

[UNIX] PForum MySQL Injection Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0116.html>

From: support@securiteam.com

Date: 02/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 18 Feb 2002 22:39:18 +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.

PForum MySQL Injection Bug

SUMMARY

<<http://www.powie.de/>> PForum is a www-board system using PHP and MySQL. Although the author seemed to try to eliminate malicious code (e.g. unwanted html-code) in the inputs, he relies on PHP's Magic-Quotes for adding slashes to some user input. Therefore, it is possible to use an SQL-Injection-Attack to log in as administrator or any other user without knowing the correct password.

DETAILS

Vulnerable systems:

PForum version 1.14 and prior

Immune systems:

PForum version 1.15

If the affected webserver has not enabled PHP's magic_quotes_gpc in the php.ini, it is possible to login as any user, admin, or moderator.

Proof of concept:

Without having Magic-Quoted enabled, just login with the username "admin" OR username='admin". If the user admin exists, you will be logged in without requiring a password. If the user admin is an administrator, you

Securiteam: [UNIX] PForum MySQL Injection Bug

have all administrator privileges on the board. The same concept works for the changing password form. In case you have forgotten your password, you get an id via mail to your registered email address, so you can change your password to a new one. Here you have to use `changePass.php` and enter your id like "123" or "a='a'" to change your password to any desired.

Temporary fix:

Enable `magic_quotes_gpc` in your `php.ini`.

Vendor status:

The vendor reacted very quickly. With some assistance, he needed about 24 hours for a patch. Although he has not made this patch until now, he has published the bug on his homepage and recommends our temporary fix (enabling `magic_quotes_gpc`) until the new version is released.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@ppp-design.de> Jens Liebchen.

=====

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

=====

=====

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: "[NT] PowerFTP Server File Reading and DoS Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)