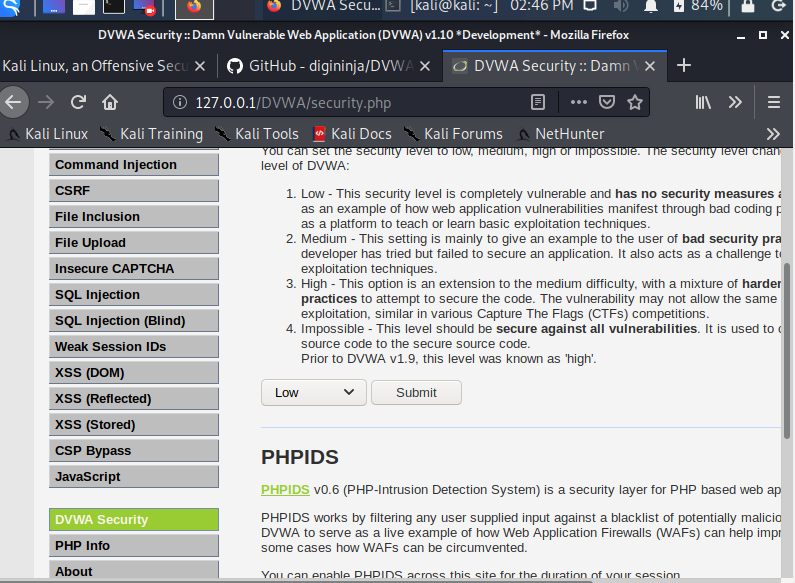
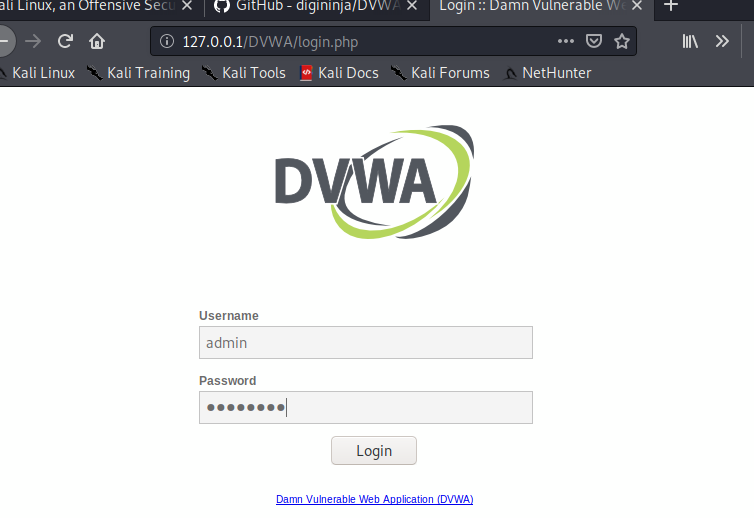
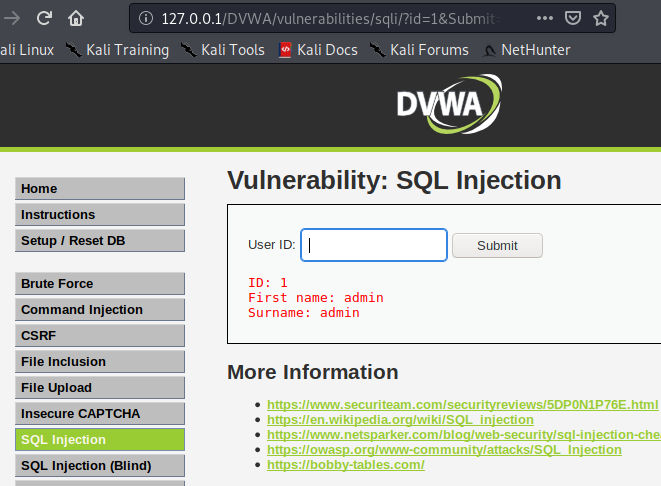
Lab 4

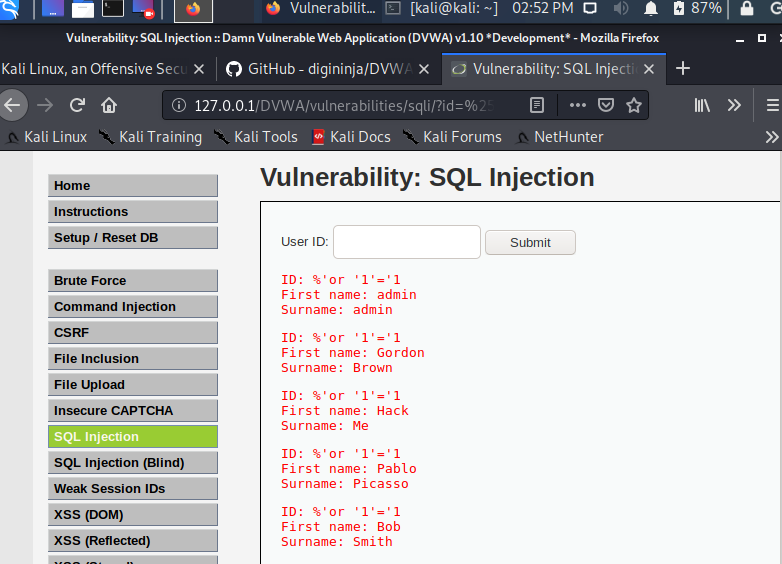
Initialization:

Login/ setting the security level low / try sql injection





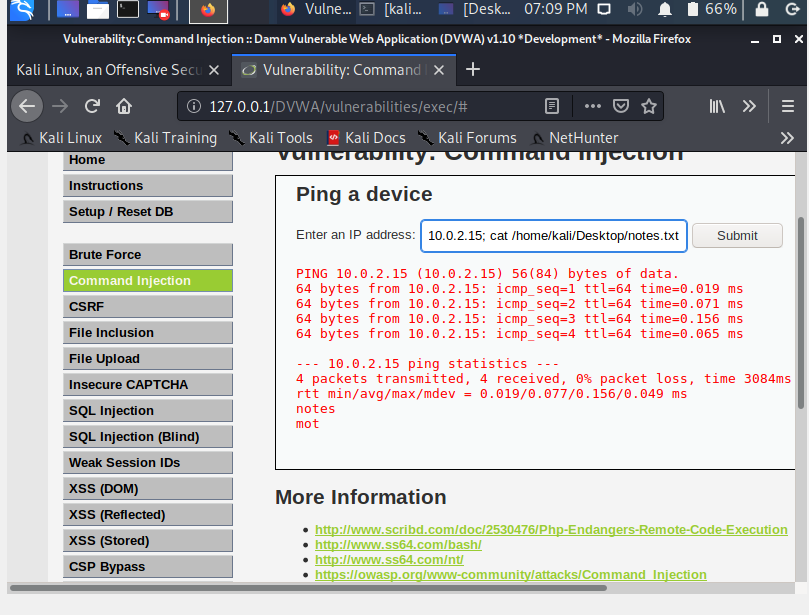
1-list of db users:



‘ or 1=1#

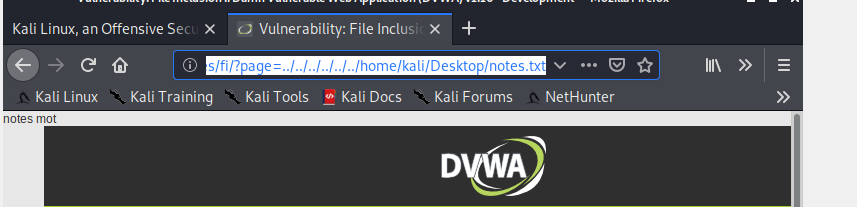
1' UNION SELECT 1,concat(user,":",password) From users;#

2-



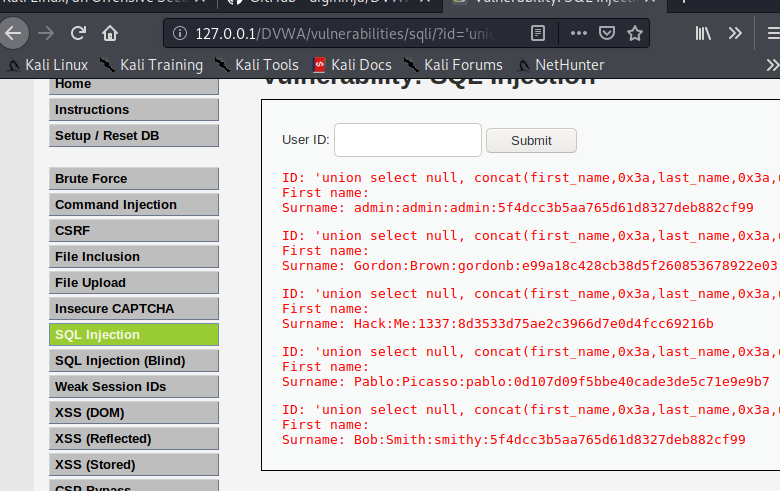
OR using file inclusion

url =127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../home/kali/Desktop/notes.txt

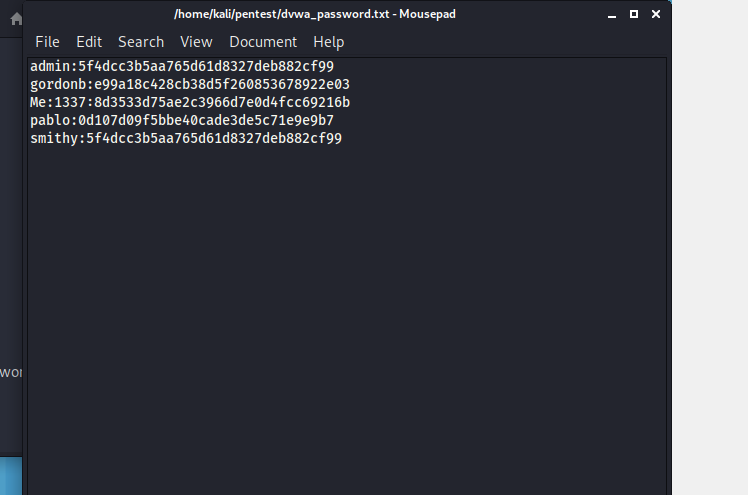


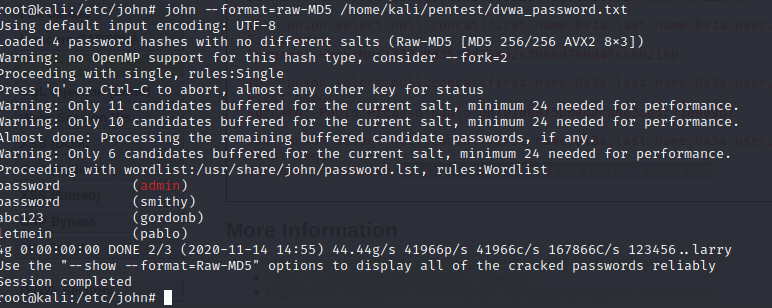
3- Display the logins and passwords of the users stored in the table

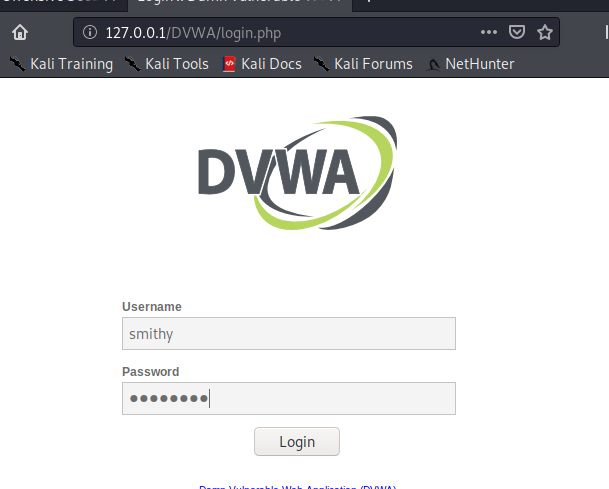
Command: ‘union select null. Concat(first\_name,0x3a,last\_name,0x3a,user,0x3a,password) from users --



4- The passwords thus recovered by SQL injections are “hashed” (Secure Hash). To be able to determine their values in clear, we will use the John the Ripper software

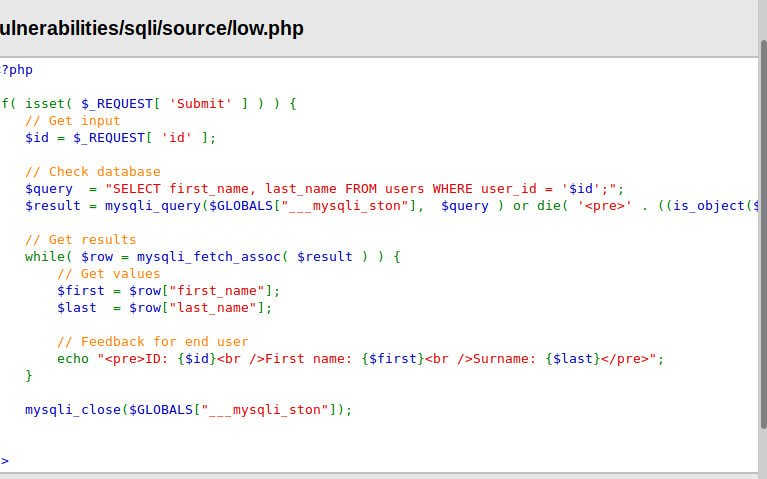






5- Now change the security level of the DVWA platform and put it in medium. How would it be possible to list the list of users by an SQL injection?

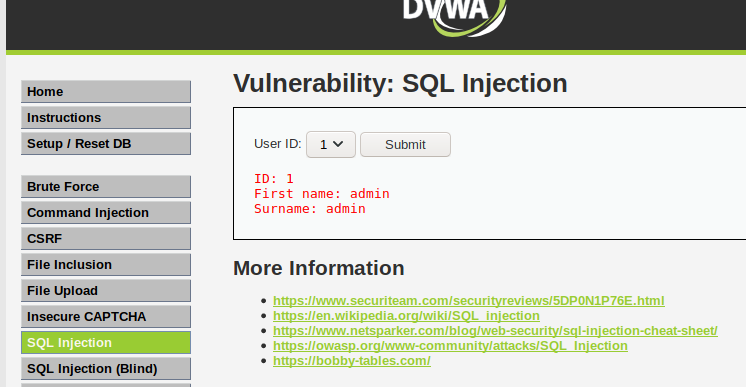
**Low:**

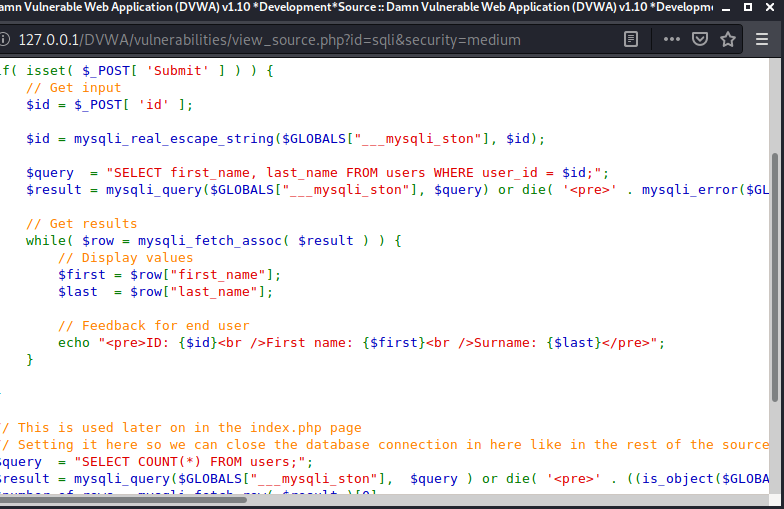
****

Executing the query as it is,without any validations no filters.

**Medium:**

It uses http post request and binding to the specific input options like in the pic below.

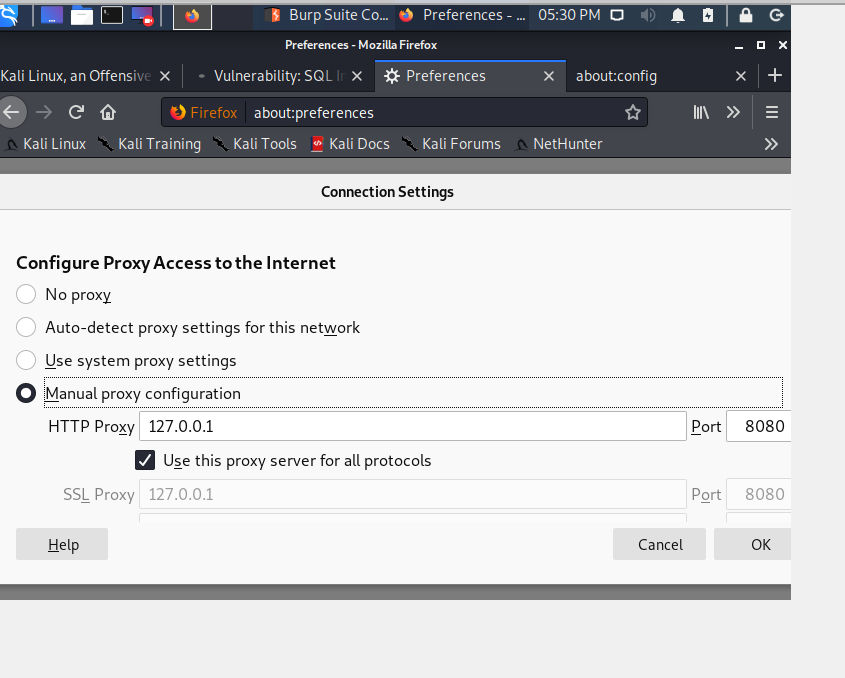


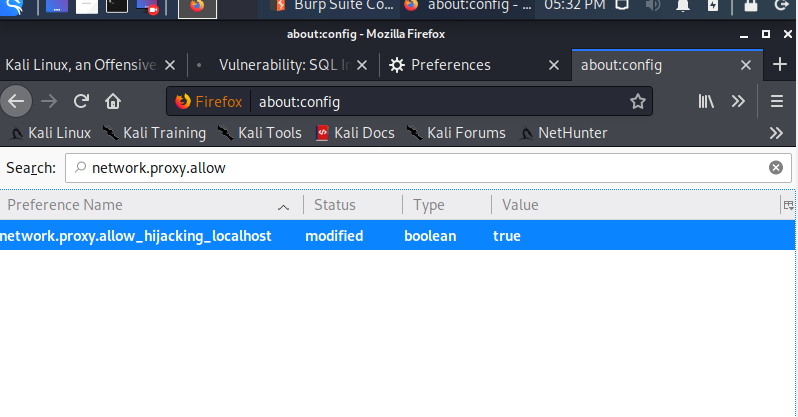


However using Burbsuite we can still display all users :

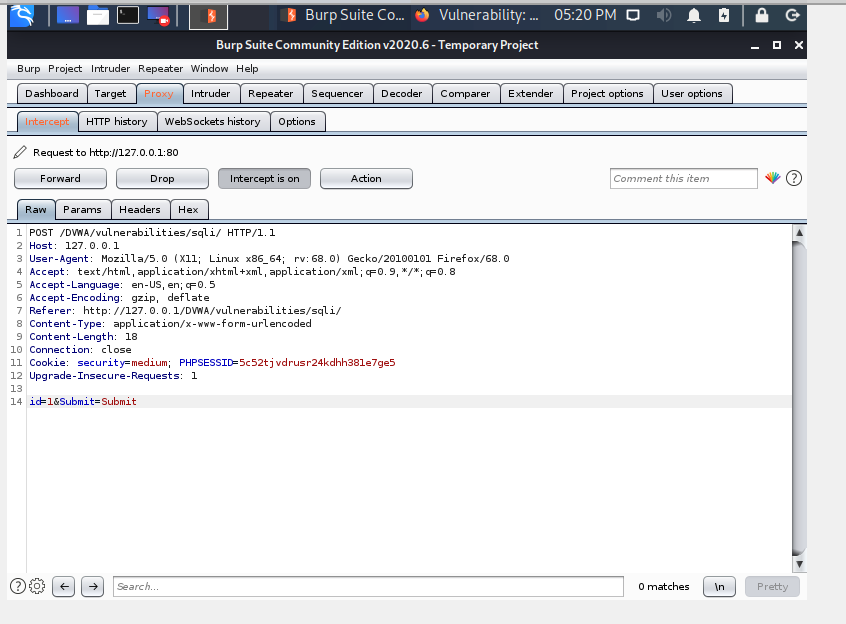
**To configure Burp suite with firewall:**

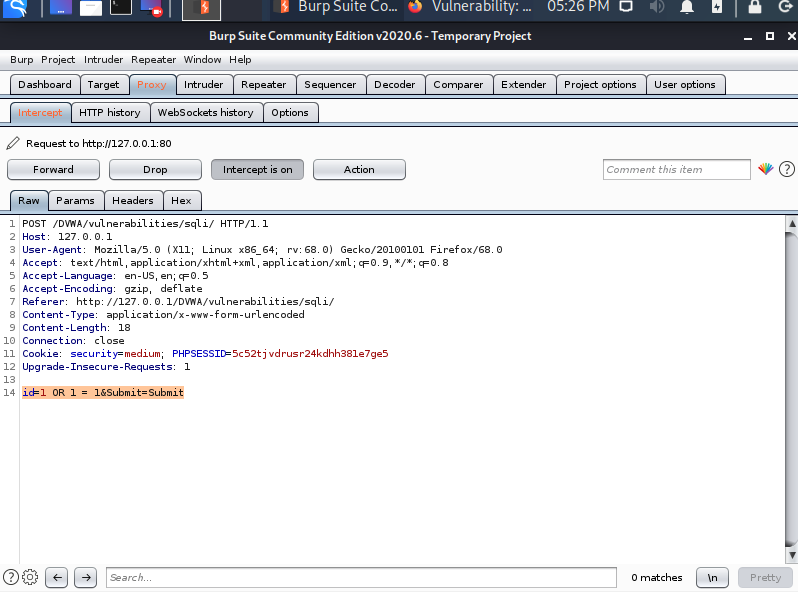
First enter network settings and configure it

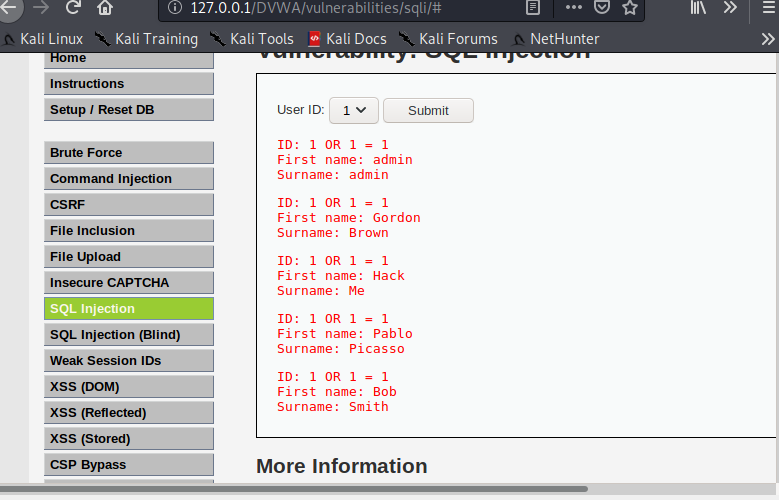
Second enter about:config in firefox search network proxy allow and change it to true



Capture the request:



Modify it and Forward to obtain list of users:



6- Now set the security level to High and check the source code of the corresponding page.

Uses a javascript to send a query

Add a limit to the outpu

