

# [UNIX] FUDforum file access and SQL Injection

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0055.html>

---

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

*Date:* 08/19/02

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

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

Date: Mon, 19 Aug 2002 10:47:17 +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.

-----

FUDforum file access and SQL Injection

---

## SUMMARY

<<http://fud.prohost.org/>> FUDforum is a robust, fully customizable, and extremely scalable forums package. It uses a powerful & speedy combination of PHP & MySQL to create a highly portable solution that can run on virtually any operating system. This highly optimized application is an ideal community solution for any website or company. FUDforum has two security holes that allow people to download or manipulate files and directories outside of FUDforum's directories. One of the holes can be exploited by everyone, while the other requires administrator access. The program also has some SQL Injection problems.

## DETAILS

Vulnerable systems:

- \* FUDforum version 2.0.2, possibly others

Immune systems:

- \* FUDforum version 2.2.0 and above

Technical details:

1) The tmp\_view.php script does not check the path of the file that will be displayed, which means that it can be used for downloading any file on the system that the httpd daemon's has access to.

## Securiteam: [UNIX] FUDforum file access and SQL Injection

You exploit it by surfing to `tmp_view.php?file=/etc/passwd`. The HTTP headers that are sent back to you will say that the file is an image, which prevents downloading of non-image files in a normal web browser. While in, you use netcat or telnet to connect directly to the web server, which will get you the file's raw data. This issue does not require any user login.

2) The `adm/admbrowse.php` script allows downloading and general manipulation (creation, deletion) of files and directories outside of the FUDforum directories. Here's how to use `admbrowse` to download `/etc/passwd`: `admbrowse.php?down=1&cur=%2Fetc%2F&dest=passwd&rid=1&S=[someid]`

FUDforum has some protection against changing the `cur` variable like this, but it mostly stops attackers from getting file listings for unauthorized directories. It does not protect against many other related issues.

This issue requires administrator access.

3) There are some SQL Injection issues in the code. They are of the easy type where we do not really have to inject anything, because there are no apostrophes or quotes around the variable data in the SQL statements. These problems can be found in the scripts `report.php`, `selmsg.php`, and `showposts.php`.

Vendor status:

The vendor was contacted on 17 June, and they replied quickly. The stable version 2.2.0, which is immune to these holes, was released on 4 July.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:ulfh@update.uu.se>> Ulf Harnhammar.

=====

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] PHPNuke Private Messaging Module Allows Compromising of Administrator Accounts"

Securiteam: [UNIX] FUDforum file access and SQL Injection

- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]