

# [NEWS] Slashdot / Slashcode Disclosing Passwords

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0035.html>

---

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

*Date:* 09/12/02

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

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

Date: Thu, 12 Sep 2002 08:12:24 +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.

-----

Slashdot / Slashcode Disclosing Passwords

---

## SUMMARY

A feature in Slashdot / Slashcode web site allows attackers to steal user's usernames and password if they have enabled the Quick Login feature (note that enabling feature will display the warning that "This [feature] is totally insecure").

## DETAILS

On certain occasions, you can find a very interesting Referer string for some visitors of pages mentioned on Slashdot / Slashcode. One of such entries:

63.XXX.XXX.175 -- [11/Sep/2002:18:13:33 +0200] "GET /newtcp/ HTTP/1.1"  
200 33541 "<http://slashdot.org/?unickname=dXXg>"  
[Mozilla/5.0 \(Windows; U; Win98; en-US; rv:1.1\) Gecko/20020826](http://mozilla.org/)"

This happens whenever any of the following prerequisites are met:

(1) A user connects to Slashdot using the "quick login";

(2) Clicks on an external link immediately, without any prior navigation within Slashdot itself. (Alternatively, navigate within Slashdot, then use

Securiteam: [NEWS] Slashdot / Slashcode Disclosing Passwords

the browser's "Back" button to go back to the initial page, and then click on the external link.)

(3) The external link gets your Slashdot username/password in the referer field.

Vendor response:

This is well documented and a warning is given to users enabling this feature that "This is totally insecure", therefore users enabling this feature are taking on themselves the risk that their password and username will be revealed to the public.

ADDITIONAL INFORMATION

The information has been provided by <mailto:lcamtuf@dione.ids.pl> Michal Zalewski, <mailto:crdic@pacbell.net> Craig Dickson and <mailto:jamie@mccarthy.vg> Jamie McCarthy.

=====

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): "[NT] Apple QuickTime ActiveX Buffer Overrun"
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)