

[VulnWatch] PHP Information Functions May Allow Cross-Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-10/0021.html>

From: Matthew Murphy (mattmurphy@kc.rr.com)

Date: 10/13/02

From: "Matthew Murphy" <mattmurphy@kc.rr.com>

To: "VulnDiscuss" <vulndiscuss@vulnwatch.org>, "VulnWatch" <vulnwatch@vulnwatch.org>, "Vuln-Dev"

Date: Sun, 13 Oct 2002 00:34:13 -0500

PHP Information Functions May Allow Cross-Site Scripting

Write-Up: <http://www.techie.hopto.org/vulns/2002-36.txt>

The `phpinfo()` debugging function is a useful tool to diagnose the causes of errors in applications, particularly those relating to individual environments. The procedure outputs information about the state of PHP and the server at the time of execution -- including an image tag that pulls up the PHP logo. To do this, the tag calls the PHP script with a query string of `"=/soinfo.php?=-PHPE9568F35-D428-11d2-A769-00AA001ACF42"` or similar (changes based on the logo desired).

The first thing I audited with this was messing with the query -- zilch. The next thing I did was add an extra question mark to the URI. The nice PHP logo miraculously transforms into that ugly Internet Explorer X -- no image to display. So, we now know that PHP forgot to strip the query off the URI before inserting it into that image tag.

Worse, we discover that PHP doesn't filter queries -- meaning that the following:

```
http://localhost/soinfo.php?">[code]
```

will cause [code] to run, provided the browser doesn't implement a paranoid encoding mechanism -- as most do. This vulnerability has a limited impact.

Solution:

Set `expose_php = Off` in `php.ini` to eliminate this. PHP Bug ID#19881 describes this issue.

The Irony:

The comment lines directly above the `expose_php` directive in the default config file specifically say that it is "no security threat", but having it

VulnWatch: [VulnWatch] PHP Information Functions May Allow Cross-Site Scripting
enabled opens you to an XSS? Food for thought...

- **Previous message:** [Olaf Schulz: "\[VulnWatch\] Apache Tomcat 3.x and 4.0.x: Remote denial-of-service vulnerability"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)