

# [UNIX] php(Reactor) Cross Site Scripting Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0031.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/09/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sun, 9 Jun 2002 19:52:33 +0200 (CEST)

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.

-----

php(Reactor) Cross Site Scripting Vulnerability

---

## SUMMARY

<<http://phpreactor.org/>> php(Reactor) is a system of integrated web applications designed to encourage user interaction and facilitate easy website maintenance. A Cross-Site Scripting vulnerability exists in php(Reactor). This would allow a remote attacker to send information to victims from untrusted web servers, and make it look as if the information came from the legitimate server.

## DETAILS

Vulnerable systems:

php(Reactor) version 1.2.7 and prior

Immune systems:

php(Reactor) version 1.2.7p11

The "browse.php", in the "comments" section does not filter user input for \$go variable. Therefore, any user may construct a malicious link, gain information about users, and even get the login information of the administrator.

## Securiteam: [UNIX] php(Reactor) Cross Site Scripting Vulnerability

Here is the proof-of-concept link example;

[http://\[target\]/comments/browse.php?fid=2&tid=4&go=<script>alert\(document.cookie\)</script>](http://[target]/comments/browse.php?fid=2&tid=4&go=<script>alert(document.cookie)</script>)

Note that, the \$fid and \$tid variables should be integers.

Solution:

The vendor replied quickly, and has released a new version on 28/05/2002, which can be downloaded at

[<http://sourceforge.net/project/showfiles.php?group\\_id=12105>](http://sourceforge.net/project/showfiles.php?group_id=12105)

[http://sourceforge.net/project/showfiles.php?group\\_id=12105](http://sourceforge.net/project/showfiles.php?group_id=12105)

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[salper@olympus.org](mailto:salper@olympus.org)> Ahmet Sabri ALPER.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[UNIX] Splatt Forum XSS"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)