

Forum:[Hack Forums](#)

Thread: [\[EXPLOIT\] Get free access to Prodigy shell booters!](#)

Starfall - August 2, 2012, 1:29 am

Today I am going to post a method of gaining free access to Prodigy source shell booters.

If we look at register.php, we will see these lines of code:

PHP Code

```
<?php
```

```
// Generates activation code simple 4 digit number
```

```
$activ_code = rand(1000,9999);
```

```
/* snip irrelevant */
```

```
$sql_insert = "INSERT into `users`
```

```
    (`full_name`,`user_email`,`pwd`,`address`,`tel`,`fax`,`website`,`date`,`users_ip`,`activation_code`,`country`,`user_name`)
```

```
VALUES
```

```
    ('$data[full_name]','$usr_email','$sha1pass','$data[address]','$data[tel]','$data[fax]','$data[web]
```

```
    ,now(),'$user_ip','$activ_code','$data[country]','$user_name'
```

```
    )
    ",
```

Forgive the kinda-ugly code, it's not mine...

Anyway, we can see that, as the author himself said, the activation code is a simple 4 digit number.

Regardless of whether or not activation links are sent in emails (they usually aren't, to ensure that you pay for the booter),

we can write a script to brute force this within a few minutes.

To keep this tutorial skiddy-proof, I won't provide such a thing...

but here's the relevant code from activate.php containing everything you need to know to make one:

PHP Code

```
<?php
```

```
/** ACTIVATION BY FORM**/
```

```
if ($_POST['doActivate']=='Activate')
```

```
{
```

```
$err = array();
```

```
$msg = array();
```

```
$user_email = mysql_real_escape_string($_POST['user_email']);
```

```
$activ = mysql_real_escape_string($_POST['activ_code']);
```

```
//check if activ code and user is valid as precaution
```

```
$rs_check = mysql_query("select id from users where user_email='$user_email' and activation_code='$activ'") or die (mysql_error());
```

```
$num = mysql_num_rows($rs_check);
```

```
// Match row found with more than 1 results - the user is authenticated.
```

```
if ( $num <= 0 ) {
```

```
    $err[] = "Sorry no such account exists or activation code invalid.";
```

```
    //header("Location: activate.php?msg=$msg");
```

```
    //exit();
```

```
}
```

```
//set approved field to 1 to activate the user
if(empty($err)) {
    $rs_activ = mysql_query("update users set approved='1' WHERE
        user_email='$user_email' AND activation_code = '$activ' ") or die(mysql_error());
    $msg[] = "Thank you. Your account has been activated.";
}
```

BattleToads - August 2, 2012, 2:08 am

omgzfg h4x0r is fake. the last exploit was soo fake this HAS to be fake. Nice troll post guys. This is HF no way there is a actual exploit on here.

Starfall - August 2, 2012, 2:09 am

Yup, absolutely fake. That's why I pasted code from the vulnerable script itself. </sarcasm>
Read the code moron.

BattleToads - August 2, 2012, 2:10 am

(Aug 2, 2012 02:09 AM)ddos_king Wrote: [\[CITE\]](#) Yup, absolutely fake. That's why I pasted code from the vulnerable script itself. </sarcasm>
Read the code moron.

This is blackhat activity and will be removed immidiantley. And rep fucked for coming up with a good exploit and trashing gay ass booters

Starfall - August 2, 2012, 2:14 am

(Aug 2, 2012 02:10 AM)BattleToads Wrote: [\[CITE\]](#) This is blackhat activity and will be removed immidiantley. And rep fucked for coming up with a good exploit and trashing gay ass booters
Ah. I see. Troll replies... Carry on, then.

BattleToads - August 2, 2012, 2:19 am

(Aug 2, 2012 02:14 AM)ddos_king Wrote: [\[CITE\]](#) Ah. I see. Troll replies... Carry on, then.
-1 reps omfg SCAM REPORT DIS BIITCH. He's probably infecting memeberzz becuz he haz -1 repz lets all rep fawk him. REEP FAWKK.

SoLong - August 2, 2012, 2:35 am

Vouch for ddos_king.
This exploit is real and legit.
Good job!

Fossil - August 2, 2012, 2:38 am

Obviously a legit exploit, BattleToads doesn't know what he's talking about :3

Phizo - August 2, 2012, 2:54 am

Very nice ddos_king, great contribution.

That is probably the worst authentication method I've ever came across. It generates a random integer between values 1000 and 9999; that would be ridiculously easy to brute force.

Diksens - August 2, 2012, 4:31 am

Quick python script I wrote which makes use of this exploit. Enjoy activating your accounts.

Link: <http://pastebin.com/qQXyhs1W>

Starfall - August 2, 2012, 4:32 am

(Aug 2, 2012 04:31 AM)Diksens Wrote: [\[CITE\]](#) Quick python script I wrote which makes use for this

exploit. Enjoy activating your accounts.

Link: <http://pastebin.com/qQXyhs1W>

I was kinda waiting for this.

RIP Prodigy source.

Phizo - August 2, 2012, 4:38 am

(Aug 2, 2012 04:31 AM)Diksens Wrote: [\[CITE\]](#) Quick python script I wrote which makes use of this exploit. Enjoy activating your accounts.

Link: <http://pastebin.com/qQXyhs1W>

That seems like a lot of code for such a simple task. Nevertheless good work :3

Then again, a lot of it is comments.

Diksens - August 2, 2012, 4:39 am

(Aug 2, 2012 04:32 AM)ddos_king Wrote: [\[CITE\]](#) I was kinda waiting for this.

RIP Prodigy source.

Haha. You might want to update the link in the quote, fixed a small issue regarding an infinite loop, which would make it keep looping if it didn't matched the regex. Nice find btw.

(Aug 2, 2012 04:38 AM)Phizo Wrote: [\[CITE\]](#) That seems like a lot of code for such a simple task. Nevertheless good work :3

Then again, a lot of it is comments.

Yeah, maybe. I'd like to comment my code, even though most of the code is simple to understand, it's mainly for people whom do not have any knowledge about python, yet they like to know what the code does. Anyway, this script will make divide the threads in half, one half will start looping from 0 to 5000, the other half from 9999 to 5000, just to speed up the process.

Th3PonyWizard - August 2, 2012, 4:39 am

I'd go over creating a PHP brute-force script for that, does anybody know where can I get the full source code? Anyway, nice find OP.

EDIT: nevermind, saw the contents of activate.php, seems to be enough.

(Aug 2, 2012 02:08 AM)BattleToads Wrote: [\[CITE\]](#) omgzfg h4x0r is fake. the last exploit was soo fake this HAS to be fake. Nice troll post guys. This is HF no way there is a actual exploit on here. Dumbass.

Starfall - August 2, 2012, 4:41 am

(Aug 2, 2012 04:39 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I'd go over creating a PHP brute-force script for that, does anybody know where can I get the full source code? Anyway, nice find OP.

Dumbass. <http://localhostr.com/download/0h1K963/Booter%20Sources%20PHP.zip>

Here's the full Prodigy source. (both "old" and "new" are affected, as well as derivatives)

Phizo - August 2, 2012, 4:42 am

(Aug 2, 2012 04:39 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I'd go over creating a PHP brute-force script for that, does anybody know where can I get the full source code? Anyway, nice find OP.

EDIT: nevermind, saw the contents of activate.php, seems to be enough.

Dumbass.

Go away, I'm writing a PHP script for it you silly whore ?

sum1 gimme a site using it kthxppls ily ??

HaxOr? - August 2, 2012, 5:04 am

I used 10 threads and it crashed my connection.
Nice find OP! :)

Phizo - August 2, 2012, 6:27 am

I finished the brute forcer, although it's kind of slow and I get that people can be impatient so I'll tweak it a bit and see if I can make it a little faster :3
Of course, I'll release a web-based version too since no one likes CLI except for me :c

First test (success but slow):

EDIT: Just made it so much faster, going pretty good :3

PHP Code

```
<?php
```

```
// From 1000 to 1050
```

Before: 0.788828

After: 0.123637

Let's see how fast I can get it :3

Sw1x - August 2, 2012, 6:37 am

Amazing job guys, I don't know much about .php but it's nice to see that so many is contributing with scripts!

Keep it up guys. :)

Th3PonyWizard - August 2, 2012, 7:31 am

(Aug 2, 2012 06:27 AM)Phizo Wrote: [\[CITE\]](#) I finished the brute forcer, although it's kind of slow and I get that people can be impatient so I'll tweak it a bit and see if I can make it a little faster :3
Of course, I'll release a web-based version too since no one likes CLI except for me :c

First test (success but slow):

<https://gyazo.com/c29059dcdc520a3d7417b7a8488f8224.png?1343913786>

EDIT: Just made it so much faster, going pretty good :3

PHP Code

```
<?php
```

```
// From 1000 to 1050
```

Before: 0.788828

After: 0.123637

Let's see how fast I can get it :3I thought about using a loop, CURL library, and simple condition.
Why you makin' everything looks complicated Q_Q

Phizo - August 2, 2012, 7:34 am

(Aug 2, 2012 07:31 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I thought about using a loop, CURL library, and simple condition. Why you makin' everything looks complicated Q_Q
That's exactly what I did :3
U MAD.

Only problem is making it web-based...it'll just sit there trying to connect until the loop is done .-.

HaxOr? - August 2, 2012, 7:38 am

(Aug 2, 2012 06:27 AM)Phizo Wrote: [\[CITE\]](#) I finished the brute forcer, although it's kind of slow and I get that people can be impatient so I'll tweak it a bit and see if I can make it a little faster :3
Of course, I'll release a web-based version too since no one likes CLI except for me :c

First test (success but slow):

EDIT: Just made it so much faster, going pretty good :3

PHP Code

<?php

// From 1000 to 1050

Before: 0.788828

After: 0.123637

Let's see how fast I can get it :3

Dude i want that.

And how did you find the booter?

Phizo - August 2, 2012, 7:39 am

(Aug 2, 2012 07:38 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Dude i want that.

And how did you find the booter?

You can have it now, it will be released soon anyway.

Want me to PM you it? :3

A friend gave me the booter so I could test :).

HaxOr? - August 2, 2012, 7:41 am

(Aug 2, 2012 07:39 AM)Phizo Wrote: [\[CITE\]](#) You can have it now, it will be released soon anyway.

Want me to PM you it? :3

A friend gave me the booter so I could test :).

Sure dude, i want to play. :3

Must create a dork to find them ...

Phizo - August 2, 2012, 7:43 am

(Aug 2, 2012 07:41 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Sure dude, i want to play. :3

Must create a dork to find them ...

Alright, I'll send you it now :3

Hell yes, we need a dork (Y).

HaxOr? - August 2, 2012, 7:45 am

(Aug 2, 2012 07:43 AM)Phizo Wrote: [\[CITE\]](#) Alright, I'll send you it now :3

Hell yes, we need a dork (Y).

I don't even know what it looks like.

Would you mind sending me that example? :3

Th3PonyWizard - August 2, 2012, 7:46 am

(Aug 2, 2012 07:34 AM)Phizo Wrote: [\[CITE\]](#) That's exactly what I did :3

U MAD.

Only problem is making it web-based...it'll just sit there trying to connect until the loop is done .-.
Oh.. That's exactly.. What you did... Hehe...

[img]http://everanyway.files.wordpress.com/2012/06/277269_papel-de-parede-meme-virando-a-mesa_1920x1200.jpg?w=407&h=378[/img]

I wanted to show off my badass php skillz. AND YES IM MAD ;_;

Edit: I won't recommend releasing it though, as the product itself comes from HF, and releasing an exploit to it is like cracking it, which is against the rules.

Phizo - August 2, 2012, 7:53 am

(Aug 2, 2012 07:46 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Oh.. That's exactly.. What you did... Hehe...

[img]http://everanyway.files.wordpress.com/2012/06/277269_papel-de-parede-meme-virando-a-mesa_1920x1200.jpg?w=407&h=378[/img]

I wanted to show off my badass php skillz. AND YES IM MAD ;_;

Edit: I won't recommend releasing it though, as the product itself comes from HF, and releasing an exploit to it is like cracking it, which is against the rules.

It's okie Pony, if you thought of that then you're a good coder :3 ?

Oh dang, didn't know Prodigy came from HF o.o

I won't release it if that's the case.

EDIT: Are you sure it was created by someone here? I can't seem to find anything but modified versions.

?asp3r - August 2, 2012, 8:08 am

can anyone post a working dork for prodigy booters? my internet is laggy as hell where im at, and its cutting back on my searches.

Th3PonyWizard - August 2, 2012, 8:17 am

(Aug 2, 2012 07:53 AM)Phizo Wrote: [\[CITE\]](#) It's okie Pony, if you thought of that then you're a good coder :3 ?

Oh dang, didn't know Prodigy came from HF o.o

I won't release it if that's the case.

EDIT: Are you sure it was created by someone here? I can't seem to find anything but modified versions. Thank you ?

That's the creator: <https://hackforums.net/member.php?action=profile&uid=127732>

Before the name change - `P R O D I G Y™

Well, he's banned, so I'm not sure if it still applies. Still though, there are a shitload of members selling booters with that source on the Marketplace section. Will you press the trigger? x3

?asp3r - August 2, 2012, 8:18 am

(Aug 2, 2012 08:17 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Thank you ?

That's the creator: <https://hackforums.net/member.php?action=profile&uid=127732>

Before the name change - `P R O D I G Y™

Well, he's banned, so I'm not sure if it still applies. Still though, there are a shitload of members selling booters with that source on the Marketplace section. Will you press the trigger? x3 you said you guys needed a dork, right?

how does this one work?

Spoiler ([Click to View](#))

"booter" inurl:"register.php"

Phizo - August 2, 2012, 8:20 am

(Aug 2, 2012 08:17 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Thank you ?

That's the creator: <https://hackforums.net/member.php?action=profile&uid=127732>

Before the name change - `P R O D I G Y™

Well, he's banned, so I'm not sure if it still applies. Still though, there are a shitload of members selling booters with that source on the Marketplace section. Will you press the trigger? x3

I don't think I'll pull the trigger, I don't want to upset anyone :3

I'll just share it to people I like, if it gets leaked then that's not my problem xD.

LoIZ Gym - August 2, 2012, 8:25 am

Could somebody provide me with a live link of a booter using it :3

I would like to write a code activator in jet another language xD

You can pm me, thanks.

SIM-209986 - August 2, 2012, 9:01 am

Prodigy booter has got a SQL Injection in the cookies as well.

Phizo - August 2, 2012, 10:08 am

(Aug 2, 2012 09:01 AM)Jurevich Wrote: [\[CITE\]](#) Prodigy booter has got a SQL Injection in the cookies as well.

In which file(s)? I'd like to check it out.

?asp3r - August 2, 2012, 10:14 am

can some1 set up a site for me to test for the best dorks on? im trying to get one that will only pick up prodigy, but to do that i need to know what it look like and what will be detected ..

Ichi - August 2, 2012, 12:44 pm

This is funny as hell. Wonderful contribution OP.

I'm sure people are gonna have a lot of fun with this one

?

Starfall - August 2, 2012, 1:23 pm

(Aug 2, 2012 09:01 AM)Jurevich Wrote: [\[CITE\]](#) Prodigy booter has got a SQL Injection in the cookies as well.And here it is! You can find this in hub.php

PHP Code

```
<?php
```

```
$query = mysql_query("SELECT * FROM `users` WHERE `id`='$$_SESSION[user_id]`  
' AND `banned`=1") or die(mysql_error());
```

```
if (mysql_num_rows($query) > 0) {
```

```
    mysql_query("update `users`
```

```
        set `ckey`= ", `ctime`= "
```

```
        where `id`='$$_SESSION[user_id]' OR `id`= '$_COOKIE[user_id]'" or die(mysql_error());
```

This is an update injection, so we have to do something like:

```
mysql> update blah where id = lolhaxandstuff' or (select 1 ) = 1;
```

to get info out of it. Yay boolean enumeration!

If someone has a better way to do this please tell me.

Just noticed there's a dup thread because the mods moved the tutorial one into this section.

Guessing you're probably drunk and trying to admin the forum, so don't delete this one, guys.

Zixem - August 2, 2012, 1:54 pm

Well done ddos_king, nice find.
(just created brute force hehe)

~*Zixem

HaxOr? - August 2, 2012, 2:01 pm

Good, this exploit is AMAZING! :]

[img]http://img600.imageshack.us/img600/4152/regionla.png[/img]

Phizo - August 2, 2012, 9:04 pm

(Aug 2, 2012 01:23 PM)ddos_king Wrote: [\[CITE\]](#) And here it is! You can find this in hub.php
PHP Code

```
<?php
```

```
$query = mysql_query("SELECT * FROM `users` WHERE `id`='$_SESSION[user_id]`  
' AND `banned`=1") or die(mysql_error());
```

```
if (mysql_num_rows($query) > 0) {
```

```
    mysql_query("update `users`
```

```
        set `ckey`= ", `ctime`= "
```

```
        where `id`='$_SESSION[user_id]' OR `id` = '$_COOKIE[user_id]'" or die(mysql_error());
```

This is an update injection, so we have to do something like:

```
mysql> update blah where id = lolhaxandstuff' or (select 1) = 1;
```

to get info out of it. Yay boolean enumeration!

If someone has a better way to do this please tell me.

Just noticed there's a dup thread because the mods moved the tutorial one into this section.
Guessing you're probably drunk and trying to admin the forum, so don't delete this one, guys.

I think I might write a script to inject that after it's activated the account.

Starfall - August 2, 2012, 11:21 pm

Upon closer inspection by myself and Phizo, the injectable code seems to only run when you're banned, so you'll have to piss off the booter admin to actually be able to attack it.

I would recommend (read: I would absolutely not recommend) attacking the administrator's local government entities with his booter in order to do this.

And when I say closer inspection, I mean actually reading it.

I feel like an idiot now.

rvltr - August 3, 2012, 12:08 am

inurl:booter/register.php

gives back a few to test on ;)

Starfall - October 17, 2012, 2:43 pm

Thanks, rvltr.

Sorry to gravedig, but this is still pretty relevant. People still sell these on the HF marketplace and I've started looking into them some more. I'll post more findings here soon :D

Bacardi_temp - October 17, 2012, 2:57 pm

Pretty cool, and it seems to easy haha :D

mem0rex - October 17, 2012, 9:01 pm

lol that python script seemed to DoS the site I was trying it on...

Givenchy - October 17, 2012, 10:25 pm

Very nice!

Vouch for this men!

Everybody enjoy activation of your account

Phizo - October 17, 2012, 11:02 pm

(Oct 17, 2012 02:43 PM)Starfall Wrote: [\[CITE\]](#) Thanks, rvltr.

Sorry to gravedig, but this is still pretty relevant. People still sell these on the HF marketplace and I've started looking into them some more. I'll post more findings here soon :D

I also see people using and recommending it in the PHP section, oblivious of the potential outcome.

lakiluki - October 18, 2012, 7:39 am

<http://hacksociety.net/Thread-EXPLOIT-Get-free-access-to-Prodigy-shell-booters>

>#Credits to Aurora my Mate.

Didn't you discover the exploit? If so... I think the guy didn't give you any credit.

I'll just leave this here.

razem - October 19, 2012, 12:56 am

This is really cool, nice find Starfall. Still learning PHP, but know enough to read the code a bit. I'm gonna try to make my own brute-forcer. ?

Starfall - October 19, 2012, 4:47 pm

(Oct 17, 2012 09:01 PM)mem0rex Wrote: [\[CITE\]](#) lol that python script seemed to DoS the site I was trying it on...

Hahaha you got firewalled! I've had this problem before. Use your script with Torify or a large proxy list and you'll get in :3

(Oct 18, 2012 07:39 AM)lakiluki Wrote: [\[CITE\]](#)

<https://hackforums.net/Thread-EXPLOIT-Get-free-access-to-Prodigy-shell-booters>

>#Credits to Aurora my Mate.

Didn't you discover the exploit? If so... I think the guy didn't give you any credit.

I'll just leave this here.

I am Aurora if you check my name changes :P

Airon - October 21, 2012, 7:21 am

I'm gonna try this soon, thanks mate.