if (tep_session_is_registered('navigation') && is_object($navigation)) {
-     if (PHP_VERSION < 4) {
-         $broken_navigation = $navigation;
-         $navigation = new navigationHistory;
-         $navigation->unserialize($broken_navigation);
-     }
- } else {
+ if (!tep_session_is_registered('navigation') || !is_object($navigation)) {
+     tep_session_register('navigation');
+     $navigation = new navigationHistory;
+ }
@@ -342,22 +320,7 @@
        if (in_array($HTTP_POST_VARS['products_id'][$i],
(is_array($HTTP_POST_VARS['cart_delete']) ? $HTTP_POST_VARS['cart_delete'] : array())) {
            $cart->remove($HTTP_POST_VARS['products_id'][$i]);
        } else {
            if (PHP_VERSION < 4) {
                // if PHP3, make correction for lack of multidimensional
array.
                reset($HTTP_POST_VARS);
                while (list($key, $value) = each($HTTP_POST_VARS)) {
                    if (is_array($value)) {
                        while (list($key2, $value2) = each($value)) {
                            if (preg_match ("/(.*)\\\[([.*/", $key2, $var)) {
                                $id2[$var[1]][$var[2]] = $value2;
                            }
                        }
                    }
                }
            }
            $attributes = ($id2[$HTTP_POST_VARS['products_id'][$i]]) ?
$id2[$HTTP_POST_VARS['products_id'][$i]] : '';
        } else {
            $attributes =
($HTTP_POST_VARS['id'][$HTTP_POST_VARS['products_id'][$i]]) ?
$HTTP_POST_VARS['id'][$HTTP_POST_VARS['products_id'][$i]] : '';
        }
+        $attributes =
($HTTP_POST_VARS['id'][$HTTP_POST_VARS['products_id'][$i]]) ?
$HTTP_POST_VARS['id'][$HTTP_POST_VARS['products_id'][$i]] : '';
        $cart->add_cart($HTTP_POST_VARS['products_id'][$i],
$HTTP_POST_VARS['cart_quantity'][$i], $attributes, false);

```

```
}  
}
```

catalog/includes/classes/sessions.php --- (deleted)



This file has been deleted.

catalog/includes/functions/compatibility.php

```
@@ -54,120 +54,6 @@  
    date_default_timezone_set(@date_default_timezone_get());  
}  
  
- if (!function_exists('array_splice')) {  
-     function array_splice(&$array, $maximum) {  
-         if (sizeof($array) >= $maximum) {  
-             for ($i=0; $i<$maximum; $i++) {  
-                 $new_array[$i] = $array[$i];  
-             }  
-             $array = $new_array;  
-         }  
-     }  
- }  
-  
- if (!function_exists('in_array')) {  
-     function in_array($lookup_value, $lookup_array) {  
-         reset($lookup_array);  
-         while (list($key, $value) = each($lookup_array)) {  
-             if ($value == $lookup_value) return true;  
-         }  
-         return false;  
-     }  
- }  
-  
- if (!function_exists('array_reverse')) {  
-     function array_reverse($array) {  
-         for ($i=0, $n=sizeof($array); $i<$n; $i++) $array_reversed[$i] = $array[($n-$i-1)];  
-         return $array_reversed;  
-     }  
- }  
-  
- if (!function_exists('constant')) {  
-     function constant($constant) {  
-         eval("\$temp=$constant;");  
-         return $temp;  
-     }  
- }  
-  
- if (!function_exists('is_null')) {  
-     function is_null($value) {  
-         if (is_array($value)) {  
-             if (sizeof($value) > 0) {  
-                 return false;  
-             } else {  
-                 return true;  
-             }  
-         } else {  
-             if (($value != '') && ($value != 'NULL') && (strlen(trim($value)) > 0)) {  
-                 return false;  
-             } else {  
-                 return true;  
-             }  
-         }  
-     }  
- }  
- }
```



```

- if (!function_exists('array_merge')) {
-     function array_merge($array1, $array2, $array3 = '') {
-         if (empty($array3) && !is_array($array3)) $array3 = array();
-         while (list($key, $val) = each($array1)) $array_merged[$key] = $val;
-         while (list($key, $val) = each($array2)) $array_merged[$key] = $val;
-         if (sizeof($array3) > 0) while (list($key, $val) = each($array3)) $array_merged[$key] =
$val;
-
-         return (array) $array_merged;
-     }
- }
-
- if (!function_exists('is_numeric')) {
-     function is_numeric($param) {
-         return preg_match('/^[0-9]{1,50}.?[0-9]{0,50}$/', $param);
-     }
- }
-
- if (!function_exists('array_slice')) {
-     function array_slice($array, $offset, $length = 0) {
-         if ($offset < 0 ) {
-             $offset = sizeof($array) + $offset;
-         }
-         $length = ((!$length) ? sizeof($array) : (($length < 0) ? sizeof($array) - $length :
$length + $offset));
-         for ($i = $offset; $i < $length; $i++) {
-             $tmp[] = $array[$i];
-         }
-
-         return $tmp;
-     }
- }
-
- if (!function_exists('array_map')) {
-     function array_map($callback, $array) {
-         if (is_array($array)) {
-             $_new_array = array();
-             reset($array);
-             while (list($key, $value) = each($array)) {
-                 $_new_array[$key] = array_map($callback, $array[$key]);
-             }
-             return $_new_array;
-         } else {
-             return $callback($array);
-         }
-     }
- }
-
- if (!function_exists('str_repeat')) {
-     function str_repeat($string, $number) {
-         $repeat = '';
-
-         for ($i=0; $i<$number; $i++) {
-             $repeat .= $string;
-         }
-
-         return $repeat;
-     }
- }
-
- if (!function_exists('checkdnsrr')) {

```

```
function checkdnsrr($host, $type) {  
    if(tep_not_null($host) && tep_not_null($type)) {
```

(AC) (UP) Improve IP Address Detection

(AC) (UP) Improve IP Address Detection

Importance: Medium | Difficulty: Easy

Improve how IP-Addresses are retrieved and add support for multiple proxy servers.

Affected Files

- [catalog/admin/includes/functions/general.php](#)
- [catalog/includes/functions/general.php](#)

[View Changes Online](#)

catalog/admin/includes/functions/general.php

```

@@ -1296,4 +1296,64 @@

    return $tmp_array;
}
+
+ function tep_validate_ip_address($ip_address) {
+     if (function_exists('filter_var') && defined('FILTER_VALIDATE_IP')) {
+         return filter_var($ip_address, FILTER_VALIDATE_IP, array('flags' => FILTER_FLAG_IPV4));
+     }
+
+     if (preg_match('/^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$/', $ip_address)) {
+         $parts = explode('.', $ip_address);
+
+         foreach ($parts as $ip_parts) {
+             if ( (intval($ip_parts) > 255) || (intval($ip_parts) < 0) ) {
+                 return false; // number is not within 0-255
+             }
+         }
+
+         return true;
+     }
+
+     return false;
+ }
+
+ function tep_get_ip_address() {
+     global $HTTP_SERVER_VARS;
+
+     $ip_address = null;
+     $ip_addresses = array();
+
+     if (isset($HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR']) &&
!empty($HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'])) {
+         foreach ( array_reverse(explode(',', $HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'])) as $x_ip )
+         {
+             $x_ip = trim($x_ip);
+
+             if (tep_validate_ip_address($x_ip)) {
+                 $ip_addresses[] = $x_ip;
+             }
+         }
+
+         if (isset($HTTP_SERVER_VARS['HTTP_CLIENT_IP']) &&
!empty($HTTP_SERVER_VARS['HTTP_CLIENT_IP'])) {
+             $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_CLIENT_IP'];
+         }
+
+         if (isset($HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP']) &&
!empty($HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP'])) {
+             $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP'];
+         }
+
+         if (isset($HTTP_SERVER_VARS['HTTP_PROXY_USER']) &&
!empty($HTTP_SERVER_VARS['HTTP_PROXY_USER'])) {
+             $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_PROXY_USER'];
+         }
+
+         $ip_addresses[] = $HTTP_SERVER_VARS['REMOTE_ADDR'];
+
+         foreach ( $ip_addresses as $ip ) {
+             if (!empty($ip) && tep_validate_ip_address($ip)) {
+                 $ip_address = $ip;
+                 break;
+             }
+         }
+
+         return $ip_address;
+     }
+ }
+
?>

```

```

@@ -1227,28 +1227,64 @@
    setcookie($name, $value, $expire, $path, (tep_not_null($domain) ? $domain : ''), $secure);
}

+ function tep_validate_ip_address($ip_address) {
+     if (function_exists('filter_var') && defined('FILTER_VALIDATE_IP')) {
+         return filter_var($ip_address, FILTER_VALIDATE_IP, array('flags' => FILTER_FLAG_IPV4));
+     }
+
+     if (preg_match('/^(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})$/', $ip_address)) {
+         $parts = explode('.', $ip_address);
+
+         foreach ($parts as $ip_parts) {
+             if ( (intval($ip_parts) > 255) || (intval($ip_parts) < 0) ) {
+                 return false; // number is not within 0-255
+             }
+         }
+
+         return true;
+     }
+
+     return false;
+ }

function tep_get_ip_address() {
    global $HTTP_SERVER_VARS;

-     if (isset($HTTP_SERVER_VARS)) {
-         if (isset($HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'])) {
-             $ip = $HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'];
-         } elseif (isset($HTTP_SERVER_VARS['HTTP_CLIENT_IP'])) {
-             $ip = $HTTP_SERVER_VARS['HTTP_CLIENT_IP'];
-         } else {
-             $ip = $HTTP_SERVER_VARS['REMOTE_ADDR'];
+         $ip_address = null;
+         $ip_addresses = array();
+
+         if (isset($HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR']) &&
!empty($HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'])) {
+             foreach ( array_reverse(explode(',', $HTTP_SERVER_VARS['HTTP_X_FORWARDED_FOR'])) as $x_ip )
+             {
+                 $x_ip = trim($x_ip);
+
+                 if (tep_validate_ip_address($x_ip)) {
+                     $ip_addresses[] = $x_ip;
+                 }
+             }
+         } else {
+             if (getenv('HTTP_X_FORWARDED_FOR')) {
+                 $ip = getenv('HTTP_X_FORWARDED_FOR');
+             } elseif (getenv('HTTP_CLIENT_IP')) {
+                 $ip = getenv('HTTP_CLIENT_IP');
+             } else {
+                 $ip = getenv('REMOTE_ADDR');
+             }
+
+             if (isset($HTTP_SERVER_VARS['HTTP_CLIENT_IP']) &&
!empty($HTTP_SERVER_VARS['HTTP_CLIENT_IP'])) {
+                 $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_CLIENT_IP'];
+             }
+
+             if (isset($HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP']) &&
!empty($HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP'])) {
+                 $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_X_CLUSTER_CLIENT_IP'];
+             }
+
+             if (isset($HTTP_SERVER_VARS['HTTP_PROXY_USER']) &&
!empty($HTTP_SERVER_VARS['HTTP_PROXY_USER'])) {
+                 $ip_addresses[] = $HTTP_SERVER_VARS['HTTP_PROXY_USER'];
+             }
+
+             $ip_addresses[] = $HTTP_SERVER_VARS['REMOTE_ADDR'];

```

```
+  
+  foreach ( $ip_addresses as $ip ) {  
+    if (!empty($ip) && tep_validate_ip_address($ip)) {  
+      $ip_address = $ip;  
+      break;  
+    }  
+  }  
  
-  return $ip;  
+  return $ip_address;  
}
```

```
function tep_count_customer_orders($id = '', $check_session = true) {
```

(A) (BUG) Don't Show Empty Menu Entries

(A) (BUG) Don't Show Empty Menu Entries

Importance: Low | Difficulty: Easy

Don't show empty menu navigation boxes.

Affected Files

- [catalog/admin/includes/classes/box.php](#)

[View Changes Online](#)

catalog/admin/includes/classes/box.php

```
@@ -52,7 +52,7 @@
    $this->heading = $this->tableBlock($heading);

    $this->table_data_parameters = 'class="menuBoxContent"';
-    $this->contents = $this->tableBlock($contents);
+    $this->contents = (!empty($contents) ? $this->tableBlock($contents) : '');

    return $this->heading . $this->contents;
}
```

(AC) (UP) Add htaccess Protection to the Images Directory

(AC) (UP) Add htaccess Protection to the Images Directory

Importance: Medium | Difficulty: Easy


Add htaccess protection to the images directory.

Affected Files

- [catalog/admin/images/.htaccess](#) --- (new file)
- [catalog/images/.htaccess](#) --- (new file)

[View Changes Online](#)

catalog/admin/images/.htaccess --- (new file)

 This is a new file. ([Download File](#))

catalog/images/.htaccess --- (new file)

 This is a new file. ([Download File](#))

(C) (UP) Optimize Tax Calculations

(C) (UP) Optimize Tax Calculations

Importance: Medium | Difficulty: Easy

Optimize database queries performing tax calculations.

Affected Files

- [catalog/includes/functions/general.php](#)

[View Changes Online](#)

catalog/includes/functions/general.php

```
@@ -311,6 +311,7 @@
// TABLES: tax_rates, zones_to_geo_zones
function tep_get_tax_rate($class_id, $country_id = -1, $zone_id = -1) {
    global $customer_zone_id, $customer_country_id;
+    static $tax_rates = array();

    if ( ($country_id == -1) && ($zone_id == -1) ) {
        if (!tep_session_is_registered('customer_id')) {
@@ -322,34 +323,45 @@
        }
    }

-    $tax_query = tep_db_query("select sum(tax_rate) as tax_rate from " . TABLE_TAX_RATES . " tr
left join " . TABLE_ZONES_TO_GEO_ZONES . " za on (tr.tax_zone_id = za.geo_zone_id) left join " .
TABLE_GEO_ZONES . " tz on (tz.geo_zone_id = tr.tax_zone_id) where (za.zone_country_id is null or
za.zone_country_id = '0' or za.zone_country_id = '" . (int)$country_id . "') and (za.zone_id is
null or za.zone_id = '0' or za.zone_id = '" . (int)$zone_id . "') and tr.tax_class_id = '" . (int
)$class_id . "' group by tr.tax_priority");
-    if (tep_db_num_rows($tax_query)) {
-        $tax_multiplier = 1.0;
-        while ($tax = tep_db_fetch_array($tax_query)) {
-            $tax_multiplier *= 1.0 + ($tax['tax_rate'] / 100);
+    if (!isset($tax_rates[$class_id][$country_id][$zone_id]['rate'])) {
+        $tax_query = tep_db_query("select sum(tax_rate) as tax_rate from " . TABLE_TAX_RATES . " tr
left join " . TABLE_ZONES_TO_GEO_ZONES . " za on (tr.tax_zone_id = za.geo_zone_id) left join " .
TABLE_GEO_ZONES . " tz on (tz.geo_zone_id = tr.tax_zone_id) where (za.zone_country_id is null or
za.zone_country_id = '0' or za.zone_country_id = '" . (int)$country_id . "') and (za.zone_id is
null or za.zone_id = '0' or za.zone_id = '" . (int)$zone_id . "') and tr.tax_class_id = '" . (int
)$class_id . "' group by tr.tax_priority");
+        if (tep_db_num_rows($tax_query)) {
+            $tax_multiplier = 1.0;
+            while ($tax = tep_db_fetch_array($tax_query)) {
+                $tax_multiplier *= 1.0 + ($tax['tax_rate'] / 100);
+            }
+
+            $tax_rates[$class_id][$country_id][$zone_id]['rate'] = ($tax_multiplier - 1.0) * 100;
+        } else {
+            $tax_rates[$class_id][$country_id][$zone_id]['rate'] = 0;
+        }
-        return ($tax_multiplier - 1.0) * 100;
-    } else {
-        return 0;
+    }
+
+    return $tax_rates[$class_id][$country_id][$zone_id]['rate'];
}

////
// Return the tax description for a zone / class
// TABLES: tax_rates;
function tep_get_tax_description($class_id, $country_id, $zone_id) {
-    $tax_query = tep_db_query("select tax_description from " . TABLE_TAX_RATES . " tr left join "
. TABLE_ZONES_TO_GEO_ZONES . " za on (tr.tax_zone_id = za.geo_zone_id) left join " .
TABLE_GEO_ZONES . " tz on (tz.geo_zone_id = tr.tax_zone_id) where (za.zone_country_id is null or
za.zone_country_id = '0' or za.zone_country_id = '" . (int)$country_id . "') and (za.zone_id is
null or za.zone_id = '0' or za.zone_id = '" . (int)$zone_id . "') and tr.tax_class_id = '" . (int
)$class_id . "' order by tr.tax_priority");
-    if (tep_db_num_rows($tax_query)) {
-        $tax_description = '';
-        while ($tax = tep_db_fetch_array($tax_query)) {
-            $tax_description .= $tax['tax_description'] . ' + ';
-        }
    }
```

```

-     $tax_description = substr($tax_description, 0, -3);
+     static $tax_rates = array();
+
+     if (!isset($tax_rates[$class_id][$country_id][$zone_id]['description'])) {
+         $tax_query = tep_db_query("select tax_description from " . TABLE_TAX_RATES . " tr left join
+ " . TABLE_ZONES_TO_GEO_ZONES . " za on (tr.tax_zone_id = za.geo_zone_id) left join " .
TABLE_GEO_ZONES . " tz on (tz.geo_zone_id = tr.tax_zone_id) where (za.zone_country_id is null or
za.zone_country_id = '0' or za.zone_country_id = '" . (int)$country_id . "') and (za.zone_id is
null or za.zone_id = '0' or za.zone_id = '" . (int)$zone_id . "') and tr.tax_class_id = '" . (int
)$class_id . "' order by tr.tax_priority");
+         if (tep_db_num_rows($tax_query)) {
+             $tax_description = '';
+             while ($tax = tep_db_fetch_array($tax_query)) {
+                 $tax_description .= $tax['tax_description'] . ' + ';
+             }
+             $tax_description = substr($tax_description, 0, -3);
+
+         return $tax_description;
+     } else {
+         return TEXT_UNKNOWN_TAX_RATE;
+         $tax_rates[$class_id][$country_id][$zone_id]['description'] = $tax_description;
+     } else {
+         $tax_rates[$class_id][$country_id][$zone_id]['description'] = TEXT_UNKNOWN_TAX_RATE;
+     }
+ }
+
+ return $tax_rates[$class_id][$country_id][$zone_id]['description'];
}

```


////

(AC) (UP) Improve Force Cookie Usage in Sessions

(AC) (UP) Improve Force Cookie Usage in Sessions

Importance: Medium | Difficulty: Easy

Set session.use_only_cookies when force cookie usage is enabled.

Affected Files

- [catalog/admin/includes/application_top.php](#)
- [catalog/includes/application_top.php](#)

[View Changes Online](#)

catalog/admin/includes/application_top.php

```
@@ -93,6 +93,8 @@
    ini_set('session.cookie_path', DIR_WS_ADMIN);
}

+ @ini_set('session.use_only_cookies', (SESSION_FORCE_COOKIE_USE == 'True') ? 1 : 0);
+
// lets start our session
tep_session_start();
```

catalog/includes/application_top.php

```
@@ -144,6 +144,8 @@
    ini_set('session.cookie_domain', $cookie_domain);
}

+ @ini_set('session.use_only_cookies', (SESSION_FORCE_COOKIE_USE == 'True') ? 1 : 0);
+
// set the session ID if it exists
if (isset($_HTTP_POST_VARS[tep_session_name()])) {
    tep_session_id($_HTTP_POST_VARS[tep_session_name()]);
}
```

(A) (BUG) Fix Automatic Removal of Manufacturer Images

(A) (BUG) Fix Automatic Removal of Manufacturer Images

Importance: High | Difficulty: Easy

Don't delete manufacturer images when editing a manufacturer and no manufacturer image was provided.

Affected Files

- [catalog/admin/manufacturers.php](#)

[View Changes Online](#)

catalog/admin/manufacturers.php

```

@@ -38,8 +38,11 @@
        tep_db_perform(TABLE_MANUFACTURERS, $sql_data_array, 'update', "manufacturers_id = '" .
(int)$manufacturers_id . "'");
    }

-        if ($manufacturers_image = new upload('manufacturers_image', DIR_FS_CATALOG_IMAGES)) {
-            tep_db_query("update " . TABLE_MANUFACTURERS . " set manufacturers_image = '" .
$manufacturers_image->filename . "' where manufacturers_id = '" . (int)$manufacturers_id . "'");
+            $manufacturers_image = new upload('manufacturers_image');
+            $manufacturers_image->set_destination(DIR_FS_CATALOG_IMAGES);
+
+            if ($manufacturers_image->parse() && $manufacturers_image->save()) {
+                tep_db_query("update " . TABLE_MANUFACTURERS . " set manufacturers_image = '" .
tep_db_input($manufacturers_image->filename) . "' where manufacturers_id = '" . (int
)$manufacturers_id . "'");
            }

        $languages = tep_get_languages();

```

(A) (UP) Add API Version Tag to Modules

(A) (UP) Add API Version Tag to Modules

Importance: Low | Difficulty: Easy

Add API version tag to modules.

Affected Files

- [catalog/admin/includes/languages/english/modules.php](#)
- [catalog/admin/modules.php](#)

[View Changes Online](#)



This changeset includes an update to an English language definition file. Please perform similar changes to other languages that are also installed.

catalog/admin/includes/languages/english/modules.php

```

@@ -20,6 +20,7 @@ define('TABLE_HEADING_ACTION', 'Action');

define('TEXT_INFO_VERSION', 'Version:');
define('TEXT_INFO_ONLINE_STATUS', 'online status');
+define('TEXT_INFO_API_VERSION', 'API Version:');

define('TEXT_MODULE_DIRECTORY', 'Module Directory:');
?>

```

catalog/admin/modules.php

```

@@ -144,7 +144,8 @@
                                'title' => $module->title,
                                'description' => $module->description,
                                'status' => $module->check(),
                                'signature' => (isset($module->signature) ? $module->signature :
- null));
+                                'signature' => (isset($module->signature) ? $module->signature :
+ null),
+                                'api_version' => (isset($module->api_version) ? $module->api_version
+ : null));

                                $module_keys = $module->keys();

@@ -257,6 +258,10 @@
                                $contents[] = array('text' => '<br>' . tep_image(DIR_WS_IMAGES . 'icon_info.gif',
                                IMAGE_ICON_INFO) . '&nbsp;<b>' . TEXT_INFO_VERSION . '</b>' . $sversion . ' (<a href="http:
                                //sig.oscommerce.com/' . $mInfo->signature . '" target="_blank">' . TEXT_INFO_ONLINE_STATUS .
                                '</a>'));
                                }

+                                if (isset($mInfo->api_version)) {
+                                $contents[] = array('text' => tep_image(DIR_WS_IMAGES . 'icon_info.gif',
                                IMAGE_ICON_INFO) . '&nbsp;<b>' . TEXT_INFO_API_VERSION . '</b>' . $mInfo->api_version);
+                                }
+
                                $contents[] = array('text' => '<br>' . $mInfo->description);
                                $contents[] = array('text' => '<br>' . $keys);
                                } else {
@@ -266,6 +271,10 @@
                                $contents[] = array('text' => '<br>' . tep_image(DIR_WS_IMAGES . 'icon_info.gif',
                                IMAGE_ICON_INFO) . '&nbsp;<b>' . TEXT_INFO_VERSION . '</b>' . $sversion . ' (<a href="http:
                                //sig.oscommerce.com/' . $mInfo->signature . '" target="_blank">' . TEXT_INFO_ONLINE_STATUS .
                                '</a>'));
                                }

+                                if (isset($mInfo->api_version)) {
+                                $contents[] = array('text' => tep_image(DIR_WS_IMAGES . 'icon_info.gif',
                                IMAGE_ICON_INFO) . '&nbsp;<b>' . TEXT_INFO_API_VERSION . '</b>' . $mInfo->api_version);
+                                }
+
                                $contents[] = array('text' => '<br>' . $mInfo->description);
                                }
                                break;

```

(C) (UP) Hide Currencies and Languages Info Boxes for Single Currencies and Languages

(C) (UP) Hide Currencies and Languages Info Boxes for Single Currencies and Languages

Importance: Low | Difficulty: Easy

Hide the currencies and languages info boxes if only one currency or language is available.

Affected Files

- [catalog/includes/boxes/currencies.php](#)
- [catalog/includes/boxes/languages.php](#)

[View Changes Online](#)

[catalog/includes/boxes/currencies.php](#)

```

@@ -10,7 +10,7 @@
Released under the GNU General Public License
*/

- if (isset($currencies) && is_object($currencies)) {
+ if (isset($currencies) && is_object($currencies) && (count($currencies->currencies) > 1)) {
?>
<!-- currencies //-->
<tr>

```

catalog/includes/boxes/languages.php

```

@@ -9,6 +9,13 @@

Released under the GNU General Public License
*/
+
+ if (!isset($lng) || (isset($lng) && !is_object($lng))) {
+ include(DIR_WS_CLASSES . 'language.php');
+ $lng = new language;
+ }
+
+ if (count($lng->catalog_languages) > 1) {
?>
<!-- languages //-->
<tr>
@@ -19,11 +26,6 @@

new infoBoxHeading($info_box_contents, false, false);

- if (!isset($lng) || (isset($lng) && !is_object($lng))) {
- include(DIR_WS_CLASSES . 'language.php');
- $lng = new language;
- }
-
$languages_string = '';
reset($lng->catalog_languages);
while (list($key, $value) = each($lng->catalog_languages)) {
@@ -39,3 +41,6 @@
</td>
</tr>
<!-- languages_eof //-->
+<?php
+ }
+?>

```

(A) (UP) Hide Language Selection if Only One Language is Installed

(A) (UP) Hide Language Selection if Only One Language is Installed

Importance: Low | Difficulty: Easy

Hide language selection if only one language is installed.

Affected Files

- [catalog/admin/index.php](#)
- [catalog/admin/login.php](#)

[View Changes Online](#)

catalog/admin/index.php

```

@@ -51,7 +51,17 @@
    <td><table border="0" width="100%" cellpadding="2" height="40">
      <tr>
        <td class="pageHeading"><?php echo STORE_NAME; ?></td>
+
+<?php
+  if (sizeof($languages_array) > 1) {
+?>
+
        <td class="pageHeading" align="right"><?php echo tep_draw_form('adminlanguage',
FILENAME_DEFAULT, '', 'get') . tep_draw_pull_down_menu('language', $languages_array,
$languages_selected, 'onChange="this.form.submit();"') . tep_hide_session_id() . '</form>';
?></td>
+
+<?php
+  }
+?>
+
      </tr>
    </table></td>
  </tr>

```

catalog/admin/login.php

```

@@ -130,7 +130,17 @@
    <td><table border="0" width="100%" cellpadding="0" height="40">
      <tr>
        <td class="pageHeading"><?php echo HEADING_TITLE; ?></td>
+
+<?php
+  if (sizeof($languages_array) > 1) {
+?>
+
        <td class="pageHeading" align="right"><?php echo tep_draw_form('adminlanguage',
FILENAME_DEFAULT, '', 'get') . tep_draw_pull_down_menu('language', $languages_array,
$languages_selected, 'onChange="this.form.submit();"') . tep_hide_session_id() . '</form>';
?></td>
+
+<?php
+  }
+?>
+
      </tr>
    </table></td>
  </tr>

```

(C) (BUG) Fix Retrieval of Special Product Prices

(C) (BUG) Fix Retrieval of Special Product Prices

Importance: Low | Difficulty: Easy

Fix retrieval of special product prices.

Affected Files

- catalog/includes/functions/general.php

[View Changes Online](#)

catalog/includes/functions/general.php

```

@@ -96,7 +96,7 @@
// Return a product's special price (returns nothing if there is no offer)
// TABLES: products
function tep_get_products_special_price($product_id) {
-   $product_query = tep_db_query("select specials_new_products_price from " . TABLE_SPECIALS . "
where products_id = '" . (int)$product_id . "' and status");
+   $product_query = tep_db_query("select specials_new_products_price from " . TABLE_SPECIALS . "
where products_id = '" . (int)$product_id . "' and status = 1");
    $product = tep_db_fetch_array($product_query);

    return $product['specials_new_products_price'];
}

```

(A) (BUG) Fix HTML E-Mails

(A) (BUG) Fix HTML E-Mails

Importance: Low | Difficulty: Easy

Some e-mail methods were not building HTML e-mails.

Affected Files

- catalog/admin/includes/modules/newsletters/newsletter.php
- catalog/admin/includes/modules/newsletters/product_notification.php
- catalog/admin/mail.php

[View Changes Online](#)

catalog/admin/includes/modules/newsletters/newsletter.php

```

@@ -59,8 +59,16 @@
function send($newsletter_id) {
    $mail_query = tep_db_query("select customers_firstname, customers_lastname,
customers_email_address from " . TABLE_CUSTOMERS . " where customers_newsletter = '1'");

-   $mimemessage = new email(array('X-Mailer: osCommerce bulk mailer'));
+   $mimemessage->add_text($this->content);
+   $mimemessage = new email(array('X-Mailer: osCommerce'));
+
+   // Build the text version
+   $text = strip_tags($this->content);
+   if (EMAIL_USE_HTML == 'true') {
+       $mimemessage->add_html($this->content, $text);
+   } else {
+       $mimemessage->add_text($text);
+   }
+
    $mimemessage->build_message();
    while ($mail = tep_db_fetch_array($mail_query)) {
        $mimemessage->send($mail['customers_firstname'] . ' ' . $mail['customers_lastname'],
        $mail['customers_email_address'], '', EMAIL_FROM, $this->title);
    }
}

```

catalog/admin/includes/modules/newsletters/product_notification.php

```

@@ -200,8 +200,16 @@ function selectAll(FormName, SelectBox) {
    }
}

-     $mimemessage = new email(array('X-Mailer: osCommerce bulk mailer'));
-     $mimemessage->add_text($this->content);
+     $mimemessage = new email(array('X-Mailer: osCommerce'));
+
+     // Build the text version
+     $text = strip_tags($this->content);
+     if (EMAIL_USE_HTML == 'true') {
+         $mimemessage->add_html($this->content, $text);
+     } else {
+         $mimemessage->add_text($text);
+     }
+
    $mimemessage->build_message();

    reset($audience);

```

catalog/admin/mail.php

```

@@ -38,8 +38,15 @@

    //Let's build a message object using the email class
    $mimemessage = new email(array('X-Mailer: osCommerce'));
-    // add the message to the object
-    $mimemessage->add_text($message);
+
+    // Build the text version
+    $text = strip_tags($message);
+    if (EMAIL_USE_HTML == 'true') {
+        $mimemessage->add_html($message, $text);
+    } else {
+        $mimemessage->add_text($message);
+    }
+
    $mimemessage->build_message();
    while ($mail = tep_db_fetch_array($mail_query)) {
        $mimemessage->send($mail['customers_firstname'] . ' ' . $mail['customers_lastname'],
        $mail['customers_email_address'], '', $from, $subject);

```

(A) (BUG) Improve Saving of Module Parameters

(A) (BUG) Improve Saving of Module Parameters

Importance: Low | Difficulty: Easy

Improve saving of module parameters.

Affected Files

- [catalog/admin/modules.php](#)

[View Changes Online](#)

catalog/admin/modules.php

```

@@ -43,6 +43,7 @@
    if (tep_not_null($action)) {
        switch ($action) {
            case 'save':
+               reset($HTTP_POST_VARS['configuration']);
                while (list($key, $value) = each($HTTP_POST_VARS['configuration'])) {
                    tep_db_query("update " . TABLE_CONFIGURATION . " set configuration_value = '" . $value
. "' where configuration_key = '" . $key . "'");
                }
            }
        }
    }
}

```

(AC) (UP) Add Pre-Populated List of Currencies

(AC) (UP) Add Pre-Populated List of Currencies

Importance: Low | Difficulty: Easy

Add a list of pre-populated currencies to choose from when adding new currencies.

Affected Files

- [catalog/admin/currencies.php](#)
- [catalog/admin/includes/languages/english.php](#)
- [catalog/admin/includes/languages/english/currencies.php](#)
- [catalog/includes/languages/english.php](#)

[View Changes Online](#)



This changeset includes updates to English language definition files. Please perform similar changes to other languages that are also installed.

catalog/admin/currencies.php

```

@@ -109,6 +109,39 @@
    break;
}
}

+
+ $currency_select = array('USD' => array('title' => 'U.S. Dollar', 'code' => 'USD',
+ 'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),
+
+ 'EUR' => array('title' => 'Euro', 'code' => 'EUR', 'symbol_left' =>
+ '', 'symbol_right' => '€', 'decimal_point' => '.', 'thousands_point' => ',', 'decimal_places' =>
+ '2'),
+
+ 'JPY' => array('title' => 'Japanese Yen', 'code' => 'JPY',
+ 'symbol_left' => '¥', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),
+
+ 'GBP' => array('title' => 'Pounds Sterling', 'code' => 'GBP',
+ 'symbol_left' => '£', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),
+
+ 'CHF' => array('title' => 'Swiss Franc', 'code' => 'CHF',
+ 'symbol_left' => '', 'symbol_right' => 'CHF', 'decimal_point' => ',', 'thousands_point' => '.',
+ 'decimal_places' => '2'),
+
+ 'AUS' => array('title' => 'Australian Dollar', 'code' => 'AUS',
+ 'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),
+
+ 'CAD' => array('title' => 'Canadian Dollar', 'code' => 'CAD',
+ 'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),
+
+ 'SEK' => array('title' => 'Swedish Krona', 'code' => 'SEK',
+ 'symbol_left' => '', 'symbol_right' => 'kr', 'decimal_point' => ',', 'thousands_point' => '.',
+ 'decimal_places' => '2'),
+
+ 'HKD' => array('title' => 'Hong Kong Dollar', 'code' => 'HKD',
+ 'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
+ 'decimal_places' => '2'),

```



```

+         'NOK' => array('title' => 'Norwegian Krone', 'code' => 'NOK',
'symbol_left' => 'kr', 'symbol_right' => '', 'decimal_point' => ',', 'thousands_point' => '.',
'decimal_places' => '2'),
+         'NZD' => array('title' => 'New Zealand Dollar', 'code' => 'NZD',
'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'MXN' => array('title' => 'Mexican Peso', 'code' => 'MXN',
'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'SGD' => array('title' => 'Singapore Dollar', 'code' => 'SGD',
'symbol_left' => '$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'BRL' => array('title' => 'Brazilian Real', 'code' => 'BRL',
'symbol_left' => 'R$', 'symbol_right' => '', 'decimal_point' => ',', 'thousands_point' => '.',
'decimal_places' => '2'),
+         'CNY' => array('title' => 'Chinese RMB', 'code' => 'CNY',
'symbol_left' => '', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'CZK' => array('title' => 'Czech Koruna', 'code' => 'CZK',
'symbol_left' => '', 'symbol_right' => 'K', 'decimal_point' => ',', 'thousands_point' => '.',
'decimal_places' => '2'),
+         'DKK' => array('title' => 'Danish Krone', 'code' => 'DKK',
'symbol_left' => '', 'symbol_right' => 'kr', 'decimal_point' => ',', 'thousands_point' => '.',
'decimal_places' => '2'),
+         'HUF' => array('title' => 'Hungarian Forint', 'code' => 'HUF',
'symbol_left' => '', 'symbol_right' => 'Ft', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'ILS' => array('title' => 'Israeli New Shekel', 'code' => 'ILS',
'symbol_left' => '', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'INR' => array('title' => 'Indian Rupee', 'code' => 'INR',
'symbol_left' => 'Rs.', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'MYR' => array('title' => 'Malaysian Ringgit', 'code' => 'MYR',
'symbol_left' => 'RM', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'PHP' => array('title' => 'Philippine Peso', 'code' => 'PHP',
'symbol_left' => 'Php', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'),
+         'PLN' => array('title' => 'Polish Zloty', 'code' => 'PLN',
'symbol_left' => '', 'symbol_right' => 'z', 'decimal_point' => ',', 'thousands_point' => '.',
'decimal_places' => '2'),
+         'THB' => array('title' => 'Thai Baht', 'code' => 'THB', 'symbol_left'
=> '', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',', 'decimal_places' =>
'2'),
+         'TWD' => array('title' => 'Taiwan New Dollar', 'code' => 'TWD',
'symbol_left' => 'NT$', 'symbol_right' => '', 'decimal_point' => '.', 'thousands_point' => ',',
'decimal_places' => '2'));
+
+ $currency_select_array = array(array('id' => '', 'text' => TEXT_INFO_COMMON_CURRENCIES));
+ foreach ($currency_select as $cs) {
+     if (!isset($currencies->currencies[$cs['code']])) {
+         $currency_select_array[] = array('id' => $cs['code'], 'text' => '[' . $cs['code'] . ']' .
$cs['title']);
+     }
+ }
+
?>
<!doctype html public "-//W3C//DTD HTML 4.01 Transitional//EN">
<html <?php echo HTML_PARAMS; ?>>
@@ -123,6 +156,30 @@
<?php require(DIR_WS_INCLUDES . 'header.php'); ?>
<!-- header_eof //-->

+<script type="text/javascript">
+var currency_select = new Array();
+<?php
+    foreach ($currency_select_array as $cs) {
+        if (!empty($cs['id'])) {
+            echo 'currency_select["' . $cs['id'] . '"] = new Array("' .
$currency_select[$cs['id']]['title'] . '", "' . $currency_select[$cs['id']]['symbol_left'] . '",
"' . $currency_select[$cs['id']]['symbol_right'] . '", "' .
$currency_select[$cs['id']]['decimal_point'] . '", "' .
$currency_select[$cs['id']]['thousands_point'] . '", "' .
$currency_select[$cs['id']]['decimal_places'] . '");' . "\n";
+        }
+    }
+

```

```

+ }
+?>
+
+function updateForm() {
+  var cs = document.forms["currencies"].cs[document.forms["currencies"].cs.selectedIndex].value;
+
+  document.forms["currencies"].title.value = currency_select[cs][0];
+  document.forms["currencies"].code.value = cs;
+  document.forms["currencies"].symbol_left.value = currency_select[cs][1];
+  document.forms["currencies"].symbol_right.value = currency_select[cs][2];
+  document.forms["currencies"].decimal_point.value = currency_select[cs][3];
+  document.forms["currencies"].thousands_point.value = currency_select[cs][4];
+  document.forms["currencies"].decimal_places.value = currency_select[cs][5];
+  document.forms["currencies"].value.value = 1;
+}
+</script>
+
+  <!-- body //-->
+<table border="0" width="100%" cellspacing="2" cellpadding="2">
+  <tr>
+    @@ -208,6 +265,7 @@
+
+    $contents = array('form' => tep_draw_form('currencies', FILENAME_CURRENCIES, 'page=' .
+  $HTTP_GET_VARS['page'] . (isset($cInfo) ? '&cID=' . $cInfo->currencies_id : '')) .
+  '&action=insert');
+    $contents[] = array('text' => TEXT_INFO_INSERT_INTRO);
+  + $contents[] = array('text' => '<br>' . tep_draw_pull_down_menu('cs',
+  $currency_select_array, '', 'onchange="updateForm();"'));
+    $contents[] = array('text' => '<br>' . TEXT_INFO_CURRENCY_TITLE . '<br>' .
+  tep_draw_input_field('title'));
+    $contents[] = array('text' => '<br>' . TEXT_INFO_CURRENCY_CODE . '<br>' .
+  tep_draw_input_field('code'));

```

```
$contents[] = array('text' => '<br>' . TEXT_INFO_CURRENCY_SYMBOL_LEFT . '<br>' . tep_draw_input_field('symbol_left'));
```

catalog/admin/includes/languages/english.php

```
@@ -37,7 +37,7 @@ function tep_date_raw($date, $reverse = false) {
    define('HTML_PARAMS','dir="ltr" lang="en"');

    // charset for web pages and emails
    -define('CHARSET', 'iso-8859-1');
    +define('CHARSET', 'utf-8');

    // page title
    define('TITLE', 'osCommerce Online Merchant Administration Tool');
```

catalog/admin/includes/languages/english/currencies.php

```
@@ -18,6 +18,7 @@ define('TABLE_HEADING_CURRENCY_VALUE', 'Value');
    define('TABLE_HEADING_ACTION', 'Action');

    define('TEXT_INFO_EDIT_INTRO', 'Please make any necessary changes');
    +define('TEXT_INFO_COMMON_CURRENCIES', '-- Common Currencies --');
    define('TEXT_INFO_CURRENCY_TITLE', 'Title:');
    define('TEXT_INFO_CURRENCY_CODE', 'Code:');
    define('TEXT_INFO_CURRENCY_SYMBOL_LEFT', 'Symbol Left:');
```

catalog/includes/languages/english.php

```
@@ -42,7 +42,7 @@ define('LANGUAGE_CURRENCY', 'USD');
    define('HTML_PARAMS','dir="LTR" lang="en"');

    // charset for web pages and emails
    -define('CHARSET', 'iso-8859-1');
    +define('CHARSET', 'utf-8');

    // page title
    define('TITLE', STORE_NAME);
```

(A) (SQL) (NEW) Introduce Security Directory Permissions Feature

(A) (SQL) (NEW) Introduce Security Directory Permissions Feature

Introduce new Security Directory Permissions feature to list all directories and show which are writable and which whitelisted directories should be writable.

Affected Files

- catalog/admin/includes/boxes/tools.php
- catalog/admin/includes/database_tables.php
- catalog/admin/includes/filenames.php
- catalog/admin/includes/languages/english.php
- catalog/admin/includes/languages/english/sec_dir_permissions.php --- (new file)
- catalog/admin/sec_dir_permissions.php --- (new file)

[View Changes Online](#)

SQL Queries

```

CREATE TABLE sec_directory_whitelist (
  id int NOT NULL auto_increment,
  directory varchar(255) NOT NULL,
  PRIMARY KEY (id)
);

INSERT INTO sec_directory_whitelist values (null, 'admin/backups');
INSERT INTO sec_directory_whitelist values (null, 'admin/images/graphs');
INSERT INTO sec_directory_whitelist values (null, 'images');
INSERT INTO sec_directory_whitelist values (null, 'images/banners');
INSERT INTO sec_directory_whitelist values (null, 'images/dvd');
INSERT INTO sec_directory_whitelist values (null, 'images/gt_interactive');
INSERT INTO sec_directory_whitelist values (null, 'images/hewlett_packard');
INSERT INTO sec_directory_whitelist values (null, 'images/matrox');
INSERT INTO sec_directory_whitelist values (null, 'images/microsoft');
INSERT INTO sec_directory_whitelist values (null, 'images/sierra');
INSERT INTO sec_directory_whitelist values (null, 'includes/work');
INSERT INTO sec_directory_whitelist values (null, 'pub');

```



This changeset includes updates to English language definition files. Please perform similar changes to other languages that are also installed.

catalog/admin/includes/boxes/tools.php

```

@@ -28,6 +28,7 @@
                                '<a href=" ' . tep_href_link(FILENAME_FILE_MANAGER) . '" class=
"menuBoxContentLink">' . BOX_TOOLS_FILE_MANAGER . '</a><br>' .
                                '<a href=" ' . tep_href_link(FILENAME_MAIL) . '" class=
"menuBoxContentLink">' . BOX_TOOLS_MAIL . '</a><br>' .
                                '<a href=" ' . tep_href_link(FILENAME_NEWSLETTERS) . '" class=
"menuBoxContentLink">' . BOX_TOOLS_NEWSLETTER_MANAGER . '</a><br>' .
+                                '<a href=" ' . tep_href_link(FILENAME_SEC_DIR_PERMISSIONS) . '"
class="menuBoxContentLink">' . BOX_TOOLS_SEC_DIR_PERMISSIONS . '</a><br>' .
                                '<a href=" ' . tep_href_link(FILENAME_SERVER_INFO) . '" class=
"menuBoxContentLink">' . BOX_TOOLS_SERVER_INFO . '</a><br>' .
                                '<a href=" ' . tep_href_link(FILENAME_WHOS_ONLINE) . '" class=
"menuBoxContentLink">' . BOX_TOOLS_WHOS_ONLINE . '</a>';
}

```

catalog/admin/includes/database_tables.php

```

@@ -48,6 +48,7 @@
define('TABLE_PRODUCTS_TO_CATEGORIES', 'products_to_categories');
define('TABLE_REVIEWS', 'reviews');
define('TABLE_REVIEWS_DESCRIPTION', 'reviews_description');
+ define('TABLE_SEC_DIRECTORY_WHITELIST', 'sec_directory_whitelist');
define('TABLE_SESSIONS', 'sessions');
define('TABLE_SPECIALS', 'specials');
define('TABLE_TAX_CLASS', 'tax_class');

```

catalog/admin/includes/filenames.php

```

@@ -40,6 +40,7 @@
define('FILENAME_PRODUCTS_ATTRIBUTES', 'products_attributes.php');
define('FILENAME_PRODUCTS_EXPECTED', 'products_expected.php');
define('FILENAME_REVIEWS', 'reviews.php');
+ define('FILENAME_SEC_DIR_PERMISSIONS', 'sec_dir_permissions.php');
define('FILENAME_SERVER_INFO', 'server_info.php');
define('FILENAME_SHIPPING_MODULES', 'shipping_modules.php');
define('FILENAME_SPECIALS', 'specials.php');

```


catalog/admin/includes/languages/english.php

```


@@ -105,6 +105,7 @@ define('BOX_TOOLS_DEFINE_LANGUAGE', 'Define Languages');
define('BOX_TOOLS_FILE_MANAGER', 'File Manager');
define('BOX_TOOLS_MAIL', 'Send Email');
define('BOX_TOOLS_NEWSLETTER_MANAGER', 'Newsletter Manager');
+define('BOX_TOOLS_SEC_DIR_PERMISSIONS', 'Security Directory Permissions');
define('BOX_TOOLS_SERVER_INFO', 'Server Info');
define('BOX_TOOLS_WHOS_ONLINE', 'Who's Online');

```

catalog/admin/includes/languages/english/sec_dir_permissions.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/sec_dir_permissions.php --- (new file)

 This is a new file. ([Download File](#))

(AC) (SQL) (NEW) Introduce Action Recorder Feature

(AC) (SQL) (NEW) Introduce Action Recorder Feature

Importance: Medium | Difficulty: Hard

Introduce new modular Action Recorder feature to log certain actions. This includes the following action recorder modules:

- Contact Us
- Tell a Friend
- Administration Tool Login

Affected Files

- catalog/admin/action_recorder.php --- (new file)
- catalog/admin/includes/application_top.php
- catalog/admin/includes/boxes/modules.php
- catalog/admin/includes/boxes/tools.php
- catalog/admin/includes/classes/action_recorder.php --- (new file)
- catalog/admin/includes/database_tables.php
- catalog/admin/includes/filenames.php
- catalog/admin/includes/languages/english.php
- catalog/admin/includes/languages/english/action_recorder.php --- (new file)
- catalog/admin/includes/languages/english/login.php
- catalog/admin/includes/languages/english/modules.php
- catalog/admin/includes/languages/english/modules/index/admin_logins.php --- (new file)
- catalog/admin/includes/modules/index/admin_logins.php --- (new file)
- catalog/admin/login.php
- catalog/admin/modules.php
- catalog/contact_us.php
- catalog/includes/application_top.php
- catalog/includes/classes/action_recorder.php --- (new file)
- catalog/includes/database_tables.php
- catalog/includes/languages/english/contact_us.php
- catalog/includes/languages/english/modules/action_recorder/ar_admin_login.php --- (new file)
- catalog/includes/languages/english/modules/action_recorder/ar_contact_us.php --- (new file)
- catalog/includes/languages/english/modules/action_recorder/ar_tell_a_friend.php --- (new file)
- catalog/includes/languages/english/tell_a_friend.php
- catalog/includes/modules/action_recorder/ar_admin_login.php --- (new file)
- catalog/includes/modules/action_recorder/ar_contact_us.php --- (new file)
- catalog/includes/modules/action_recorder/ar_tell_a_friend.php --- (new file)
- catalog/tell_a_friend.php

[View Changes Online](#)

SQL Queries

```

CREATE TABLE action_recorder (
  id int NOT NULL auto_increment,
  module varchar(255) NOT NULL,
  user_id int,
  user_name varchar(255),
  identifier varchar(255) NOT NULL,
  success char(1),
  date_added datetime NOT NULL,
  PRIMARY KEY (id),
  KEY idx_action_recorder_module (module),
  KEY idx_action_recorder_user_id (user_id),
  KEY idx_action_recorder_identifier (identifier),
  KEY idx_action_recorder_date_added (date_added)
);

INSERT INTO configuration (configuration_title, configuration_key, configuration_value,
configuration_description, configuration_group_id, sort_order, date_added) VALUES ('Installed
Modules', 'MODULE_ACTION_RECORDER_INSTALLED',
'ar_admin_login.php;ar_contact_us.php;ar_tell_a_friend.php', 'List of action recorder module
filenames separated by a semi-colon. This is automatically updated. No need to edit.', '6', '0',
now());
INSERT INTO configuration (configuration_title, configuration_key, configuration_value,
configuration_description, configuration_group_id, sort_order, date_added) VALUES ('Minimum
Minutes Per E-Mail', 'MODULE_ACTION_RECORDER_CONTACT_US_EMAIL_MINUTES', '15', 'Minimum number of
minutes to allow 1 e-mail to be sent (eg, 15 for 1 e-mail every 15 minutes)', '6', '0', now());
INSERT INTO configuration (configuration_title, configuration_key, configuration_value,
configuration_description, configuration_group_id, sort_order, date_added) VALUES ('Minimum
Minutes Per E-Mail', 'MODULE_ACTION_RECORDER_TELL_A_FRIEND_EMAIL_MINUTES', '15', 'Minimum number
of minutes to allow 1 e-mail to be sent (eg, 15 for 1 e-mail every 15 minutes)', '6', '0', now());
INSERT INTO configuration (configuration_title, configuration_key, configuration_value,
configuration_description, configuration_group_id, sort_order, date_added) VALUES ('Allowed
Minutes', 'MODULE_ACTION_RECORDER_ADMIN_LOGIN_MINUTES', '5', 'Number of minutes to allow login
attempts to occur.', '6', '0', now());
INSERT INTO configuration (configuration_title, configuration_key, configuration_value,
configuration_description, configuration_group_id, sort_order, date_added) VALUES ('Allowed
Attempts', 'MODULE_ACTION_RECORDER_ADMIN_LOGIN_ATTEMPTS', '3', 'Number of login attempts to allow
within the specified period.', '6', '0', now());

```



This changeset includes updates to English language definition files. Please perform similar changes to other languages that are also installed.

catalog/admin/action_recorder.php --- (new file)



This is a new file. ([Download File](#))

catalog/admin/includes/application_top.php

```

@@ -199,6 +199,9 @@
  // file uploading class
  require(DIR_WS_CLASSES . 'upload.php');

+// action recorder
+ require(DIR_WS_CLASSES . 'action_recorder.php');
+
  // calculate category path
  if (isset($HTTP_GET_VARS['cPath'])) {
    $cPath = $HTTP_GET_VARS['cPath'];
  }

```

catalog/admin/includes/boxes/modules.php


```

@@ -11,6 +11,7 @@
 */

// define the filenames used in the project
+ define('FILENAME_ACTION_RECORDER', 'action_recorder.php');
define('FILENAME_ADMINISTRATORS', 'administrators.php');
define('FILENAME_BACKUP', 'backup.php');
define('FILENAME_BANNER_MANAGER', 'banner_manager.php');

```

catalog/admin/includes/languages/english.php

```

@@ -67,6 +67,7 @@ define('BOX_HEADING_MODULES', 'Modules');
define('BOX_MODULES_PAYMENT', 'Payment');
define('BOX_MODULES_SHIPPING', 'Shipping');
define('BOX_MODULES_ORDER_TOTAL', 'Order Total');
+define('BOX_MODULES_ACTION_RECORDER', 'Action Recorder');

// categories box text in includes/boxes/catalog.php
define('BOX_HEADING_CATALOG', 'Catalog');
@@ -98,6 +99,7 @@ define('BOX_REPORTS_ORDERS_TOTAL', 'Customer Orders-Total');

// tools text in includes/boxes/tools.php
define('BOX_HEADING_TOOLS', 'Tools');
+define('BOX_TOOLS_ACTION_RECORDER', 'Action Recorder');
define('BOX_TOOLS_BACKUP', 'Database Backup');
define('BOX_TOOLS_BANNER_MANAGER', 'Banner Manager');
define('BOX_TOOLS_CACHE', 'Cache Control');
@@ -263,6 +265,7 @@ define('TEXT_DISPLAY_NUMBER_OF_BANNERS', 'Displaying <b>%d</b> to <b>%d</b>
(of
define('TEXT_DISPLAY_NUMBER_OF_COUNTRIES', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
countries)');
define('TEXT_DISPLAY_NUMBER_OF_CUSTOMERS', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
customers)');
define('TEXT_DISPLAY_NUMBER_OF_CURRENCIES', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
currencies)');
+define('TEXT_DISPLAY_NUMBER_OF_ENTRIES', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
entries)');
define('TEXT_DISPLAY_NUMBER_OF_LANGUAGES', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
languages)');
define('TEXT_DISPLAY_NUMBER_OF_MANUFACTURERS', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
manufacturers)');
define('TEXT_DISPLAY_NUMBER_OF_NEWSLETTERS', 'Displaying <b>%d</b> to <b>%d</b> (of <b>%d</b>
newsletters)');

```

catalog/admin/includes/languages/english/action_recorder.php --- (new file)



This is a new file. ([Download File](#))

catalog/admin/includes/languages/english/login.php

```

@@ -21,4 +21,6 @@ define('ERROR_INVALID_ADMINISTRATOR', 'Error: Invalid administrator login attemp

define('BUTTON_LOGIN', 'Login');
define('BUTTON_CREATE_ADMINISTRATOR', 'Create Administrator');
+
+define('ERROR_ACTION_RECORDER', 'Error: The maximum number of login attempts has been reached.
Please try again in %s minutes.');
```

catalog/admin/includes/languages/english/modules.php



```
@@ -13,6 +13,7 @@
define('HEADING_TITLE_MODULES_PAYMENT', 'Payment Modules');
define('HEADING_TITLE_MODULES_SHIPPING', 'Shipping Modules');
define('HEADING_TITLE_MODULES_ORDER_TOTAL', 'Order Total Modules');
+define('HEADING_TITLE_MODULES_ACTION_RECORDER', 'Action Recorder Modules');

define('TABLE_HEADING_MODULES', 'Modules');
define('TABLE_HEADING_SORT_ORDER', 'Sort Order');
```

catalog/admin/includes/languages/english/modules/index/admin_logins.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/includes/modules/index/admin_logins.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/login.php

```

@@ -33,35 +33,46 @@
    $password = tep_db_prepare_input($HTTP_POST_VARS['password']);
}

-    $check_query = tep_db_query("select id, user_name, user_password from " .
TABLE_ADMINISTRATORS . " where user_name = '" . tep_db_input($username) . "'");
+    $actionRecorder = new actionRecorderAdmin('ar_admin_login', null, $username);

-    if (tep_db_num_rows($check_query) == 1) {
-        $check = tep_db_fetch_array($check_query);
+    if ($actionRecorder->canPerform()) {
+        $check_query = tep_db_query("select id, user_name, user_password from " .
TABLE_ADMINISTRATORS . " where user_name = '" . tep_db_input($username) . "'");

-        if (tep_validate_password($password, $check['user_password'])) {
-            tep_session_register('admin');
+        if (tep_db_num_rows($check_query) == 1) {
+            $check = tep_db_fetch_array($check_query);

-            $admin = array('id' => $check['id'],
-                          'username' => $check['user_name']);
+            if (tep_validate_password($password, $check['user_password'])) {
+                tep_session_register('admin');

-            if (tep_session_is_registered('redirect_origin')) {
-                $page = $redirect_origin['page'];
-                $get_string = '';
+                $admin = array('id' => $check['id'],
+                              'username' => $check['user_name']);

-                $admin = array('id' => $check['id'],
-                              'username' => $check['user_name']);

-                if (function_exists('http_build_query')) {
-                    $get_string = http_build_query($redirect_origin['get']);
-                }
+                $actionRecorder->_user_id = $admin['id'];
+                $actionRecorder->record();

+                if (tep_session_is_registered('redirect_origin')) {
+                    $page = $redirect_origin['page'];
+                    $get_string = '';

+                    if (function_exists('http_build_query')) {
+                        $get_string = http_build_query($redirect_origin['get']);
+                    }

-                tep_session_unregister('redirect_origin');
+                tep_session_unregister('redirect_origin');

-                tep_redirect(tep_href_link($page, $get_string));
-            } else {
-                tep_redirect(tep_href_link(FILENAME_DEFAULT));
+                tep_redirect(tep_href_link($page, $get_string));
+            } else {
+                tep_redirect(tep_href_link(FILENAME_DEFAULT));
+            } else {
+                tep_redirect(tep_href_link(FILENAME_DEFAULT));
+            }
+        }
+    }

+    $messageStack->add(ERROR_INVALID_ADMINISTRATOR, 'error');
+    } else {
+        $messageStack->add(sprintf(ERROR_ACTION_RECORDER,
(defined('MODULE_ACTION_RECORDER_ADMIN_LOGIN_MINUTES') ? (int
)MODULE_ACTION_RECORDER_ADMIN_LOGIN_MINUTES : 5)));
+    }

-    $messageStack->add(ERROR_INVALID_ADMINISTRATOR, 'error');
+    $actionRecorder->record(false);

    break;

```

```

@@ -28,6 +28,12 @@
    $module_key = 'MODULE_ORDER_TOTAL_INSTALLED';
    define('HEADING_TITLE', HEADING_TITLE_MODULES_ORDER_TOTAL);
    break;
+   case 'actionrecorder':
+       $module_type = 'action_recorder';
+       $module_directory = DIR_FS_CATALOG_MODULES . 'action_recorder/';
+       $module_key = 'MODULE_ACTION_RECORDER_INSTALLED';
+       define('HEADING_TITLE', HEADING_TITLE_MODULES_ACTION_RECORDER);
+       break;
    case 'payment':
    default:
        $module_type = 'payment';

```

catalog/contact_us.php

```

@@ -14,21 +14,35 @@

require(DIR_WS_LANGUAGES . $language . '/' . FILENAME_CONTACT_US);

- $error = false;
- if (isset($HTTP_GET_VARS['action']) && ($HTTP_GET_VARS['action'] == 'send') &&
isset($HTTP_POST_VARS['formid']) && ($HTTP_POST_VARS['formid'] == $sessiontoken)) {
+ $error = false;
+
    $name = tep_db_prepare_input($HTTP_POST_VARS['name']);
    $email_address = tep_db_prepare_input($HTTP_POST_VARS['email']);
    $enquiry = tep_db_prepare_input($HTTP_POST_VARS['enquiry']);

-   if (tep_validate_email($email_address)) {
-       tep_mail(STORE_OWNER, STORE_OWNER_EMAIL_ADDRESS, EMAIL_SUBJECT, $enquiry, $name,
$email_address);
-
-       tep_redirect(tep_href_link(FILENAME_CONTACT_US, 'action=success'));
-   } else {
+   if (!tep_validate_email($email_address)) {
        $error = true;

        $messageStack->add('contact', ENTRY_EMAIL_ADDRESS_CHECK_ERROR);
    }
+
+   $actionRecorder = new actionRecorder('ar_contact_us',
(tep_session_is_registered('customer_id') ? $customer_id : null), $name);
+   if (!$actionRecorder->canPerform()) {
+       $error = true;
+
+       $actionRecorder->record(false);
+
+       $messageStack->add('contact', sprintf(ERROR_ACTION_RECORDER,
(defined('MODULE_ACTION_RECORDER_CONTACT_US_EMAIL_MINUTES') ? (int
)MODULE_ACTION_RECORDER_CONTACT_US_EMAIL_MINUTES : 15)));
+   }
+
+   if ($error == false) {
        tep_mail(STORE_OWNER, STORE_OWNER_EMAIL_ADDRESS, EMAIL_SUBJECT, $enquiry, $name,
$email_address);
+
+       $actionRecorder->record();
+
+       tep_redirect(tep_href_link(FILENAME_CONTACT_US, 'action=success'));
+   }
}

$breadcrumb->add(NAVBAR_TITLE, tep_href_link(FILENAME_CONTACT_US));

```

catalog/includes/application_top.php


```

@@ -298,6 +298,9 @@
    }
    $navigation->add_current_page();

+// action recorder
+ include('includes/classes/action_recorder.php');
+
+ // Shopping cart actions
+if (isset($_HTTP_GET_VARS['action'])) {
+ // redirect the customer to a friendly cookie-must-be-enabled page if cookies are disabled

```

catalog/includes/classes/action_recorder.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/database_tables.php

```

@@ -11,6 +11,7 @@
 */

// define the database table names used in the project
+ define('TABLE_ACTION_RECORDER', 'action_recorder');
define('TABLE_ADDRESS_BOOK', 'address_book');
define('TABLE_ADDRESS_FORMAT', 'address_format');
define('TABLE_ADMINISTRATORS', 'administrators');


```

catalog/includes/languages/english/contact_us.php


```

@@ -18,4 +18,6 @@ define('EMAIL_SUBJECT', 'Enquiry from ' . STORE_NAME);
define('ENTRY_NAME', 'Full Name:');
define('ENTRY_EMAIL', 'E-Mail Address:');
define('ENTRY_ENQUIRY', 'Enquiry:');
+
+define('ERROR_ACTION_RECORDER', 'Error: An enquiry has already been sent. Please try again in %s
minutes.');
```


catalog/includes/languages/english/modules/action_recorder/ar_admin_login.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/languages/english/modules/action_recorder/ar_contact_us.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/languages/english/modules/action_recorder/ar_tell_a_friend.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/languages/english/tell_a_friend.php

```

@@ -34,4 +34,5 @@ define('ERROR_TO_NAME', 'Error: Your friends name must not be empty.');
```

```

define('ERROR_TO_ADDRESS', 'Error: Your friends e-mail address must be a valid e-mail address.');
```

```

define('ERROR_FROM_NAME', 'Error: Your name must not be empty.');
```

```

define('ERROR_FROM_ADDRESS', 'Error: Your e-mail address must be a valid e-mail address.');
```

```

+define('ERROR_ACTION_RECORDER', 'Error: An e-mail has already been sent. Please try again in %s
```


```

minutes.');
```


```

?>
```


catalog/includes/modules/action_recorder/ar_admin_login.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/modules/action_recorder/ar_contact_us.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/modules/action_recorder/ar_tell_a_friend.php --- (new file)

 This is a new file. ([Download File](#))

catalog/tell_a_friend.php

```

@@ -66,6 +66,15 @@
    $messageStack->add('friend', ERROR_TO_ADDRESS);
}

+    $actionRecorder = new actionRecorder('ar_tell_a_friend',
+ (tep_session_is_registered('customer_id') ? $customer_id : null), $from_name);
+    if (!$actionRecorder->canPerform()) {
+        $error = true;
+
+        $actionRecorder->record(false);
+
+        $messageStack->add('friend', sprintf(ERROR_ACTION_RECORDER,
+ (defined('MODULE_ACTION_RECORDER_TELL_A_FRIEND_EMAIL_MINUTES') ? (int
+ )MODULE_ACTION_RECORDER_TELL_A_FRIEND_EMAIL_MINUTES : 15)));
+    }
+
+    if ($error == false) {
+        $email_subject = sprintf(TEXT_EMAIL_SUBJECT, $from_name, STORE_NAME);
+        $email_body = sprintf(TEXT_EMAIL_INTRO, $to_name, $from_name,
+ $product_info['products_name'], STORE_NAME) . "\n\n";
@@ -79,6 +88,8 @@

        tep_mail($to_name, $to_email_address, $email_subject, $email_body, $from_name,
$from_email_address);

+        $actionRecorder->record();
+
+        $messageStack->add_session('header', sprintf(TEXT_EMAIL_SUCCESSFUL_SENT,
+ $product_info['products_name'], tep_output_string_protected($to_name)), 'success');

        tep_redirect(tep_href_link(FILENAME_PRODUCT_INFO, 'products_id=' . (int
+ )$HTTP_GET_VARS['products_id']));
```

(AC) (UP) Cleanup Language Definitions

(AC) (UP) Cleanup Language Definitions

Importance: Low | Difficulty: Easy

Cleanup language definitions.

Affected Files

- [catalog/admin/customers.php](#)
- [catalog/admin/includes/languages/english.php](#)
- [catalog/includes/languages/english.php](#)

[View Changes Online](#)

catalog/admin/customers.php

```
@@ -482,11 +482,7 @@ function check_form() {
    <td class="main">

    <?php
        if ($error == true) {
-         if ($entry_company_error == true) {
-             echo tep_draw_input_field('entry_company', $cInfo->entry_company, 'maxlength="32"') .
'&nbsp;' . ENTRY_COMPANY_ERROR;
-         } else {
-             echo $cInfo->entry_company . tep_draw_hidden_field('entry_company');
-         }
+         echo $cInfo->entry_company . tep_draw_hidden_field('entry_company');
        } else {
            echo tep_draw_input_field('entry_company', $cInfo->entry_company, 'maxlength="32"');
        }
    @@ -528,11 +524,7 @@ function check_form() {
    <td class="main">

    <?php
        if ($error == true) {
-         if ($entry_suburb_error == true) {
-             echo tep_draw_input_field('suburb', $cInfo->entry_suburb, 'maxlength="32"') . ' &nbsp;' .
ENTRY_SUBURB_ERROR;
-         } else {
-             echo $cInfo->entry_suburb . tep_draw_hidden_field('entry_suburb');
-         }
+         echo $cInfo->entry_suburb . tep_draw_hidden_field('entry_suburb');
        } else {
            echo tep_draw_input_field('entry_suburb', $cInfo->entry_suburb, 'maxlength="32"');
        }
    }
```

catalog/admin/includes/languages/english.php

```

@@ -169,11 +169,9 @@ define('ENTRY_EMAIL_ADDRESS_ERROR', '&nbsp;<span class="errorText">min ' .
ENTRY
    define('ENTRY_EMAIL_ADDRESS_CHECK_ERROR', '&nbsp;<span class="errorText">The email address
doesn\'t appear to be valid!</span>');
    define('ENTRY_EMAIL_ADDRESS_ERROR_EXISTS', '&nbsp;<span class="errorText">This email address
already exists!</span>');
    define('ENTRY_COMPANY', 'Company name:');
-define('ENTRY_COMPANY_ERROR', '');
    define('ENTRY_STREET_ADDRESS', 'Street Address:');
    define('ENTRY_STREET_ADDRESS_ERROR', '&nbsp;<span class="errorText">min ' .
ENTRY_STREET_ADDRESS_MIN_LENGTH . ' chars</span>');
    define('ENTRY_SUBURB', 'Suburb:');
-define('ENTRY_SUBURB_ERROR', '');
    define('ENTRY_POST_CODE', 'Post Code:');
    define('ENTRY_POST_CODE_ERROR', '&nbsp;<span class="errorText">min ' . ENTRY_POSTCODE_MIN_LENGTH
. ' chars</span>');
    define('ENTRY_CITY', 'City:');
@@ -181,15 +179,13 @@ define('ENTRY_CITY_ERROR', '&nbsp;<span class="errorText">min ' .
ENTRY_CITY_MIN
    define('ENTRY_STATE', 'State:');
    define('ENTRY_STATE_ERROR', '&nbsp;<span class="errorText">required</span>');
    define('ENTRY_COUNTRY', 'Country:');
-define('ENTRY_COUNTRY_ERROR', '');
+define('ENTRY_COUNTRY_ERROR', 'You must select a country from the Countries pull down menu.');
```

```

    define('ENTRY_TELEPHONE_NUMBER', 'Telephone Number:');
    define('ENTRY_TELEPHONE_NUMBER_ERROR', '&nbsp;<span class="errorText">min ' .
ENTRY_TELEPHONE_MIN_LENGTH . ' chars</span>');
    define('ENTRY_FAX_NUMBER', 'Fax Number:');
-define('ENTRY_FAX_NUMBER_ERROR', '');
    define('ENTRY_NEWSLETTER', 'Newsletter:');
    define('ENTRY_NEWSLETTER_YES', 'Subscribed');
    define('ENTRY_NEWSLETTER_NO', 'Unsubscribed');
-define('ENTRY_NEWSLETTER_ERROR', '');

// images
define('IMAGE_ANI_SEND_EMAIL', 'Sending E-Mail');
```

catalog/includes/languages/english.php

```

@@ -160,7 +160,6 @@ define('CATEGORY_OPTIONS', 'Options');
define('CATEGORY_PASSWORD', 'Your Password');

define('ENTRY_COMPANY', 'Company Name:');
-define('ENTRY_COMPANY_ERROR', '');
define('ENTRY_COMPANY_TEXT', '');
define('ENTRY_GENDER', 'Gender:');
define('ENTRY_GENDER_ERROR', 'Please select your Gender.');
```

```

@@ -183,7 +182,6 @@ define('ENTRY_STREET_ADDRESS', 'Street Address:');
define('ENTRY_STREET_ADDRESS_ERROR', 'Your Street Address must contain a minimum of ' .
ENTRY_STREET_ADDRESS_MIN_LENGTH . ' characters.');
```

```

define('ENTRY_STREET_ADDRESS_TEXT', '*');
define('ENTRY_SUBURB', 'Suburb:');
-define('ENTRY_SUBURB_ERROR', '');
define('ENTRY_SUBURB_TEXT', '');
define('ENTRY_POST_CODE', 'Post Code:');
define('ENTRY_POST_CODE_ERROR', 'Your Post Code must contain a minimum of ' .
ENTRY_POSTCODE_MIN_LENGTH . ' characters.');
```

```

@@ -202,13 +200,11 @@ define('ENTRY_TELEPHONE_NUMBER', 'Telephone Number:');
define('ENTRY_TELEPHONE_NUMBER_ERROR', 'Your Telephone Number must contain a minimum of ' .
ENTRY_TELEPHONE_MIN_LENGTH . ' characters.');
```

```

define('ENTRY_TELEPHONE_NUMBER_TEXT', '*');
define('ENTRY_FAX_NUMBER', 'Fax Number:');
-define('ENTRY_FAX_NUMBER_ERROR', '');
define('ENTRY_FAX_NUMBER_TEXT', '');
define('ENTRY_NEWSLETTER', 'Newsletter:');
define('ENTRY_NEWSLETTER_TEXT', '');
define('ENTRY_NEWSLETTER_YES', 'Subscribed');
define('ENTRY_NEWSLETTER_NO', 'Unsubscribed');
```

```

-define('ENTRY_NEWSLETTER_ERROR', '');
define('ENTRY_PASSWORD', 'Password:');
define('ENTRY_PASSWORD_ERROR', 'Your Password must contain a minimum of ' .
ENTRY_PASSWORD_MIN_LENGTH . ' characters.');
```

```

define('ENTRY_PASSWORD_ERROR_NOT_MATCHING', 'The Password Confirmation must match your
Password.');
```

(AC) (NEW) Move Installation Checks to New Security Checks Modules

(AC) (NEW) Move Installation Checks to New Security Checks Modules

Importance: Medium | Difficulty: Easy

Move installation checks to new Security Checks modules. Installation messages shown on the Catalog side have been moved to the Administration Tool Index Summary page.

Affected Files

- catalog/admin/images/ms_error.png --- (new file)
- catalog/admin/images/ms_error_bg.png --- (new file)
- catalog/admin/images/ms_info.png --- (new file)
- catalog/admin/images/ms_info_bg.png --- (new file)
- catalog/admin/images/ms_success.png --- (new file)
- catalog/admin/images/ms_success_bg.png --- (new file)
- catalog/admin/images/ms_warning.png --- (new file)
- catalog/admin/images/ms_warning_bg.png --- (new file)
- catalog/admin/includes/application_top.php
- catalog/admin/includes/configure.php
- catalog/admin/includes/languages/english.php
- catalog/admin/includes/languages/english/modules/index/security_checks.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/config_file_catalog.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/default_currency.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/default_language.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/download_directory.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/file_uploads.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/install_directory.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/session_auto_start.php --- (new file)
- catalog/admin/includes/languages/english/modules/security_check/session_storage.php --- (new file)
- catalog/admin/includes/modules/index/security_checks.php --- (new file)

- catalog/admin/includes/modules/security_check/config_file_catalog.php --- (new file)
- catalog/admin/includes/modules/security_check/default_currency.php --- (new file)
- catalog/admin/includes/modules/security_check/default_language.php --- (new file)
- catalog/admin/includes/modules/security_check/download_directory.php --- (new file)
- catalog/admin/includes/modules/security_check/file_uploads.php --- (new file)
- catalog/admin/includes/modules/security_check/install_directory.php --- (new file)
- catalog/admin/includes/modules/security_check/session_auto_start.php --- (new file)
- catalog/admin/includes/modules/security_check/session_storage.php --- (new file)
- catalog/includes/application_top.php
- catalog/includes/header.php
- catalog/includes/languages/english.php

[View Changes Online](#)



This changeset includes updates to English language definition files. Please perform similar changes to other languages that are also installed.

catalog/admin/images/ms_error.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_error_bg.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_info.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_info_bg.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_success.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_success_bg.png --- (new file)



This is a new file. ([Download File](#))

catalog/admin/images/ms_warning.png --- (new file)



This is a new file. ([Download File](#))


catalog/admin/images/ms_warning_bg.png --- (new file)




This is a new file. ([Download File](#))

catalog/admin/includes/application_top.php


catalog/admin/includes/languages/english/modules/security_check/default_currency.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/default_language.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/download_directory.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/file_uploads.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/install_directory.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/session_auto_start.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/languages/english/modules/security_check/session_storage.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/index/security_checks.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/config_file_catalog.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/default_currency.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/default_language.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/download_directory.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/file_uploads.php --- (new file)

 This is a new file. ([Download File](#))


catalog/admin/includes/modules/security_check/install_directory.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/includes/modules/security_check/session_auto_start.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/includes/modules/security_check/session_storage.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/application_top.php

```
@@ -475,11 +475,4 @@
// initialize the message stack for output messages
require(DIR_WS_CLASSES . 'message_stack.php');
$messageStack = new messageStack;
-
-// set which precautions should be checked
- define('WARN_INSTALL_EXISTENCE', 'true');
- define('WARN_CONFIG_WRITEABLE', 'true');
- define('WARN_SESSION_DIRECTORY_NOT_WRITEABLE', 'true');
- define('WARN_SESSION_AUTO_START', 'true');
- define('WARN_DOWNLOAD_DIRECTORY_NOT_READABLE', 'true');
?>
```

catalog/includes/header.php

```

@@ -10,44 +10,6 @@
Released under the GNU General Public License
*/

-// check if the 'install' directory exists, and warn of its existence
- if (WARN_INSTALL_EXISTENCE == 'true') {
-     if (file_exists(dirname($HTTP_SERVER_VARS['SCRIPT_FILENAME']) . '/install')) {
-         $messageStack->add('header', WARNING_INSTALL_DIRECTORY_EXISTS, 'warning');
-     }
- }
-
-// check if the configure.php file is writeable
- if (WARN_CONFIG_WRITEABLE == 'true') {
-     if ( (file_exists(dirname($HTTP_SERVER_VARS['SCRIPT_FILENAME']) . '/includes/configure.php'))
-     && (is_writeable(dirname($HTTP_SERVER_VARS['SCRIPT_FILENAME']) . '/includes/configure.php')) ) {
-         $messageStack->add('header', WARNING_CONFIG_FILE_WRITEABLE, 'warning');
-     }
- }
-
-// check if the session folder is writeable
- if (WARN_SESSION_DIRECTORY_NOT_WRITEABLE == 'true') {
-     if (STORE_SESSIONS == '') {
-         if (!is_dir(tep_session_save_path())) {
-             $messageStack->add('header', WARNING_SESSION_DIRECTORY_NON_EXISTENT, 'warning');
-         } elseif (!is_writeable(tep_session_save_path())) {
-             $messageStack->add('header', WARNING_SESSION_DIRECTORY_NOT_WRITEABLE, 'warning');
-         }
-     }
- }
-
-// check session.auto_start is disabled
- if ( (function_exists('ini_get')) && (WARN_SESSION_AUTO_START == 'true') ) {
-     if (ini_get('session.auto_start') == '1') {
-         $messageStack->add('header', WARNING_SESSION_AUTO_START, 'warning');
-     }
- }
-
- if ( (WARN_DOWNLOAD_DIRECTORY_NOT_READABLE == 'true') && (DOWNLOAD_ENABLED == 'true') ) {
-     if (!is_dir(DIR_FS_DOWNLOAD)) {
-         $messageStack->add('header', WARNING_DOWNLOAD_DIRECTORY_NON_EXISTENT, 'warning');
-     }
- }
-
- if ($messageStack->size('header') > 0) {
-     echo $messageStack->output('header');
- }

```

catalog/includes/languages/english.php

```

@@ -299,12 +299,6 @@ define('TEXT_UNKNOWN_TAX_RATE', 'Unknown tax rate');
define('TEXT_REQUIRED', '<span class="errorText">Required</span>');

define('ERROR_TEP_MAIL', '<font face="Verdana, Arial" size="2" color="#ff0000"><b><small>TEP
ERROR:</small> Cannot send the email through the specified SMTP server. Please check your php.ini
setting and correct the SMTP server if necessary.</b></font>');
-define('WARNING_INSTALL_DIRECTORY_EXISTS', 'Warning: Installation directory exists at: ' .
dirname($HTTP_SERVER_VARS['SCRIPT_FILENAME']) . '/install. Please remove this directory for
security reasons.');
```

```

-define('WARNING_CONFIG_FILE_WRITEABLE', 'Warning: I am able to write to the configuration file: '
. dirname($HTTP_SERVER_VARS['SCRIPT_FILENAME']) . '/includes/configure.php. This is a potential
security risk - please set the right user permissions on this file.');
```

```

-define('WARNING_SESSION_DIRECTORY_NON_EXISTENT', 'Warning: The sessions directory does not exist:
' . tep_session_save_path() . '. Sessions will not work until this directory is created.');
```

```

-define('WARNING_SESSION_DIRECTORY_NOT_WRITEABLE', 'Warning: I am not able to write to the
sessions directory: ' . tep_session_save_path() . '. Sessions will not work until the right user
permissions are set.');
```

```

-define('WARNING_SESSION_AUTO_START', 'Warning: session.auto_start is enabled - please disable
this php feature in php.ini and restart the web server.');
```

```

-define('WARNING_DOWNLOAD_DIRECTORY_NON_EXISTENT', 'Warning: The downloadable products directory
does not exist: ' . DIR_FS_DOWNLOAD . '. Downloadable products will not work until this directory
is valid.');
```

```

define('TEXT_CCVAL_ERROR_INVALID_DATE', 'The expiry date entered for the credit card is invalid.
Please check the date and try again.');
```

```

define('TEXT_CCVAL_ERROR_INVALID_NUMBER', 'The credit card number entered is invalid. Please
check the number and try again.');
```

(A) (UP) Introduce Windows Compatible is_writable() Function

(A) (UP) Introduce Windows Compatible is_writable() Function

Importance: Low | Difficulty: Easy

Introduce a Windows platform compatible is_writable function.

Affected Files

- catalog/admin/administrators.php
- catalog/admin/backup.php
- catalog/admin/banner_manager.php
- catalog/admin/banner_statistics.php
- catalog/admin/cache.php
- catalog/admin/categories.php
- catalog/admin/define_language.php
- catalog/admin/includes/classes/upload.php
- catalog/admin/includes/functions/general.php
- catalog/admin/includes/modules/security_check/config_file_catalog.php
- catalog/admin/includes/modules/security_check/session_storage.php
- catalog/admin/sec_dir_permissions.php

[View Changes Online](#)

catalog/admin/administrators.php

```

@@ -22,7 +22,7 @@
                                'Require valid-user',
                                '##### OSCOMMERCE ADMIN PROTECTION - END #####');

-   if (file_exists(DIR_FS_ADMIN . '.htpasswd_oscommerce') && is_writable(DIR_FS_ADMIN .
'.htpasswd_oscommerce') && file_exists(DIR_FS_ADMIN . '.htaccess') && is_writable(DIR_FS_ADMIN .
'.htaccess')) {
+   if (file_exists(DIR_FS_ADMIN . '.htpasswd_oscommerce') && tep_is_writable(DIR_FS_ADMIN .
'.htpasswd_oscommerce') && file_exists(DIR_FS_ADMIN . '.htaccess') && tep_is_writable(DIR_FS_ADMIN
. '.htaccess')) {
        $htaccess_array = array();
        $htpasswd_array = array();

```

catalog/admin/backup.php

```

@@ -317,7 +317,7 @@
    // check if the backup directory exists
    $dir_ok = false;
    if (is_dir(DIR_FS_BACKUP)) {
-       if (is_writeable(DIR_FS_BACKUP)) {
+       if (tep_is_writable(DIR_FS_BACKUP)) {
            $dir_ok = true;
        } else {
            $messageStack->add(ERROR_BACKUP_DIRECTORY_NOT_WRITEABLE, 'error');

```

catalog/admin/banner_manager.php

```

@@ -125,7 +125,7 @@
    $banner = tep_db_fetch_array($banner_query);

    if (is_file(DIR_FS_CATALOG_IMAGES . $banner['banners_image'])) {
-       if (is_writeable(DIR_FS_CATALOG_IMAGES . $banner['banners_image'])) {
+       if (tep_is_writable(DIR_FS_CATALOG_IMAGES . $banner['banners_image'])) {
            unlink(DIR_FS_CATALOG_IMAGES . $banner['banners_image']);
        } else {
            $messageStack->add_session(ERROR_IMAGE_IS_NOT_WRITEABLE, 'error');
@@ -140,25 +140,25 @@

    if (function_exists('imagecreate') && tep_not_null($banner_extensio)) {
        if (is_file(DIR_WS_IMAGES . 'graphs/banner_infobox-' . $banners_id . '.' .
$banner_extension)) {
-           if (is_writeable(DIR_WS_IMAGES . 'graphs/banner_infobox-' . $banners_id . '.' .
$banner_extension)) {
+           if (tep_is_writable(DIR_WS_IMAGES . 'graphs/banner_infobox-' . $banners_id . '.' .
$banner_extension)) {
                unlink(DIR_WS_IMAGES . 'graphs/banner_infobox-' . $banners_id . '.' .
$banner_extension);
            }
        }

        if (is_file(DIR_WS_IMAGES . 'graphs/banner_yearly-' . $banners_id . '.' .
$banner_extension)) {
-           if (is_writeable(DIR_WS_IMAGES . 'graphs/banner_yearly-' . $banners_id . '.' .
$banner_extension)) {
+           if (tep_is_writable(DIR_WS_IMAGES . 'graphs/banner_yearly-' . $banners_id . '.' .
$banner_extension)) {
                unlink(DIR_WS_IMAGES . 'graphs/banner_yearly-' . $banners_id . '.' .
$banner_extension);
            }
        }

        if (is_file(DIR_WS_IMAGES . 'graphs/banner_monthly-' . $banners_id . '.' .
$banner_extension)) {
-           if (is_writeable(DIR_WS_IMAGES . 'graphs/banner_monthly-' . $banners_id . '.' .
$banner_extension)) {
+           if (tep_is_writable(DIR_WS_IMAGES . 'graphs/banner_monthly-' . $banners_id . '.' .
$banner_extension)) {
                unlink(DIR_WS_IMAGES . 'graphs/banner_monthly-' . $banners_id . '.' .
$banner_extension);
            }
        }

        if (is_file(DIR_WS_IMAGES . 'graphs/banner_daily-' . $banners_id . '.' .
$banner_extension)) {
-           if (is_writeable(DIR_WS_IMAGES . 'graphs/banner_daily-' . $banners_id . '.' .
$banner_extension)) {
+           if (tep_is_writable(DIR_WS_IMAGES . 'graphs/banner_daily-' . $banners_id . '.' .
$banner_extension)) {
                unlink(DIR_WS_IMAGES . 'graphs/banner_daily-' . $banners_id . '.' .
$banner_extension);
            }
        }
@@ -175,7 +175,7 @@
    $dir_ok = false;
    if (function_exists('imagecreate') && tep_not_null($banner_extension)) {
        if (is_dir(DIR_WS_IMAGES . 'graphs')) {
-           if (is_writeable(DIR_WS_IMAGES . 'graphs')) {
+           if (tep_is_writable(DIR_WS_IMAGES . 'graphs')) {
                $dir_ok = true;
            } else {
                $messageStack->add(ERROR_GRAPHFS_DIRECTORY_NOT_WRITEABLE, 'error');

```



```

@@ -20,7 +20,7 @@
$dir_ok = false;
if (function_exists('imagecreate') && tep_not_null($banner_extension)) {
    if (is_dir(DIR_WS_IMAGES . 'graphs')) {
-       if (is_writeable(DIR_WS_IMAGES . 'graphs')) {
+       if (tep_is_writable(DIR_WS_IMAGES . 'graphs')) {
            $dir_ok = true;
        } else {
            $messageStack->add(ERROR_GRAPHS_DIRECTORY_NOT_WRITEABLE, 'error');

```

catalog/admin/cache.php

```

@@ -24,7 +24,7 @@

// check if the cache directory exists
if (is_dir(DIR_FS_CACHE)) {
-   if (!is_writeable(DIR_FS_CACHE)) $messageStack->add(ERROR_CACHE_DIRECTORY_NOT_WRITEABLE,
'error');
+   if (!tep_is_writable(DIR_FS_CACHE)) $messageStack->add(ERROR_CACHE_DIRECTORY_NOT_WRITEABLE,
'error');
    } else {
        $messageStack->add(ERROR_CACHE_DIRECTORY_DOES_NOT_EXIST, 'error');
    }

```

catalog/admin/categories.php

```

@@ -327,7 +327,7 @@

// check if the catalog image directory exists
if (is_dir(DIR_FS_CATALOG_IMAGES)) {
-   if (!is_writeable(DIR_FS_CATALOG_IMAGES))
$messageStack->add(ERROR_CATALOG_IMAGE_DIRECTORY_NOT_WRITEABLE, 'error');
+   if (!tep_is_writable(DIR_FS_CATALOG_IMAGES))
$messageStack->add(ERROR_CATALOG_IMAGE_DIRECTORY_NOT_WRITEABLE, 'error');
    } else {
        $messageStack->add(ERROR_CATALOG_IMAGE_DIRECTORY_DOES_NOT_EXIST, 'error');
    }

```

catalog/admin/define_language.php

```

@@ -24,7 +24,7 @@
    if (!in_array($filename, $exclude_array)) {
        $file = array('name' => $path . $filename,
-           'is_dir' => is_dir($path . $filename),
+           'writable' => is_writable($path . $filename),
+           'writable' => tep_is_writable($path . $filename),
            'size' => filesize($path . $filename),
            'last_modified' => strftime(DATE_TIME_FORMAT, filemtime($path .
$filename)));

@@ -72,7 +72,7 @@
    if (isset($HTTP_GET_VARS['lngdir']) && isset($HTTP_GET_VARS['filename'])) {
        $file = DIR_FS_CATALOG_LANGUAGES . $HTTP_GET_VARS['filename'];

-       if (file_exists($file) && is_writable($file)) {
+       if (file_exists($file) && tep_is_writable($file)) {
            $new_file = fopen($file, 'w');
            $file_contents = stripslashes($HTTP_POST_VARS['file_contents']);
            fwrite($new_file, $file_contents, strlen($file_contents));

@@ -128,7 +128,7 @@
        $contents = implode('', $file_array);

        $file_writable = true;
-       if (!is_writable($file)) {
+       if (!tep_is_writable($file)) {
            $file_writable = false;
            $messageStack->reset();
            $messageStack->add(sprintf(ERROR_FILE_NOT_WRITEABLE, $file), 'error');

@@ -185,7 +185,7 @@
        </tr>
        <tr class="dataTableRow" onmouseover="rowOverEffect(this)" onmouseout=
"rowOutEffect(this)">
            <td class="dataTableContent"><a href="<?php echo
tep_href_link(FILENAME_DEFINE_LANGUAGE, 'lngdir=' . $HTTP_GET_VARS['lngdir'] . '&filename=' .
$filename); ?>"><b><?php echo $filename; ?></b></a></td>
-            <td class="dataTableContent" align="center"><?php echo tep_image(DIR_WS_IMAGES .
'icons/' . ((is_writable(DIR_FS_CATALOG_LANGUAGES . $filename) == true) ? 'tick.gif' :
'cross.gif')); ?></td>
+            <td class="dataTableContent" align="center"><?php echo tep_image(DIR_WS_IMAGES .
'icons/' . ((tep_is_writable(DIR_FS_CATALOG_LANGUAGES . $filename) == true) ? 'tick.gif' :
'cross.gif')); ?></td>
            <td class="dataTableContent" align="right"><?php echo strftime(DATE_TIME_FORMAT,
filemtime(DIR_FS_CATALOG_LANGUAGES . $filename)); ?></td>
        </tr>
    </php

```

catalog/admin/includes/classes/upload.php

```

@@ -139,7 +139,7 @@
    function check_destination() {
        global $messageStack;

-       if (!is_writable($this->destination)) {
+       if (!tep_is_writable($this->destination)) {
            if (is_dir($this->destination)) {
                if ($this->message_location == 'direct') {
                    $messageStack->add(sprintf(ERROR_DESTINATION_NOT_WRITEABLE, $this->destination),
'error');

```

catalog/admin/includes/functions/general.php

```

@@ -1010,7 +1010,7 @@
    $dir = dir($source);
    while ($file = $dir->read()) {
        if ( ($file != '.') && ($file != '..') ) {
-         if (is_writeable($source . '/' . $file)) {
+         if (tep_is_writable($source . '/' . $file)) {
            tep_remove($source . '/' . $file);
        } else {
            $messageStack->add(sprintf(ERROR_FILE_NOT_REMOVEABLE, $source . '/' . $file),
'error');
@@ -1020,14 +1020,14 @@
    }
    $dir->close();

-    if (is_writeable($source)) {
+    if (tep_is_writable($source)) {
        rmdir($source);
    } else {
        $messageStack->add(sprintf(ERROR_DIRECTORY_NOT_REMOVEABLE, $source), 'error');
        $step_remove_error = true;
    }
-    if (is_writeable($source)) {
+    if (tep_is_writable($source)) {
        unlink($source);
    } else {
        $messageStack->add(sprintf(ERROR_FILE_NOT_REMOVEABLE, $source), 'error');
@@ -1356,4 +1356,35 @@
    return $ip_address;
}

+
+/////
+// Wrapper function for is_writable() for Windows compatibility
+function tep_is_writable($file) {
+    if (strtolower(substr(PHP_OS, 0, 3)) === 'win') {
+        if (file_exists($file)) {
+            $file = realpath($file);
+            if (is_dir($file)) {
+                $result = @tempnam($file, 'osc');
+                if (is_string($result) && file_exists($result)) {
+                    unlink($result);
+                    return (strpos($result, $file) === 0) ? true : false;
+                }
+            } else {
+                $handle = @fopen($file, 'r+');
+                if (is_resource($handle)) {
+                    fclose($handle);
+                    return true;
+                }
+            }
+        } else {
+            $dir = dirname($file);
+            if (file_exists($dir) && is_dir($dir) && tep_is_writable($dir)) {
+                return true;
+            }
+        }
+        return false;
+    } else {
+        return is_writable($file);
+    }
+}
+
?>

```

```

@@ -20,7 +20,7 @@
    }

    function pass() {
-       return (file_exists(DIR_FS_CATALOG . 'includes/configure.php') &&
!is_writable(DIR_FS_CATALOG . 'includes/configure.php'));
+       return (file_exists(DIR_FS_CATALOG . 'includes/configure.php') &&
!tep_is_writable(DIR_FS_CATALOG . 'includes/configure.php'));
    }

    function getMessage() {

```

catalog/admin/includes/modules/security_check/session_storage.php

```

@@ -20,14 +20,14 @@
    }

    function pass() {
-       return ((STORE_SESSIONS != '') || (is_dir(tep_session_save_path()) &&
is_writable(tep_session_save_path())));
+       return ((STORE_SESSIONS != '') || (is_dir(tep_session_save_path()) &&
tep_is_writable(tep_session_save_path())));
    }

    function getMessage() {
        if (STORE_SESSIONS == '') {
            if (!is_dir(tep_session_save_path())) {
                return WARNING_SESSION_DIRECTORY_NON_EXISTENT;
-            } elseif (!is_writable(tep_session_save_path())) {
+            } elseif (!tep_is_writable(tep_session_save_path())) {
                return WARNING_SESSION_DIRECTORY_NOT_WRITEABLE;
            }
        }
    }

```

catalog/admin/sec_dir_permissions.php

```

@@ -24,7 +24,7 @@
    if (!in_array($filename, $exclude_array)) {
        $file = array('name' => $path . $filename,
-            'is_dir' => is_dir($path . $filename),
+            'writable' => is_writable($path . $filename));
+            'writable' => tep_is_writable($path . $filename));

        $result[] = $file;
    }

```

(A) (UP) Bypass HTTP Authentication for IIS Webservers

(A) (UP) Bypass HTTP Authentication for IIS Webservers

Importance: Low | Difficulty: Easy

Bypass Administration Tool HTTP Authentication for IIS Webservers.

Affected Files

- [catalog/admin/administrators.php](#)

[View Changes Online](#)

catalog/admin/administrators.php

```

@@ -14,6 +14,7 @@

    $htaccess_array = null;
    $htpasswd_array = null;
+   $is_iis = strpos($_SERVER_VARS['SERVER_SOFTWARE'], 'iis');

    $authuserfile_array = array('##### OSCOMMERCE ADMIN PROTECTION - BEGIN #####',
                                'AuthType Basic',

@@ -22,7 +23,7 @@

                                'Require valid-user',
                                '##### OSCOMMERCE ADMIN PROTECTION - END #####');

-   if (file_exists(DIR_FS_ADMIN . '.htpasswd_oscommerce') && tep_is_writable(DIR_FS_ADMIN .
'.htpasswd_oscommerce') && file_exists(DIR_FS_ADMIN . '.htaccess') && tep_is_writable(DIR_FS_ADMIN
'.htaccess')) {
+   if (!$is_iis && file_exists(DIR_FS_ADMIN . '.htpasswd_oscommerce') &&
tep_is_writable(DIR_FS_ADMIN . '.htpasswd_oscommerce') && file_exists(DIR_FS_ADMIN . '.htaccess')
&& tep_is_writable(DIR_FS_ADMIN . '.htaccess')) {
        $htaccess_array = array();
        $htpasswd_array = array();

@@ -225,7 +226,7 @@
    } else {
        $secMessageStack->add(HTPASSWD_SECURED, 'success');
    }
-   } else {
+   } else if (!$is_iis) {
        $secMessageStack->add(HTPASSWD_PERMISSIONS, 'error');
    }
?>
@@ -283,8 +284,13 @@
    $aInfo = new objectInfo($admins);
}

+
    $htpasswd_secured = tep_image(DIR_WS_IMAGES . 'icon_status_red.gif', 'Not Secured', 10, 10);

+   if ($is_iis) {
+       $htpasswd_secured = 'N/A';
+   }
+
    if (is_array($htpasswd_array)) {
        for ($i=0, $n=sizeof($htpasswd_array); $i<$n; $i++) {
            list($ht_username, $ht_password) = explode(':', $htpasswd_array[$i], 2);

```

(AC) (UP) Update PHP_SELF Value

(AC) (UP) Update PHP_SELF Value

Importance: Low | Difficulty: Easy

Update PHP_SELF value.

Affected Files

- [catalog/admin/includes/application_top.php](#)
- [catalog/includes/application_top.php](#)

[View Changes Online](#)

catalog/admin/includes/application_top.php

```

@@ -34,7 +34,7 @@
    require(DIR_WS_FUNCTIONS . 'compatibility.php');

    // set php_self in the local scope
-   $PHP_SELF = (isset($HTTP_SERVER_VARS['PHP_SELF']) ? $HTTP_SERVER_VARS['PHP_SELF'] :
$HTTP_SERVER_VARS['SCRIPT_NAME']);
+   $PHP_SELF = (((strlen(ini_get('cgi.fix_pathinfo')) > 0) && ((bool)ini_get('cgi.fix_pathinfo')
== false)) || !isset($HTTP_SERVER_VARS['SCRIPT_NAME'])) ? basename($HTTP_SERVER_VARS['PHP_SELF'])
: basename($HTTP_SERVER_VARS['SCRIPT_NAME']);

    // Used in the "Backup Manager" to compress backups
define('LOCAL_EXE_GZIP', '/usr/bin/gzip');

```

catalog/includes/application_top.php

```

@@ -43,7 +43,7 @@
    $request_type = (getenv('HTTPS') == 'on') ? 'SSL' : 'NONSSL';

    // set php_self in the local scope
-   if (!isset($PHP_SELF)) $PHP_SELF = $HTTP_SERVER_VARS['PHP_SELF'];
+   $PHP_SELF = (((strlen(ini_get('cgi.fix_pathinfo')) > 0) && ((bool)ini_get('cgi.fix_pathinfo')
== false)) || !isset($HTTP_SERVER_VARS['SCRIPT_NAME'])) ? basename($HTTP_SERVER_VARS['PHP_SELF'])
: basename($HTTP_SERVER_VARS['SCRIPT_NAME']);

    if ($request_type == 'NONSSL') {
        define('DIR_WS_CATALOG', DIR_WS_HTTP_CATALOG);
    }

```

(A) (NEW) Introduce Easy Store Logo Uploader

(A) (NEW) Introduce Easy Store Logo Uploader

Importance: Low | Difficulty: Easy

Introduce a new Administration Tool section to easily allow a new store logo to be uploaded.

Affected Files

- catalog/admin/includes/boxes/configuration.php
- catalog/admin/includes/filenames.php
- catalog/admin/includes/languages/english.php
- catalog/admin/includes/languages/english/store_logo.php --- (new file)
- catalog/admin/store_logo.php --- (new file)

[View Changes Online](#)



This changeset includes updates to English language definition files. Please perform similar changes to other languages that are also installed.

catalog/admin/includes/boxes/configuration.php

```

@@ -21,7 +21,8 @@
                                'link' => tep_href_link(FILENAME_CONFIGURATION,
'gID=1&selected_box=configuration'));

    if ($selected_box == 'configuration') {
-        $cfg_groups = '<a href="' . tep_href_link(FILENAME_ADMINISTRATORS, '', 'NONSSL') . '" class=
"menuBoxContentLink">' . BOX_CONFIGURATION_ADMINISTRATORS . '</a><br>';
+        $cfg_groups = '<a href="' . tep_href_link(FILENAME_ADMINISTRATORS, '', 'NONSSL') . '" class=
"menuBoxContentLink">' . BOX_CONFIGURATION_ADMINISTRATORS . '</a><br>' .
+        '<a href="' . tep_href_link(FILENAME_STORE_LOGO, '', 'NONSSL') . '" class=
"menuBoxContentLink">' . BOX_CONFIGURATION_STORE_LOGO . '</a><br>';
        $configuration_groups_query = tep_db_query("select configuration_group_id as cgID,
configuration_group_title as cgTitle from " . TABLE_CONFIGURATION_GROUP . " where visible = '1'
order by sort_order");
        while ($configuration_groups = tep_db_fetch_array($configuration_groups_query)) {
            $cfg_groups .= '<a href="' . tep_href_link(FILENAME_CONFIGURATION, 'gID=' .
$configuration_groups['cgID'], 'NONSSL') . '" class="menuBoxContentLink">' .
$configuration_groups['cgTitle'] . '</a><br>';

```

catalog/admin/includes/filenames.php

```

@@ -48,6 +48,7 @@
define('FILENAME_STATS_CUSTOMERS', 'stats_customers.php');
define('FILENAME_STATS_PRODUCTS_PURCHASED', 'stats_products_purchased.php');
define('FILENAME_STATS_PRODUCTS_VIEWED', 'stats_products_viewed.php');
+ define('FILENAME_STORE_LOGO', 'store_logo.php');
define('FILENAME_TAX_CLASSES', 'tax_classes.php');
define('FILENAME_TAX_RATES', 'tax_rates.php');
define('FILENAME_VERSION_CHECK', 'version_check.php');

```

catalog/admin/includes/languages/english.php


```

@@ -61,6 +61,7 @@ define('BOX_CONFIGURATION_MYSTORE', 'My Store');
define('BOX_CONFIGURATION_LOGGING', 'Logging');
define('BOX_CONFIGURATION_CACHE', 'Cache');
define('BOX_CONFIGURATION_ADMINISTRATORS', 'Administrators');
+define('BOX_CONFIGURATION_STORE_LOGO', 'Store Logo');


// modules box text in includes/boxes/modules.php
define('BOX_HEADING_MODULES', 'Modules');

```

catalog/admin/includes/languages/english/store_logo.php --- (new file)

 This is a new file. ([Download File](#))

catalog/admin/store_logo.php --- (new file)

 This is a new file. ([Download File](#))

(AC) (SQL) (UP) Update Password Hashing to Phpass

(AC) (SQL) (UP) Update Password Hashing to Phpass

Importance: High | Difficulty: Easy

Update password hashing to Phpass for increased security. Existing customer and administrator passwords are automatically and transparently hashed with Phpass when the customer or administrator logs in.

Affected Files

- catalog/admin/includes/classes/passwordhash.php --- (new file)
- catalog/admin/includes/functions/password_funcs.php
- catalog/admin/login.php
- catalog/includes/classes/passwordhash.php --- (new file)
- catalog/includes/functions/password_funcs.php
- catalog/login.php

[View Changes Online](#)

SQL Queries

```
alter table administrators modify user_password varchar(60) NOT NULL;
alter table customers modify customers_password varchar(60) NOT NULL;
```

catalog/admin/includes/classes/passwordhash.php --- (new file)



This is a new file. ([Download File](#))

catalog/admin/includes/functions/password_funcs.php

```
@@ -11,10 +11,31 @@
 */

    ///
    -// This function validates a plain text password with an
    -// encrypted password
    +// This function validates a plain text password with a
    +// salted or phpass password
    function tep_validate_password($plain, $encrypted) {
        if (tep_not_null($plain) && tep_not_null($encrypted)) {
            +   if (tep_password_type($encrypted) == 'salt') {
            +       return tep_validate_old_password($plain, $encrypted);
            +   }
            +   if (!class_exists('PasswordHash')) {
            +       include(DIR_WS_CLASSES . 'passwordhash.php');
            +   }
            +   $hasher = new PasswordHash(10, true);
            +   return $hasher->CheckPassword($plain, $encrypted);
            +   }
            +   return false;
            +   }
            +   }
            +   }

    +// This function validates a plain text password with a
    +// salted password
    + function tep_validate_old_password($plain, $encrypted) {
    +     if (tep_not_null($plain) && tep_not_null($encrypted)) {
    +         // split apart the hash / salt
    +         $stack = explode(':', $encrypted);

    @@ -29,8 +50,22 @@
    }

    ///
    -// This function makes a new password from a plaintext password.
    +// This function encrypts a phpass password from a plaintext
    +// password.
    function tep_encrypt_password($plain) {
        +   if (!class_exists('PasswordHash')) {
        +       include(DIR_WS_CLASSES . 'passwordhash.php');
        +   }
        +   $hasher = new PasswordHash(10, true);
```



```

+
+     return $hasher->HashPassword($plain);
+ }
+
+////
+// This function encrypts a salted password from a plaintext
+// password.
+ function tep_encrypt_old_password($plain) {
+     $password = '';
+
+     for ($i=0; $i<10; $i++) {
+@@ -45,6 +80,17 @@
+     }
+
+     ///
+// This function returns the type of the encrypted password
+// (phpass or salt)
+ function tep_password_type($encrypted) {
+     if (preg_match('/^[A-Z0-9]{32}\:[A-Z0-9]{2}$/i', $encrypted) === 1) {
+         return 'salt';
+     }
+
+     return 'phpass';
+ }
+
+////
+// This function produces a crypted string using the APR-MD5 algorithm

```

```
// Source: http://www.php.net/crypt
function tep_crypt_apr_md5($password, $salt = null) {
```


catalog/admin/login.php

```
@@ -42,6 +42,11 @@
    $check = tep_db_fetch_array($check_query);

    if (tep_validate_password($password, $check['user_password'])) {
+// migrate old hashed password to new phpass password
+    if (tep_password_type($check['user_password']) != 'phpass') {
+        tep_db_query("update " . TABLE_ADMINISTRATORS . " set user_password = '" .
tep_encrypt_password($password) . "' where id = '" . (int)$check['id'] . "'");
+    }
+
    tep_session_register('admin');

    $admin = array('id' => $check['id'],
```

catalog/includes/classes/passwordhash.php --- (new file)

 This is a new file. ([Download File](#))

catalog/includes/functions/password_funcs.php

```
@@ -11,10 +11,31 @@
*/

////
-// This function validates a plain text password with an
-// encrypted password
+// This function validates a plain text password with a
+// salted or phpass password
function tep_validate_password($plain, $encrypted) {
    if (tep_not_null($plain) && tep_not_null($encrypted)) {
+    if (tep_password_type($encrypted) == 'salt') {
+        return tep_validate_old_password($plain, $encrypted);
+    }
+
    if (!class_exists('PasswordHash')) {
        include(DIR_WS_CLASSES . 'passwordhash.php');
    }

    $hasher = new PasswordHash(10, true);

    return $hasher->CheckPassword($plain, $encrypted);
+ }
+
+ return false;
+ }

+////
+// This function validates a plain text password with a
+// salted password
+ function tep_validate_old_password($plain, $encrypted) {
+     if (tep_not_null($plain) && tep_not_null($encrypted)) {
+         // split apart the hash / salt
+         $stack = explode(':', $encrypted);

@@ -29,8 +50,22 @@
    }

    ////
-// This function makes a new password from a plaintext password.
+// This function encrypts a phpass password from a plaintext
+// password.
```

```

function tep_encrypt_password($plain) {
+   if (!class_exists('PasswordHash')) {
+       include(DIR_WS_CLASSES . 'passwordhash.php');
+   }
+
+   $hasher = new PasswordHash(10, true);
+
+   return $hasher->HashPassword($plain);
+ }
+
+////
+// This function encrypts a salted password from a plaintext
+// password.
+ function tep_encrypt_old_password($plain) {
+     $password = '';

+     for ($i=0; $i<10; $i++) {
@@ -43,4 +78,15 @@

+         return $password;
+     }
+ }
+
+////
+// This function returns the type of the encrypted password
+// (phpass or salt)
+ function tep_password_type($encrypted) {
+     if (preg_match('/^[A-Z0-9]{32}\:[A-Z0-9]{2}$/', $encrypted) === 1) {
+         return 'salt';
+     }
+
+     return 'phpass';

```

```
+ }  
+?>
```

catalog/login.php

```
@@ -38,6 +38,11 @@  
    tep_session_recreate();  
}  
  
+// migrate old hashed password to new phpass password  
+    if (tep_password_type($check_customer['customers_password']) != 'phpass') {  
+        tep_db_query("update " . TABLE_CUSTOMERS . " set customers_password = '" .  
tep_encrypt_password($password) . "' where customers_id = '" . (int)  
)$check_customer['customers_id'] . "'");  
+    }  
+  
    $check_country_query = tep_db_query("select entry_country_id, entry_zone_id from " .  
TABLE_ADDRESS_BOOK . " where customers_id = '" . (int)$check_customer['customers_id'] . "' and  
address_book_id = '" . (int)$check_customer['customers_default_address_id'] . "'");  
    $check_country = tep_db_fetch_array($check_country_query);
```

(C) (BUG) Fix Length Check of Customer Passwords

(C) (BUG) Fix Length Check of Customer Passwords

Importance: Low | Difficulty: Easy

Fix the length check of customer passwords.

Affected Files

- [catalog/account_password.php](#)
- [catalog/includes/form_check.js.php](#)

[View Changes Online](#)

catalog/account_password.php

```
@@ -27,11 +27,7 @@  
  
    $error = false;  
  
-    if (strlen($password_current) < ENTRY_PASSWORD_MIN_LENGTH) {  
-        $error = true;  
-  
-        $messageStack->add('account_password', ENTRY_PASSWORD_CURRENT_ERROR);  
-    } elseif (strlen($password_new) < ENTRY_PASSWORD_MIN_LENGTH) {  
+    if (strlen($password_new) < ENTRY_PASSWORD_MIN_LENGTH) {  
        $error = true;  
  
        $messageStack->add('account_password', ENTRY_PASSWORD_NEW_ERROR);
```

catalog/includes/form_check.js.php

```

@@ -73,25 +73,6 @@ function check_password(field_name_1, field_name_2, field_size, message_1,
messa
    }
}

-function check_password_new(field_name_1, field_name_2, field_name_3, field_size, message_1,
message_2, message_3) {
-   if (form.elements[field_name_1] && (form.elements[field_name_1].type != "hidden")) {
-       var password_current = form.elements[field_name_1].value;
-       var password_new = form.elements[field_name_2].value;
-       var password_confirmation = form.elements[field_name_3].value;
-
-       if (password_current.length < field_size) {
-           error_message = error_message + "* " + message_1 + "\n";
-           error = true;
-       } else if (password_new.length < field_size) {
-           error_message = error_message + "* " + message_2 + "\n";
-           error = true;
-       } else if (password_new != password_confirmation) {
-           error_message = error_message + "* " + message_3 + "\n";
-           error = true;
-       }
-   }
-}
-
function check_form(form_name) {
    if (submitted == true) {
        alert("<?php echo JS_ERROR_SUBMITTED; ?>");
@@ -121,7 +102,7 @@ function check_form(form_name) {
    check_input("telephone", "<?php echo ENTRY_TELEPHONE_MIN_LENGTH; ?>", "<?php echo
ENTRY_TELEPHONE_NUMBER_ERROR; ?>");

    check_password("password", "confirmation", "<?php echo ENTRY_PASSWORD_MIN_LENGTH; ?>", "<?php
echo ENTRY_PASSWORD_ERROR; ?>", "<?php echo ENTRY_PASSWORD_ERROR_NOT_MATCHING; ?>");
-   check_password_new("password_current", "password_new", "password_confirmation", "<?php echo
ENTRY_PASSWORD_MIN_LENGTH; ?>", "<?php echo ENTRY_PASSWORD_ERROR; ?>", "<?php echo
ENTRY_PASSWORD_NEW_ERROR; ?>", "<?php echo ENTRY_PASSWORD_NEW_ERROR_NOT_MATCHING; ?>");
+   check_password("password_new", "password_confirmation", "<?php echo ENTRY_PASSWORD_MIN_LENGTH;
?>", "<?php echo ENTRY_PASSWORD_NEW_ERROR; ?>", "<?php echo ENTRY_PASSWORD_NEW_ERROR_NOT_MATCHING;
?>");

    if (error == true) {
        alert(error_message);
    }
}

```

(C) (BUG) Fix Notice When Products Without Attributes are Added to the Shopping Cart

(C) (BUG) Fix Notice When Products Without Attributes are Added to the Shopping Cart

Importance: Low | Difficulty: Easy

Fix a PHP notice when products without attributes are added to the shopping cart.

Affected Files

- [catalog/includes/application_top.php](#)

[View Changes Online](#)

catalog/includes/application_top.php

```

@@ -333,7 +333,8 @@
                                break;
        // customer adds a product from the products page
    case 'add_product' :    if (isset($HTTP_POST_VARS['products_id']) &&
is_numeric($HTTP_POST_VARS['products_id'])) {
    -
                                $cart->add_cart($HTTP_POST_VARS['products_id'],
$cart->get_quantity(tep_get_uprid($HTTP_POST_VARS['products_id'], $HTTP_POST_VARS['id']))+1,
$HTTP_POST_VARS['id']);
    +
                                $attributes = isset($HTTP_POST_VARS['id']) ?
$HTTP_POST_VARS['id'] : '';
    +
                                $cart->add_cart($HTTP_POST_VARS['products_id'],
$cart->get_quantity(tep_get_uprid($HTTP_POST_VARS['products_id'], $attributes))+1, $attributes);
                                }
                                tep_redirect(tep_href_link($goto,
tep_get_all_get_params($parameters)));
                                break;

```

(C) (BUG) Verify Languages Currency Exists

(C) (BUG) Verify LANGUAGE_CURRENCY Exists

Importance: Low | Difficulty: Easy

Verify that the languages currency exists.

Affected Files

- [catalog/includes/application_top.php](#)

[View Changes Online](#)

catalog/includes/application_top.php

```

@@ -287,7 +287,7 @@
    if (isset($HTTP_GET_VARS['currency']) && $currencies->is_set($HTTP_GET_VARS['currency'])) {
        $currency = $HTTP_GET_VARS['currency'];
    } else {
    -
        $currency = (USE_DEFAULT_LANGUAGE_CURRENCY == 'true') ? LANGUAGE_CURRENCY :
DEFAULT_CURRENCY;
    +
        $currency = ((USE_DEFAULT_LANGUAGE_CURRENCY == 'true') &&
$currencies->is_set(LANGUAGE_CURRENCY)) ? LANGUAGE_CURRENCY : DEFAULT_CURRENCY;
    }
}

```

(C) (BUG) Allow Quoted Words to be Searched

(C) (BUG) Allow Quoted Words to be Searched

Importance: Low | Difficulty: Easy

Allow quoted keywords to be searched.

Affected Files

- [catalog/advanced_search_result.php](#)
- [catalog/includes/functions/general.php](#)

[View Changes Online](#)

catalog/advanced_search_result.php

```

@@ -48,7 +48,7 @@
    }

    if (isset($HTTP_GET_VARS['keywords'])) {
-       $keywords = $HTTP_GET_VARS['keywords'];
+       $keywords = tep_db_prepare_input($HTTP_GET_VARS['keywords']);
    }

    $date_check_error = false;
@@ -300,7 +300,7 @@
    $where_str .= " group by p.products_id, tr.tax_priority";
    }

-   if ( (!isset($HTTP_GET_VARS['sort'])) || (!preg_match('/[1-8][ad]/i', $HTTP_GET_VARS['sort']))
|| (substr($HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
+   if ( (!isset($HTTP_GET_VARS['sort'])) || (!preg_match('/^[1-8][ad]$/', $HTTP_GET_VARS['sort']))
|| (substr($HTTP_GET_VARS['sort'], 0, 1) > sizeof($column_list)) ) {
       for ($i=0, $n=sizeof($column_list); $i<$n; $i++) {
           if ($column_list[$i] == 'PRODUCT_LIST_NAME') {
               $HTTP_GET_VARS['sort'] = $i+1 . 'a';

```

catalog/includes/functions/general.php

```

@@ -654,7 +654,7 @@
    // Turn the flag off for future iterations
    $flag = 'off';

-       $objects[] = trim($pieces[$k]);
+       $objects[] = trim(preg_replace('/"/', ' ', $pieces[$k]));

    for ($j=0; $j<count($post_objects); $j++) {
        $objects[] = $post_objects[$j];

```