

# [UNIX] phpCMS Cross Site Scripting and Information Disclosure Issues

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0099.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 11/29/04

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

Date: 29 Nov 2004 10:56:41 +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>

-----

phpCMS Cross Site Scripting and Information Disclosure Issues

---

## SUMMARY

" <<http://www.phpcms.de/>> phpCMS is a content management system, which convinces in particular by small system requirements, high performance and above all its flexibility. phpCMS is suitable for small private web pages and also for complex professional appearances and high traffic websites including the integration of webservices and external applications."

An input validation error in the system's code paves the way for an XSS vulnerability which is exploitable through at least one argument.

## DETAILS

Vulnerable Systems:

- \* phpCMS version 1.2.1 and prior

Immune Systems:

- \* phpCMS version 1.2.1.pl1

An implementation error in the validation of the user input may lead to an XSS vulnerability allowing the malicious user to conduct cross site

## Securiteam: [UNIX] phpCMS Cross Site Scripting and Information Disclosure Issues

scripting attacks. In addition, the specifics of the problem allow the malicious attacker to gain information about the server's configuration when phpCMS is configured in non-stealth mode with debug mode enabled.

Example:

```
http://[somehost]/parser/parser.php?file=<scr!pt>alert(document.cookie)</scr!pt>
```

The error page displays the input supplied by the user, without filtering, and in addition the full path to the phpCMS root directory.

Proof of concept:

```
http://[somehost]/parser/parser.php?file=donotexist
```

->

phpCMS 1.2.1

Error: 07: could not find file for parsing.

```
/var/www/localhost/htdocsdonotexists/index.htm
```

Vendor Status:

The vendor has already supplied a fixed version of the system. Users are encouraged to upgrade to the newer 1.2.1.pl1 version. In any case it would be best not to run the system in non-stealth mode combined with debug mode with untrusted access.

Disclosure Timeline:

2004/11/24 – Vulnerability discovered

2004/11/24 – Vendor notified

2004/11/25 – Vendor response

2004/11/25 – Fix released

### ADDITIONAL INFORMATION

The information has been provided by <mailto:cb-lse@ifrance.com> Cyrille Barthelemy.

=====

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.