

[REVS] XST Strikes Back

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00088.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 25 Jan 2006 09:39:46 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

XST Strikes Back

SUMMARY

This is yet another example of peripheral web security issue, such as the ones discussed in

<<http://www.securiteam.com/securityreviews/5YP0I1FG0G.html>> "Meanwhile, at the other side of the web server". A web application may be compromised through issues that are beyond the control of the web site owner – in this case, support for TRACE in browsers and proxy servers. In fact, in many cases the site owner has no way of even knowing that the attack took place, because the TRACE request is answered at the proxy server, and never arrives at the web server (of course, if the first proxy server is the site's reverse proxy server, or if no proxy server at all is present, then the site owner may find out).

It seems that the TRACE method should be disabled across the board – not just in web servers, but also in proxy servers and in browsers (and possibly in other web devices).

DETAILS

About three years ago, the concept of "

<http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf> Cross

[REVS] XST Strikes Back

Site Tracing" was introduced to the web application security community. In essence, the classic XST is about amplifying an existing XSS vulnerability such that HttpOnly cookies and HTTP authentication credentials can be compromised. This is done using a client side XmlHttpRequest object that sends a TRACE request back to the server, receives the request echoed back by the server's TRACE function, and extracts the information from the echoed back request.

The <http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf> recommendation in is to turn off TRACE support in the web server, which indeed takes care of the attack as described.

It seems that the TRACE method should be disabled across the board – not just in web servers, but also in proxy servers and in browsers (and possibly in other web devices).

Forcing the first proxy server in the chain to respond to the TRACE request (rather than forward it) is as simple as including an HTTP request header " <<http://www.ietf.org/rfc/rfc2616.txt>> Max-Forwards: 0" (section 14.31 of RFC 2616).

So, for IE (up to and including 6.0 SP1) and for Mozilla/Firefox (up to and including Firefox 1.0.6), the XSS payload should be (IE code, Mozilla/Firefox modifications commented):

```
var x = new ActiveXObject("Microsoft.XMLHTTP");
// var x = new XMLHttpRequest();
x.open("TRACE", "", false);
x.setRequestHeader("Max-Forwards", "0");
x.send();
// x.send("");
alert(x.responseText);
```

In IE 6.0 SP2, it seems that Microsoft silently removed support for TRACE in the XmlHttpRequest object. That is, no method starting with "TRACE" is allowed. However, a simple trick, involving a technique similar to the one used in <<http://www.securityfocus.com/archive/107/308433>> "XS(T) attack variants which can, in some cases, eliminate the need for TRACE" and <<http://www.securityfocus.com/archive/1/411585>> "Exploiting the XmlHttpRequest object in IE – Referrer spoofing, and a lot more..." can be used to bypass this protection. Instead of using "TRACE" for the method, one can simply use "\r\nTRACE". To quote <<http://www.ietf.org/rfc/rfc2616.txt>> from section 4.1 of RFC 2616:

"In the interest of robustness, servers SHOULD ignore any empty line(s) received where a Request-Line is expected. In other words, if the server is reading the protocol stream at the beginning of a message and receives a CRLF first, it should ignore the CRLF."

So the XSS payload for IE 6.0 SP2 would be:

```
var x = new ActiveXObject("Microsoft.XMLHTTP");
```

[REVS] XST Strikes Back

```
x.open("\r\nTRACE","/",false);
x.setRequestHeader("Max-Forwards","0");
x.send();
alert(x.responseText);
```

Squid (2.5stable10/NT), Apache (2.0.54 mod_proxy) and other popular proxy servers were found to support TRACE and Max-Forwards.

Workaround:

Proxy server vendors:

1. Ship proxy servers with default secure configuration, namely no TRACE support disabled.
2. In the least, enable turning off support for TRACE via a configuration option.

Proxy server owners/maintainers:

Disable support for TRACE.

1. For Squid, add the following to the Squid configuration file (squid.conf):

```
acl TRACE method TRACE
```

```
...
```

```
http_access deny TRACE
```

2. For Apache, use mod_rewrite to prevent support for http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf > TRACE. Make sure to place the directive in the <proxy> section of the httpd.conf file. Also, It would be a good idea to append the "[nocase]" flag to the RewriteCond directive, to ensure case insensitive comparison (though it seems that Apache will only serve fully uppercase HTTP methods).

Browser vendors:

Disable support for TRACE in the XmlHttpRequest object. Make sure you do it right though.

Web site owners:

As a workaround (perhaps not too practical), enable SSL traffic only to your site.

ADDITIONAL INFORMATION

The information has been provided by <mailto:aksecurity@xxxxxxxxxxx> Amit Klein (AKsecurity).

=====

[REVS] XST Strikes Back

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- Prev by Date: [*\[UNIX\] TYPO3 Web Content Manager File System Path Disclosure*](#)
 - Next by Date: [*\[NT\] TFTPd Filename Format String*](#)
 - Previous by thread: [*\[UNIX\] TYPO3 Web Content Manager File System Path Disclosure*](#)
 - Next by thread: [*\[NT\] TFTPd Filename Format String*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)