**LAB EXPERIMENT – 10**

**File Inclusion and File Upload**

One of the most common types of attacks against web servers stems from file inclusion vulnerabilities. File inclusion vulnerabilities can be primarily found on web applications that utilize a scripting runtime. These vulnerabilities give attackers access to sensitive files on their web servers or allow them to utilize include functionality to carry out malicious files on their servers. With access to unauthorized files, attackers can attain sensitive information or further compromise the victim’s networks.

Some Local File Inclusion Payloads: -

/etc/issue

/etc/passwd

/etc/shadow

/etc/group

/etc/hosts

/etc/motd

/etc/mysql/my.cnf

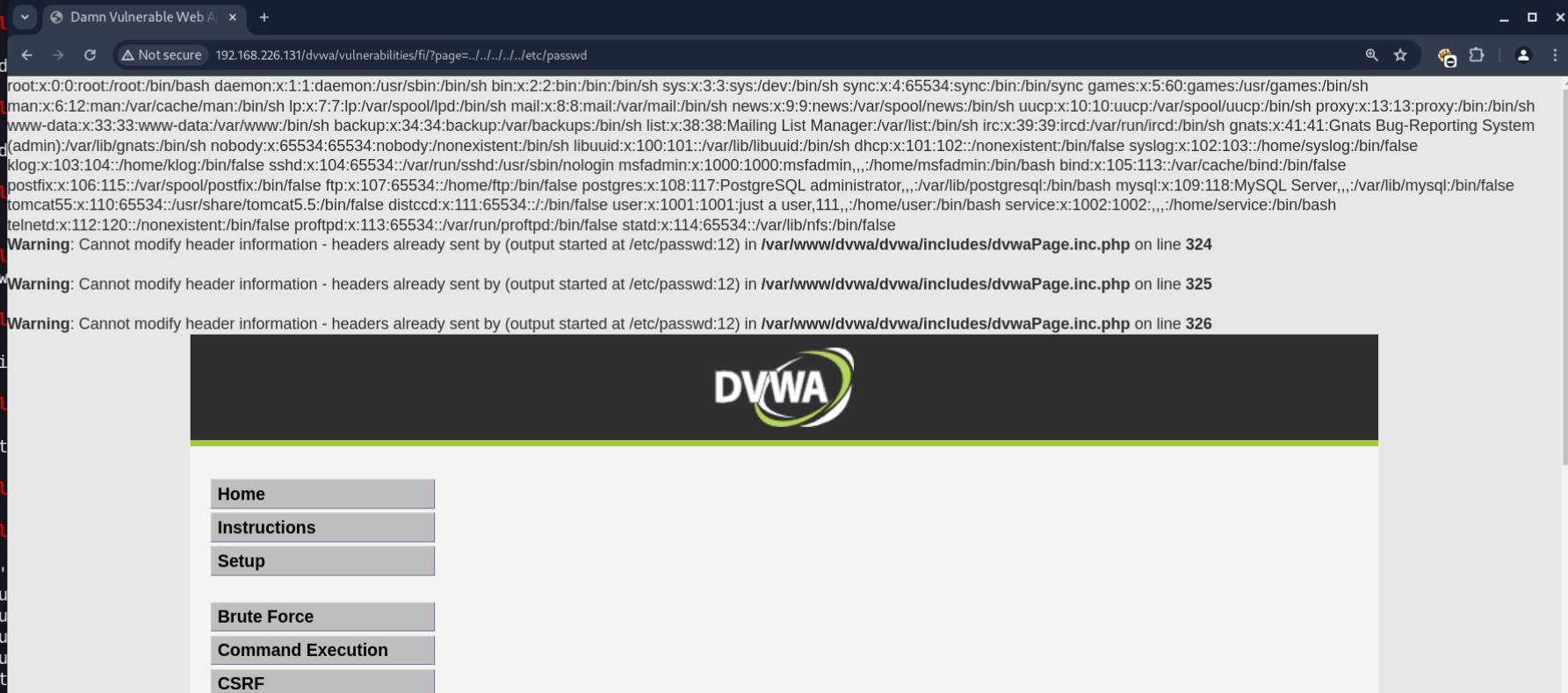
/proc/[0-9]\*/fd/[0-9]\* (first number is the PID, second is the filedescriptor)

/proc/self/environ

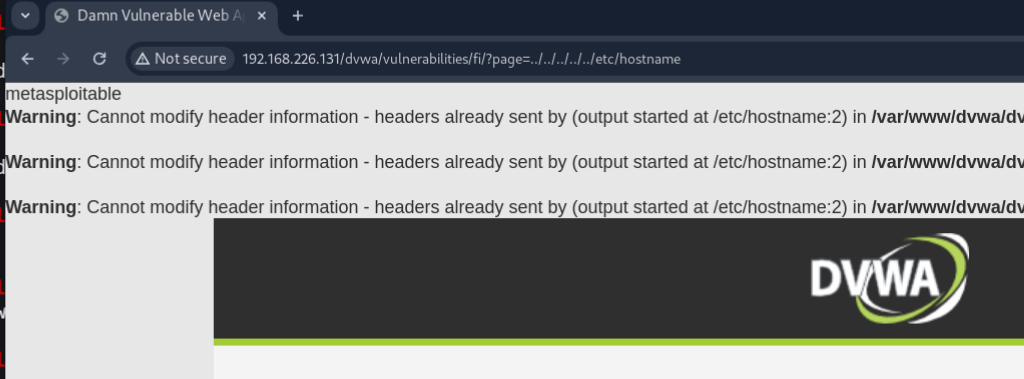
/proc/version

/proc/cmdline

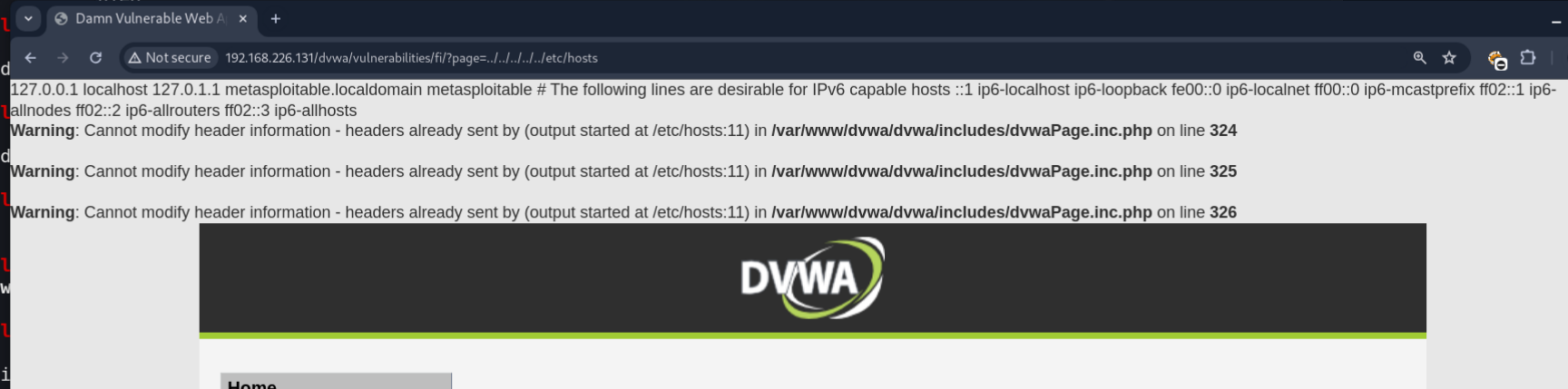
1)



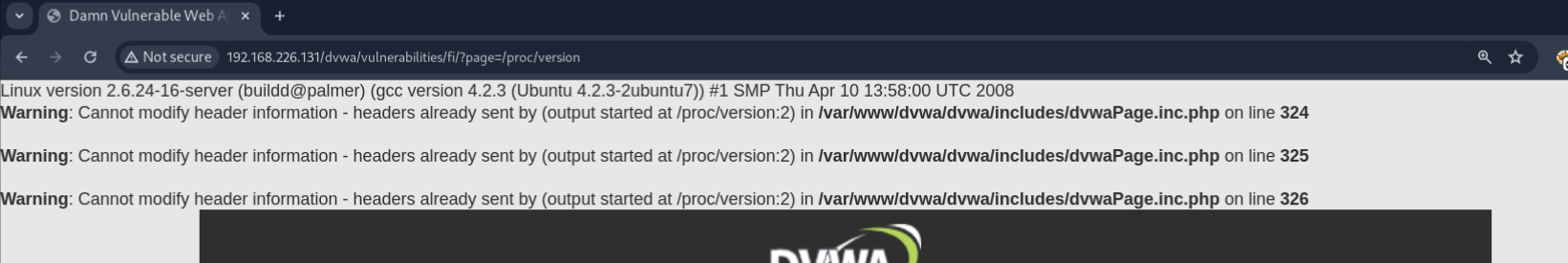
2)



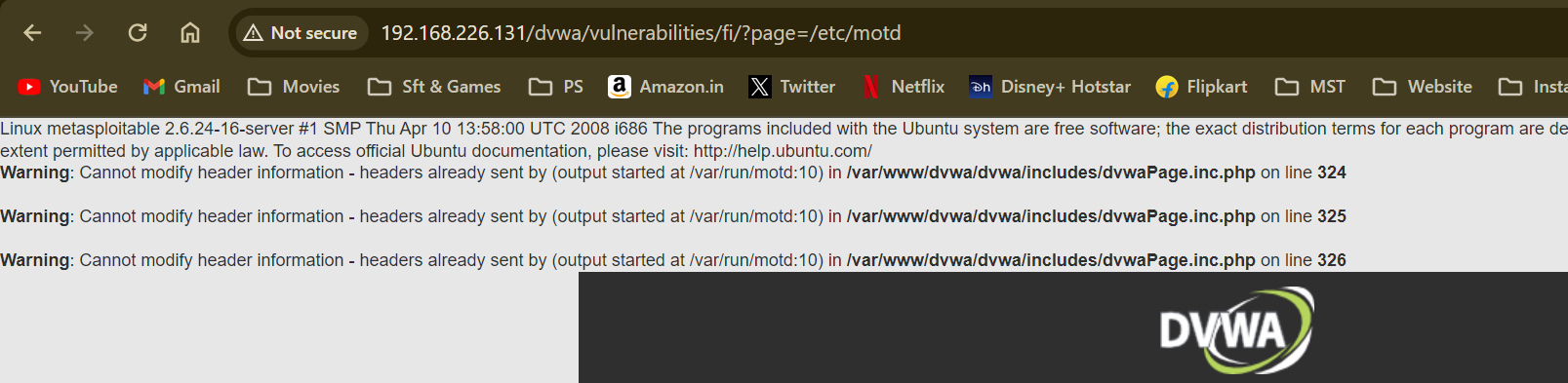
3)



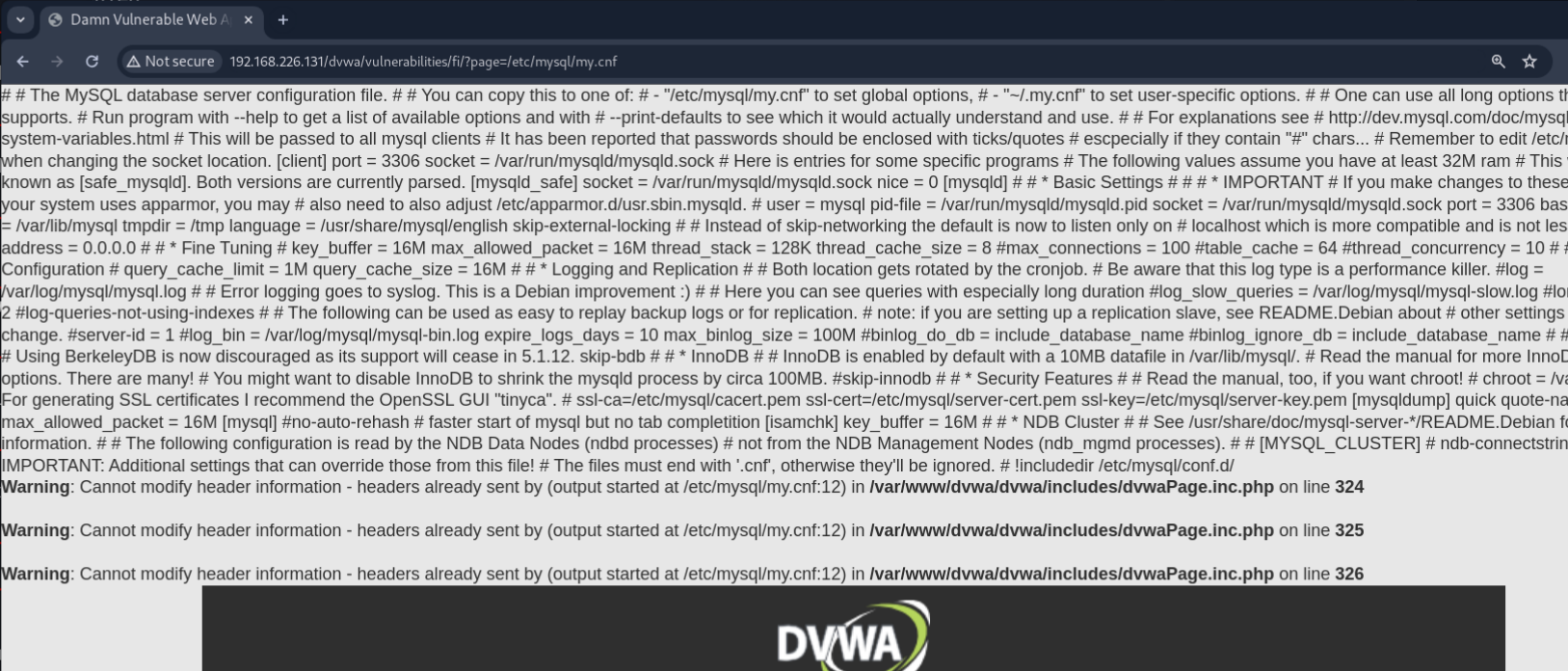
4)



5)



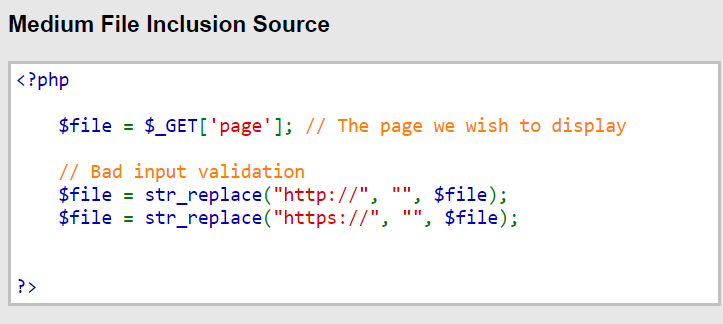
6)



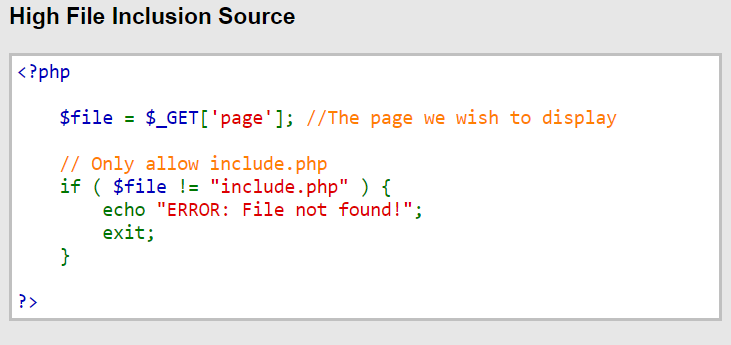
Low



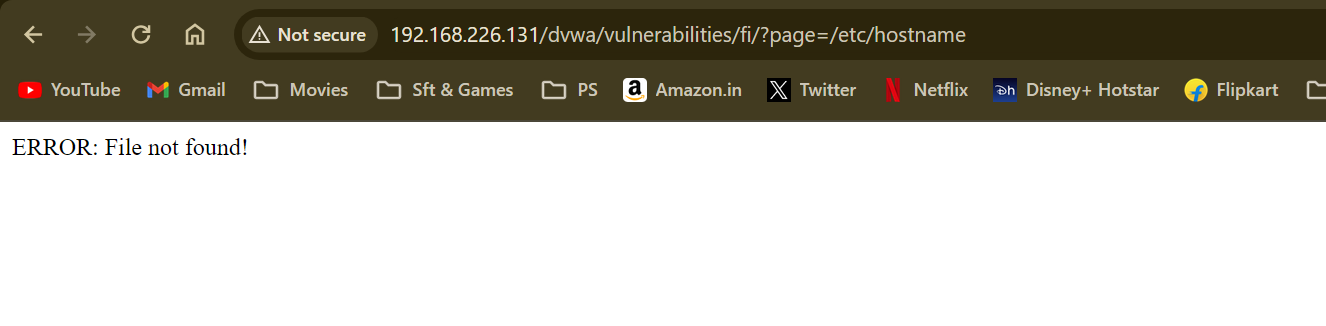
Medium



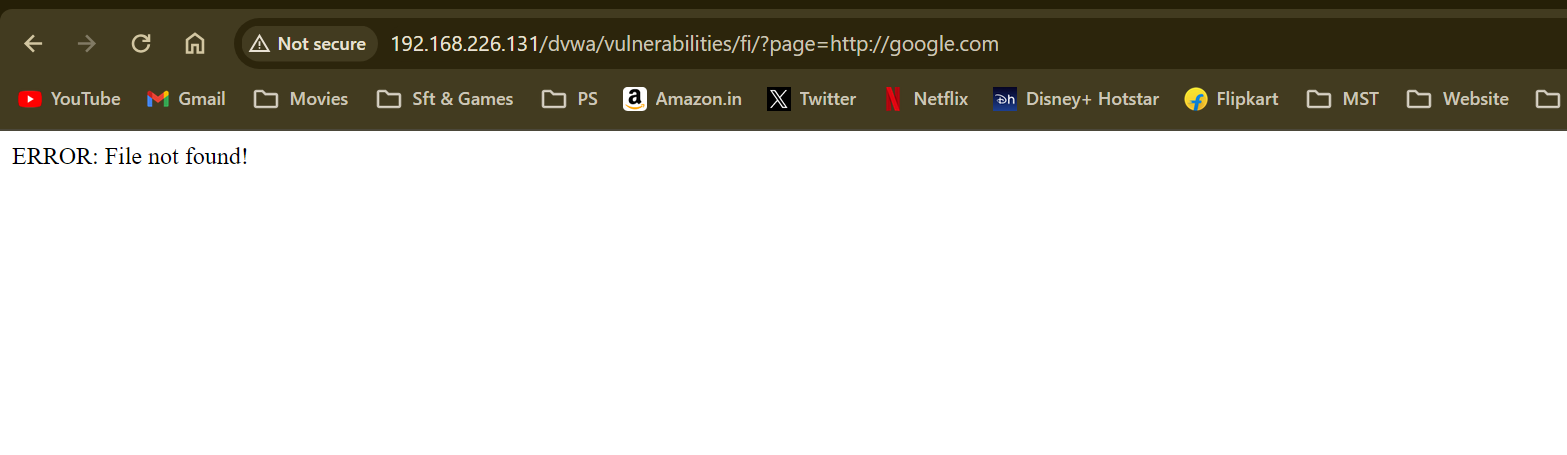
High

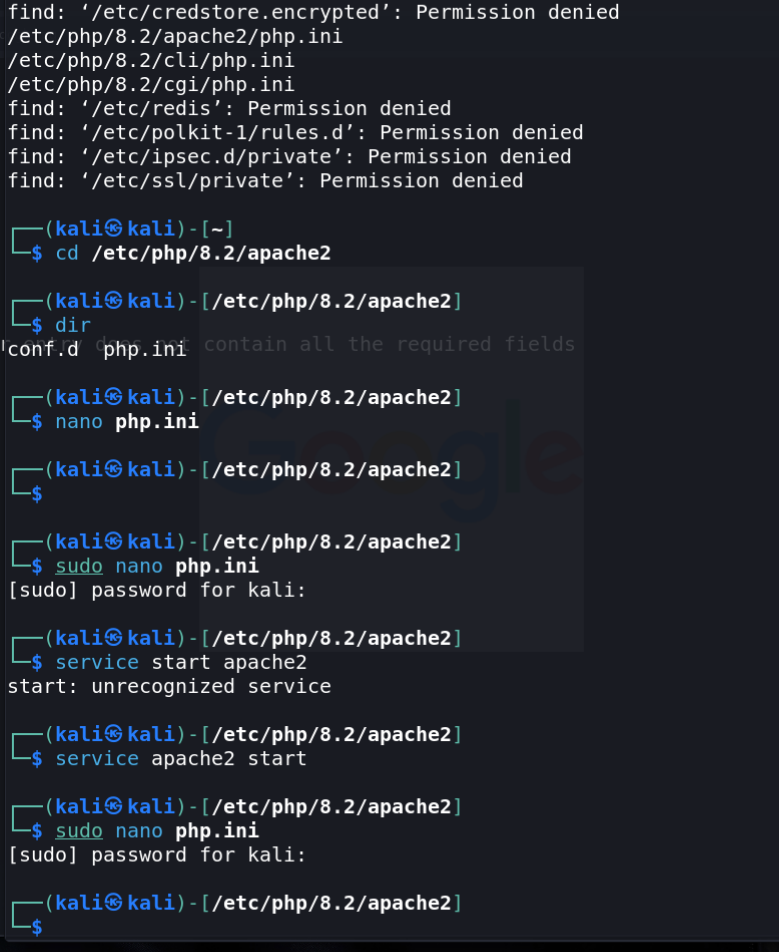


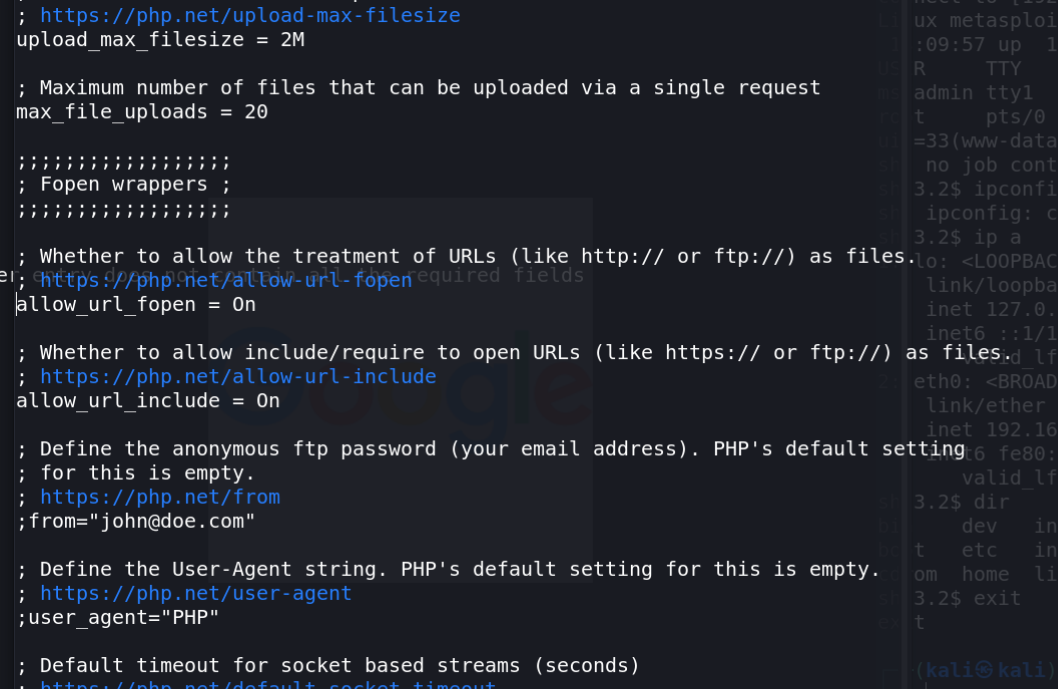
Local File Inclusion Tested on High Security gives you the ERROR! (File Not FOUND!)

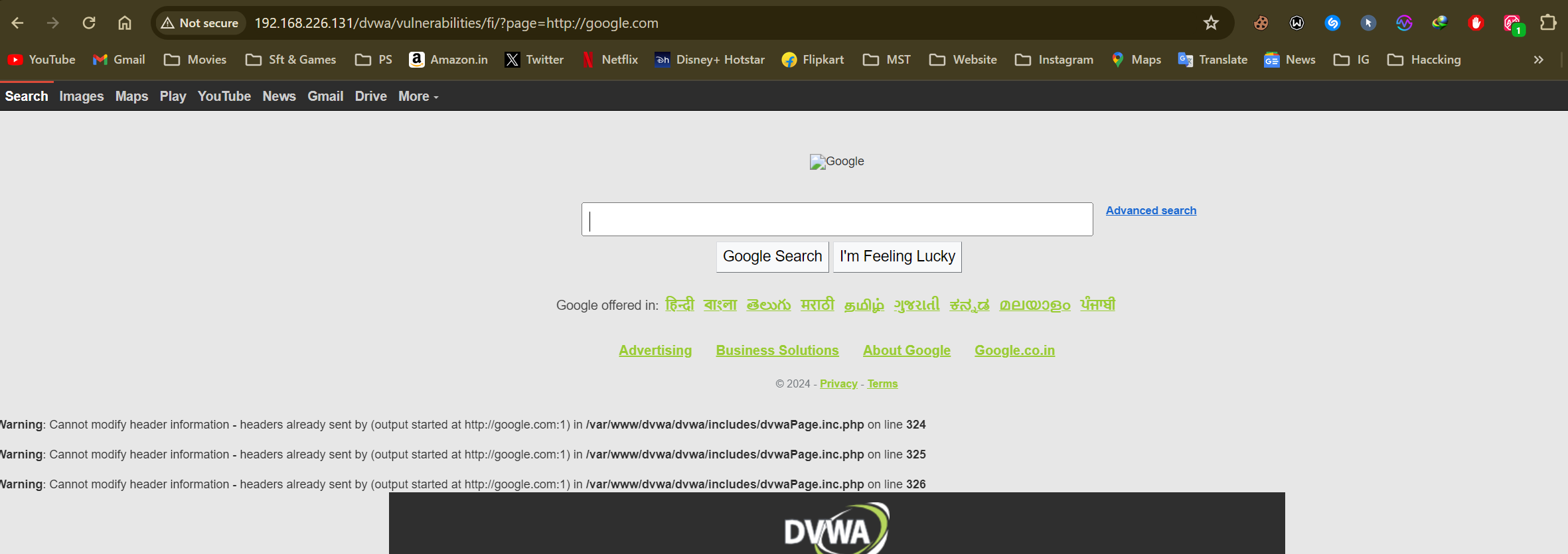


Remote File Inclusion Tested on High Security gives you the ERROR! (File Not FOUND!)



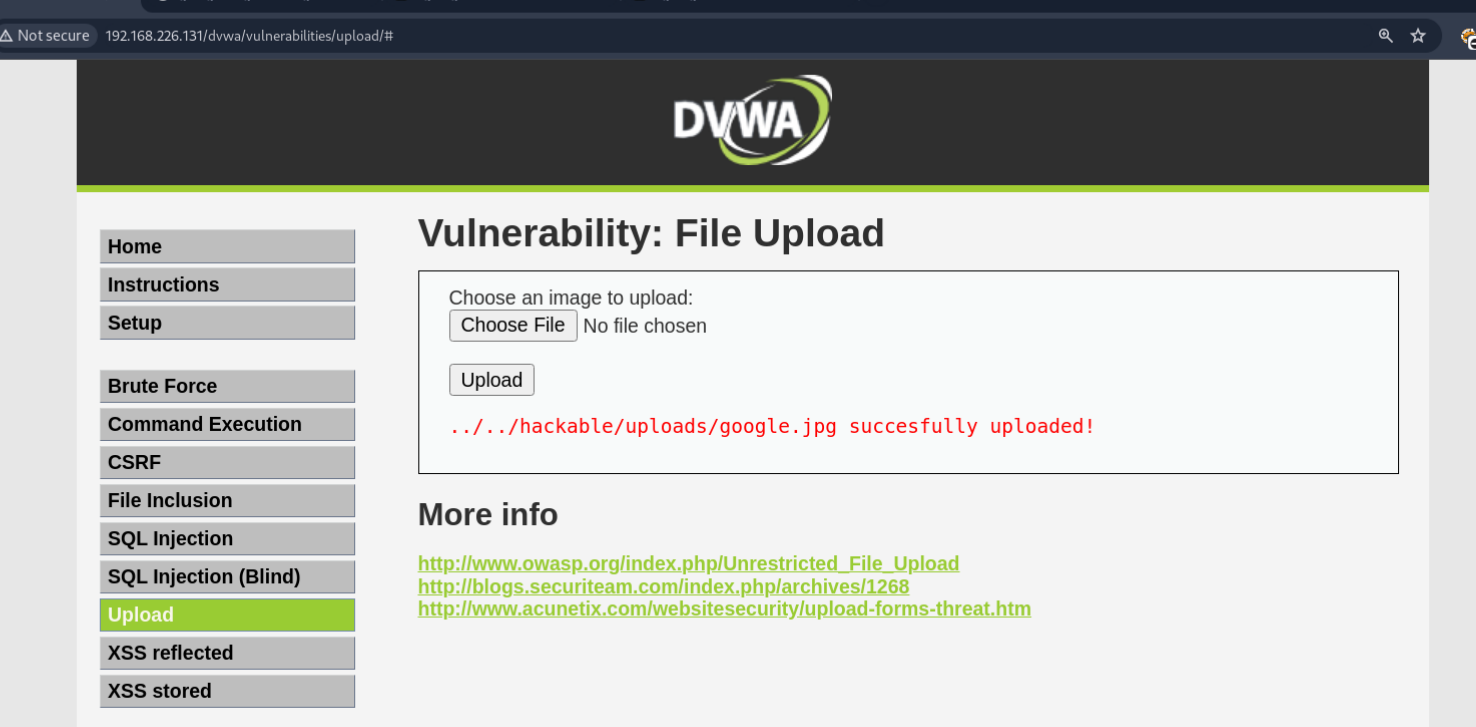




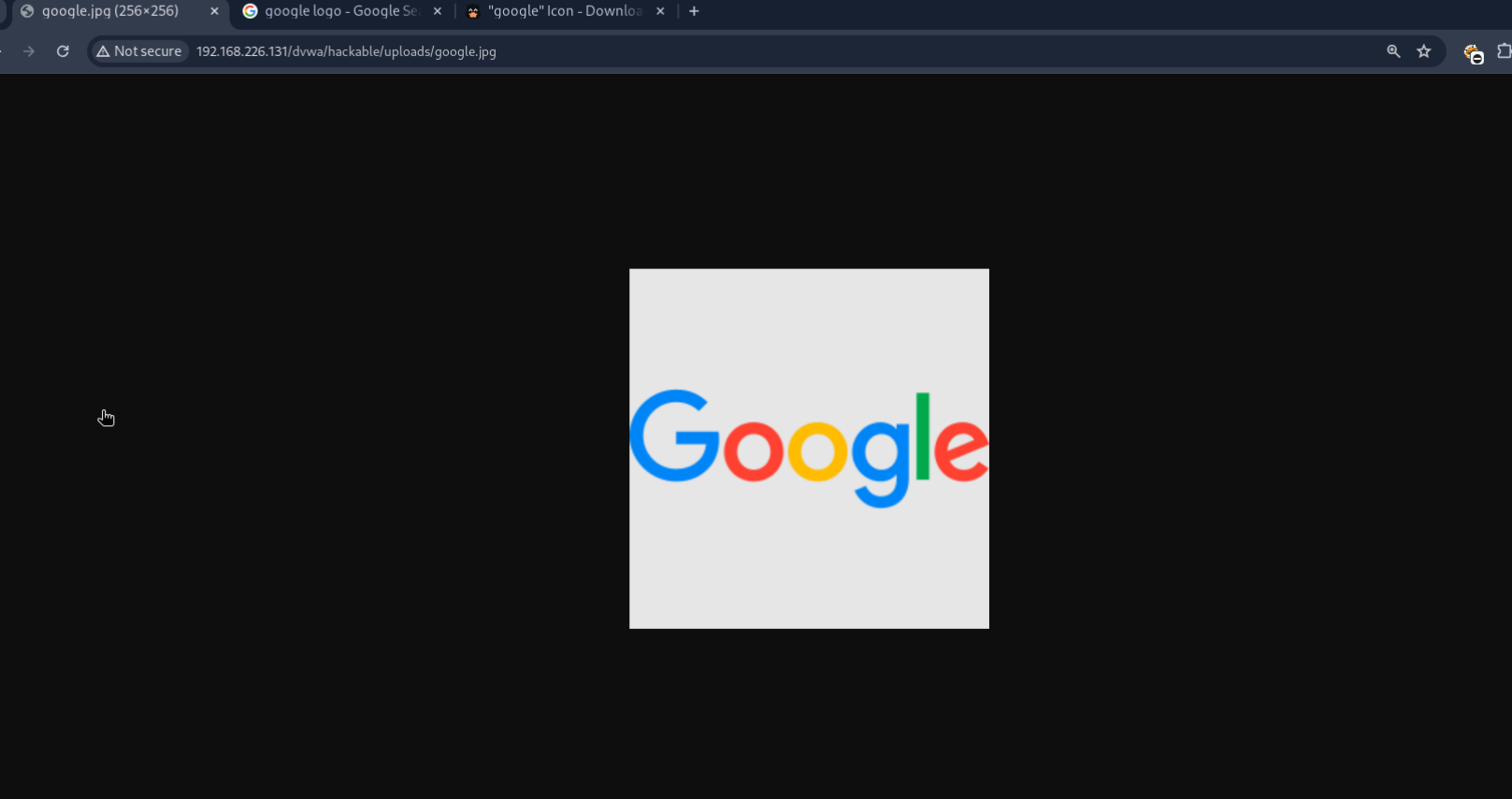


**FILE UPLOAD**

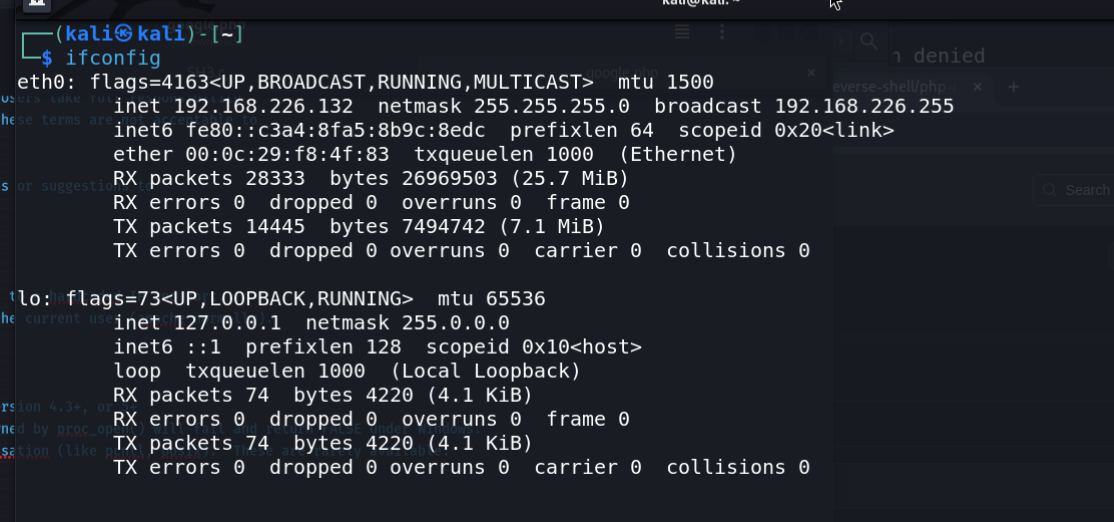
Download and Upload Image to be uploaded in the Database.



Open The file in the location of the DB.

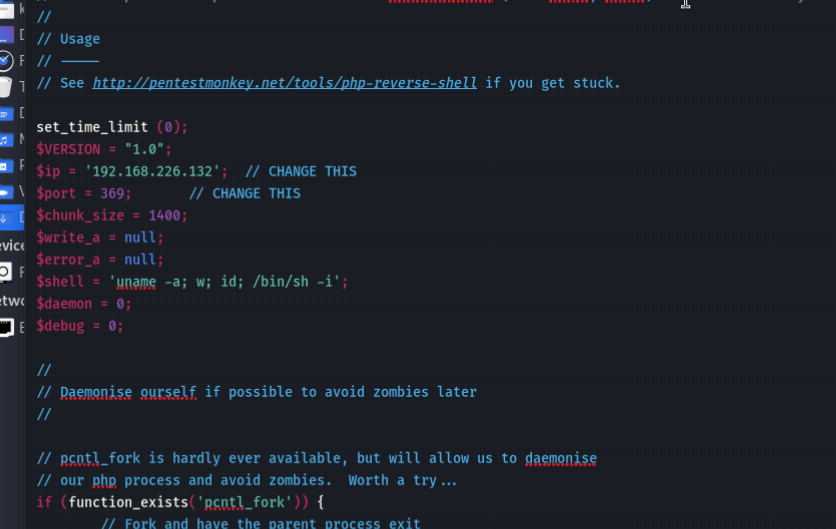


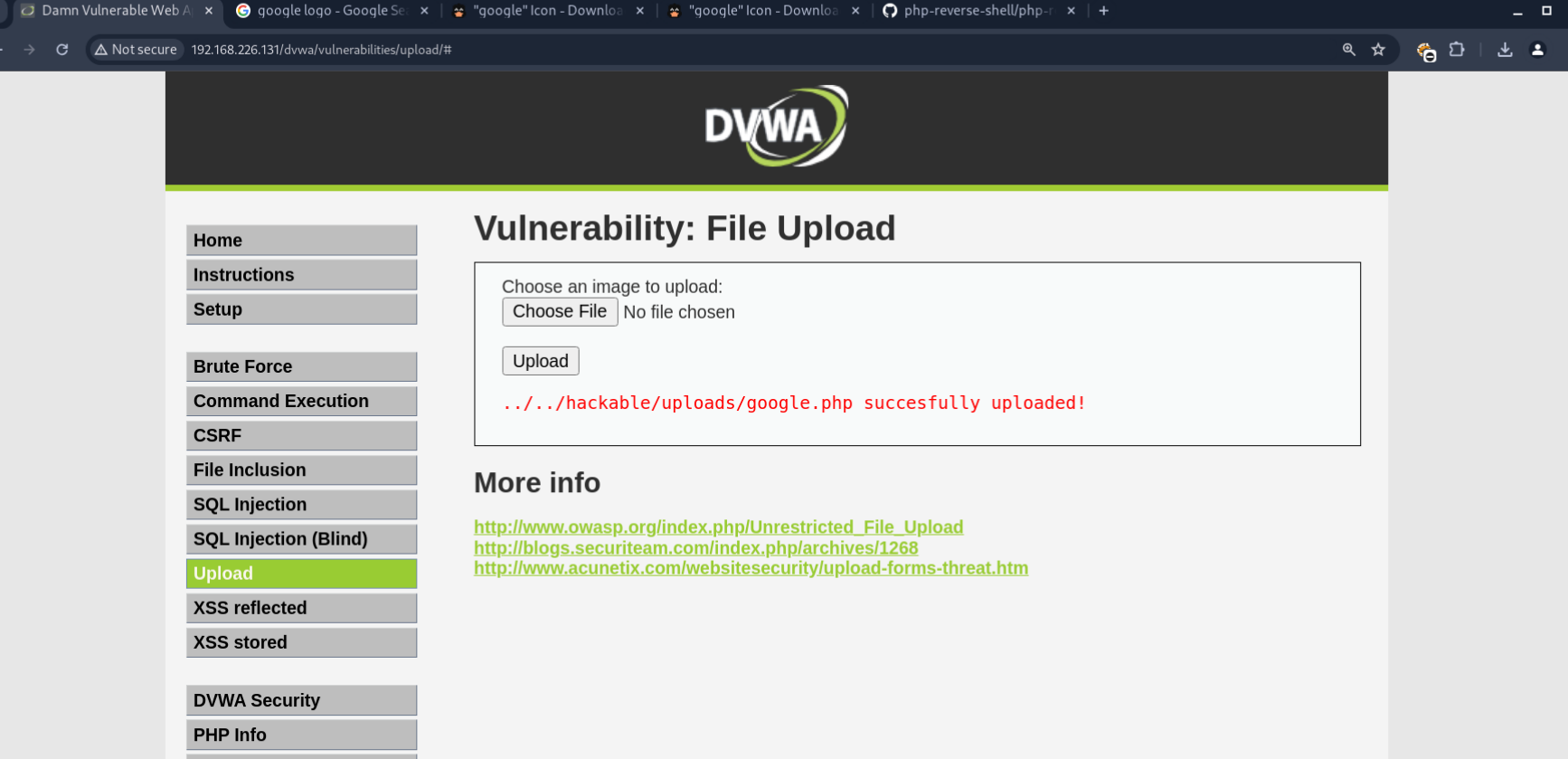
Check the IP for your Kali System and copy it in the clipboard.

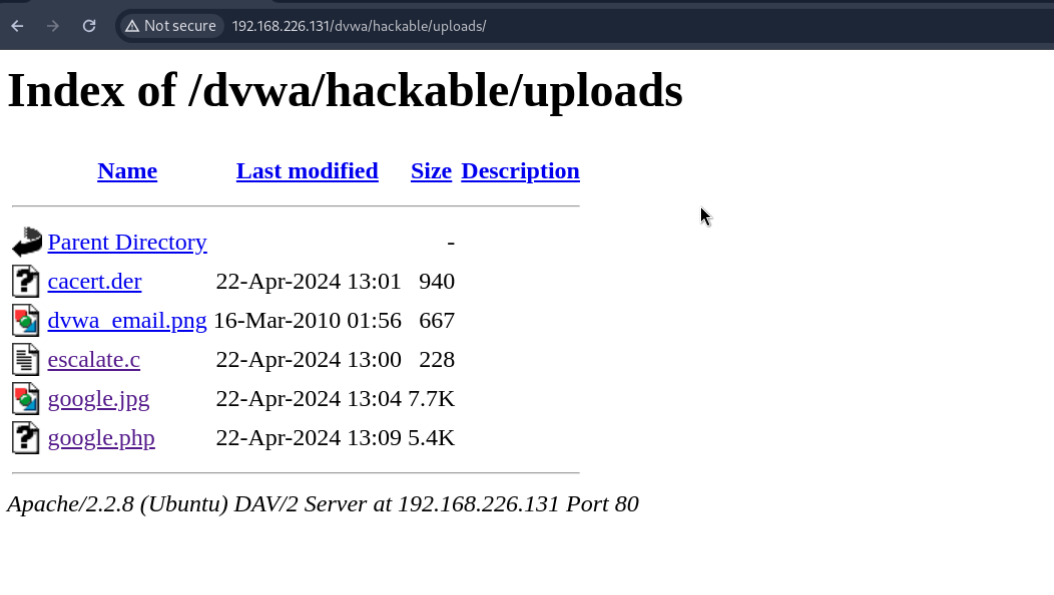


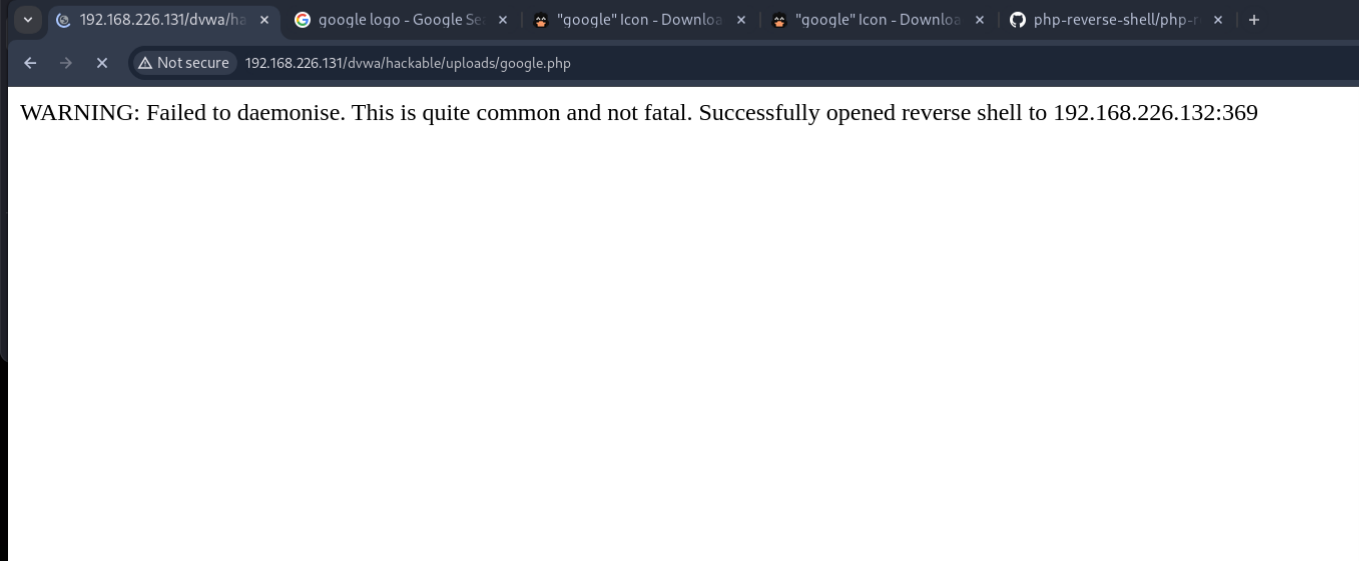
Download the revere shell PHP payload from internet and replace the IP and Port number with the Kali’s IP and rename the Port of your choice.

Also rename the PHP with the same name of the image.









Hence, we gained the shell Access.

