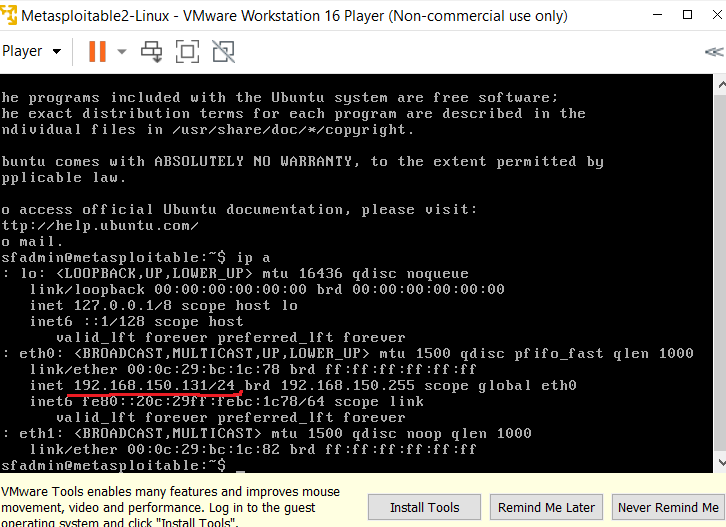
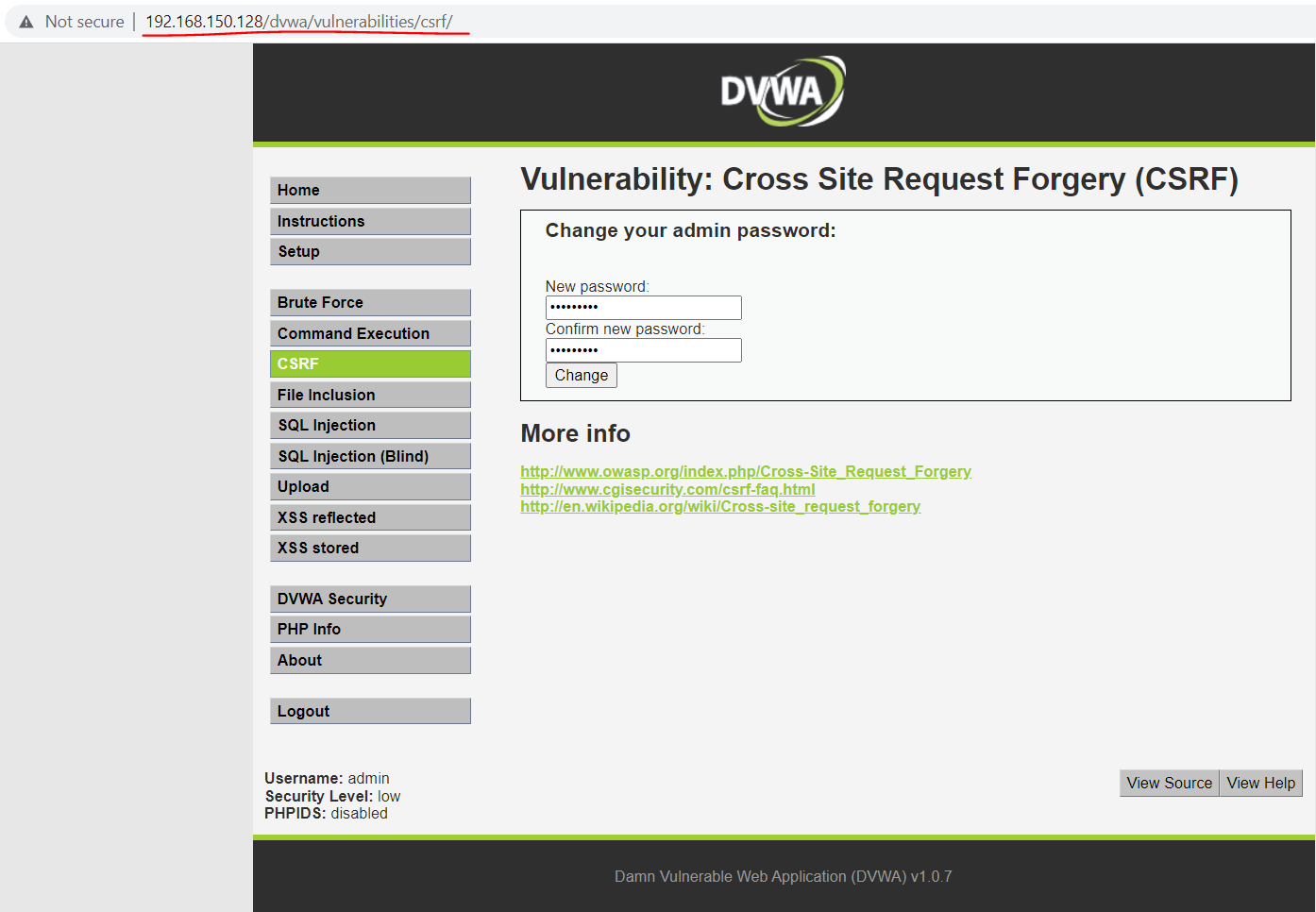
**Web application Security Project**

**Task 1**: Using your metasploitable VM, check for the ip settings. Let's say for example the IP address is 192.168.x.x Enter the IP address in the address bar in your browser. You will see the GUI of the metasploitable environment. Click on DVWA Tasks to be performed: 1. Privilege escalation 2. CSRF 3. SQL injection 4. XSS Document the above attack methodology and explain your findings. Make use of tools like Burp Suite, ZAP.

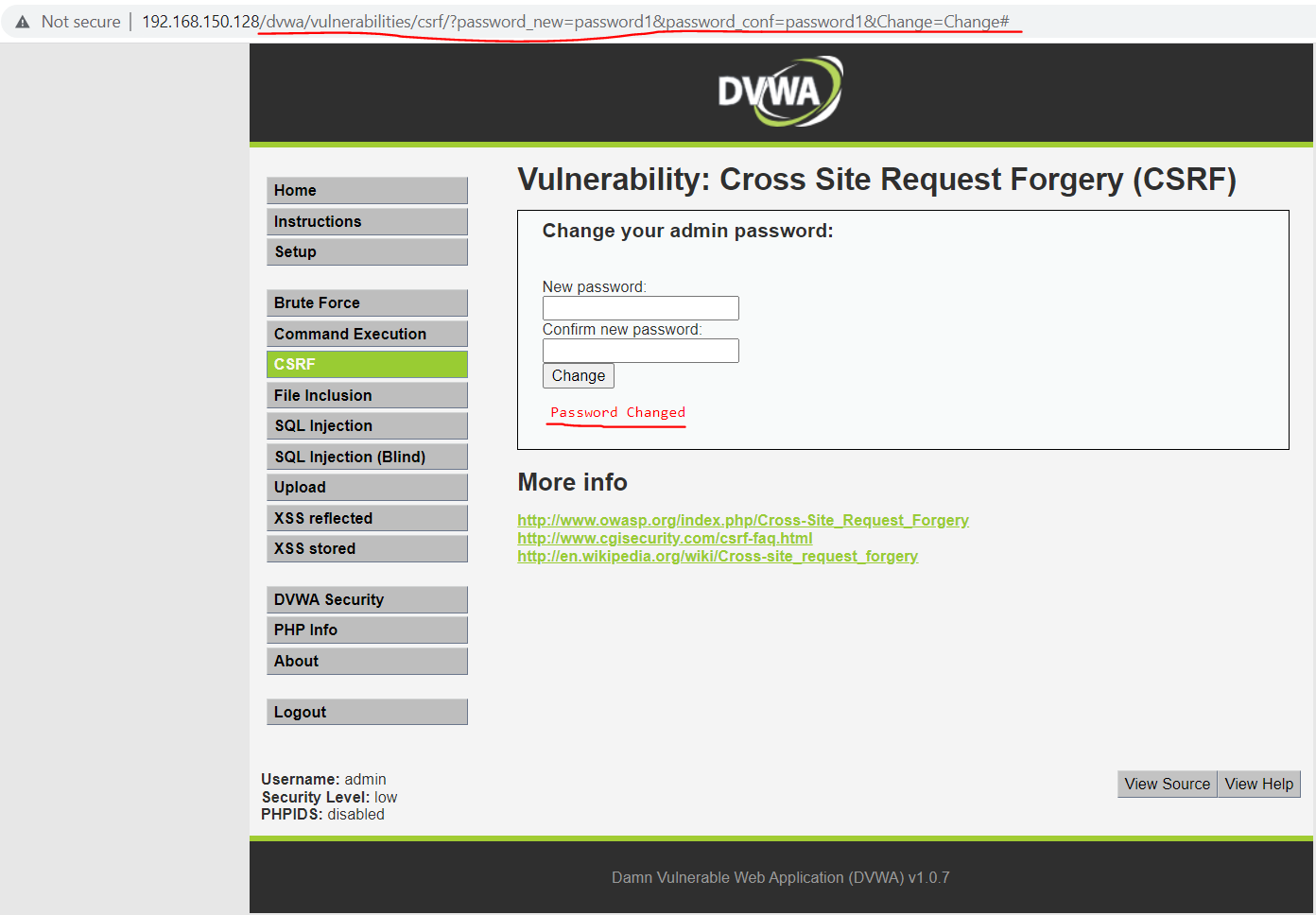


The IP address of my machine is **192.168.150.131**

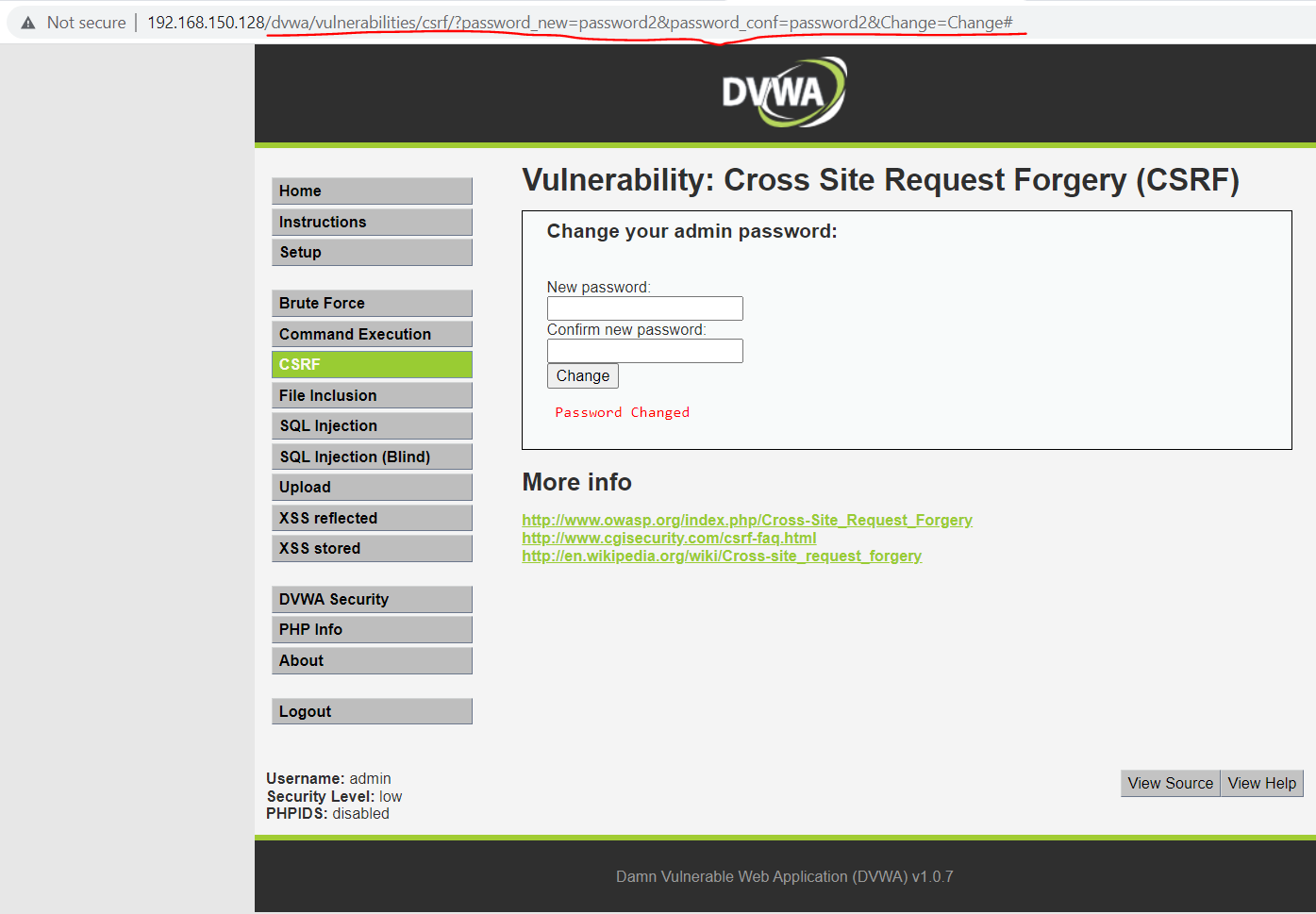
**2. CSRF**



Changing the password to password1.

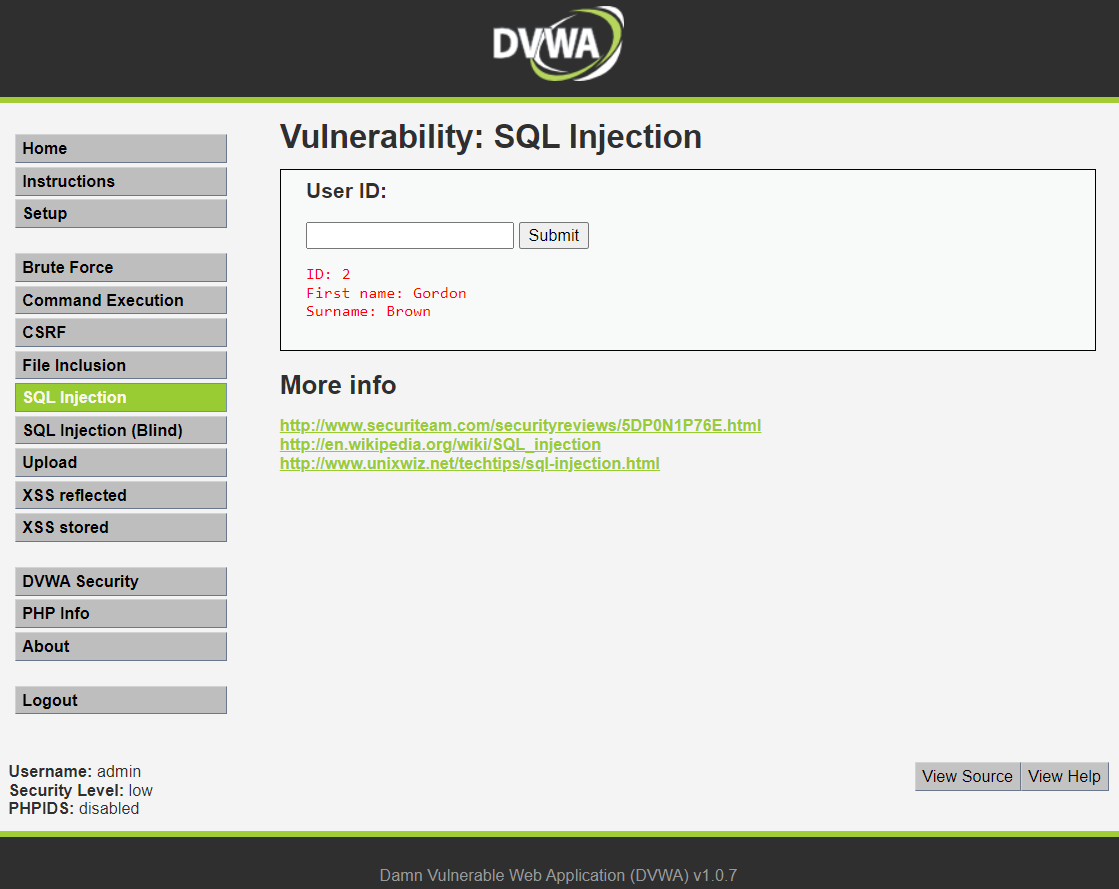


When I change the Password my URL gets changed. It is the input which is going back. It shows my new entered password and confirmed new password.

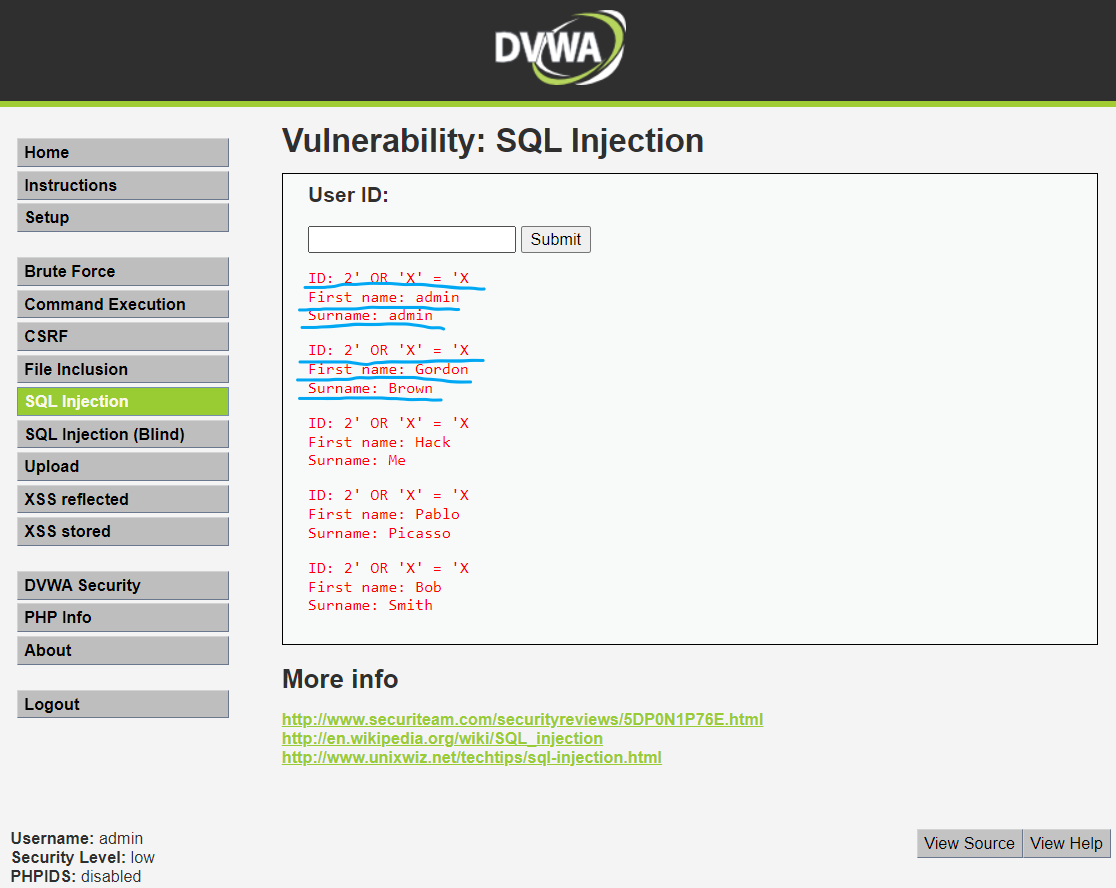


Copying and pasting the URL in other tab with some changes in the new password opens the same page.

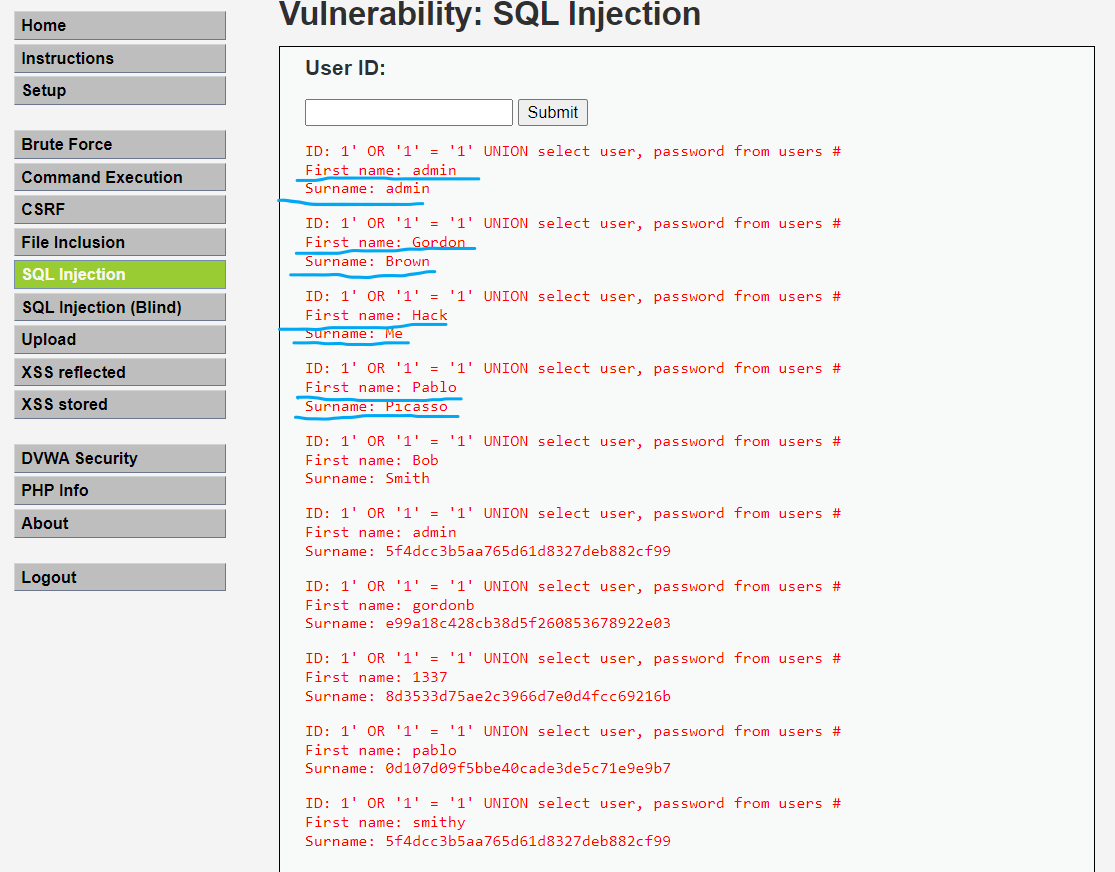
**3. SQL injection**

****

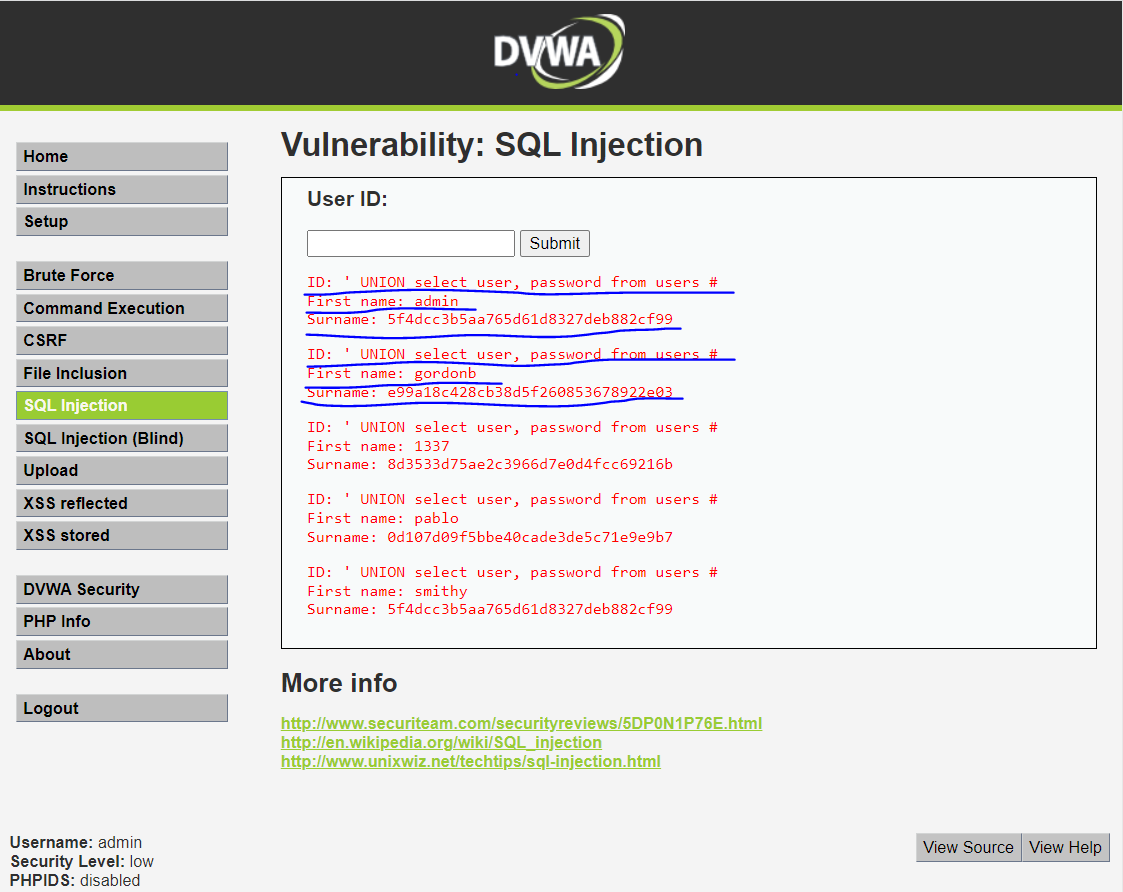
When I enter 2 it gives me the first name and the surname of ID 2.



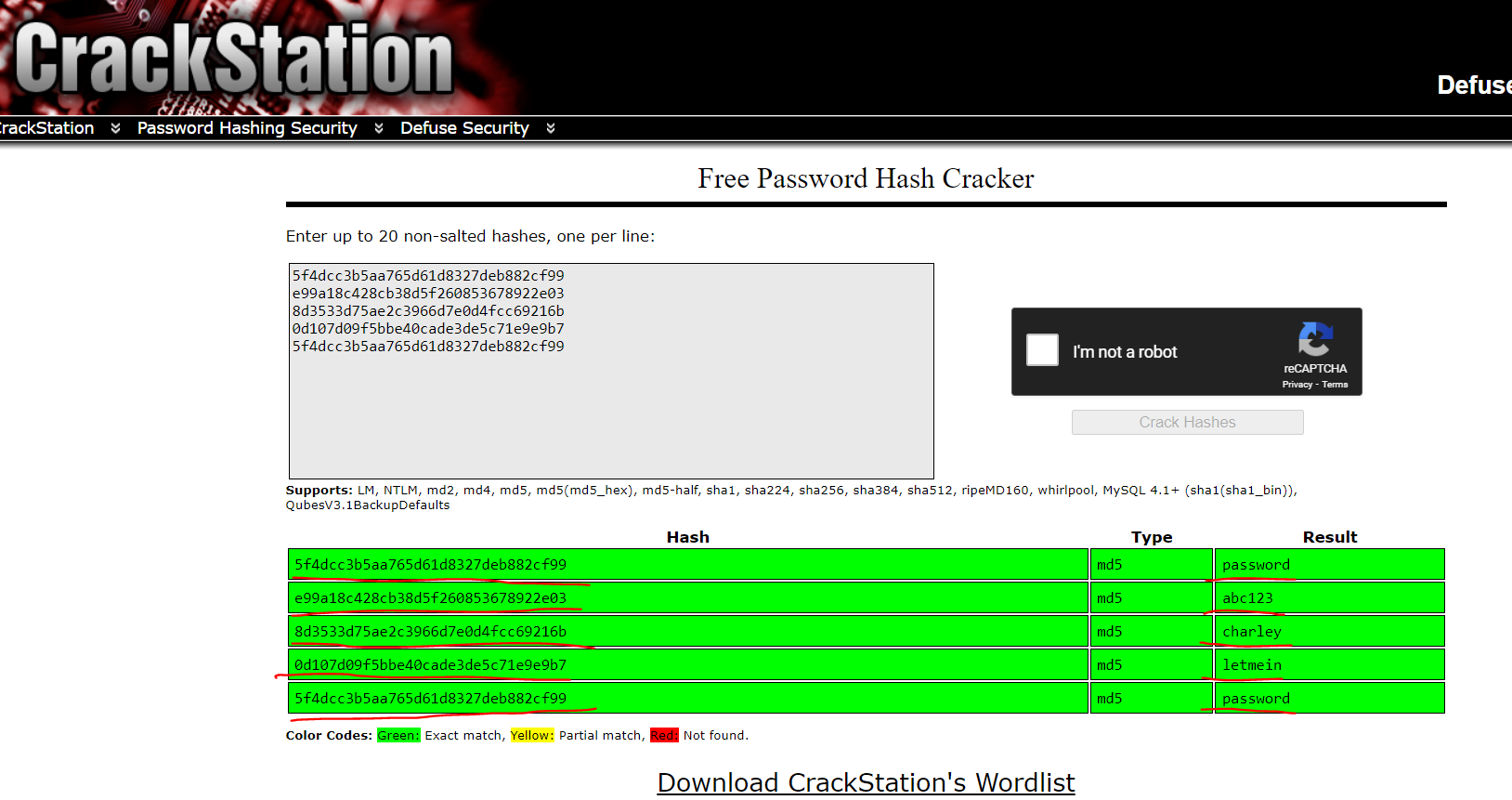
When I enter the condition **2’ OR ‘X’ = ‘X**, it gives me all the first name and surnames of the 5 users



To know Who is id number 1,2,3,4 and 5, I used the condition **1' OR '1' = '1' UNION select user, password from users #**

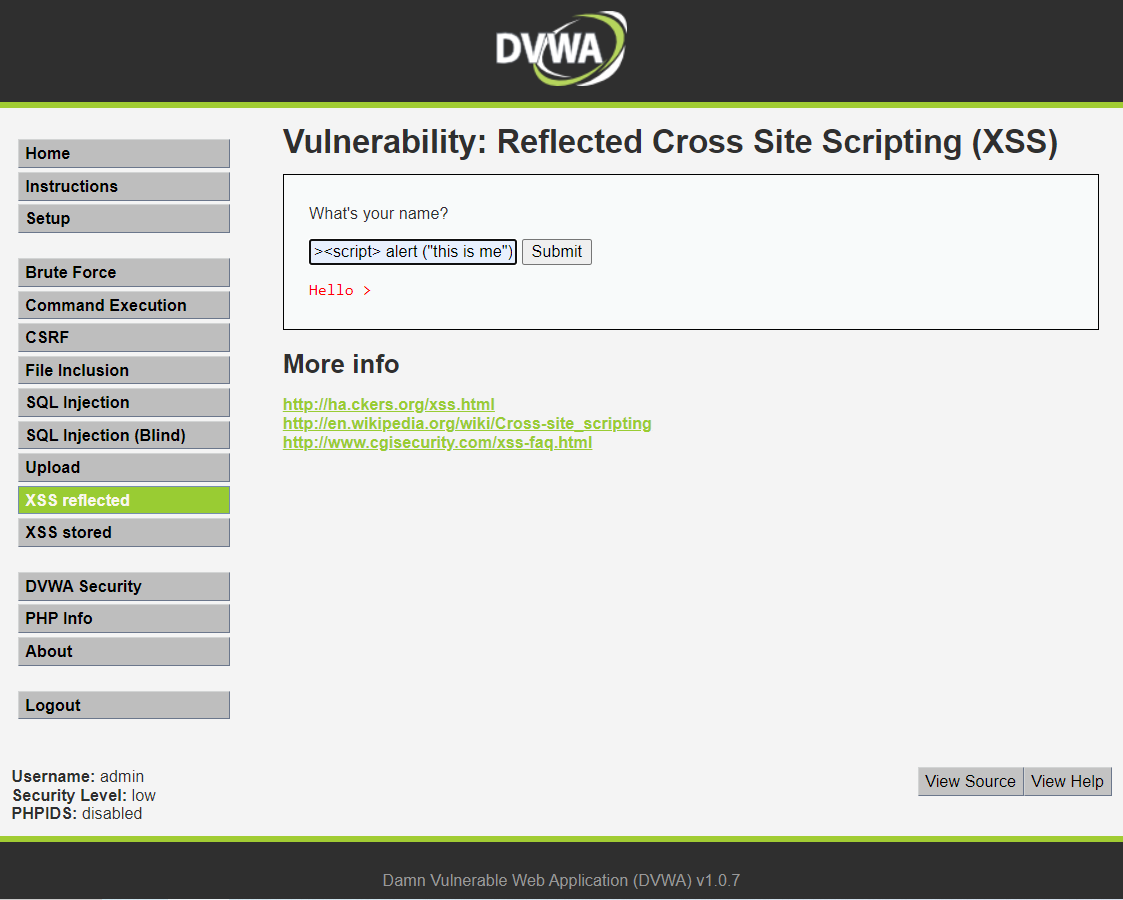


When I used the condition **' UNION select user, password from users #** It is also giving me passwords of those IDs

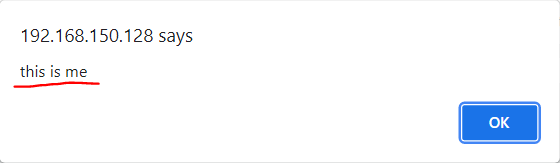


The passwords are in the hash form. To crack these passwords I used [www.crackstation.com](http://www.crackstation.com).

**4. XSS**

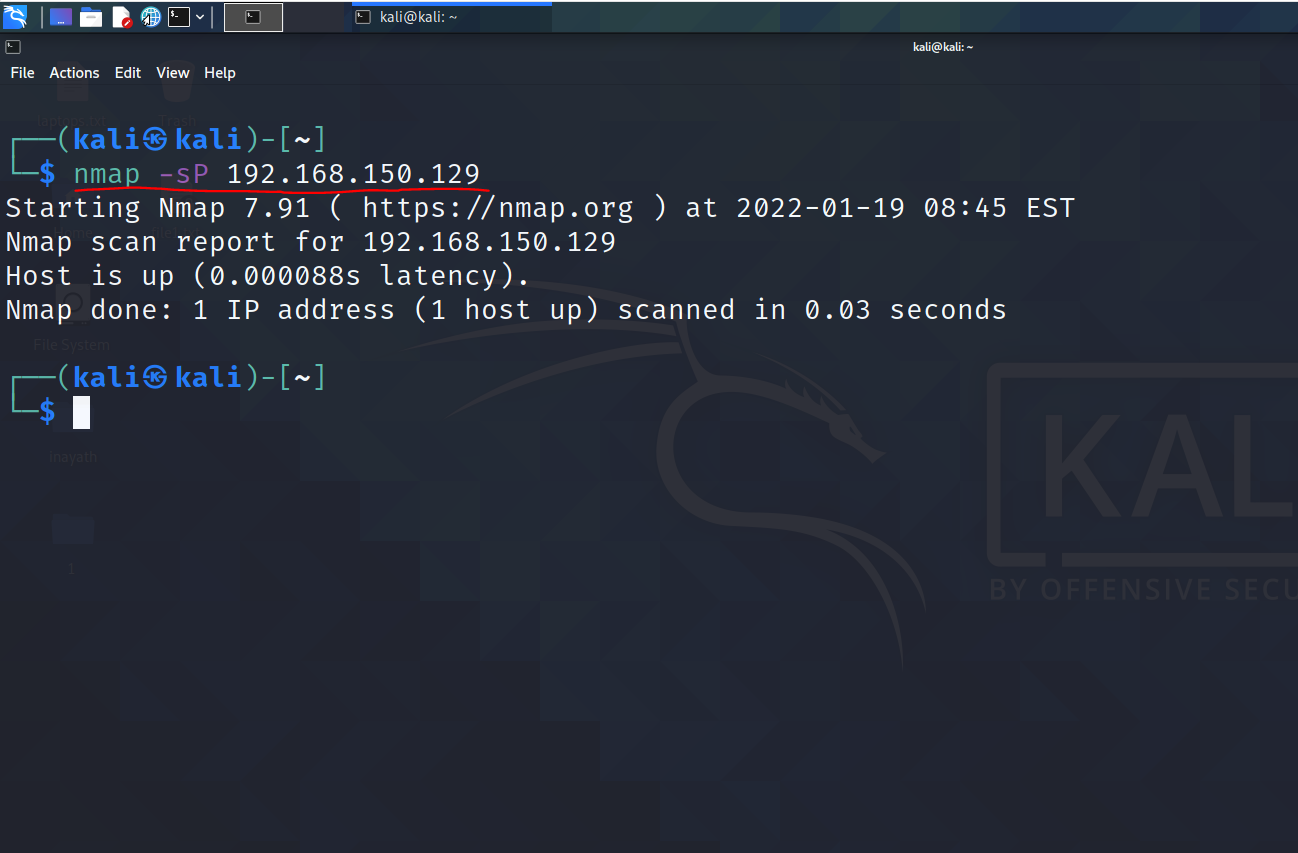
****

Entering PHP script as **><script> alert ("this is me") </script>**

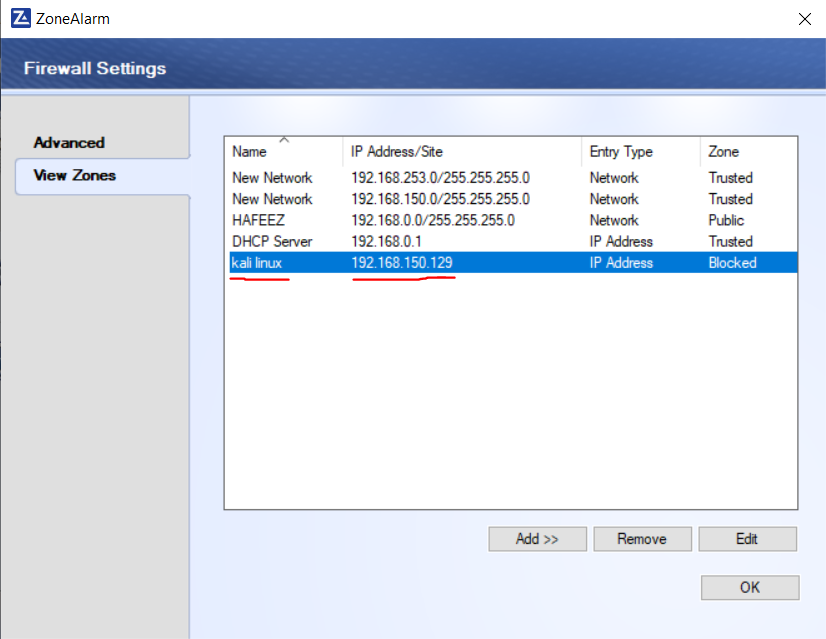


which pops up a message as “this is me”. This is called cross site scripting.

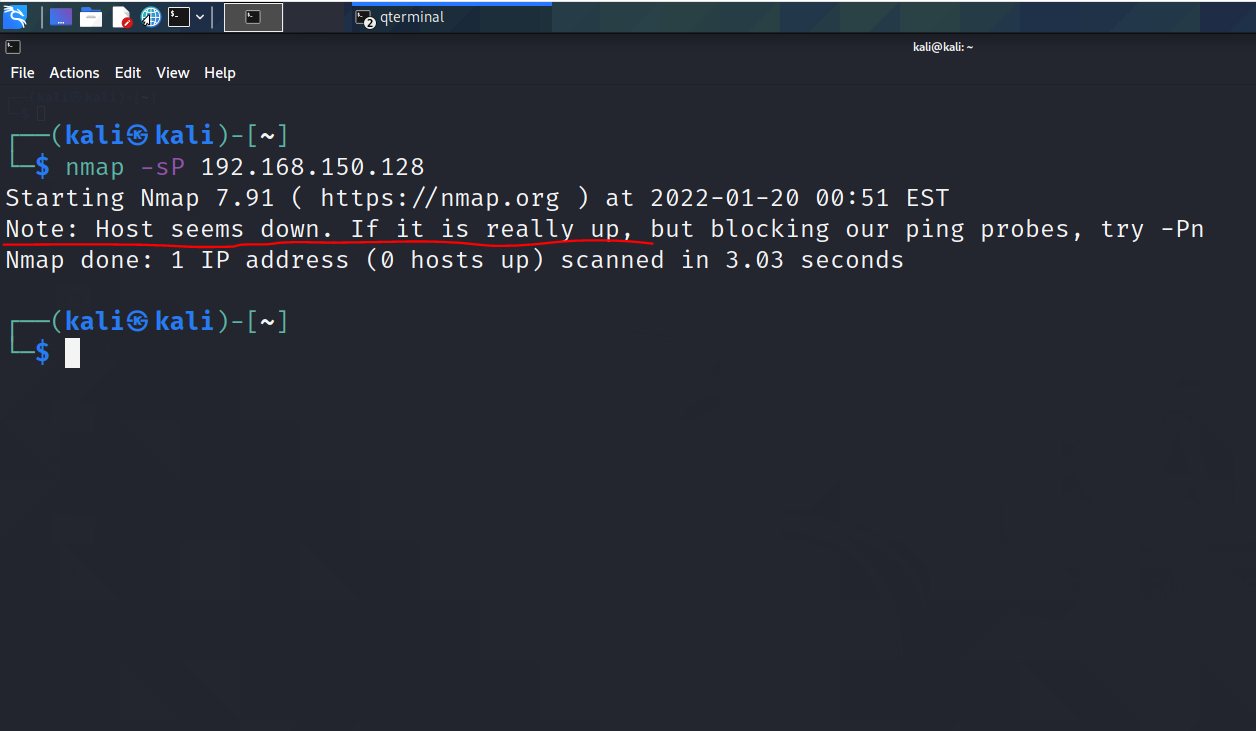
**Task 2**: Download and Install Zone Alarm firewall in your windows VM. ● Try performing a ping scan from kali linux.(You must be able to perform this.) ● Now open settings in the Zone alarm firewall go to Advanced settings>zones>add host. ● Add kali linux Ip address and from the drop down select block. ● Now try pinging the windows VM. (You shouldnt be able to ping). ● Go to tool>logs. You should be able to identify all the logs made by the firewall. Take a screenshot of both the logs and the kali terminal where ping cannot be done.



The command I have used for ping scan for the IP address is **nmap -sp 192.168.150.129.**

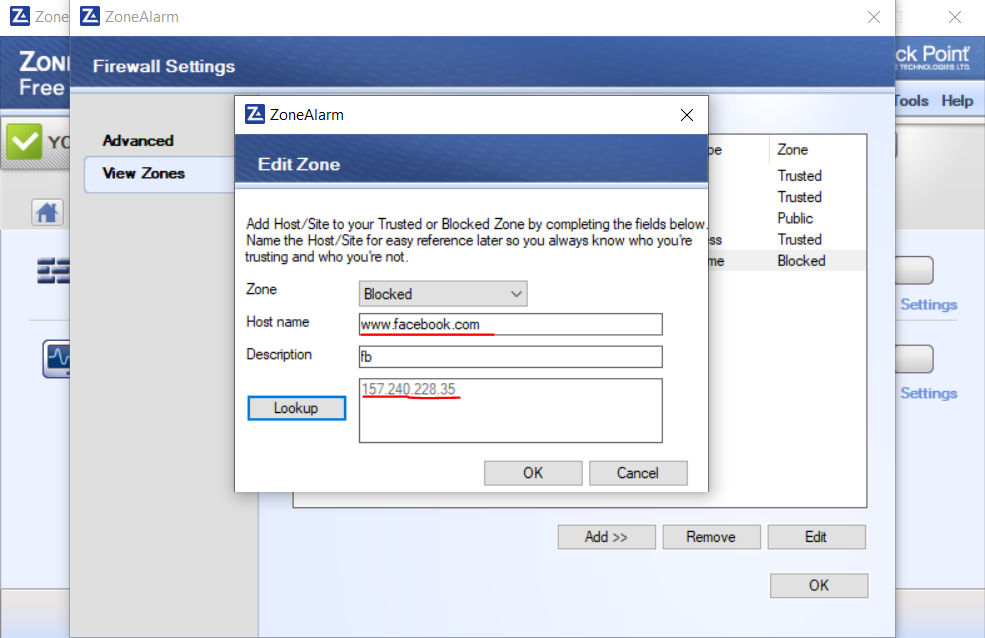
****

I have added IP address of my kali linux and blocked it.

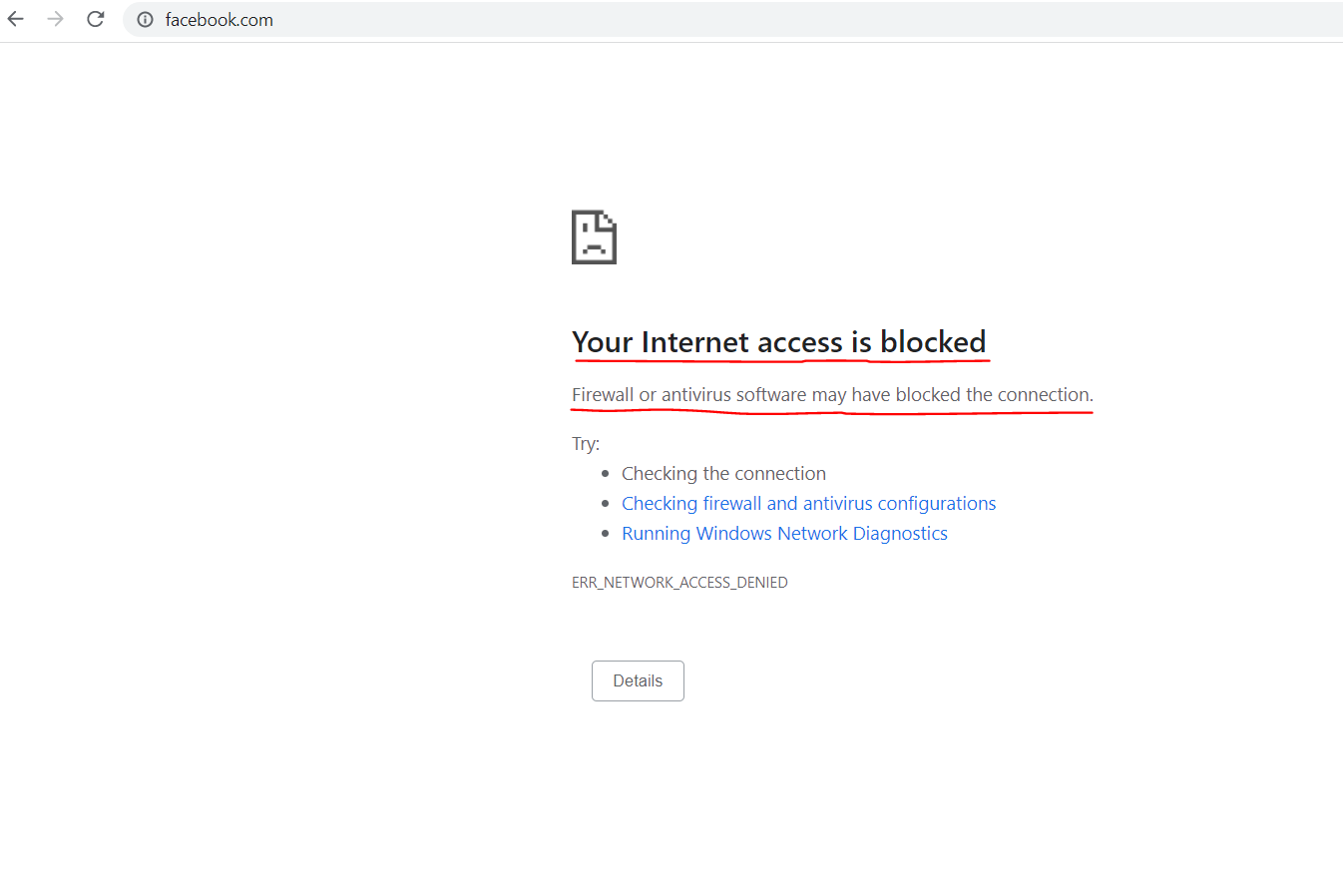


The highlights show that the host seems to be down.

I have done this by opening my zone alarm firewall>firewall tab>view zones>add IP address then added the IP address of my kali machine and set the zone to blocked.



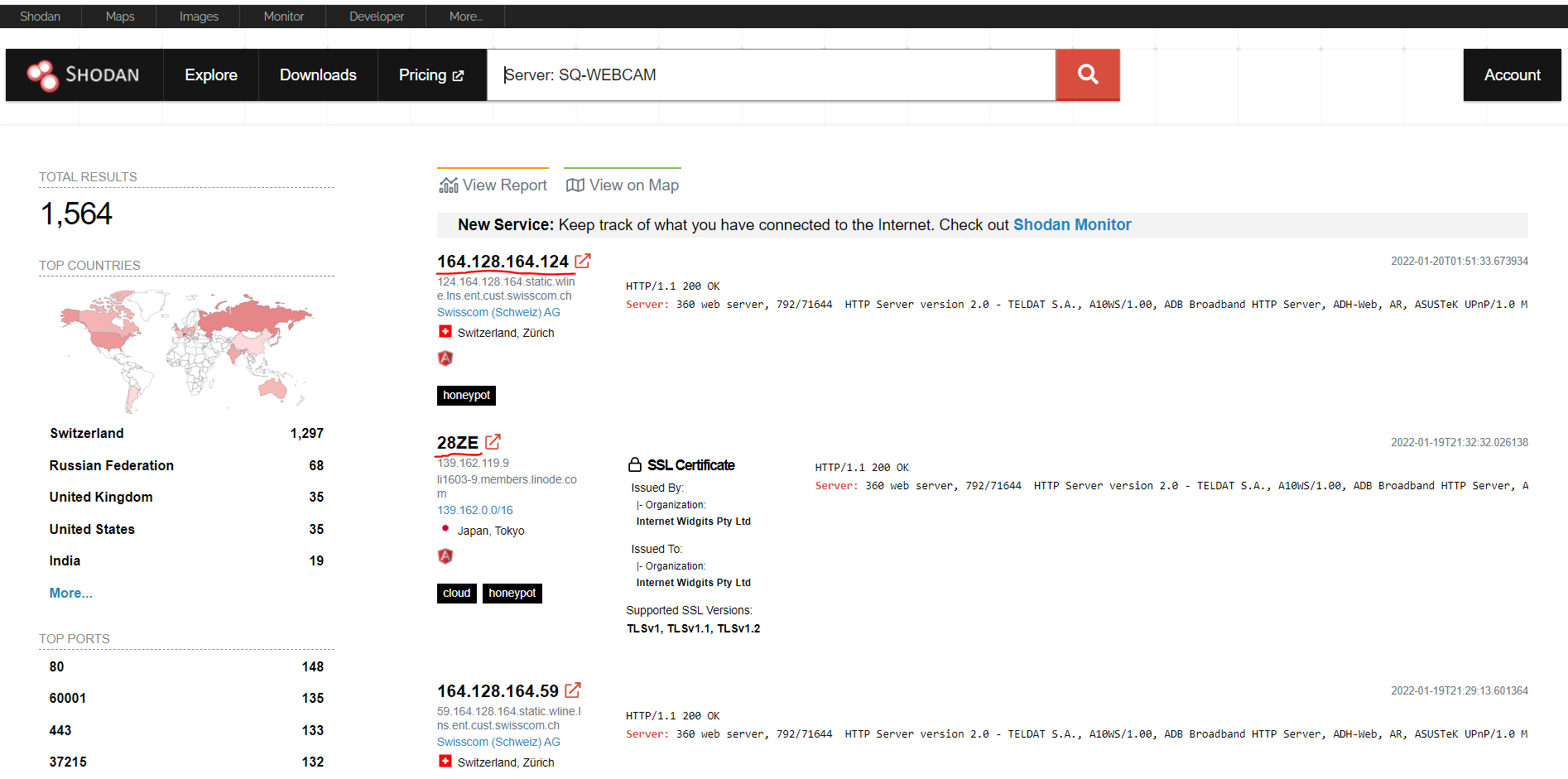
I have added Facebook website URL to the block list.



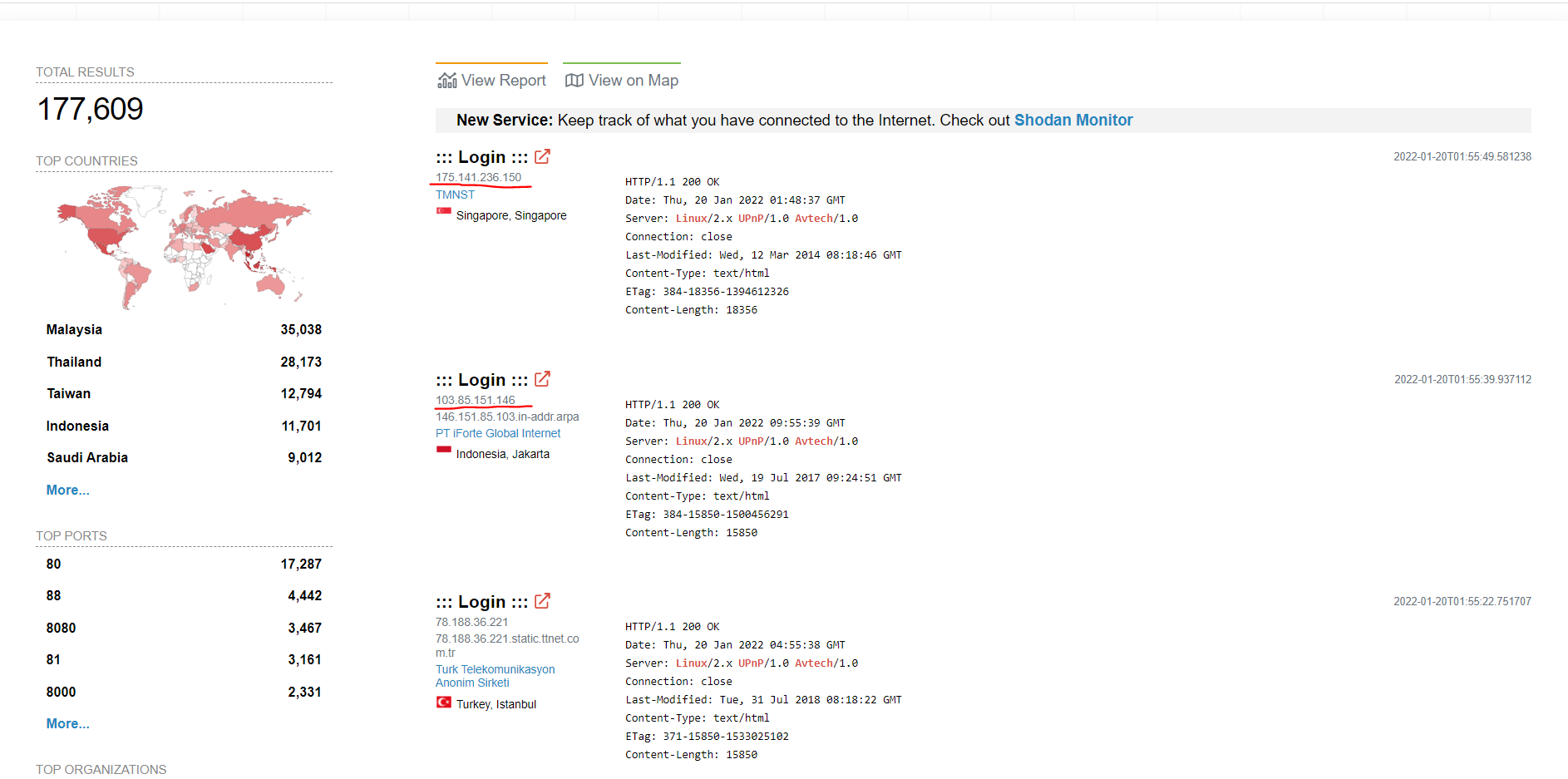
When I access [www.facebook.com](http://www.facebook.com) from my browser it cannot be accessed.

I have done this by opening my zone alarm firewall>firewall tab>view zones>add host then added the website URL and set the zone to blocked.

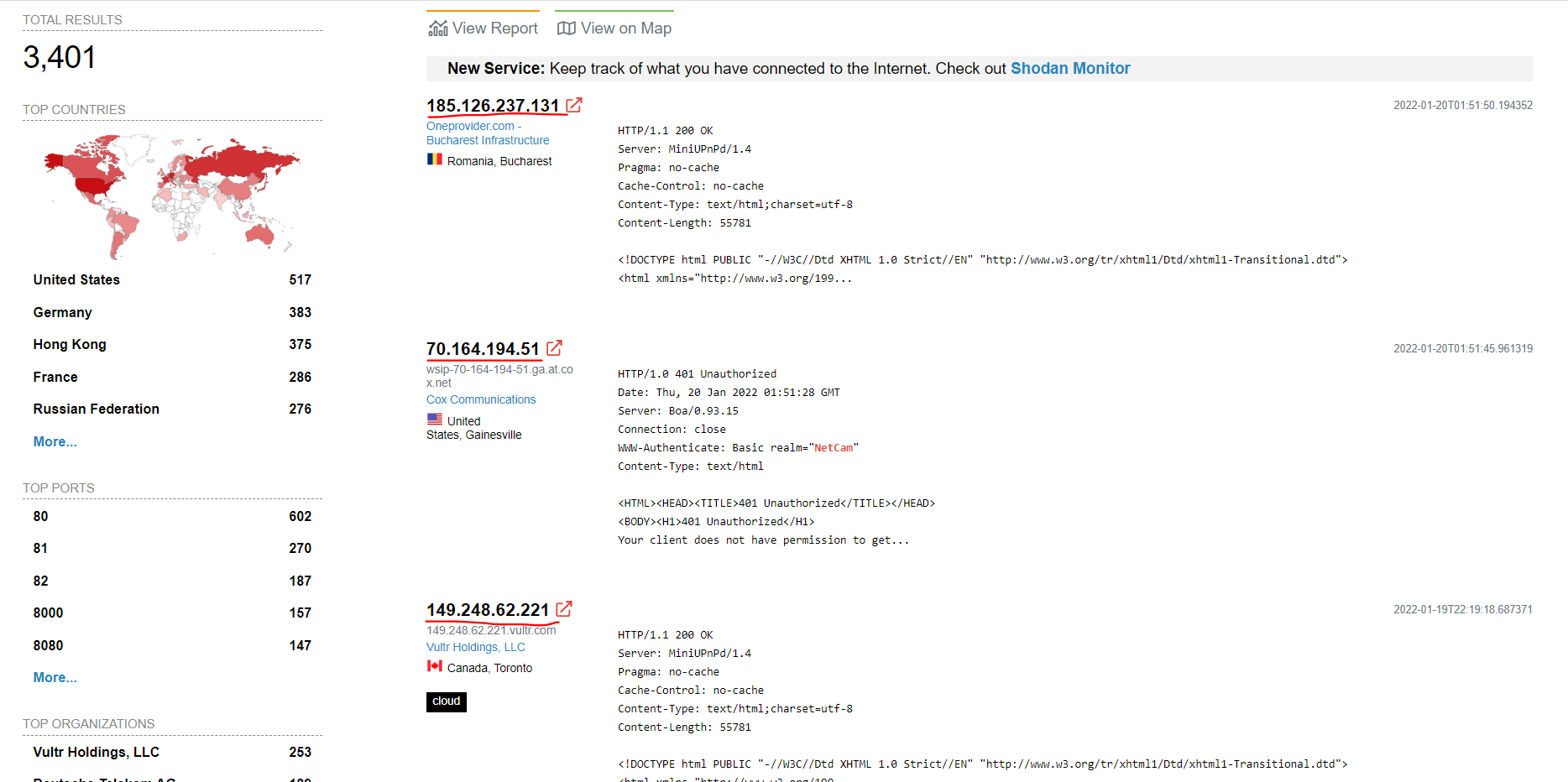
**Task 3:** With the help of Shodan, try to find as many vulnerable webcams across the globe. Include screenshots. Also use shodan to show how it can detect the presence of a web application firewall in a particular website. (Examples : Amazon EC2, Cloudflare etc.)



The highlights show best open IP cams I have found.



The highlights show different vulnerable cams across the globe.



The highlights show the different netcams that are vulnerable around the globe.