Sense of Security	Authorisation. Jason Edelstein
	Release date. 24 February 2009.

Sense of Security – Security Advisory – SOS-09-002.

Magento Multiple Cross-Site Scripting Vulnerabilities.

24 February 2009.

Magento Multiple Cross-Site Scripting Vulnerabilities - Security Advisory – SOS-09-002

Release Date.	24-Feb-2009
Last Update.	-
Vendor Notification Date.	21-Jan-2009
Product.	Magento
Platform.	Linux / PHP (verified), possibly others
Affected versions.	Magento 1.2.0 (verified), possibly others
Severity Rating.	Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch not yet available
CVE reference.	CVE-2009-0541

Details.

Magento is an ecommerce application. During an application penetration test Sense of Security identified multiple cross-site scripting vulnerabilities in the administrator logon, administrator password reminder and update downloader features of the Magento application. This occurred as a result of the application not properly filtering HTML tags which allowed malicious JavaScript to be embedded. When input is incorrectly validated and not properly sanitised and then displayed in a web page, attackers can trick users into viewing the web page and causing malicious code to be executed.

Proof of Concept.

The following steps were tested prior to releasing this document on the Magento demo site at http://demo-admin.magentocommerce.com/index.php/admin/

Admin Login Page:

On a failed login, the value entered into the username field of the admin login page is reflected back to the user without any output encoding.

Steps to reproduce:

1. Go to http://magento/index.php/admin/
2. Enter the following into the username field: "><script>alert('xss')</script>
3. Enter a nonsense value into the password field such as 'xxx'
4. Click the Login button
5. You will be presented with a JavaScript alert dialog box containing 'xss'

Password Reminder:

The password reminder function contains a similar vulnerability to the previous one. The value of the email address field is reflected back to the user without any output encoding if the entered email does not exist.

Steps to reproduce:

1. Go to http://magento/index.php/admin/index/forgotpassword/
2. Enter the following into the email address field: "><script>alert('xss')</script>
3. Click the Retrieve Password button
4. You will be presented with a JavaScript alert dialog box containing 'xss'

Magento Connect Downloader:

The Downloader contains a slightly different bug to two previously described. The 'return' parameter of the URL query string is inserted into an <a href=""> tag with no output encoding to facilitate the 'Return to Magento Administration' link.

Steps to reproduce:

1. Go to http://magento/downloader/?return=%22%3Cscript%3Ealert('xss')%3C/script%3E
2. You will be presented with a JavaScript alert dialog box containing 'xss'

Solution.

The vendor has advised that the fix will be made available in the near future.

Discovered by.

Loukas Kalenderidis from SOS Labs.

About us.

Sense of Security is a leading provider of IT security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application security consultancy and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au