

[UNIX] AutoRank PHP SQL Injection Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0065.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/03

To: list@securiteam.com

Date: 22 Dec 2003 13:58:01 +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>

AutoRank PHP SQL Injection Vulnerabilities

SUMMARY

<<http://www.jmbsoft.com/software/arphp/>> AutoRank PHP is "our next generation toplist software, written completely in PHP and backed by a MySQL database". AutoRank PHP is vulnerable to SQL Injection attacks.

DETAILS

Vulnerable systems:

- * AutoRank PHP version 2.0.4

The vulnerabilities can be exploited by injecting SQL queries into the user & password fields when editing an account, the email field when requesting a lost password and the username field when registering an account. If a malicious attacker logs in with the username and password '--- he will automatically be given access to the first account cataloged in the database. He can then view the HTML source code to view that user's password in plain text. This also leaves the database being used by AutoRank PHP open for attack. The affected file is accounts.php.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@gulftech.org>>

Securiteam: [UNIX] AutoRank PHP SQL Injection Vulnerabilities

JeiAr.

=====

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.