

# [UNIX] Slashcode Login Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0044.html>

---

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

*Date:* 01/11/02

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

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

Date: Fri, 11 Jan 2002 15:50:51 +0100 (CET)

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.

-----

Slashcode Login Vulnerability

---

## SUMMARY

Slash, the code that runs Slashdot and many other web sites, has a vulnerability in recent versions that allows any logged-in user to log in as any other user.

This allows users to take nearly full control of a Slash system (post and delete stories, posting stories, edit users, post as other users, etc., and do anything that a Slash user can do) by logging in to an administrator's Slash account.

## DETAILS

Vulnerable systems:

Any system running Slash version 2.1.x (development versions for 2.2), 2.2.0, 2.2.1, or 2.2.2, and sites using the development code from CVS.

Slash 2.0.x and previous are unaffected

Immune systems:

Slash version 2.2.3

Workaround:

In the meantime, if upgrading is not possible or will not happen immediately, site administrators should either shut down the web site or

## Securiteam: [UNIX] Slashcode Login Vulnerability

disable admin.pl and users.pl by moving them elsewhere or disabling the execution bits (Apache may need to be restarted following this).

Further, site administrators should change their passwords, and check the "seclev" field in the users table to make sure no one has a seclev greater to or equal than "100" who should not have administrator privileges:

```
mysql> SELECT uid, nickname, seclev FROM users WHERE seclev >= 100;
```

That should list only users with some administrator privileges.

Site administrators should subscribe to the slashcode-general or slashcode-announce mailing lists, to keep up to date on the latest releases and security notices. Subscription information is on the Slashcode site at <http://slashcode.com/>.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:daniel@satus.com> Daniel Bowers.

=====

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): "[EXPL] Improper Input Validation in Bugzilla (Exploit)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)