

TASK 15

# DVWA

SQL INJECTION

VARSHA M

SL No:	CONTENTS	PAGE NO:
1	INSTALL DVWA	3
2	SQL INJECTION(LOW)	6
3	SQL INJECTION(MEDIUM)	7
4	SQL INJECTION(HIGH)	9

# INSTALL DVWA

Cloned pentestlab.github .For installing DVWA docker is used

```
kali@kali: ~ - /pentestlab
File Actions Edit View Help
kali@kali: ~ x kali@kali: /var/www/html/dvwa/config x kali@kali: /var/www/html/dvwa/config x kali@kali: ~ x kali@kali: ~ /pentestlab x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ git clone https://github.com/eystsen/pentestlab.git
Cloning into 'pentestlab'...
remote: Enumerating objects: 153, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 153 (delta 7), reused 13 (delta 7), pack-reused 136 (from 1)
Receiving objects: 100% (153/153), 42.69 KiB | 615.00 KiB/s, done.
Resolving deltas: 100% (73/73), done.
(kali@kali)~$ cd pentestlab
(kali@kali)~/pentestlab$ ls
install_docker_kali_x64.sh pentestlab.sh README.md
(kali@kali)~/pentestlab$ ./pentestlab.sh lis
[sudo] password for kali:
Local PentestLab Management Script (Docker based)

Usage: ./pentestlab.sh {list|status|info|start|startpublic|stop} [projectname]

This scripts uses docker and hosts alias to make web apps available on localhost

Ex.
./pentestlab.sh list          List all available projects
./pentestlab.sh status       Show status for all projects
./pentestlab.sh start bwapp   Start project and make it available on localhost
./pentestlab.sh startpublic bwapp Start project and make it publicly available (to anyone with network connectivity to the machine)
./pentestlab.sh info bwapp   Show information about bwapp projejt

Dockerfiles from:
DVWA - Ryan Dewhurst (vulnerables/web-dvwa)
Mutillidae II - OWASP Project (citizenstig/nowasp)
bwapp - Rory McCune (raesene/bwapp)
Webgoat(s) - OWASP Project
Juice Shop - OWASP Project (bkimminich/juice-shop)
Vulnerable Wordpress - Custom made from github.com/wpscanteam/VulnerableWordpress
Security Ninjas - OpenDNS Security Ninjas AppSec Training
```

```
kali@kali: ~/pentestlab

File Actions Edit View Help

kali@kali: ~ x kali@kali: /var/www/html/dvwa/config x kali@kali: /var/www/html/dvwa/config x kali@kali: ~ x kali@kali: ~/pentestlab x

(kali@kali)~/pentestlab
$ ./pentestlab.sh start dvwa
Starting Damn Vulnerable Web Application
Adding dvwa to your /etc/hosts
127.8.0.1 dvwa was added successfully to /etc/hosts
not set
Running command: docker run --name dvwa -d -p 127.8.0.1:80:80 vulnerables/web-dvwa
Unable to find image 'vulnerables/web-dvwa:latest' locally
latest: Pulling from vulnerables/web-dvwa
3e17c6eae66c: Pull complete
0c57df616dbf: Pull complete
eb05d18be401: Pull complete
e9998e99102: Pull complete
2cd72da8257: Pull complete
6cff5f35147f: Pull complete
098cfff43466: Pull complete
b3d64a33242d: Pull complete
Digest: sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337daa7
Status: Downloaded newer image for vulnerables/web-dvwa:latest
7118f50114efaa906489c518e1278f60b07bb1d75a99c3a6d491c21467d9a706
docker: Error response from daemon: driver failed programming external connectivity on endpoint dvwa (05cd2d8f67d62e7959ed53ddfad26a63721771f4db5241747e828626c23ab3b8): Error starting userland proxy: listen tcp4 127.8.0.1:80: bind: address already in use.
DONE!

Docker mapped to http://dvwa or http://127.8.0.1

Default username/password: admin/password
Remember to click on the CREATE DATABASE Button before you start

(kali@kali)~/pentestlab
$
```

```
(kali@kali)~/pentestlab
$ ./pentestlab.sh start dvwa
Starting Damn Vulnerable Web Application
dvwa already exists in /etc/hosts
Running command: docker start dvwa
dvwa
DONE!

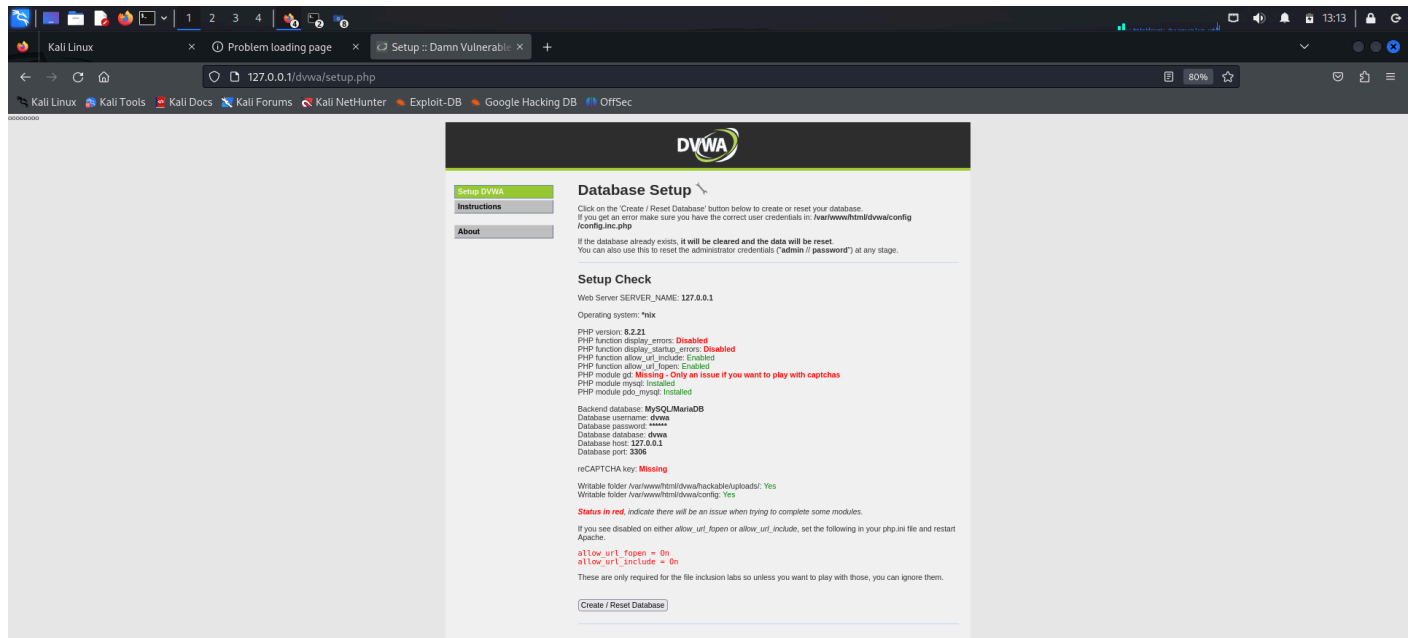
Docker mapped to http://dvwa or http://127.8.0.1

Default username/password: admin/password
Remember to click on the CREATE DATABASE Button before you start

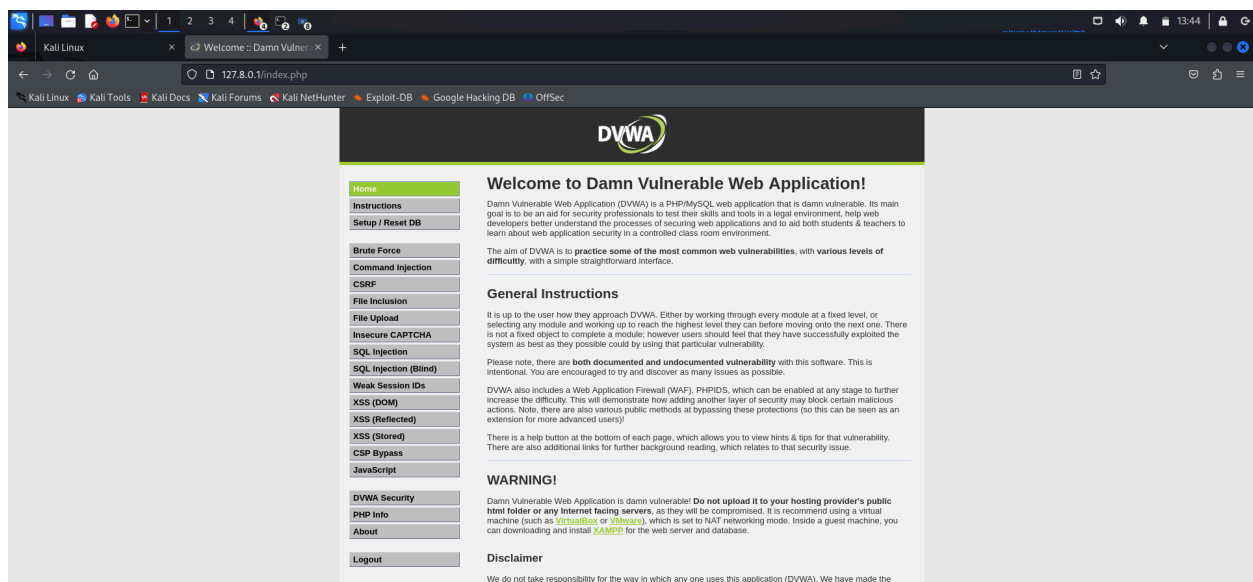
(kali@kali)~/pentestlab
$
```

Now we can access it via web browser at:

- <http://dvwa>
- <http://127.8.0.1>



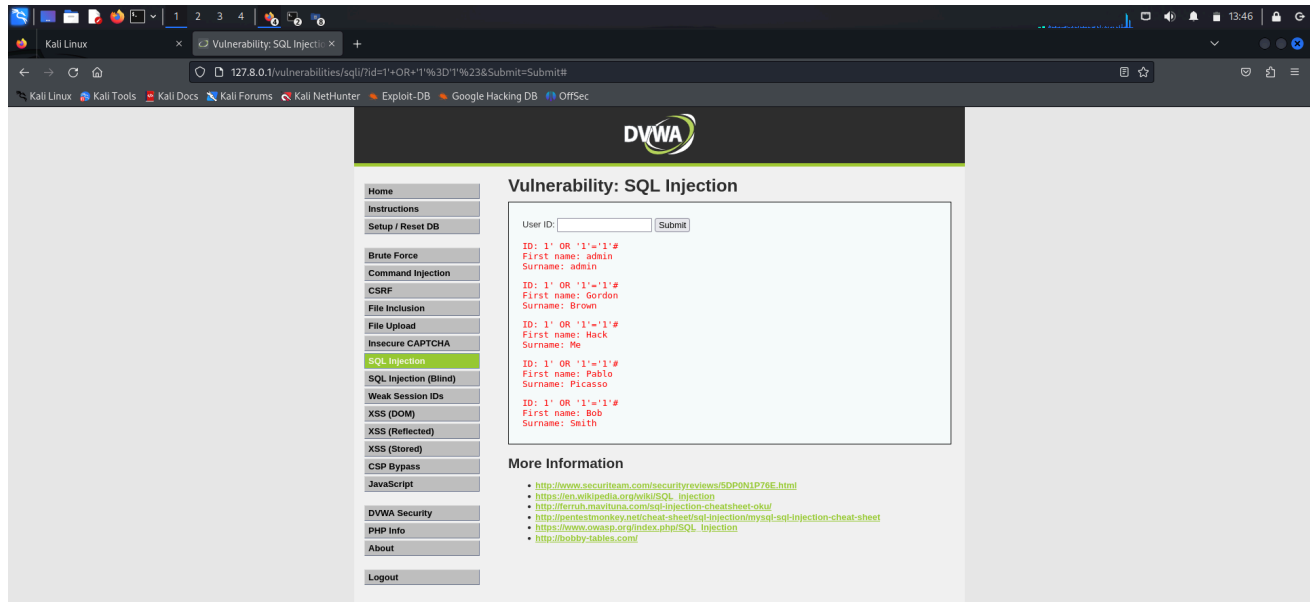
The default username is admin and password is password. Then in the next page you should be asked for reset your database. Click that button. Installation complete.



Then once again you will be redirected to login page, use the default credentials again. Then you will get to see this page.

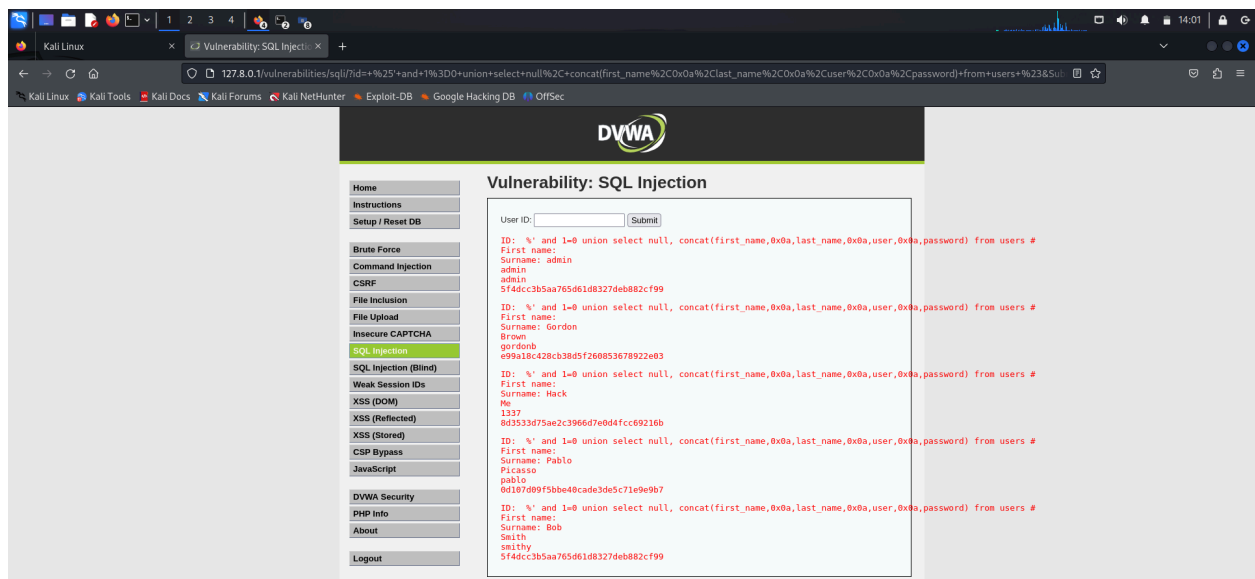
# SQL injection(low)

We can easily inject the code in the user ID form.



Using `1' OR '1'='1'#`, it is able to see first name and surname.

Using `%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`, Got the first and last names and cookies of the users.

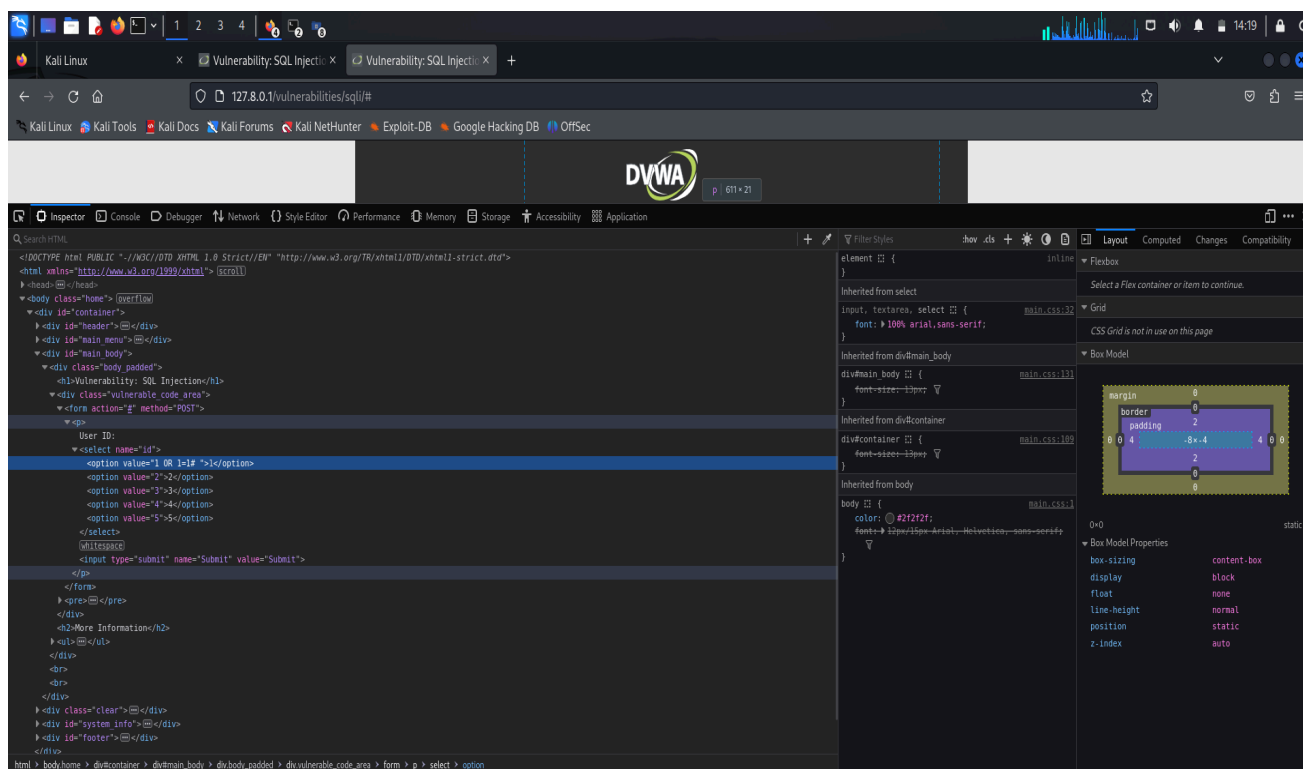


# SQL injection(medium)

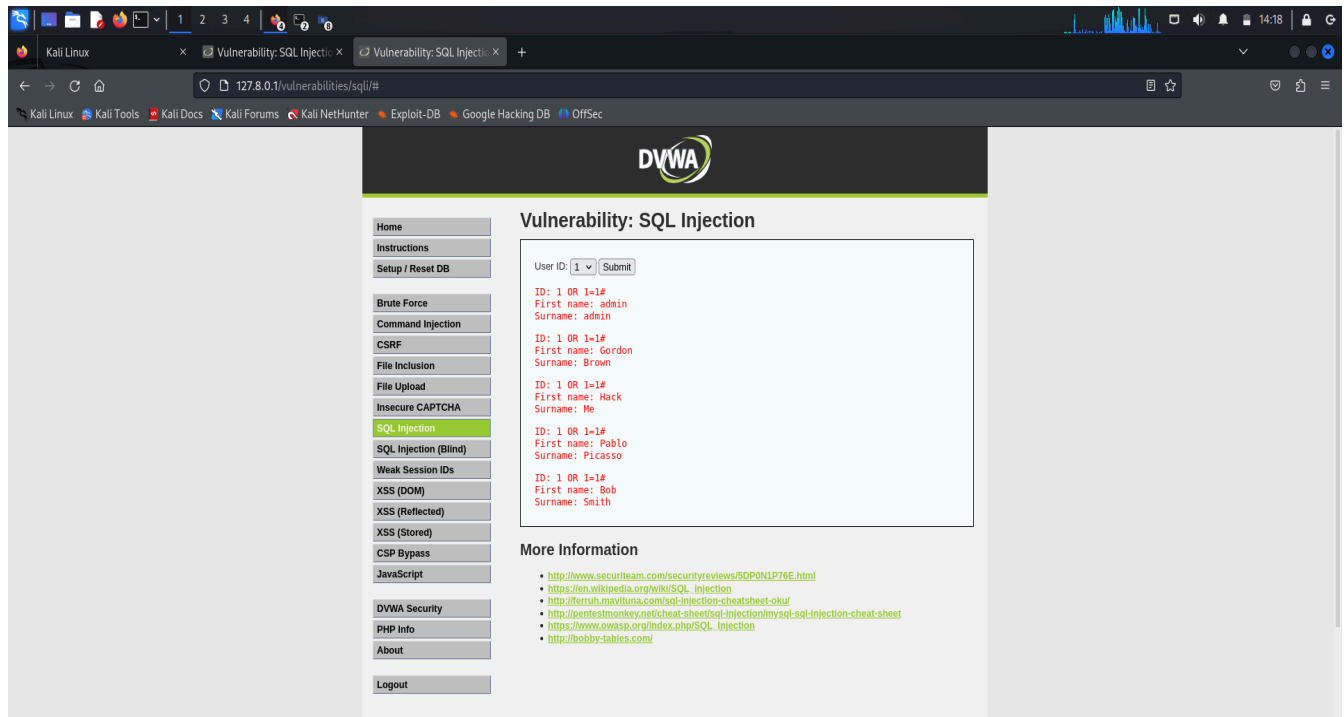
No comment options to inject in medium level.



Then i inspect the page after submitting the User ID as 1.Then injected OR 1=1#



command on any value of the userID button and then I clicked submit.

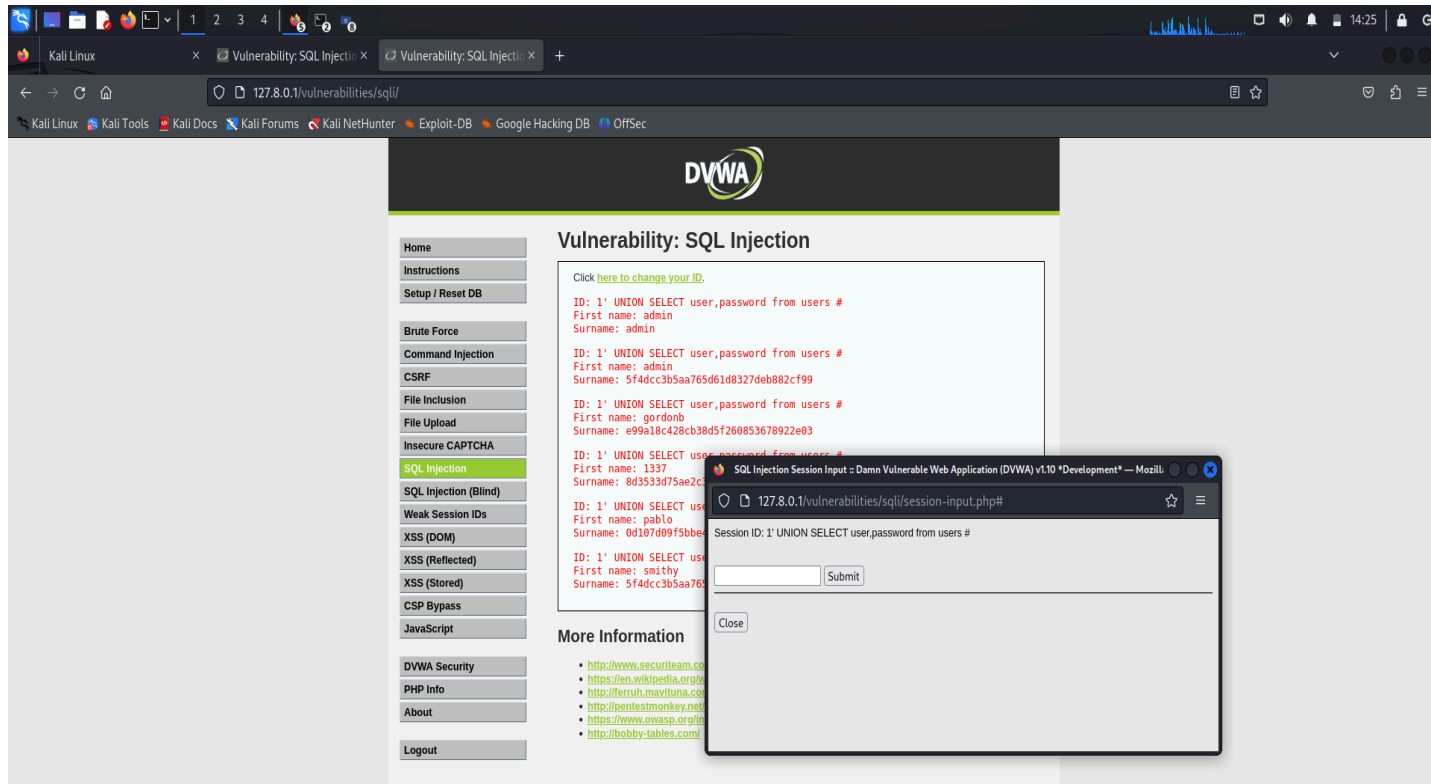


Able to see other users first name and last name.



# SQL injection(High)

In this phase clicking the link another window of a box to text session id is available.



Injecting **1' UNION SELECT user,password from users #** in the box.I got the first names and session cookies of the users.