

[UNIX] PHPKit SQL Injection and XSS Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0085.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/23/04

To: list@securiteam.com

Date: 23 Nov 2004 18:17:57 +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>

PHPKit SQL Injection and XSS Vulnerabilities

SUMMARY

<<http://www.phpkit.de>> PHPKIT is "a modular developed homepage software which enables simple management messages contents, guest book, forums and more".

Due to improper sanity validation checks it is possible for an attacker to manipulate an SQL query and launch cross site scripting attacks.

DETAILS

Vulnerable Systems:

* PHPKit version 1.6.03 to 1.6.1 inclusive

The cross site scripting attack is viable through the exploitation of the 'img' HTTP parameter in the 'popup.php' script. Example:

[<http://www.target.com/phpkit/popup.php?img="><script>alert\(document.cookie\)</script>](http://www.target.com/phpkit/popup.php?img=)

Manipulation of the SQL command sent to the database is possible via the 'id' parameter in the 'include.php' script. Example:

<http://www.target.com/phpkit/include.php?path=guestbook/print.php&id=1>

Securiteam: [UNIX] PHPKit SQL Injection and XSS Vulnerabilities

The relevant piece of code is:

```
<?php
if (isset($_REQUEST['id'])) $id=$_REQUEST['id'];
$gbookinfo=$DB->fetch_array($DB->query("SELECT * FROM ".$db_tab['gbook']."
WHERE gbook_id='".$id.'" LIMIT 1"));
eval ("\"$site_body.= \".getTemplate('guestbook/print')."\"");
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:steve01@chello.at> Steve.

=====

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.