**IT LAB EXPERIMENT -9**

**MAN IN MIDDLE ATTACK**

STEP 1

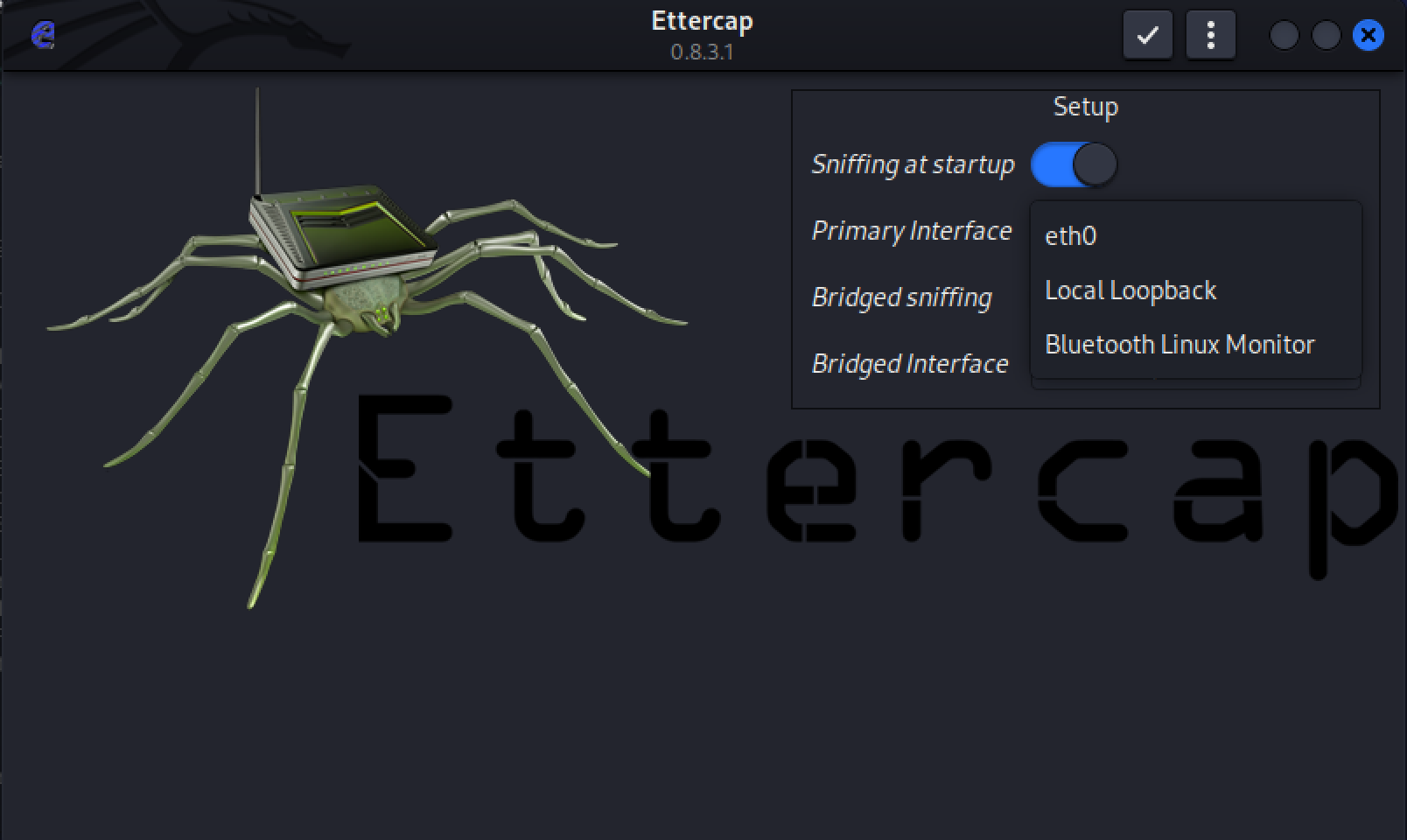
Start ettercap but first see the help file for ettercap by

Ettecap -h



Now we start ettercap by :

Ettercap -G

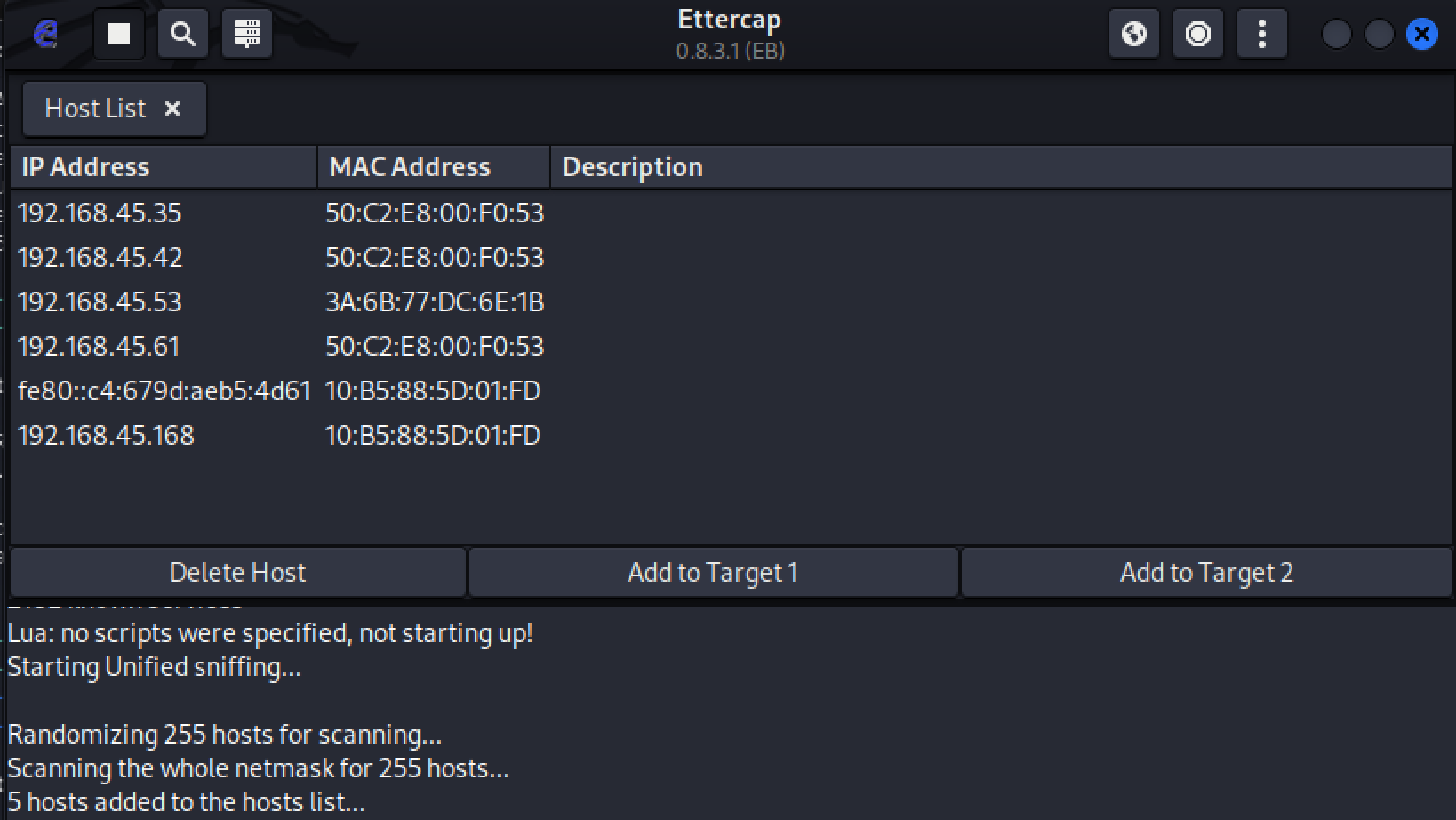


First step is to start an MiTM attack is to start sniffing .

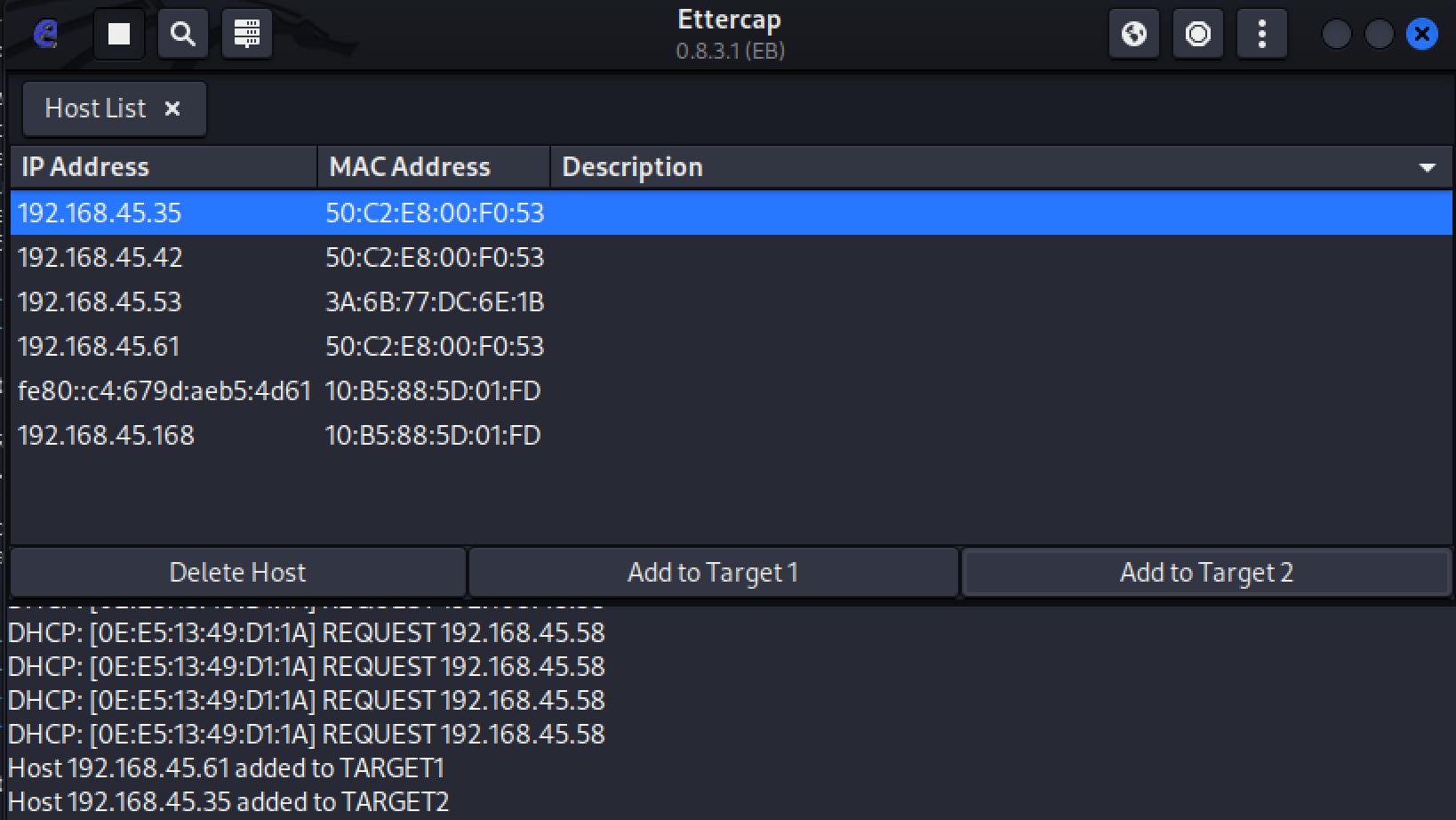
Go to the menu that says sniff and click on unified Sniffing

And click on host tab and select “ scan for host “, now ettercap will start to scan

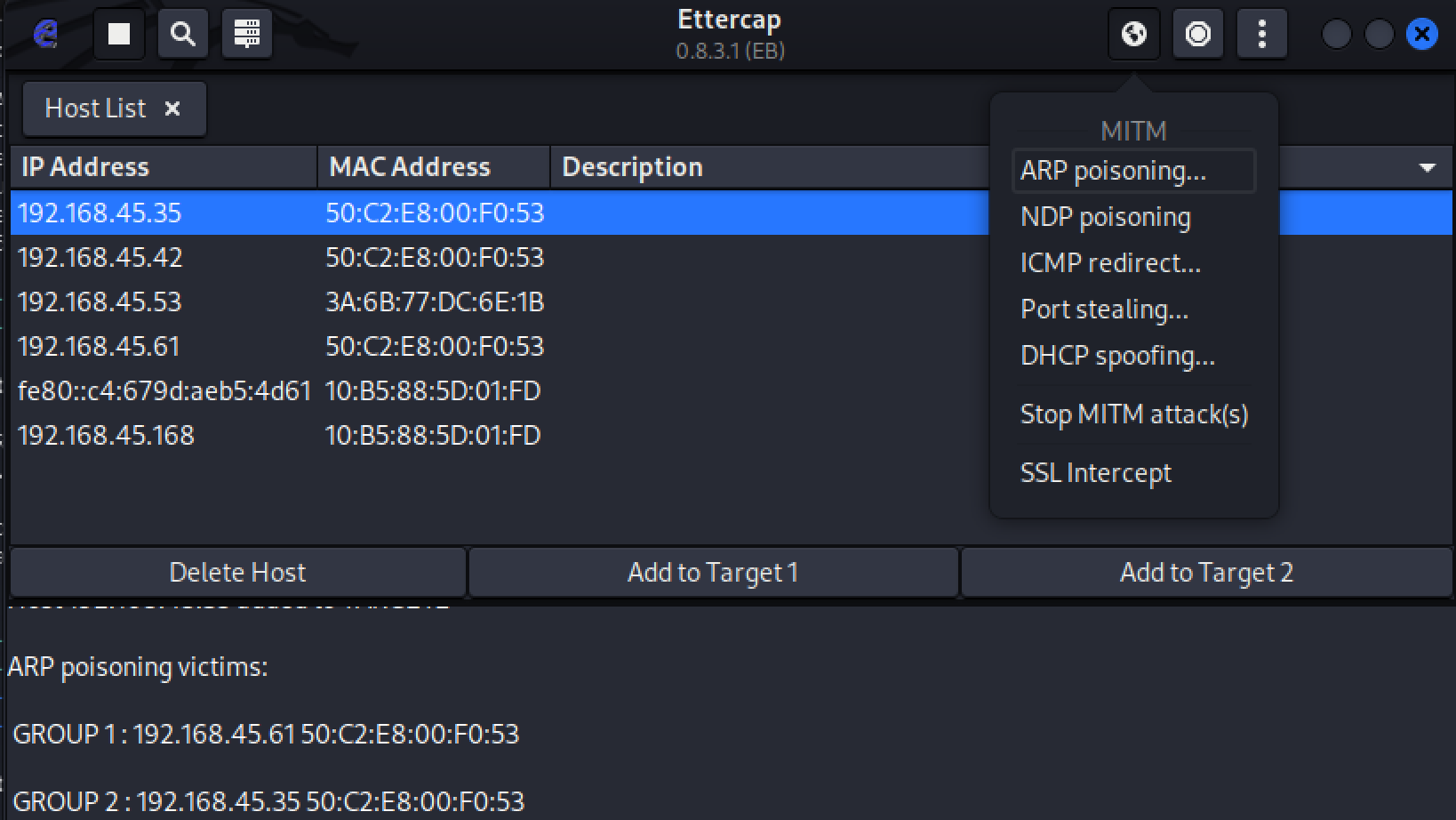




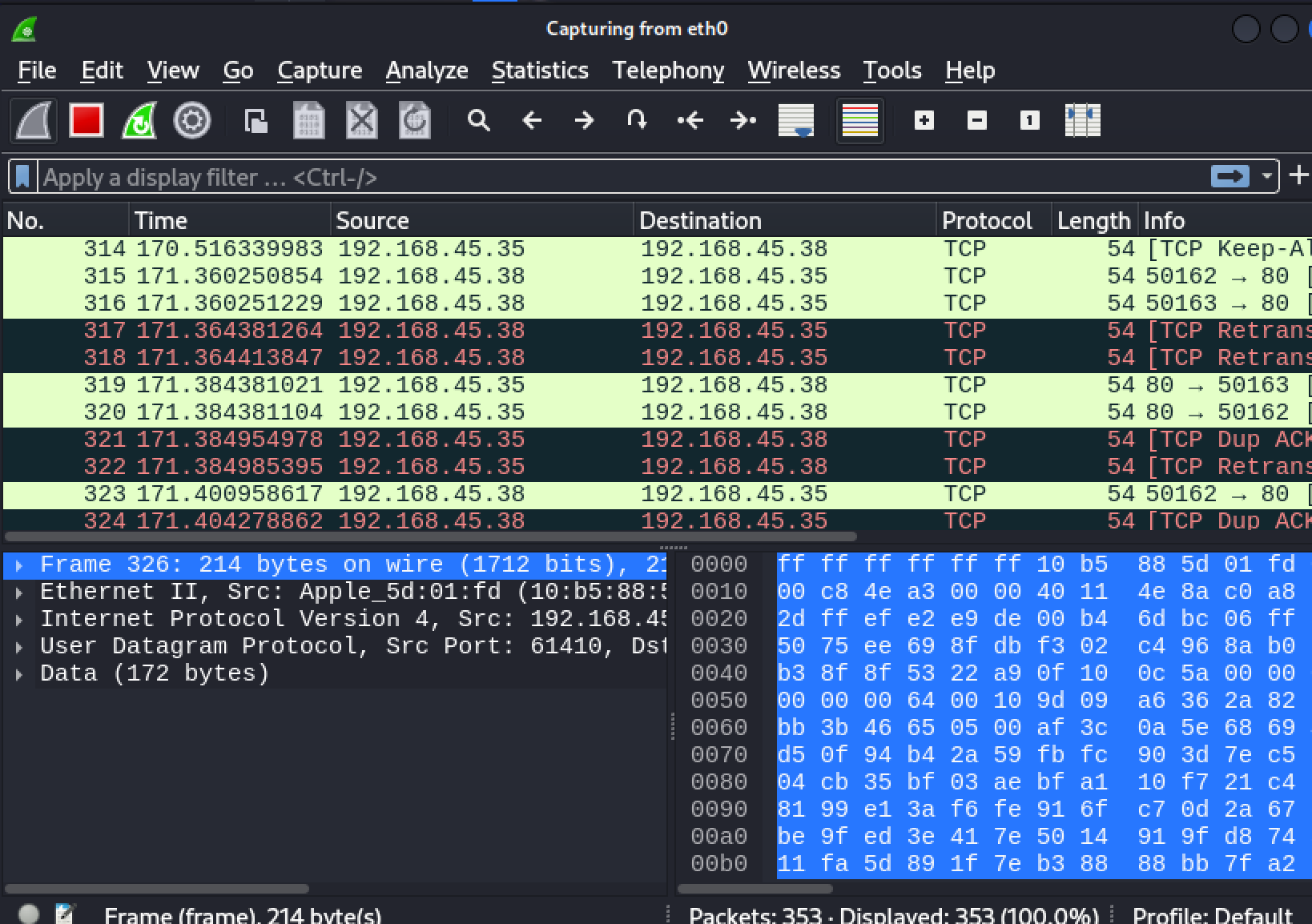
Select ips



Start MiTM attack



And we open wireshark and check for ARP packects and iF WE OPEN metaexplitable we can see TCP packets aswell



**EXPERIMENT 10**

**FILE Inclusion**

There are 2 different types of file inclusion attacks

LFI : LOCAL FILE INCLUSION

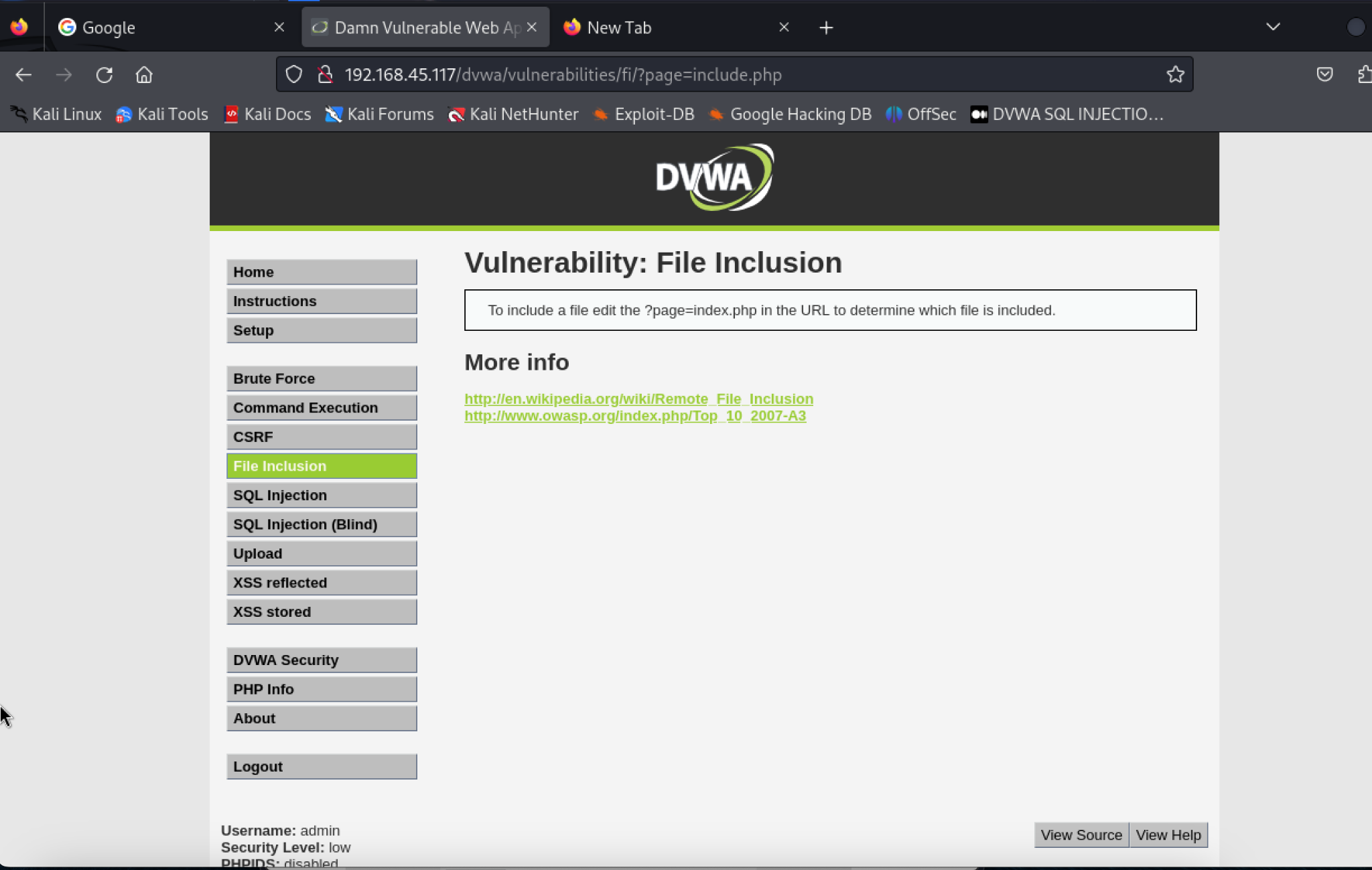
RFL : REMOTE FILE INCLUSION

FIRST WITH LFI

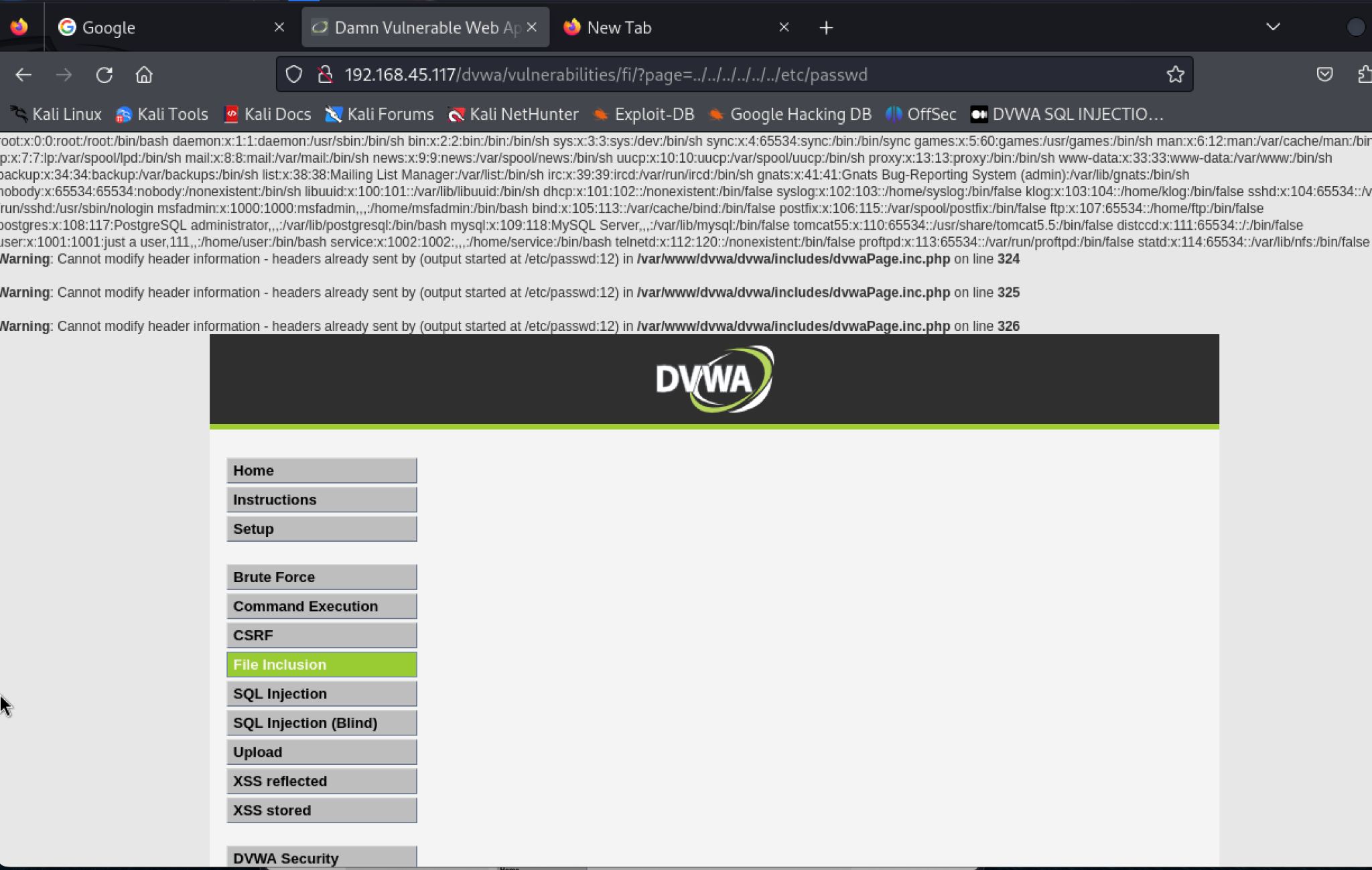
Toogle to LOW security

Open the file inclusion tab

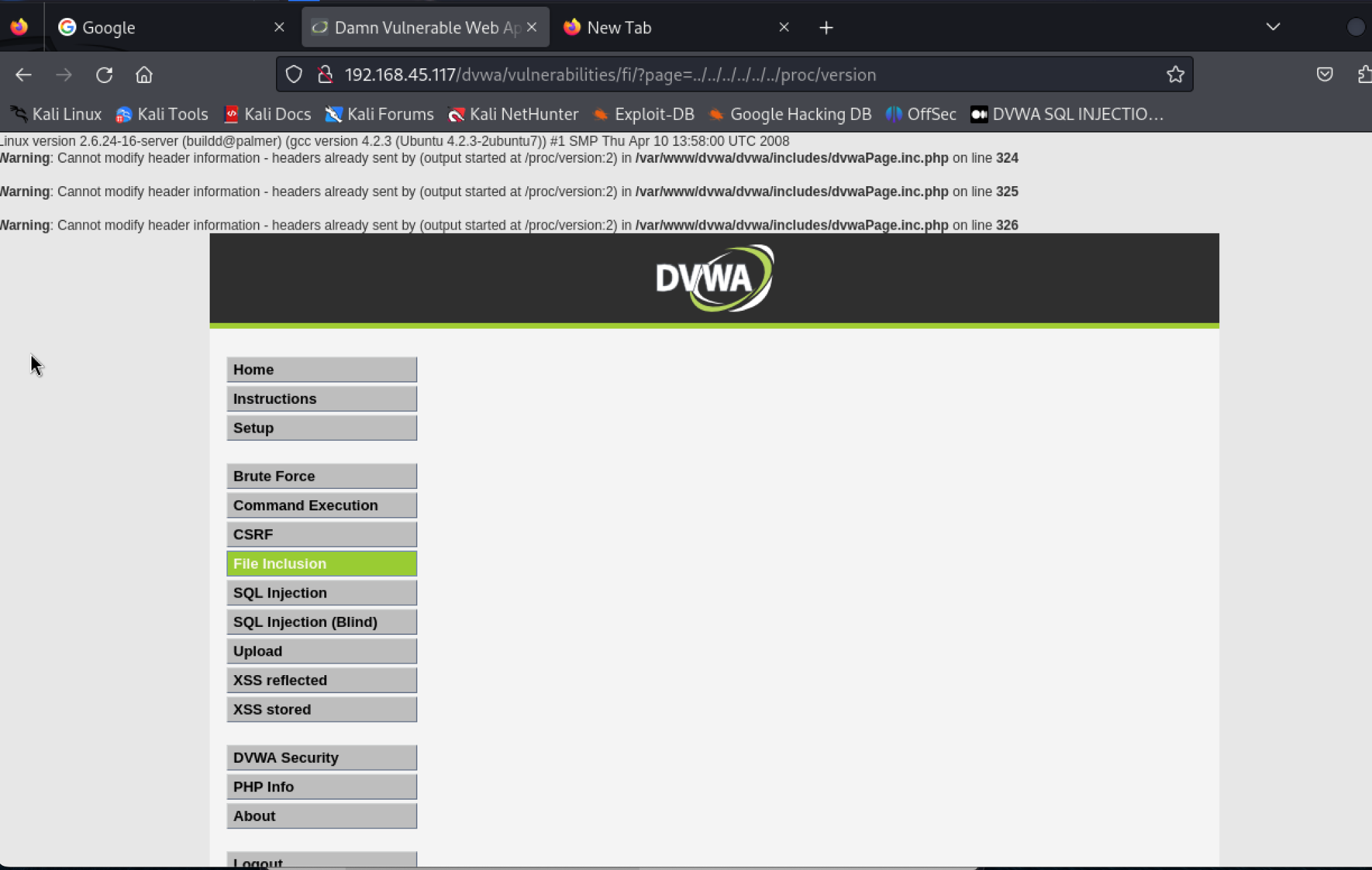
And go to the url bar



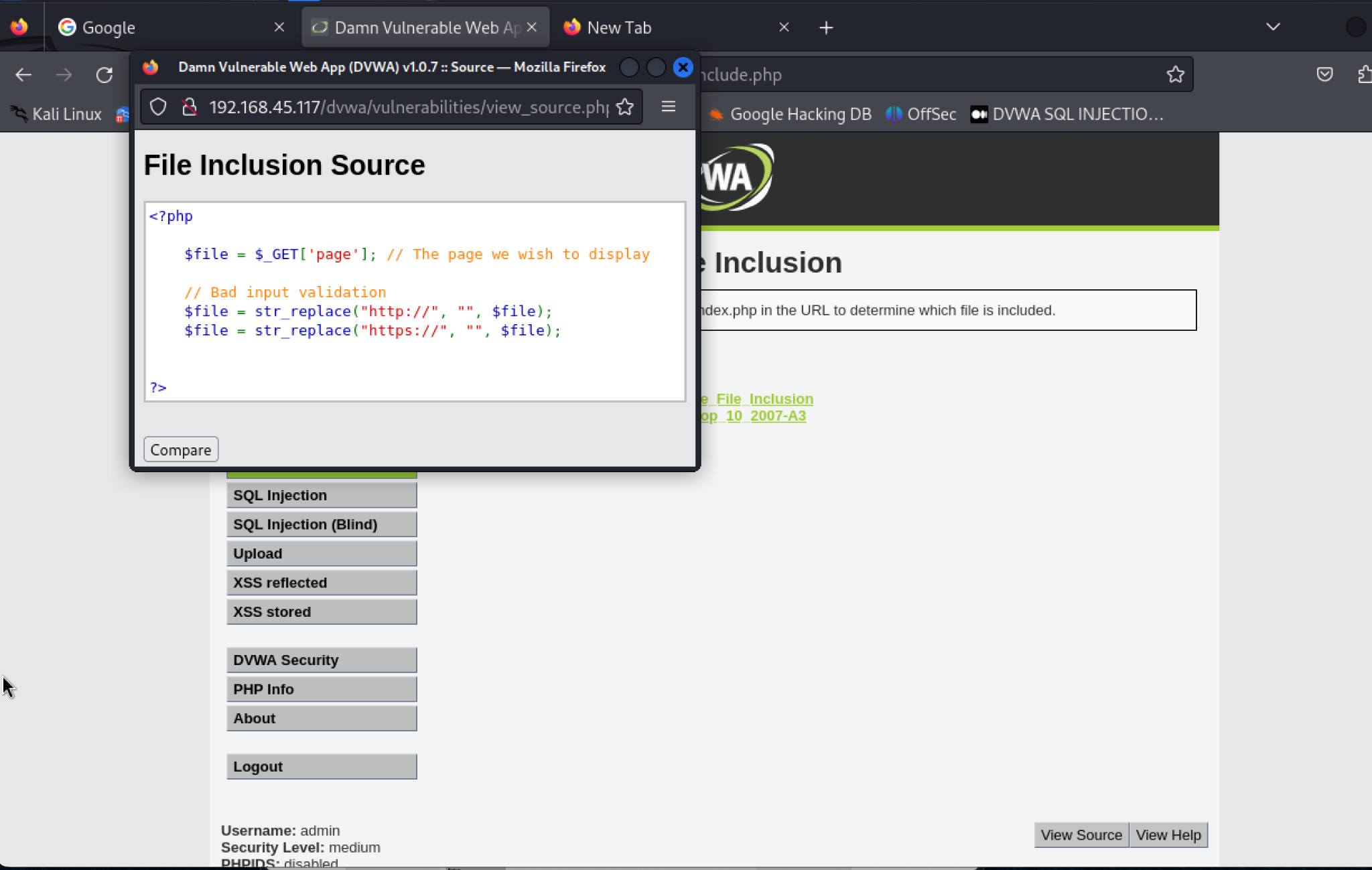
Change the URL from **/?page=include.php** to **?page=../../../../../../etc/passwd**



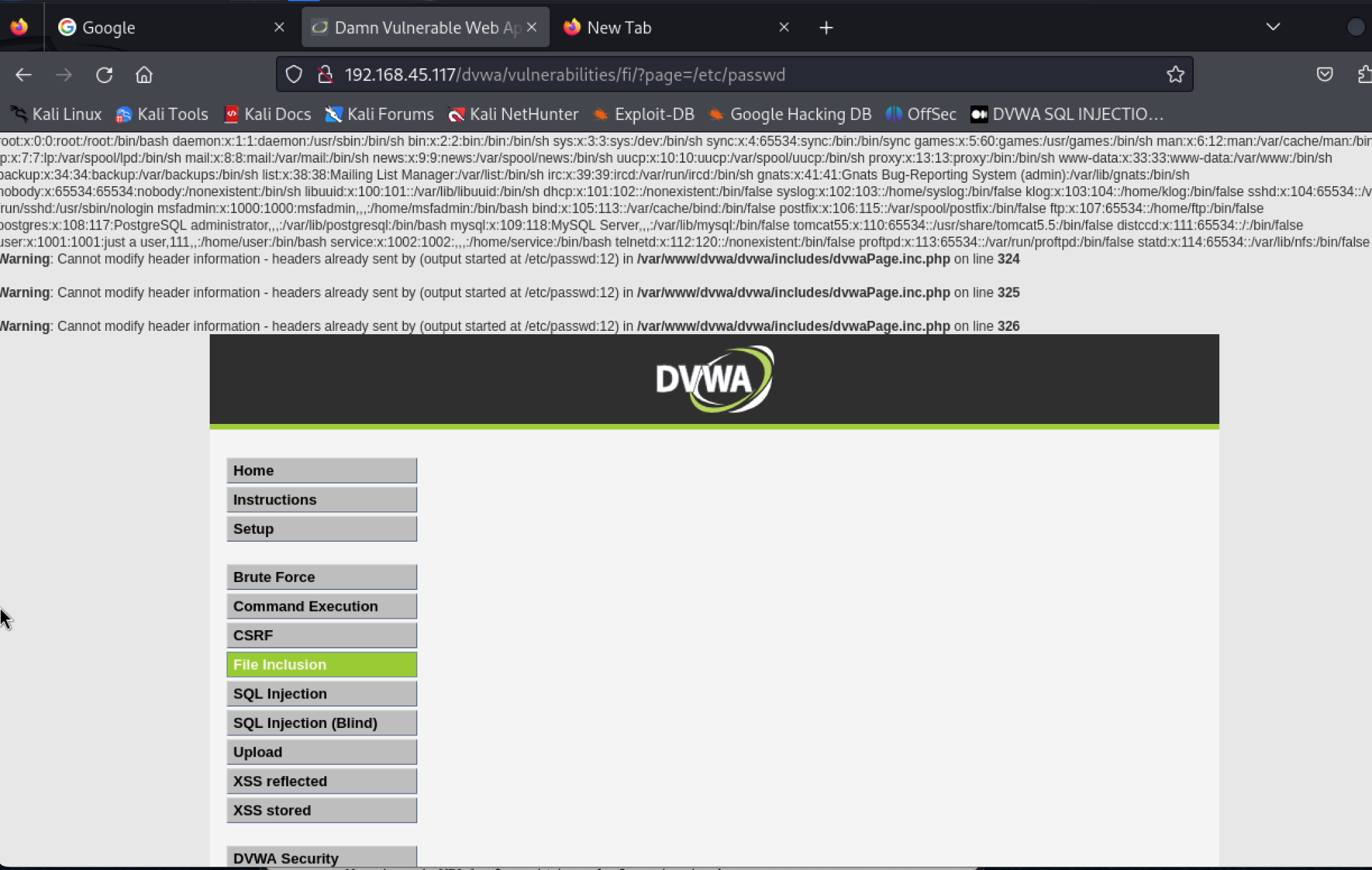
Now to **../../../../../../proc/version**



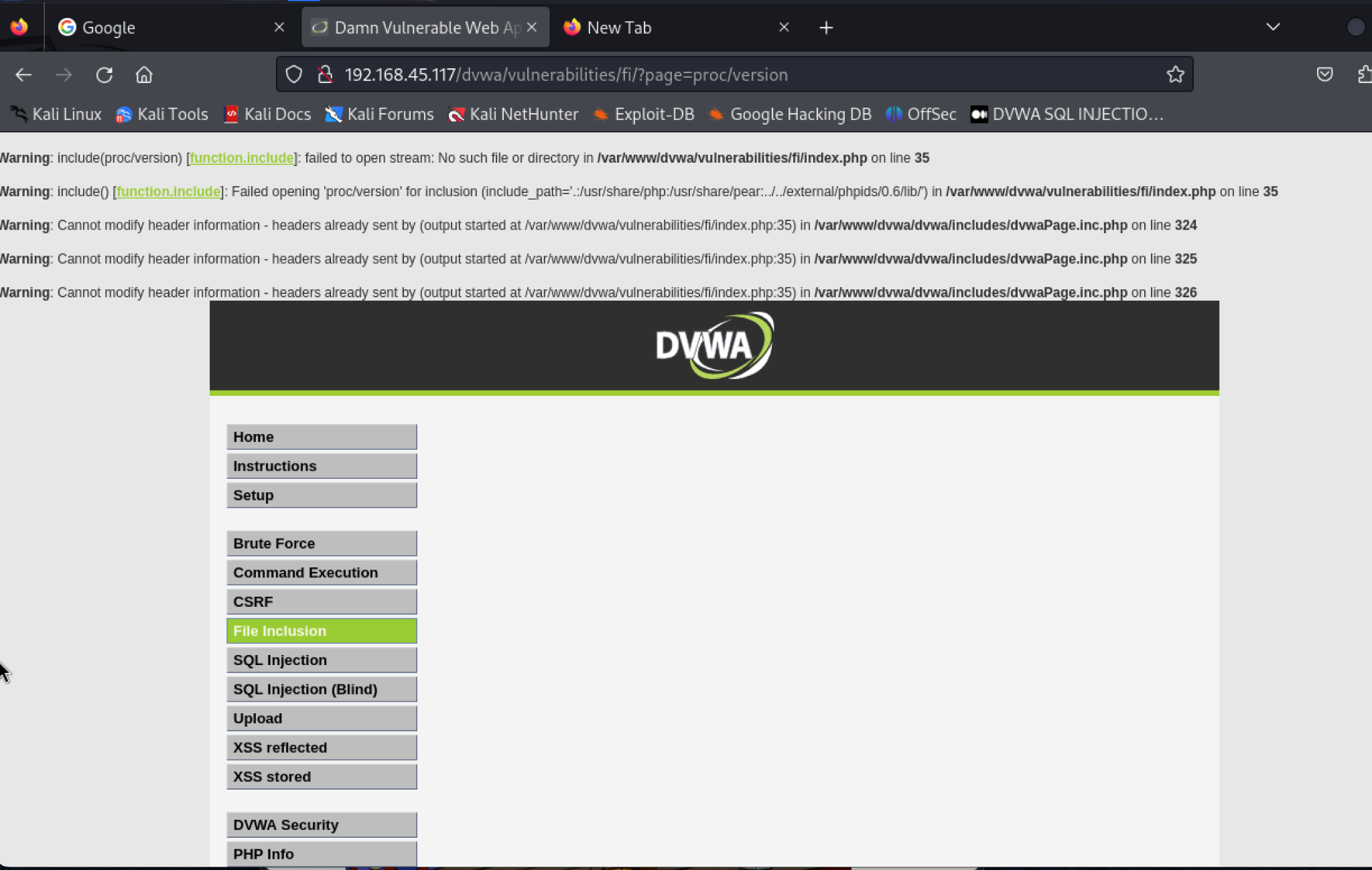
Now we go to Medium settings



And use **/etc/passwd**



Now to **/proc/version**

****

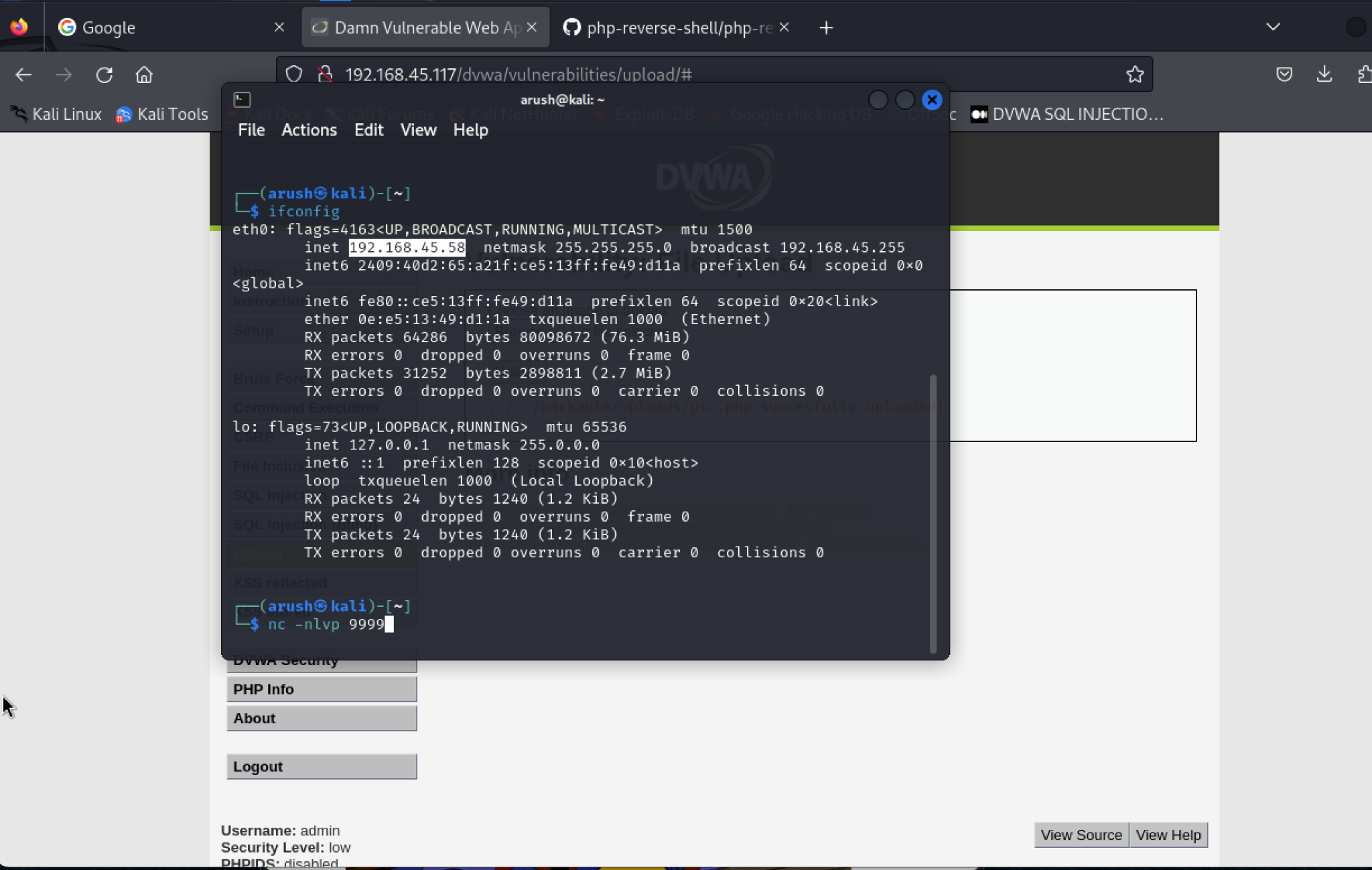
**Not possible for HIGH SETTINGS**

**FILE UPLOAD**

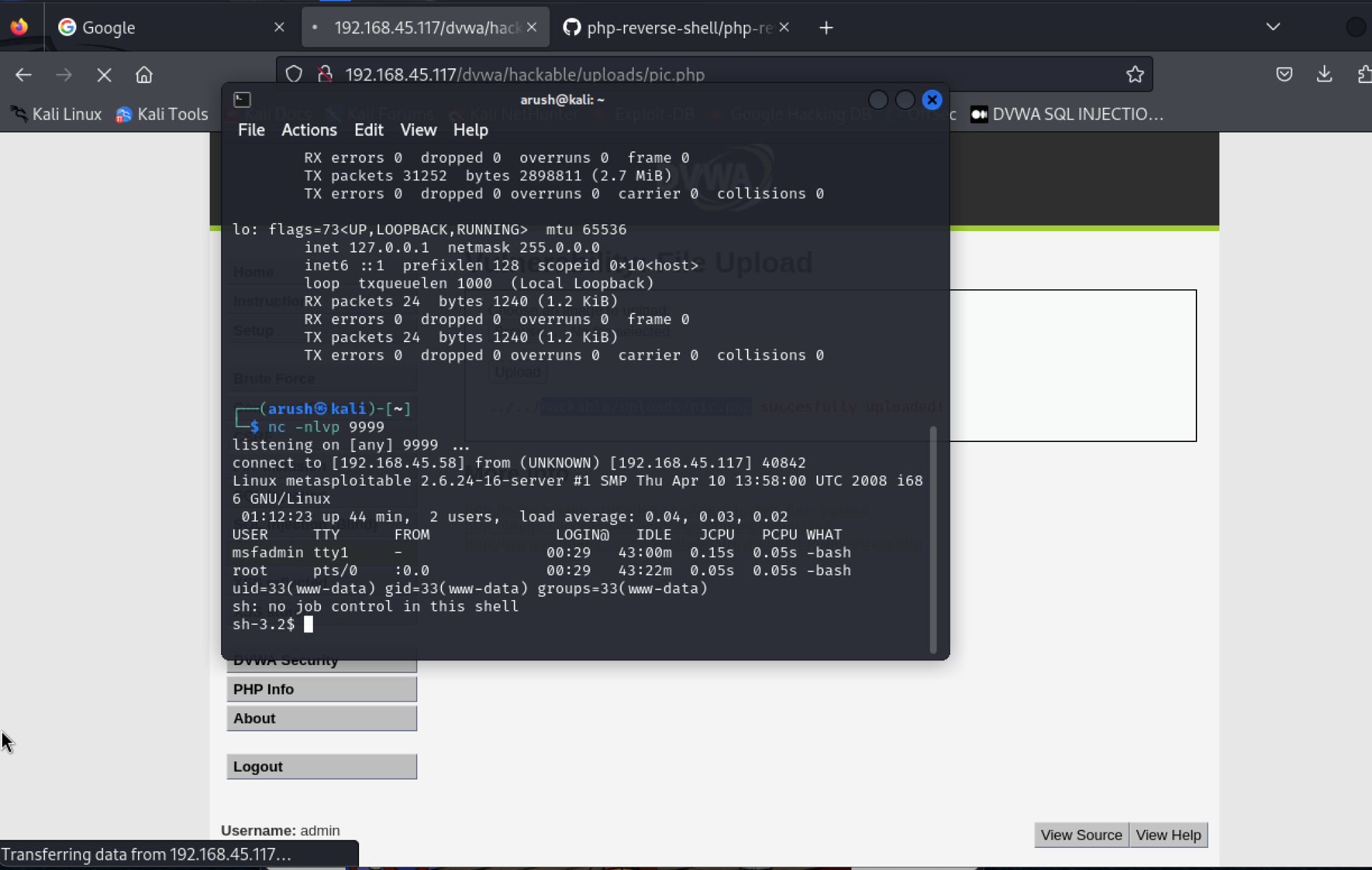
**After I upload a file pic.php into DVWA nad change port to 9999 and ip to my ip 192.168.45.58**

****

**Now we use the command nc -nlvp 9999**

****

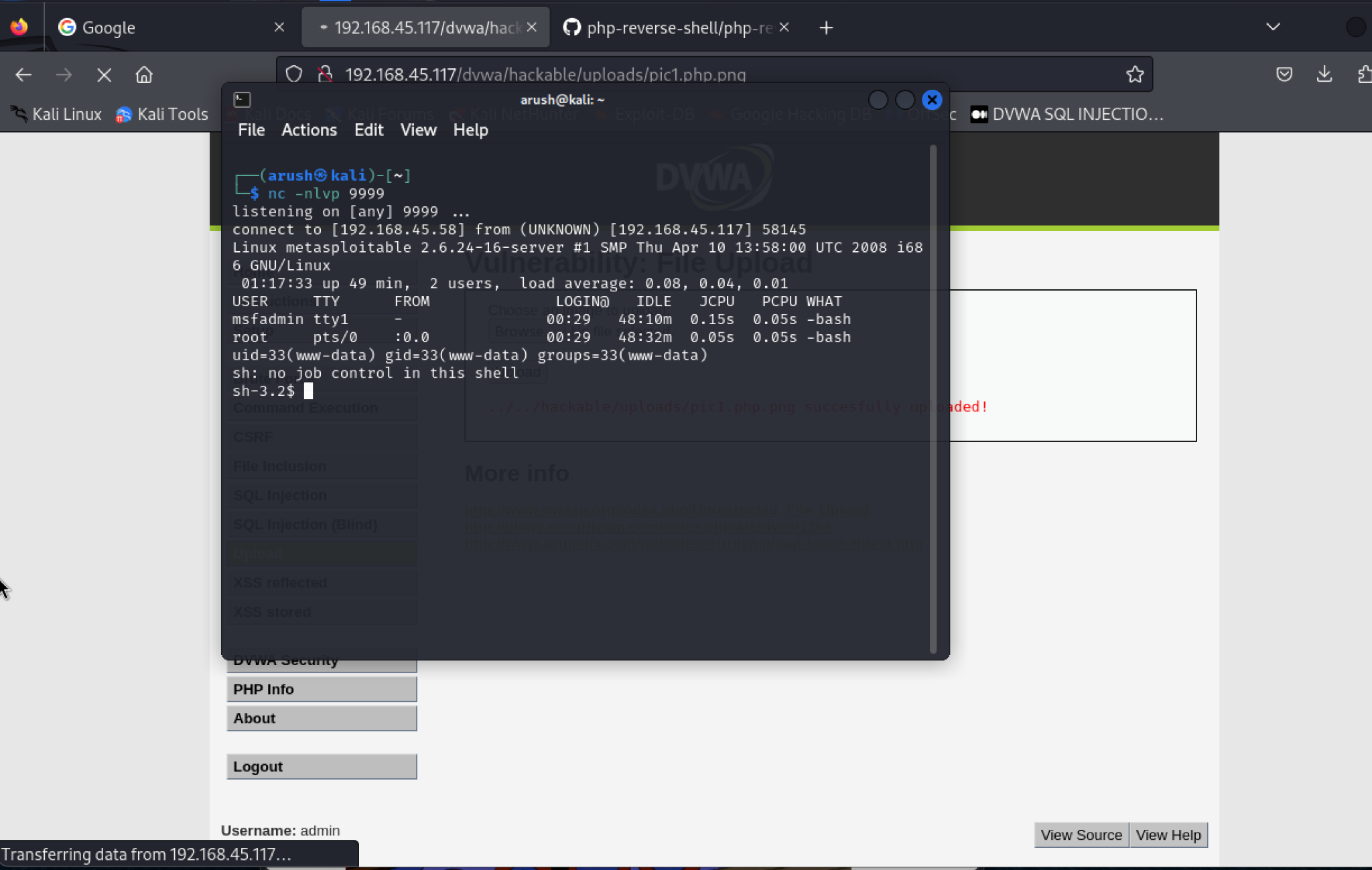
**Now in terminal we can see the shell we got**

****

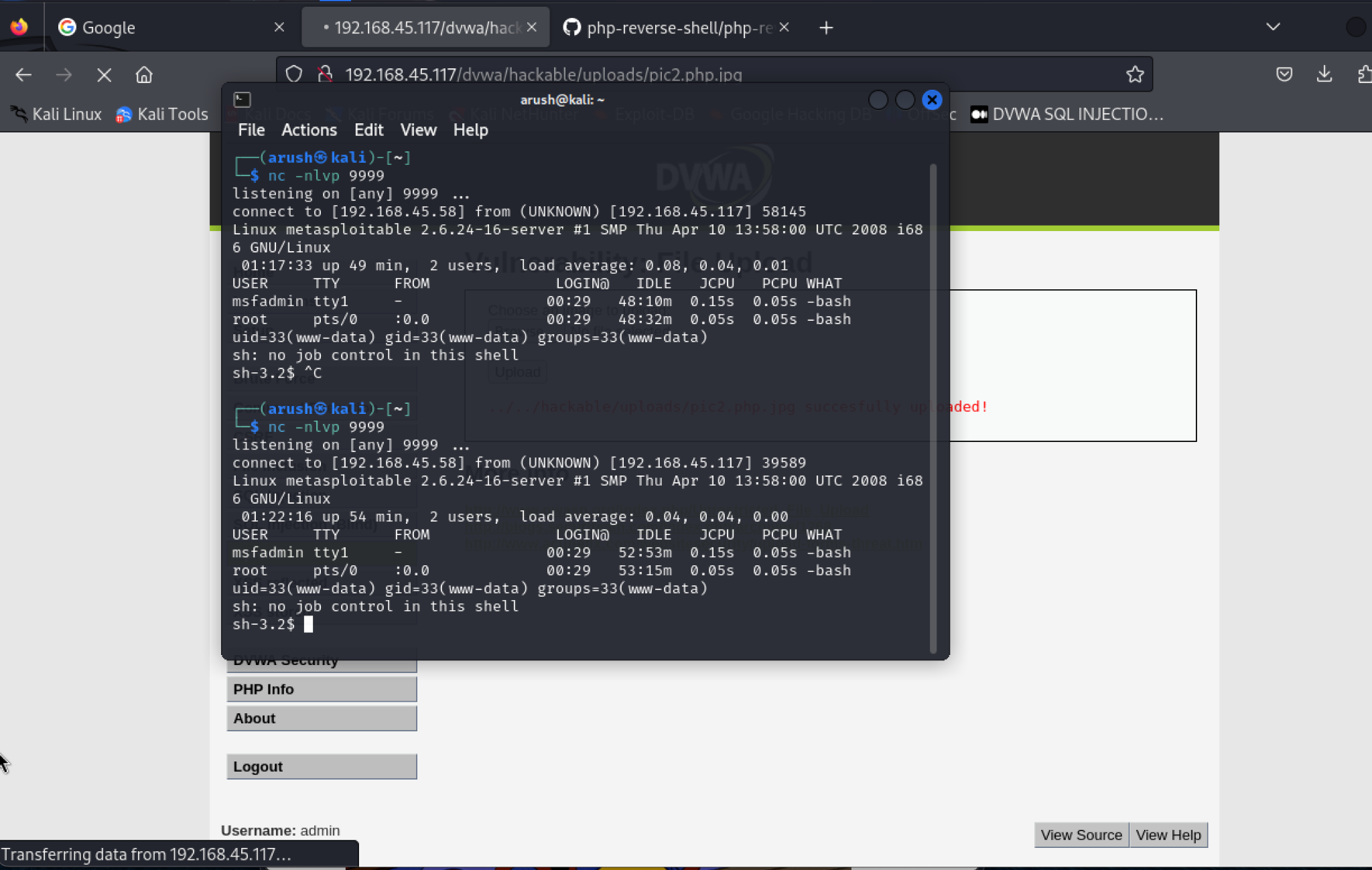
**Now in medium we have to first change the name and the types of file**

**Restart the shell**

**From pic.php to pic1.php.png**

****

**Now in high we have to change the pic1.php.png to pic1.png.jpg**

****