

[Full-disclosure] Facebook script injection vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-07/msg00029.html>

- *From:* "Jouko Pynnonen" <jouko@xxxxxx>
 - *Date:* Thu, 3 Jul 2008 02:01:28 +0300
-

Hello,

This is a summary of various Facebook security issues found and reported since June 13, 2008. Two of the vulnerabilities still remain on the site, so no details of them are disclosed here. The rest have been fixed.

Any of these could be exploited to take over the victim's web browser temporarily to e.g. read inbox messages, forcibly install FB applications, manipulate friend lists, post messages as the victim user, etc. Any of these would also allow creation of a self-propagating JavaScript virus/worm.

Most of the issues require the victim user to click on a profile box or visit a canvas page of an application in order to trigger the injected JavaScript. Issues 2) and 3) don't require mouse clicks.

The vulnerabilities were tested with two browsers: Firefox 3 (Linux + Windows) and Internet Explorer 7.

1) Escaping JS sandbox with literal Function constructor reference

Impact: execution of unrestricted JS on canvas pages or profiles (mousedown required on profile pages)

Description: The JS sandbox denies references to Function.constructor but using a literal such as "function f() { }" in the code and referring to its constructor with the "bracket syntax" was possible.

The example below uses this method and calls the constructor with a string argument, then calls the resulting Function object.

Browsers: FF, IE

Reported: June 13, 2008

Fixed: yes

Example:

```
(function f(){}["constructor"]("alert('any javascript here');"))();
```

2) Fb:silverlight JS injection

Impact: execution of unrestricted JS on canvas pages, profiles

Description: Simple XSS, described in the previous message to full-disclosure.

Browsers: FF, IE

Reported: June 16, 2008

Fixed: yes

Example:

```
<fb:silverlight silverlightsrc="a"
width="\ height=",any_javascript_code_here);//" />
```

3) Injecting JS in Feeds

Impact: execution of unrestricted JS when viewing Feeds on profile page or the "home" page

Description: Insufficient input validation in the publishTemplatizedAction API method.

Browsers: FF, IE

Reported: June 16, 2008

Fixed: yes

Example:

using the perl API

```
$facebook->feed->publish_templatized_action( title => "My Title",
title_template => "{actor} is testing feed stories",
body_template => "hello",
image_1 => "http://www.mysite.com/image.gif\"
onload=(function&#9;f(){['constructor']('alert(1)'))();",
image_1_link => "http://www.mysite.com );
```

4) Escaping JS sandbox with literal Number reference

Impact: execution of unrestricted JS on canvas pages or profiles (mouseclick required on profile pages)

Description: Using the "bracket syntax" to reference the parent property of a floating point number to get a Window object reference, then calling its eval() to run arbitrary code. IE doesn't support the property.

Browsers: FF

Reported: June 18, 2008

Fixed: yes

Example:

```
<script>
1.[ "parent " ].eval("alert('any javascript here');");
</script>
```

5) Injecting JS in video attachments

Impact: execution of unrestricted JS when a inbox, wall or forum message is viewed (mousedown required)

Description: When sharing video content with the <http://www.facebook.com/sharer.php> form, some input fields can be modified e.g. with JavaScript. The example below can be typed in the address bar to inject JS in a message.

Browsers: FF, IE

Reported: June 20, 2008

Fixed: yes

Example:

```
javascript:f=document.forms[0]:fl'attachment[params][video][src'].value="#"  
a=b>
```

6) Escaping JS sandbox with E4X

Impact: execution of unrestricted JS on canvas pages or profiles (mousedown required on profile pages). Works in browsers supporting E4X (Firefox)

Description: JS parser in browsers supporting E4X understand XML, which can contain multi-line strings. Facebook's JS sandbox technology didn't expect XML and multi-line strings. The example below demonstrates how this could be used to fool the sandbox logic.

Browsers: FF

Reported: June 26, 2008

Fixed: yes

Example:

```
<script>  
<x x="  
x" {alert('any javascript')}="x"  
>  
</script>
```

7) Escaping JS sandbox

Impact: execution of unrestricted JS on canvas pages or profiles (mousedown required on profile pages)

Browsers: FF

Reported: June 21, 2008

Fixed: no

8) Escaping JS sandbox

Impact: execution of unrestricted JS on canvas pages or profiles

[Full-disclosure] Facebook script injection vulnerabilities

(mouseclick required on profile pages)

Browsers: FF

Reported: June 21, 2008

Fixed: no

==

Jouko Pynnönen <jouko@xxxxxx>

<http://iki.fi/jouko>

Finland

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>