

Cisco Applied Mitigation Bulletin: Understanding Cross-Site Scripting (XSS) Threat Vectors

Document ID: 71616

<http://www.cisco.com/warp/public/707/cisco-amb-20060922-understanding-xss.shtml>

Revision 1.0

For Public Release 2006 September 22 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)
[Device-Specific Mitigation and Identification](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)
[Related Information](#)

Cisco Response

Vulnerability Characteristics

XSS exploits have become one of the most common web application vulnerabilities and are achieved through three standard attack vectors: reflected, stored, and advanced. The results of XSS attacks are the same regardless of the vector; these results can consist of installation or execution of malicious code, account compromise, session cookie hijacking, revelation or modification of local files, and site redirection (which could be to a vulnerable server or malicious website).

XSS attacks use obfuscation by encoding tags or malicious portions of the script using the Unicode method so that the link or HTML content is disguised to the end user browsing to the site. The origins of XSS attacks are difficult to identify using traceback methods because the vulnerable server is used to inject the malicious code to the users' browsers, thus concealing the identity of the malicious user.

Reflected Attack Vector

A reflected attack, also known as nonpersistent, takes place when malicious code or scripts are injected by a vulnerable web server via any method that produces a response as part of a valid HTTP request. Some common examples of responses are error messages, search engine results, or submitted web forms. An example of a reflected XSS attack is a case in which an unsuspecting user is enticed to follow a malicious link to a vulnerable server that injects (reflects) the malicious code back to the user's browser. The browser then executes the code or script because the vulnerable server is usually a known or trusted site. Standard methods of delivery for XSS exploits are via e-mail, instant messenger applications, or search engines.

Stored Attack Vector

A stored attack, also known as persistent, takes place when the malicious code or script is permanently stored on a vulnerable or malicious server using a database, blog entries, newsgroup or web forum posts, or any other permanent storage method. An example of a stored XSS attack is a case in which a user requests the

stored information from the vulnerable or malicious server, which then injects the requested malicious script into the user's browser. The browser then executes the code or script because the vulnerable server is usually a known or trusted site.

Advanced Attack Vectors

Advanced attack vectors use HTML `img` and `frame` constructs (``, `<frame>`, `<iframe>`) or POST method. The use of HTML constructs allows attackers to disguise embedded malicious code into web pages or web-based e-mail messages. Using web-based e-mail messages as the attack vector allows a malicious user to send unsolicited e-mail to many end users with a high probability that at least a few unsuspecting users will fall victim to the embedded scripting. The malicious code is executed by the browser upon rendering the HTML content from the web page. A more complicated attack vector is via a server that is vulnerable to HTTP POST method. The HTTP POST method takes place when a user accesses a page on a website that uses variables to express the malicious code. The malicious page sends the POST command to the vulnerable server, which then injects the malicious script to the user's browser or redirects the user to a malicious site.

Cross-site scripting, also known as XSS, is a flaw within web applications that enables malicious users, vulnerable websites, or owners of malicious websites to send malicious code to the browsers of unsuspecting users. The malicious code is usually in the form of a script embedded in the URL of a link or the code may be stored on the vulnerable server or malicious website. The browser will execute the malicious script because the web content is assumed to be from a trusted site and the browser does not have a way to validate the URL or HTML content. A main source of XSS attacks is websites that do not properly validate user-submitted content for dynamically generated web pages. The development of websites that are not vulnerable to XSS threats begins with web application developers who employ secure coding and input validation techniques, as well as browser manufacturers who verify both transmitted and received HTML content.

Mitigation Technique Overview

User Education and Security Awareness Training

To reduce the risk that users will be victims of XSS attacks, it is advisable to educate them about safe browsing. Countermeasures should also be implemented at the application level (browser) through scripting controls made available in the browser. Scripting controls would allow the ability to define policies to restrict code execution. Attackers also use web-based e-mail as an XSS vector, either through embedded scripting or links that can result in the execution of malicious code in the browser. A standard user strategy should consist of the following:

- Disable all scripting languages interpreted by the browser.



Caution: Caution: Disabling scripting may result in a loss of functionality because many web applications use scripting. Take care to ensure that all required business applications are fully functional with scripting disabled.

- Only follow links to known websites you receive from trusted sources.
- Check links for use of suspicious-looking characters.
- Be suspicious of excessively long links.
- Install the latest patches for the browser.
- Access only websites that are known and trusted locations. If there are any questions or suspicions, contact the webmaster and/or the company hosting the website immediately.
- Delete unsolicited e-mail messages or read them in plain text to help prevent the execution of malicious code.

Device-Specific Mitigation and Identification

Cisco products provide mitigation capabilities that identify and help protect users and company assets that may be susceptible to XSS attacks. The following list provides information about current IPS signatures (as of Signature Update S249) that can be used against XSS threats:

IPS Signatures

- 5232/1 – URL with XSS
- 5807/0 – Indexing Service Cross-Site Scripting Vulnerability
- 5757/0 – Microsoft Exchange Server Cross-Site Scripting
- 6007/0 – Management Console (Microsoft MMC) Cross-Site Scripting
- 5763/0 – Wireless Control System Cross-Server Site Scripting
- 5750/0 – WLSE Cross-Site Scripting
- 5687/0 – IE Frame Cross-Site or Cross-Zone Scripting
- 5655/0 – Cobolt RaQ Cross-Site Scripting Vulnerability
- 5551/0 – Outlook Web Access (OWA) Cross-Site Scripting Vulnerability
- 5566/0 – Potential IE Cross-Frame Scripting
- 5527/0 – IIS Index HTW Cross-Site Scripting
- 5418/0 – IIS Cross-Site Scripting .htw
- 5343/0 – Apache Host Header Cross-Site Scripting
- 5232/0 – URL with XSS 5201/0 – PHP-Nuke Cross-Site Scripting
- 5201/1 – PHP-Nuke Cross-Site Scripting
- 5201/2 – PHP-Nuke Cross-Site Scripting
- 5209/0 – Agora.cgi Cross-Site Scripting

Additional Information

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.0	2006-September-22	Initial public release.
--------------	-------------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [IPS 5.x Signature Downloads](#) ([registered](#) customers only)
- [Signatures by Release Version](#) ([registered](#) customers only)
- [Open Web Application Security Project \(OWASP\)](#)

- [Web Application Security Consortium \(WASC\)](#)
 - [The Anatomy of Cross-Site Scripting by Gavin Zuchlinski](#)
 - [Advanced Cross-Site Scripting by Gavin Zuchlinski](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Sep 22, 2006

Document ID: 71616
