



Magento Security and Vulnerabilities



eltrino Roman Stepanov



<http://ice.eltrino.com/>

Table of contents



- Introduction
- Open Web Application Security Project
- OWASP TOP 10 List
- Common issues in Magento
 - A1 – Injection
 - A3 – Cross-Site Scripting (XSS)
 - A8 – Cross-Site Request Forgery (CSRF)
 - A5 – Security Misconfiguration
 - 3rd party integrations
- QA

The Open Web Application Security Project



<https://www.owasp.org/>

- The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. It's mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
- Everyone is free to participate in OWASP and all of our materials are available under a free and open software license

OWASP TOP 10 List 2013



<https://www.owasp.org/>

The Open Web Application Security Project

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Components with Known Vulnerabilities

A10 – Unvalidated Redirects and Forwards

A1 – Injection



Injection flaws, such as SQL, OS injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

A1 – Injection



Welcome, Eltrino Eltrino! [Send Invitations](#) | [Log Out](#)

MY ACCOUNT | MY WISHLIST | **MY CART (1)** | CHECKOUT

test

Shopping Cart

Test was added to your shopping cart.

PRODUCT NAME	MOVE TO WISHLIST	UNIT PRICE	QTY	SUBTOTAL	REMOVE
Test	Edit <input type="checkbox"/>	\$100.00	<input type="text" value="1"/>	\$100.00	<input type="button" value="X"/>

[Continue Shopping](#) [UPDATE SHOPPING CART](#)

Discount Codes
Enter your coupon code if you have one.
 [APPLY COUPON](#)

Gift Cards
Enter the gift card code
 [ADD GIFT CARD](#)
[Check Gift Card status and balance](#)

Estimate Shipping and Tax
Enter your destination to get a shipping estimate.

Country:

State/Province:

Zip/Postal Code:

This is a required field.

[GET A QUOTE](#)

Subtotal \$100.00

Grand Total \$100.00

[Proceed to Checkout](#)

[Checkout with Multiple Addresses](#)

SIGN UP FOR OUR NEWSLETTER
Sign up for our newsletter:
 [SUBSCRIBE](#)

[Site Map](#) | [Search Terms](#) | [Advanced Search](#) | [Contact Us](#)
[About Us](#) | [Customer Service](#)

© 2009 Magento Enterprise Edition Demo Store. All Rights Reserved.

10)); CREATE TABLE a (id INT); - 100

Name

- a
- admin_assert
- admin_role
- admin_rule
- admin_user
- adminnotification_inbox
- api_assert
- api_role



Black Box

- Check every customer using vulnerable patterns:
 - ‘ (single quote)
 - “ (double quote)
 - ` (back quote)
 - ; (semicolon)
- Enable system and exception logging
- Enable advanced sql logging
- Do not forget! Different logic for different kinds of provided data

White Box

- Code review
 - Search patterns
- Dedicated “A-Team”
 - Information and education inside company
 - Code review of new functionality
- Communication

A1 – Injection: How to...



```
105
106  /**
107     * Safely quotes a value for an SQL statement.
108     *
109     * If an array is passed as the value, the array values are quoted
110     * and then returned as a comma-separated string.
111     *
112     * @param mixed $value The value to quote.
113     * @param mixed $type OPTIONAL the SQL datatype name, or constant, or null.
114     *                               Zend_Db::INT_TYPE, Zend_Db::BIGINT_TYPE or Zend_Db::FLOAT_TYPE
115     * @return mixed An SQL-safe quoted value (or string of separated values).
116     */
117     Zend_Db_Adapter_Abstract::quote($value, $type = null);
118
119
```

A1 – Injection: How to...



```
105
106  /**
107     * Quotes a value and places into a piece of text at a placeholder.
108     *
109     * The placeholder is a question-mark; all placeholders will be replaced
110     * with the quoted value.
111     *
112     * @param string $text The text with a placeholder.
113     * @param mixed $value The value to quote.
114     * @param string $type OPTIONAL SQL datatype
115     * @param integer $count OPTIONAL count of placeholders to replace
116     * @return string An SQL-safe quoted value placed into the original text.
117     */
118  Zend_Db_Adapter_Abstract::quoteInto($text, $value, $type = null, $count = null);
119
```

A1 – Injection: How to...

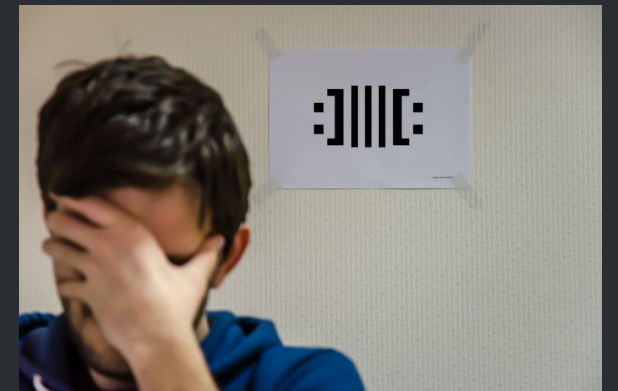


```
94
95
96     Zend_Db_Select::where($condition, $value = null, $type = null);
97     Zend_Db_Select::orWhere($condition, $value = null, $type = null);
98     Zend_Db_Select::having($condition, $value = null, $type = null);
99     Zend_Db_Select::orHaving($condition, $value = null, $type = null);
100
101
102     Varien_Db_Adapter_Interface::prepareSqlCondition($fieldName, $condition);
103     Varien_Data_Collection_Db::addFieldToFilter($field, $condition = null);
104     Mage_Eav_Model_Entity_Collection_Abstract::addAttributeToFilter($attribute,
105         $condition = null, $joinType = 'inner');
106     Mage_Eav_Model_Entity_Collection_Abstract::addFieldToFilter($attribute,
107         $condition = null);
108
```

A1 – Injection: How to...



```
x 416     $someValue_a = 'params1';
x 417     $someValue_b = 'params2';
x 418     $select = $this->getSelect();
x 419     $adapter = $select->getAdapter();
x 420
x 421     /* Good */
x 422     $condition = $adapter->quoteInto('table.field = ?', $someValue_a);
x 423
x 424     /* Bad */
x 425     $condition = 'table.field = ' . $someValue_a;
426     $condition = $adapter->quoteInto('table.field_a = ? && table.field_b = ' . $someValue_a, $someValue_b);
427
```

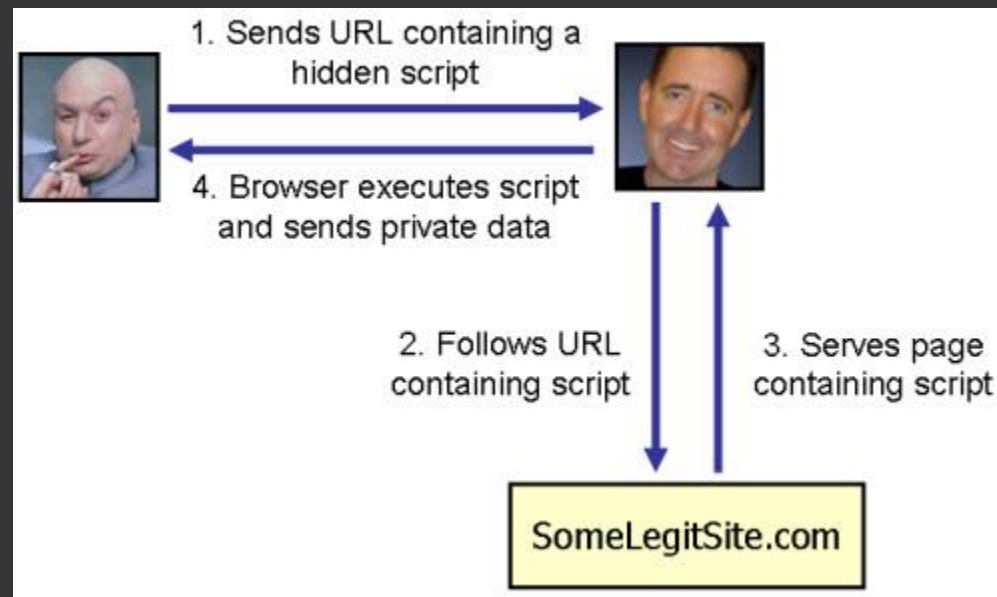


Remember about type hinting!

A3 – Cross-Site Scripting (XSS)



XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.



A3 – Cross-Site Scripting (XSS)



Magento

Forgot your user name or password?

Email Address:

[« Back to Login](#) [Retrieve Password](#)

Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.

Magento

Forgot your user name or password?

Email Address:

[« Back to Login](#) [Retrieve Password](#)

Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.

Magento

Forgot your user name or password?

Cannot find the email address.

Email Address:

[« Back to Login](#) [Retrieve Password](#)

Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.

A3 – Cross-Site Scripting (XSS)



System

- My Account
- Notifications
- Tools
- Content Staging
- Web Services
- Design
- Import/Export
- Manage Currency Rates
- Transactional Emails
- Custom Variables
- Permissions
- Admin Actions Log
- Manage Encryption
- Magento Connections
- Cache Management
- Index Management
- Manage Stores
- Order Statuses
- Configuration

Report

Archive

Global Record Search

Customers Promotions Newsletter CMS Reports **System**

Cache, Blocks HTML output. Click here to go to [Cache Management](#) and refresh cache types.

[Lead details](#)

Attributes, Catalog URL Rewrites, Product Flat Data, Category Flat Data, Category Products, Catalog Search Index, Stock Status, Tag Aggregate

Total 4 records found

Export to: CSV

Action	Result	Full Action Name
1		
login	Success	adminhtml_ind
forgotpassword	Failure	adminhtml_ind

Подтвердите действие на eltrino.lan

OK

- If it is possible, sanitize data on input;
- Always escape special characters on output in templates;
- Use WhiteBox testing. All variables used in input forms should be analyzed;
- Remember, that stored XSS does not need a malicious link to be exploited. A successful exploitation occurs when a user visits a page with a stored XSS.
- Quotation (' , ") or other ways to escape characters isn't enough because of
`<script>alert(String.fromCharCode(88,83,83))</script>`

A3 – Cross-Site Scripting (XSS): How to...



```
418
x 419  /**
x 420     * Escape html entities
x 421     */
422 Mage_Core_Helper_Abstract::escapeHtml($data, $allowedTags = null);
x 423 Mage_Core_Block_Abstract::escapeHtml($data, $allowedTags = null);
x 424
x 425  /**
x 426     * Wrapper for standard strip_tags() function with extra functionality for html entities
x 427     */
428 Mage_Core_Helper_Abstract::stripTags($data, $allowableTags = null, $allowHtmlEntities = false);
x 429 Mage_Core_Block_Abstract::stripTags($data, $allowableTags = null, $allowHtmlEntities = false);
x 430
x 431
x 432
x 433  /**
x 434     * Filter for removing malicious code from HTML
x 435     */
436 Mage_Core_Model_Input_Filter_MaliciousCode::filter($value);
437
```

A8 – Cross-Site Request Forgery (CSRF)



A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A8 – Cross-Site Request Forgery (CSRF)

A screenshot of the 'Forgot your user name or password?' form on a Magento website. The form has a title 'Forgot your user name or password?' and a label 'Email Address:' above an empty text input field. Below the input field are two buttons: 'Back to Login' and 'Retrieve Password'. At the bottom of the form, it says 'Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.'A screenshot of the 'Forgot your user name or password?' form on a Magento website. The form has a title 'Forgot your user name or password?' and a label 'Email Address:' above a text input field containing the JavaScript payload '<script>alert(1);</script>'. Below the input field are two buttons: 'Back to Login' and 'Retrieve Password'. At the bottom of the form, it says 'Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.'

document.location.href="http://eltrino.lan/index.php/admin/system_account/save/?username=hack&firstname=admin&lastname=admin&email=admin@admin.com&new_password=hack&password_confirmation=hack"

A screenshot of the 'Forgot your user name or password?' form on a Magento website. The form has a title 'Forgot your user name or password?' and a label 'Email Address:' above an empty text input field. Above the input field, there is a red error message box with a white exclamation mark icon and the text 'Cannot find the email address.'. Below the input field are two buttons: 'Back to Login' and 'Retrieve Password'. At the bottom of the form, it says 'Magento is a trademark of Magento Inc. Copyright © 2013 Magento Inc.'

A8 – Cross-Site Request Forgery (CSRF)



A screenshot of the Magento Enterprise System menu. The menu is a vertical list of items, with 'System' at the top. The items listed are: My Account, Notifications, Tools, Content Staging, Web Services, Design, Import/Export, Manage Currency Rates, Transactional Emails, Custom Variables, Permissions, Admin Actions Log, Manage Encryption, Magento Connections, Cache Management, Index Management, Manage Stores, Order Statuses, and Configuration. A sub-menu is open for 'Admin Actions Log', showing 'Report' and 'Archive' options.

A screenshot of the Magento Enterprise 'My Account' page. The browser address bar shows 'eltrino.lan/index.php/admin/system_account/'. The page header includes the Magento Enterprise logo, a search bar, and the user 'hack' logged in on Wednesday, March 13, 2013. The navigation menu includes Dashboard, Sales, Catalog, Mobile, Customers, Promotions, Newsletter, CMS, Reports, and System. A notification banner at the top contains three messages: 'One or more of the Cache Types are invalidated', 'Latest Message: Imagine 2013 Registration is Now Open!', and 'One or more of the Indexes are not up to date'. A green success message states 'The account has been saved.' Below this, the 'My Account' section has 'Reset' and 'Save Account' buttons. The 'Account Information' section contains a form with the following fields: User Name (hack), First Name (admin), Last Name (admin), Email (admin@admin.com), New Password, and Password Confirmation.

A8 – Cross-Site Request Forgery (CSRF)



- Verify that secure hash is used for URLs
- Verify that HTML forms have form_key attribute, and form cannot be submitted with incorrect form_key

A8 – Cross-Site Request Forgery (CSRF)



```
118  /**
119     * Retrieve Session Form Key
120     *
121     * @return string A 16 bit unique key for forms
122     */
123  Mage_Core_Model_Session::getFormKey();
124
125  /**
126     * Adds form_key field to form
127     */
128  Varien_Data_Form::toHtml();
129
130  /**
131     * Validates for secret key if request was submitted via Post
132     */
133  Mage_Core_Controller_Varien_Action::preDispatch();
134
135  /**
136     * Generate secret key for controller and action based on form key
137     */
138  Mage_Adminhtml_Model_Url::getSecretKey($controller = null, $action = null);
139
140  /**
141     * Adds secure key to URL if needed
142     */
143  Mage_Adminhtml_Model_Url::getUrl($routeProvider=null, $routeParams=null);
```

A5 – Security Misconfiguration



Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many systems are shipped with defaults that are not secure enough. This also means keeping all software up to date on a regular basis.

A5 – Security Misconfiguration



```
eltrino.lan/RELEASE_NOTE x
eltrino.lan/RELEASE_NOTES.txt

==== 1.10.0.0 ====

=== Major Highlights ===
Gift Wrapping functionality
Added Payflow Link using HSS (Hosted Sole Solution)
Balance Response, Partial Authorization Transactions, Authorization Reversals Support for MasterCard and Discover with Authorize.net
3D Secure Authentication for Authorize.net payment method
Authorize.Net SIM payment method
Improved Import/Export functionality
Ability to order composite products from backend including:
- reconfigure already added products on front end
- adding preconfigured products in wish-list
Alternative media storage options
- Database
- CDN
Order status management
- ability to add new status and assign to some state
Database now stored in DB table instead of configuration file
```


- Consider the threats you plan to protect this data from (e.g., insider attack, external user), make sure you encrypt all sensitive data at rest and in transit in a manner that defends against these threats.
- Don't store sensitive data unnecessarily. Discard it as soon as possible. Data you don't have can't be stolen.
- Ensure strong standard algorithms and strong keys are used, and proper key management is in place.
- Disable autocomplete on forms collecting sensitive data and disable caching for pages displaying sensitive data.

3rd party integrations



Most of eCommerce solutions required integration with 3rd part systems like

- Payment methods
- Shipping methods
- ERP systems

In result of incorrect implementation

- Sensitive information about your client or his customers could be exposed to attacker.
- Attacker can change workflow in system for his own needs (order status, payments etc)

How to prevent it?

- If 3rd party system allows usage of some secret keys/words/hashes/.../etc always perform validation of these parameters for each request
- Don't place export files with sensitive information into folders accessible through the web
- Don't use encryption/decryption of data using Magento Secret Key which can be posted outside
- If it's possible accept connections only from certain ip range

QA

Roman Stepanov
roman@eltrino.com
skype: mail2punk



Q&A