MINI PROJECT

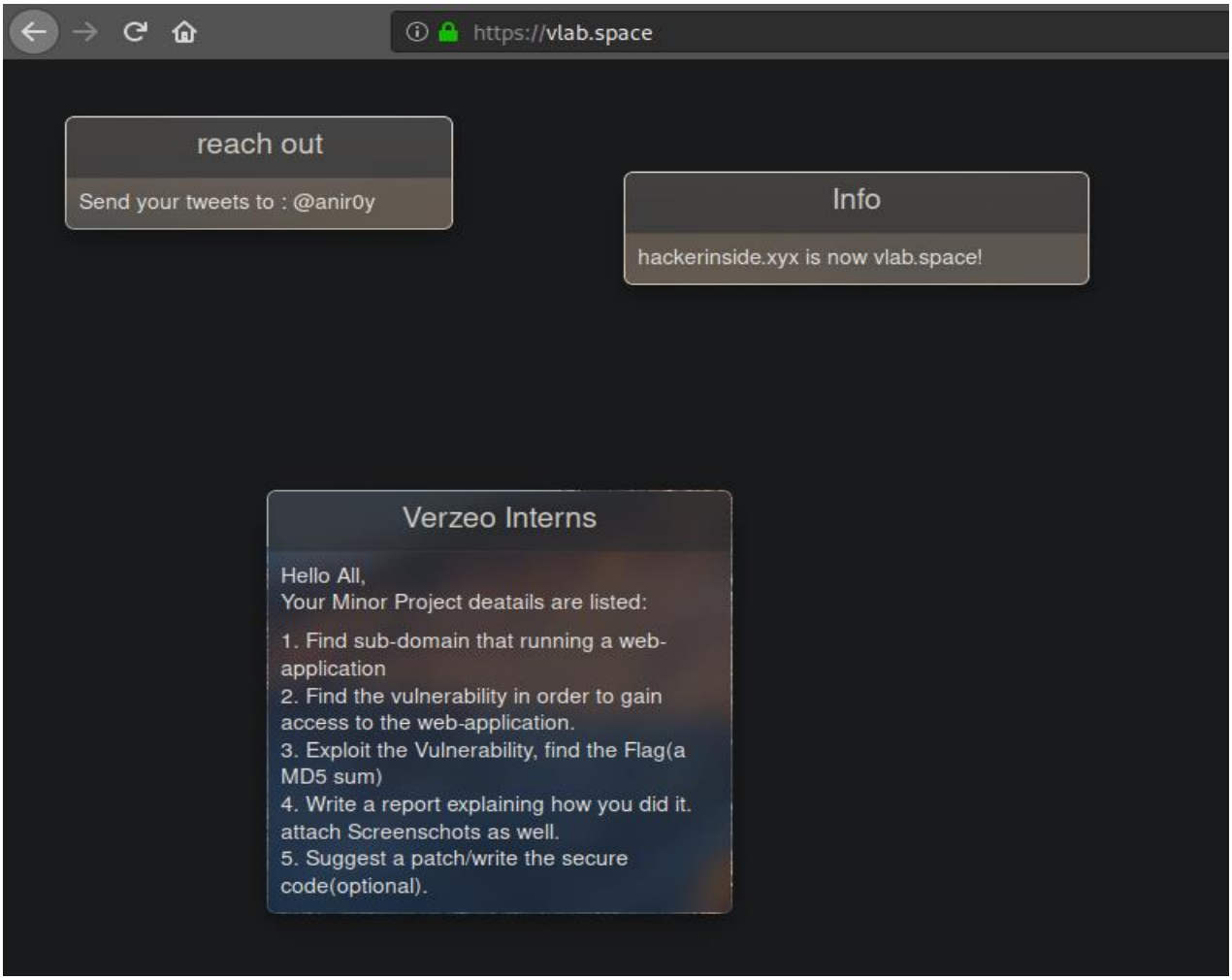
CS-MINOR-JULY-CS-07B2

NAME- VISHAL KUMAR SINGH
EMAIL: vishalbit99@gmail.com

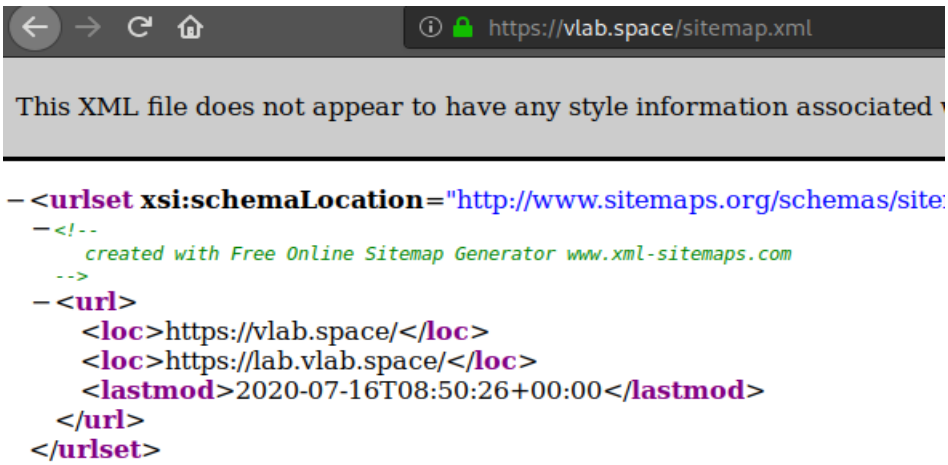
1. SQLI

In this task we were given a link https://vlab.space .

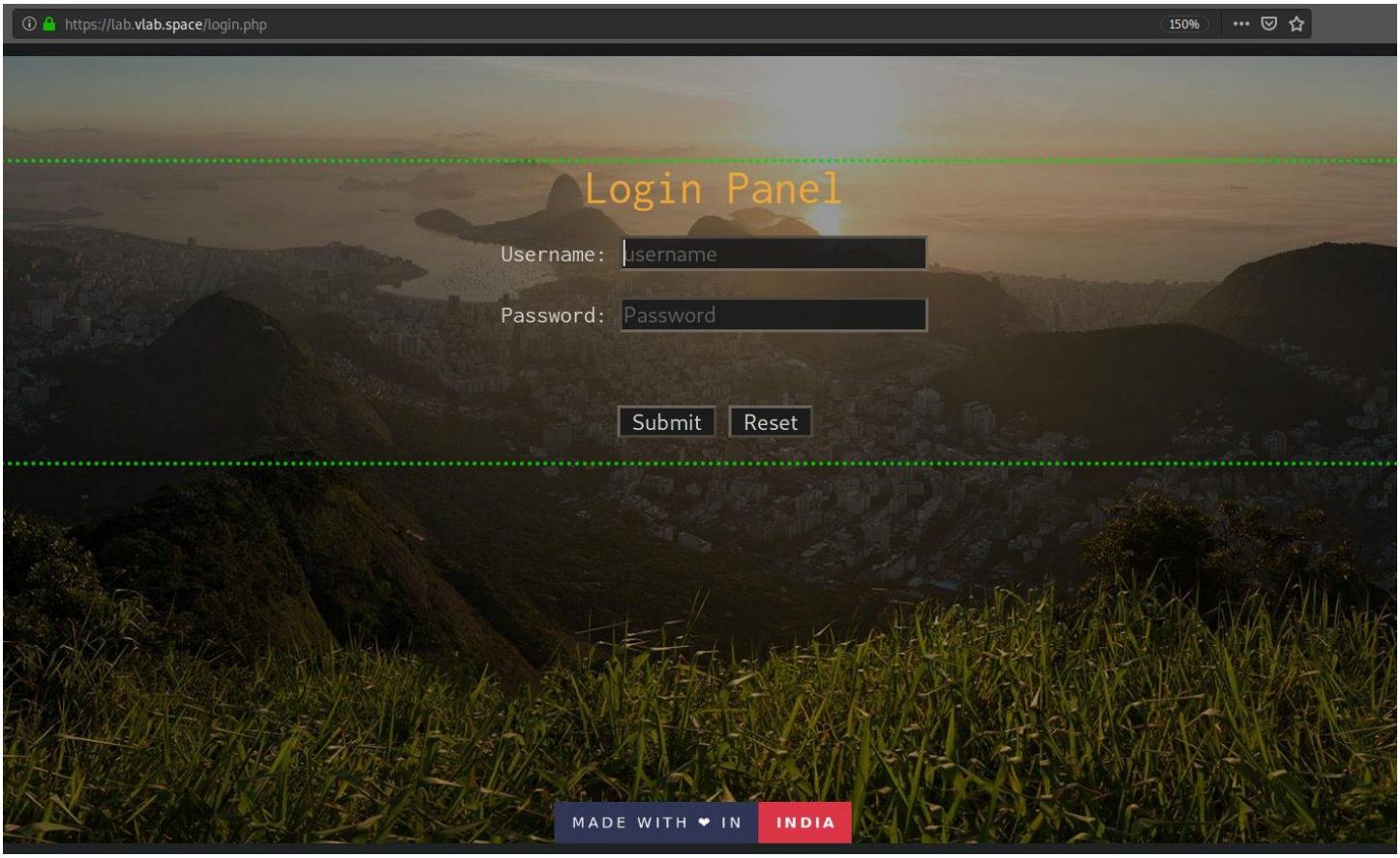
On visiting the link I couldn't find anything.



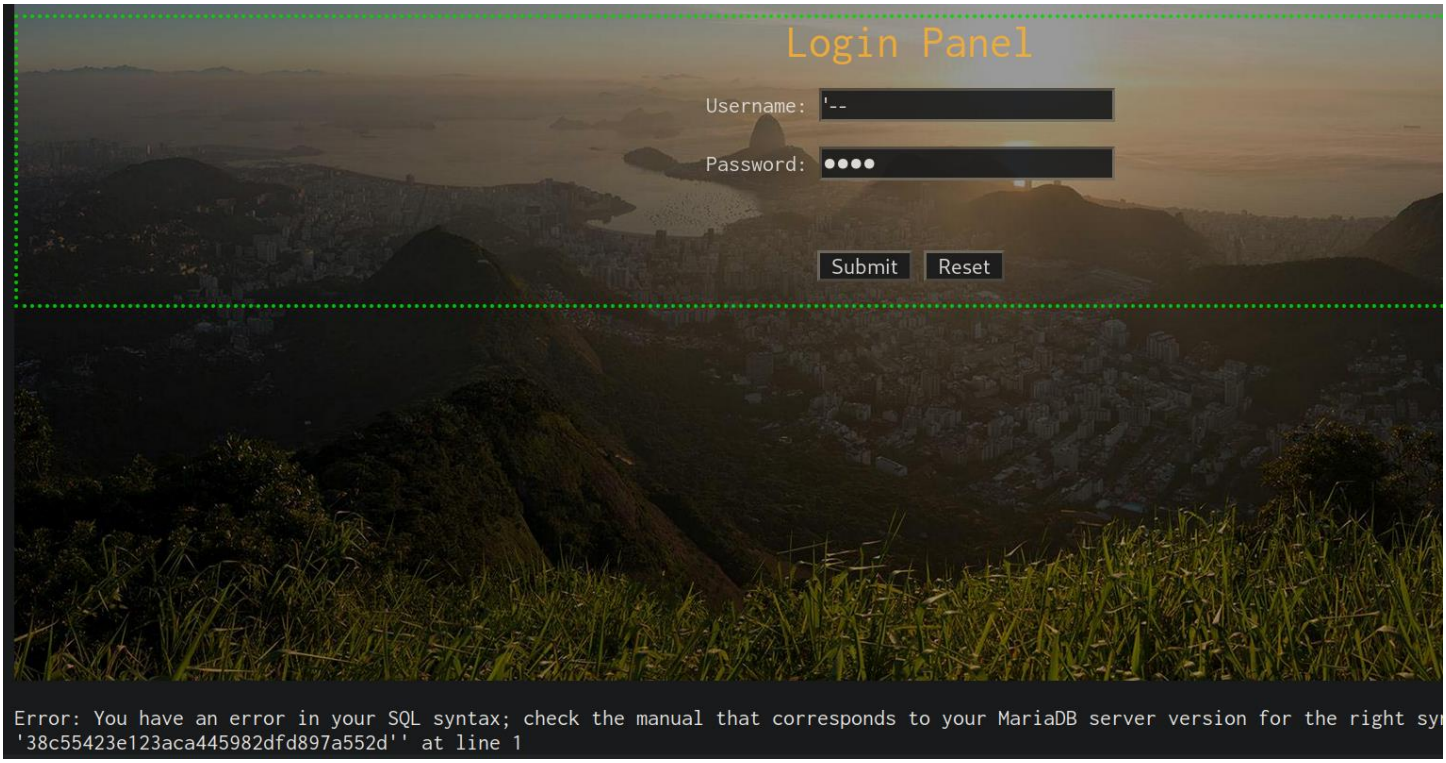
I tried accessing the sitemap, where I got the link to a login page.



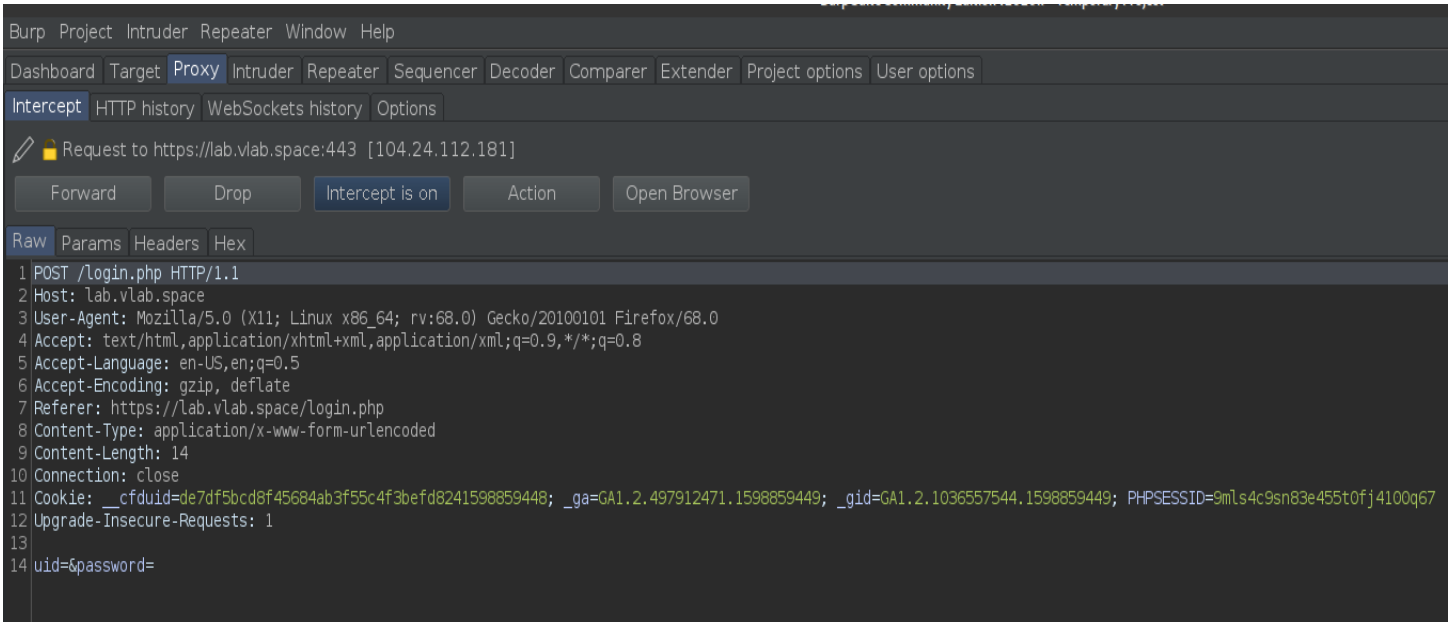
The login page looked like this,



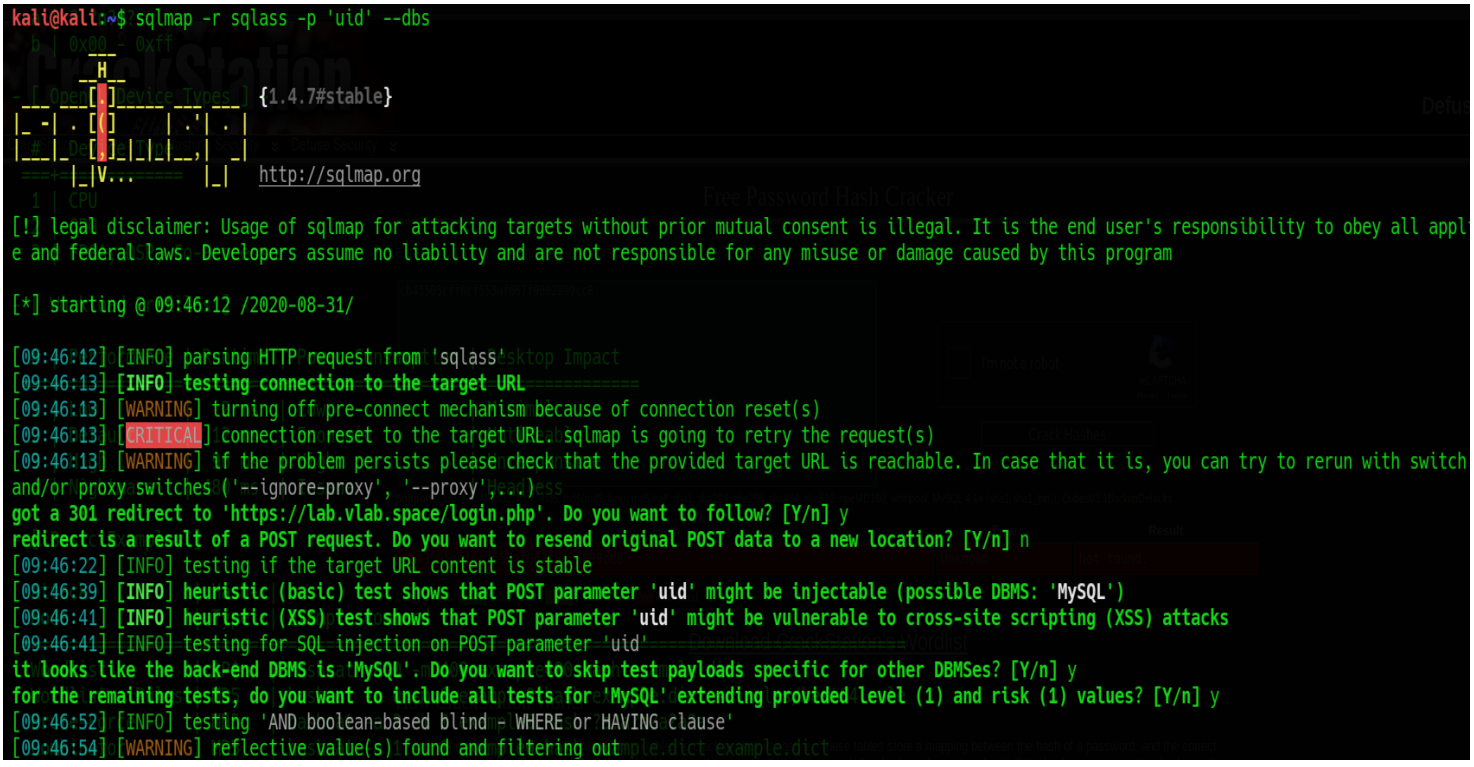
On trying some Sql injections, I found out that the username field was susceptible to Sqli .



I saved the burp request on a file .



Using the SQlmap with the request file. We get,

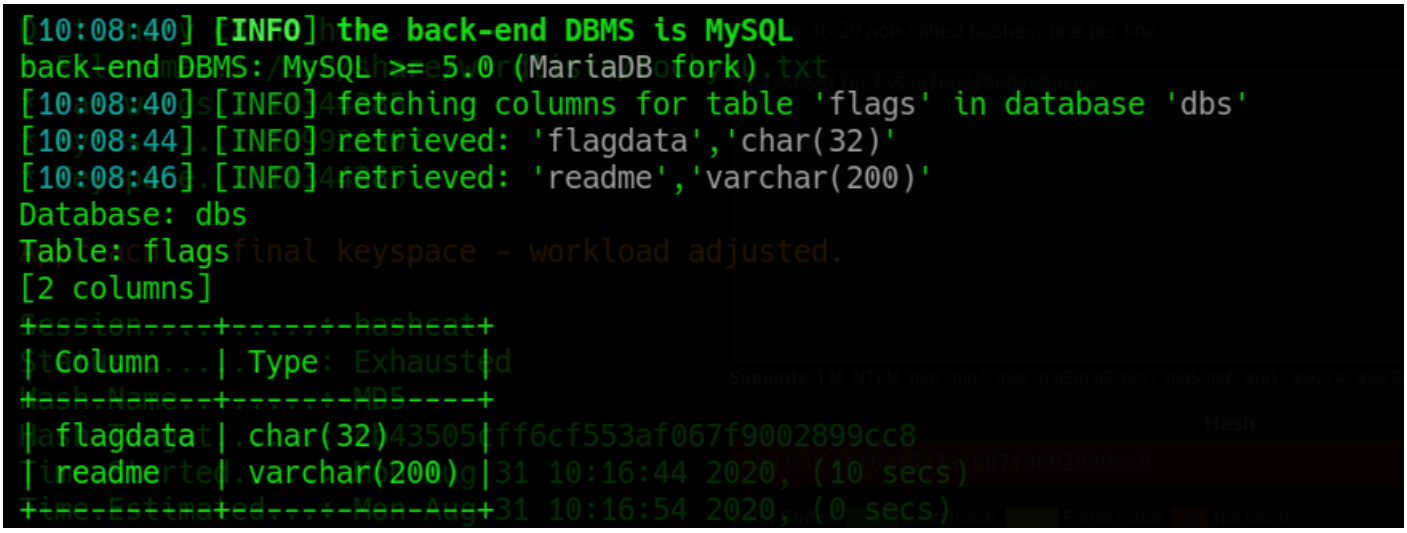


We get 2 database :

1. dbs

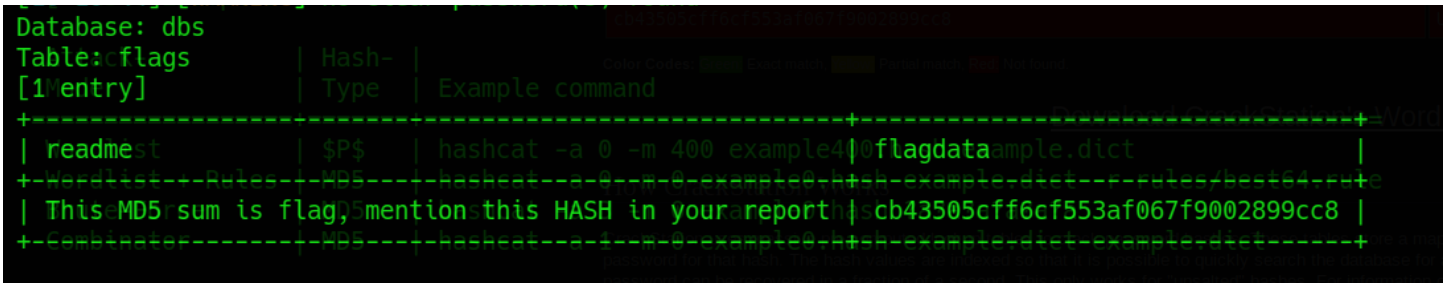
2. information_schemea

On dumping tables from dbs. We get,



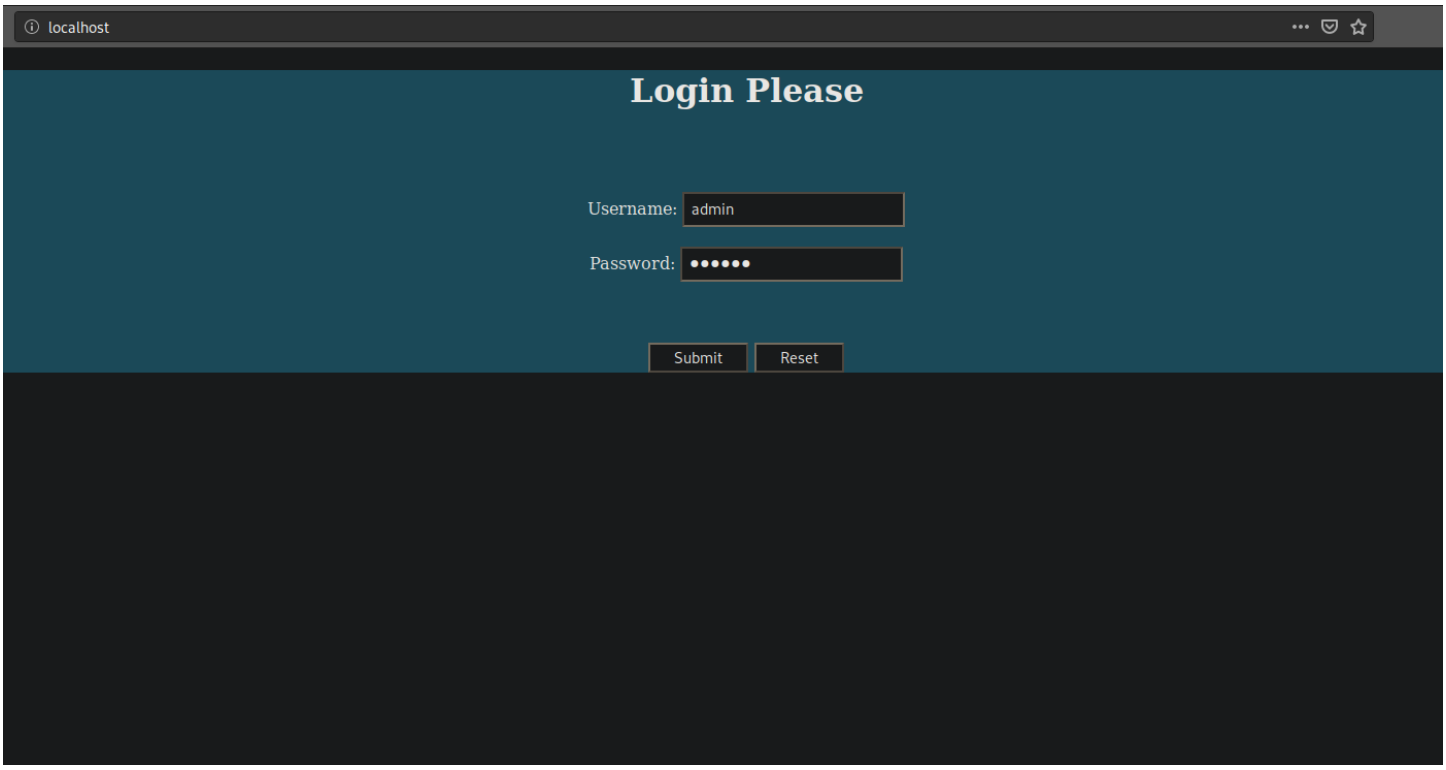
We get the flag by dumping the columns from above table.

>> **mysql -r /request_file.txt -D dbs -T flags --dump**

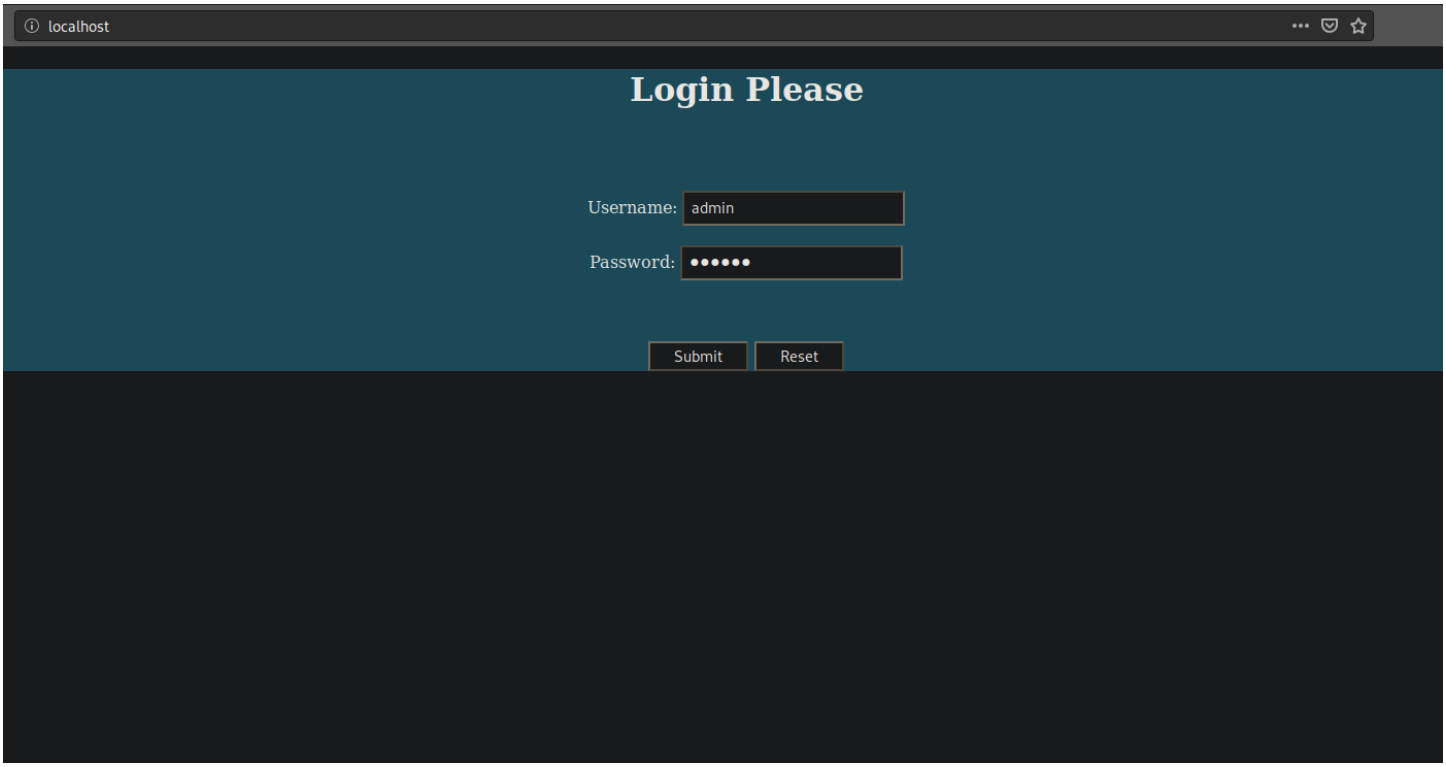


2. Wireshark

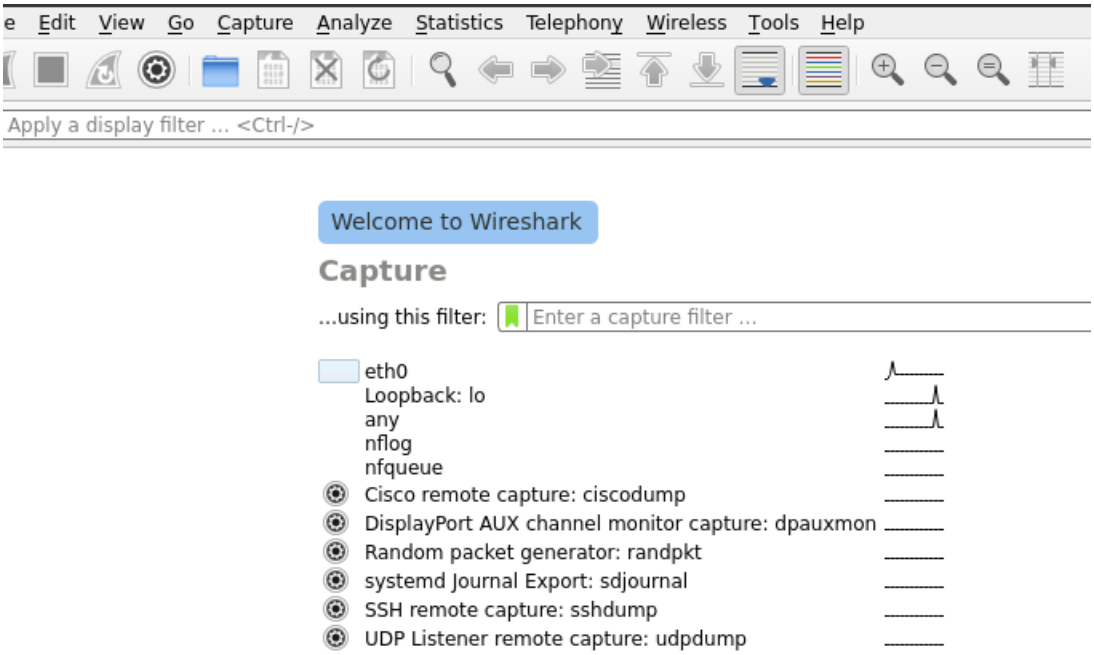
For this task I had hosted a http local site on apache2 so that the wireshark can capture the plain text password and username.

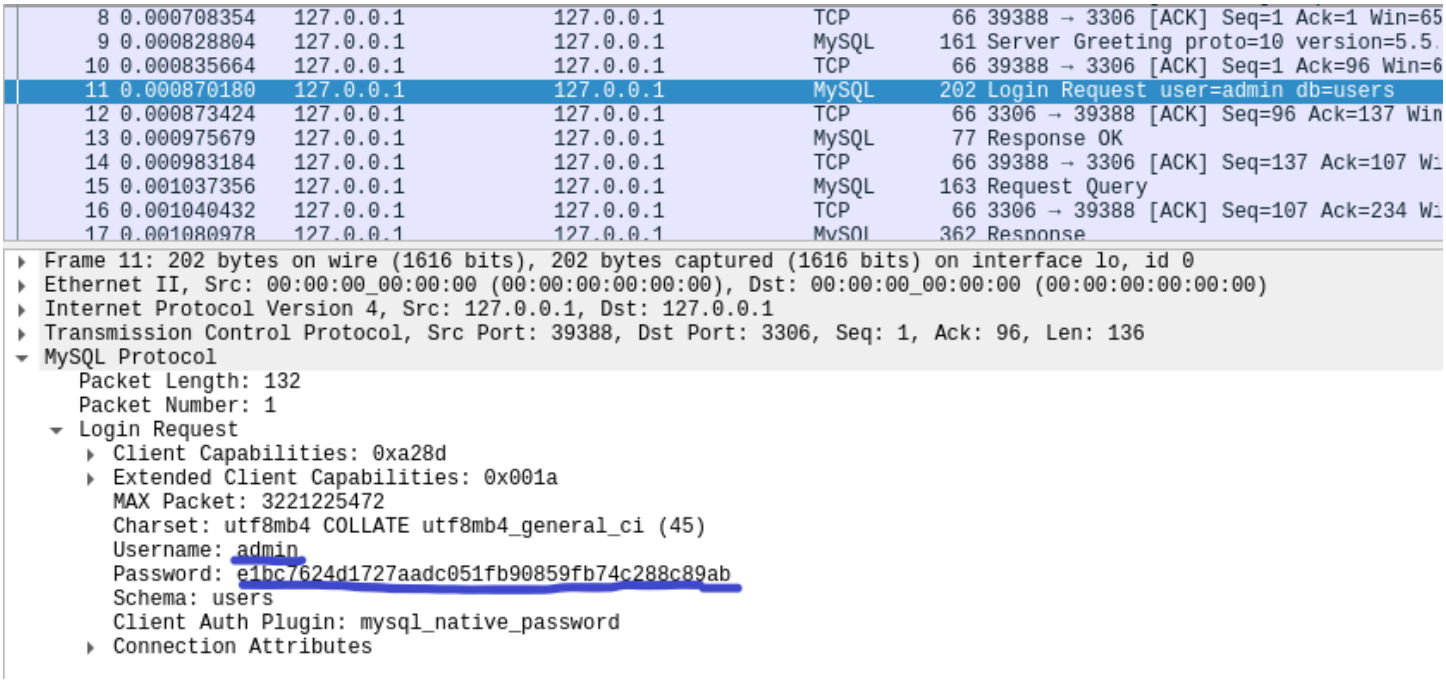


You can see that there is no padlock on the left side of localhost which means the connection is not secure.



Opening wireshark, we start capturing packets on **‘lo’** as the server is hosted on local server.

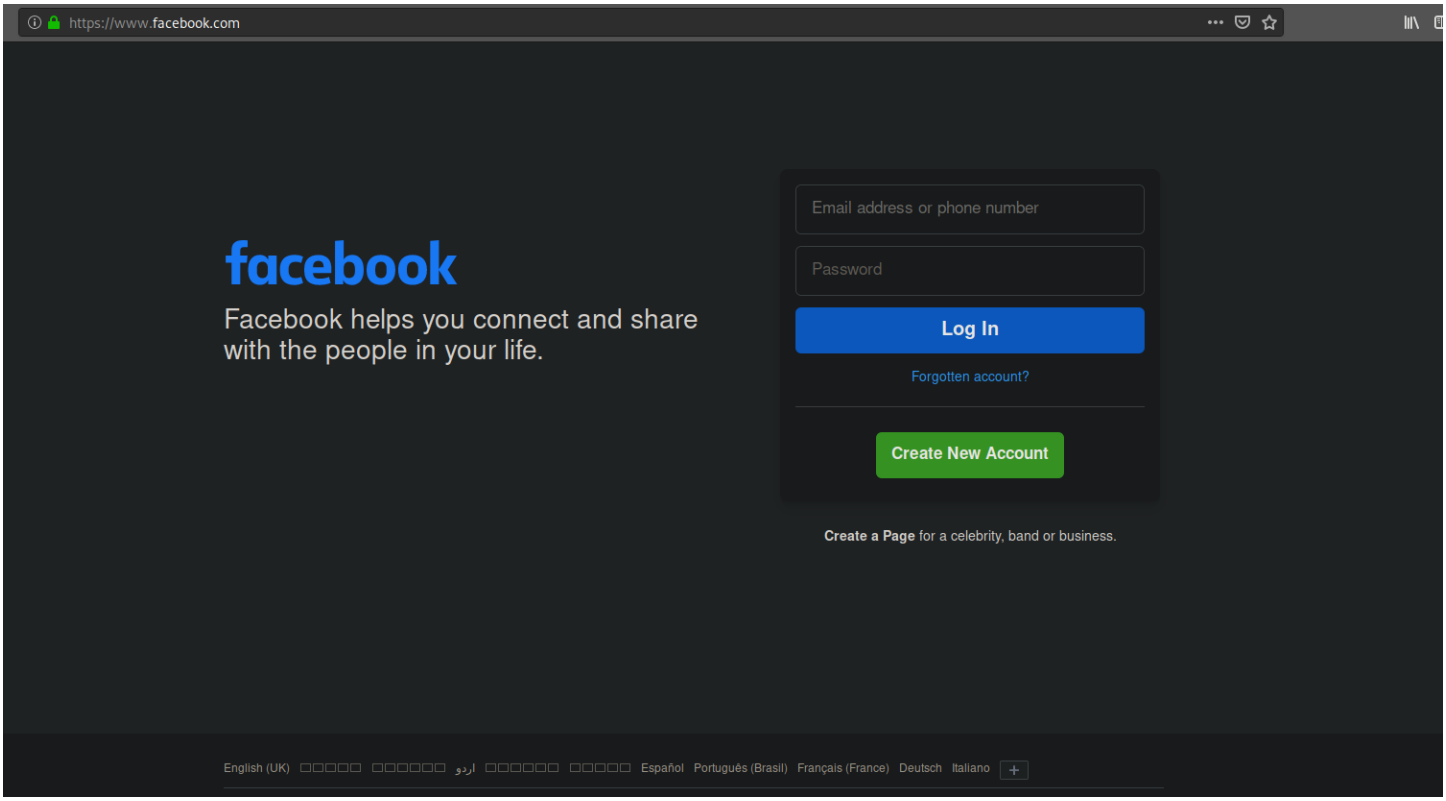




In the above image we can see that there is Mysql packet.

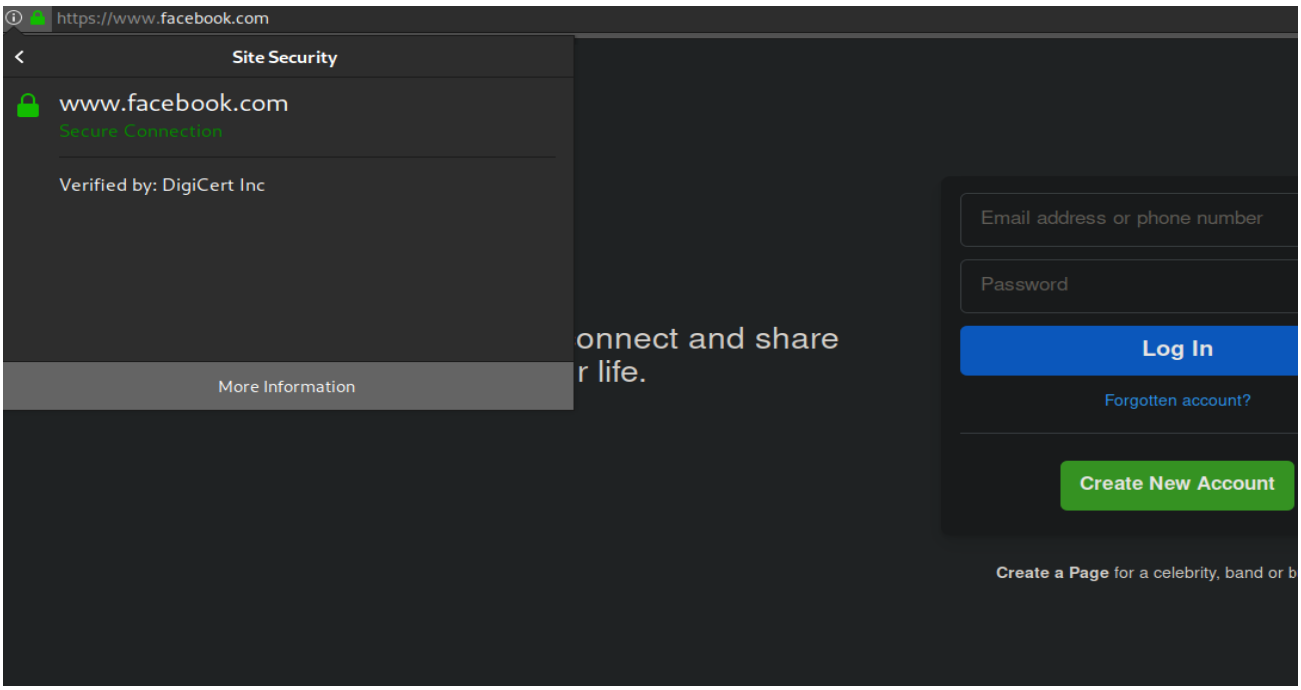
3. CA Path

I have selected facebook.com for this task.



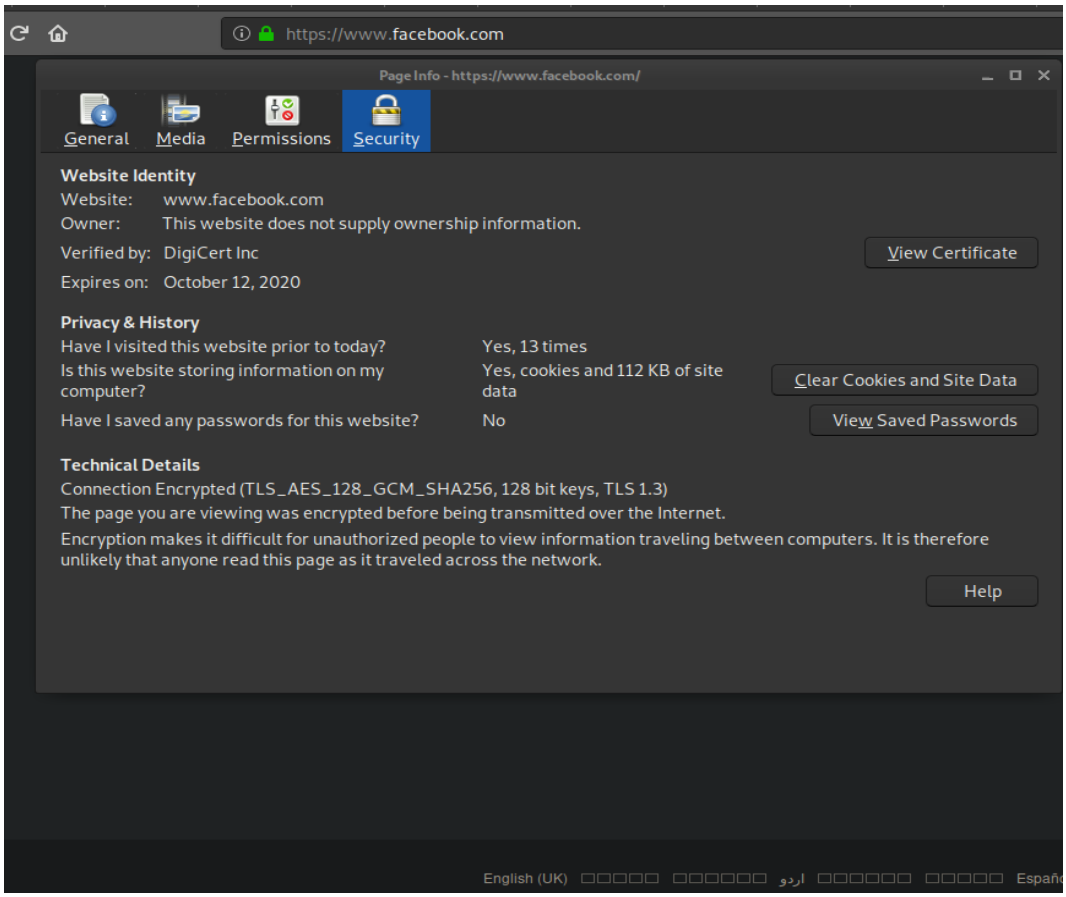
To inspect the certificates of the site :

1. Go to the padlock

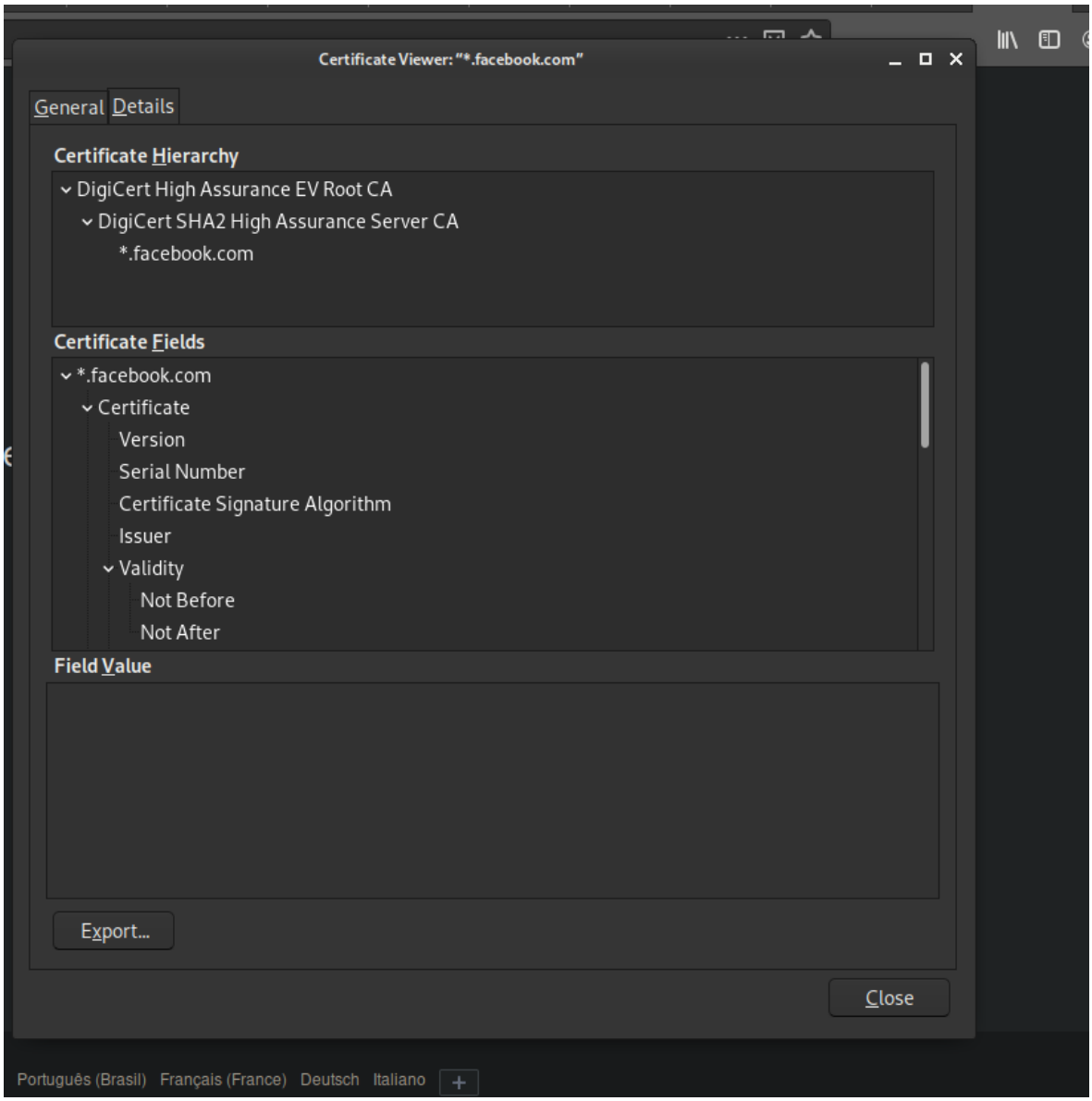


2. we can see that the certificate was verified by Digicert inc .

3. we go to more info and then view certificate.



4. below is the certificate path.



ROOT CA -Digicert

SERVER CA- Digicert

And then comes facebook certificate.