osCommerce Online Merchant v2.3.3.1

osCommerce Online Merchant v2.3.3.1 is a security and general maintenance release focusing on improving core features.

This release is in preparation of v2.3.4 containing additional improvements.

This document can be found online at:

http://library.oscommerce.com/Online&en&oscom_2_3&release_notes&v2_3_3_1

Code Changes

The following changes have been applied:

Title	Description	Bug	Severity
Who's Online (1 file)	Parse REQUEST_URI with tep_db_prepare_input() before storing the value in the database. Replace REMOTE_ADDR with tep_get_ip_address().		High
Administration Tool -> Catalog -> Categories/Products (1 file)	Fix product price gross tax calculations when adding or editing products.	519	Low
Session (3 files)	Register a shutdown function to close and write the session data. Also check for and allow , (comma) and - (minus) characters in the session ID.		Low
tep_redirect() (1 file)	When redirecting from HTTPS -> HTTP and replacing the url with a HTTPS version, also take DIR_WS_HTTPS_CATALOG into consideration which may differ from DIR_WS_HTTP_CATALOG.	492	Low
Version Update (1 file)	Update version to v2.3.3.1.		

Upgrading from v2.3.3

Modified Files

Files that have been modified in this release include:

Modified Files
admin/includes/functions/general.php
admin/includes/functions/sessions.php
includes/functions/general.php
includes/functions/sessions.php
includes/functions/whos_online.php
includes/version.php

File Changes

Who's Online (1 file)

includes/functions/whos_online.php

around line 29, change:

```
$wo_ip_address = getenv('REMOTE_ADDR');
$wo_last_page_url = getenv('REQUEST_URI');
```

to:

```
$wo_ip_address = tep_get_ip_address();
$wo_last_page_url = tep_db_prepare_input(getenv('REQUEST_URI'));
```

View online at GitHub

Administration Tool -> Catalog -> Categories/Products (1 file)

admin/includes/functions/general.php

change tep_get_tax_rate_value() from:

```
function tep_get_tax_rate_value($class_id) {
  $tax_query = tep_db_query("select SUM(tax_rate) as tax_rate from " . TABLE_TAX_RATES . " where tax_cl
ass_id = '" . (int)$class_id . "' group by tax_priority");
  if (tep_db_num_rows($tax_query)) {
    $tax_multiplier = 0;
    while ($tax = tep_db_fetch_array($tax_query)) {
      $tax_multiplier += $tax['tax_rate'];
    }
    return $tax_multiplier;
  } else {
    return 0;
  }
}
```

to:

```
function tep_get_tax_rate_value($class_id) {
  return tep_get_tax_rate($class_id, -1, -1);
}
```

View online at GitHub

Session (3 files)

admin/includes/functions/sessions.php

change tep_session_start() from:

```
function tep_session_start() {
  global $HTTP_GET_VARS, $HTTP_POST_VARS, $HTTP_COOKIE_VARS;

  $sane_session_id = true;

  if (isset($HTTP_GET_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_GET_VARS[tep_session_name()]) == false) {
      unset($HTTP_GET_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_POST_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_POST_VARS[tep_session_name()]) == false) {
      unset($HTTP_POST_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_COOKIE_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_COOKIE_VARS[tep_session_name()]) == false) {
      $session_data = session_get_cookie_params();

      setcookie(tep_session_name(), '', time()-42000, $session_data['path'], $session_data['domain']);

      $sane_session_id = false;
    }
  }

  if ($sane_session_id == false) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  return session_start();
}
```

to:

```
function tep_session_start() {
  global $HTTP_GET_VARS, $HTTP_POST_VARS, $HTTP_COOKIE_VARS;

  $sane_session_id = true;

  if (isset($HTTP_GET_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_GET_VARS[tep_session_name()]) == false) {
      unset($HTTP_GET_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_POST_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_POST_VARS[tep_session_name()]) == false) {
      unset($HTTP_POST_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_COOKIE_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_COOKIE_VARS[tep_session_name()]) == false) {
      $session_data = session_get_cookie_params();

      setcookie(tep_session_name(), '', time()-42000, $session_data['path'], $session_data['domain']);

      $sane_session_id = false;
    }
  }

  if ($sane_session_id == false) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  register_shutdown_function('session_write_close');

  return session_start();
}
```

includes/functions/general.php

change tep_exit() from:

```
////
// Stop from parsing any further PHP code
  function tep_exit() {
    tep_session_close();
    exit();
  }
```

to:

```
////
// Stop from parsing any further PHP code
// v2.3.3.1 now closes the session through a registered shutdown function
  function tep_exit() {
    exit();
  }
```

includes/functions/sessions.php

change tep_session_start() from:

```
function tep_session_start() {
  global $HTTP_GET_VARS, $HTTP_POST_VARS, $HTTP_COOKIE_VARS;

  $sane_session_id = true;

  if (isset($HTTP_GET_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_GET_VARS[tep_session_name()]) == false) {
      unset($HTTP_GET_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_POST_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_POST_VARS[tep_session_name()]) == false) {
      unset($HTTP_POST_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_COOKIE_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9]+$/', $HTTP_COOKIE_VARS[tep_session_name()]) == false) {
      $session_data = session_get_cookie_params();

      setcookie(tep_session_name(), '', time()-42000, $session_data['path'], $session_data['domain']);

      $sane_session_id = false;
    }
  }

  if ($sane_session_id == false) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  return session_start();
}
```

to:

```
function tep_session_start() {
  global $HTTP_GET_VARS, $HTTP_POST_VARS, $HTTP_COOKIE_VARS;

  $sane_session_id = true;

  if (isset($HTTP_GET_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_GET_VARS[tep_session_name()]) == false) {
      unset($HTTP_GET_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_POST_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_POST_VARS[tep_session_name()]) == false) {
      unset($HTTP_POST_VARS[tep_session_name()]);

      $sane_session_id = false;
    }
  } elseif (isset($HTTP_COOKIE_VARS[tep_session_name()])) {
    if (preg_match('/^[a-zA-Z0-9,-]+$/', $HTTP_COOKIE_VARS[tep_session_name()]) == false) {
      $session_data = session_get_cookie_params();

      setcookie(tep_session_name(), '', time()-42000, $session_data['path'], $session_data['domain']);

      $sane_session_id = false;
    }
  }

  if ($sane_session_id == false) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  register_shutdown_function('session_write_close');

  return session_start();
}
```

View online at GitHub

tep_redirect() (1 file)

includes/functions/general.php

change tep_redirect() from:

```
function tep_redirect($url) {
  if ( (strstr($url, "\n") != false) || (strstr($url, "\r") != false) ) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  if ( (ENABLE_SSL == true) && (getenv('HTTPS') == 'on') ) { // We are loading an SSL page
    if (substr($url, 0, strlen(HTTP_SERVER)) == HTTP_SERVER) { // NONSSL url
      $url = HTTPS_SERVER . substr($url, strlen(HTTP_SERVER)); // Change it to SSL
    }
  }

  if ( strpos($url, '&amp;') !== false ) {
    $url = str_replace('&amp;', '&', $url);
  }

  header('Location: ' . $url);

  tep_exit();
}
```

to:

```
function tep_redirect($url) {
  if ( (strstr($url, "\n") != false) || (strstr($url, "\r") != false) ) {
    tep_redirect(tep_href_link(FILENAME_DEFAULT, '', 'NONSSL', false));
  }

  if ( (ENABLE_SSL == true) && (getenv('HTTPS') == 'on') ) { // We are loading an SSL page
    if (substr($url, 0, strlen(HTTP_SERVER . DIR_WS_HTTP_CATALOG)) == HTTP_SERVER . DIR_WS_HTTP_CATALOG
) { // NONSSL url
      $url = HTTPS_SERVER . DIR_WS_HTTPS_CATALOG . substr($url, strlen(HTTP_SERVER . DIR_WS_HTTP_CATALO
G)); // Change it to SSL
    }
  }

  if ( strpos($url, '&amp;') !== false ) {
    $url = str_replace('&amp;', '&', $url);
  }

  header('Location: ' . $url);

  tep_exit();
}
```

View online at GitHub

Version Update (1 file)

includes/version.php

change line 1 from:

```
2.3.3
```

to:

```
2.3.3.1
```

Thank You!

We'd like to thank the community for their feedback on our releases. In addition, we thank the following people who participated in the development of this release.

Bug Reporters
VanAlles
jerico

Reference

A full list of source code changes can be seen at:

https://github.com/osCommerce/oscommerce2/compare/v2.3.3...upgrade2331

Acknowledgements

We'd like to thank Chris Wood for bringing a security issue to our attention.