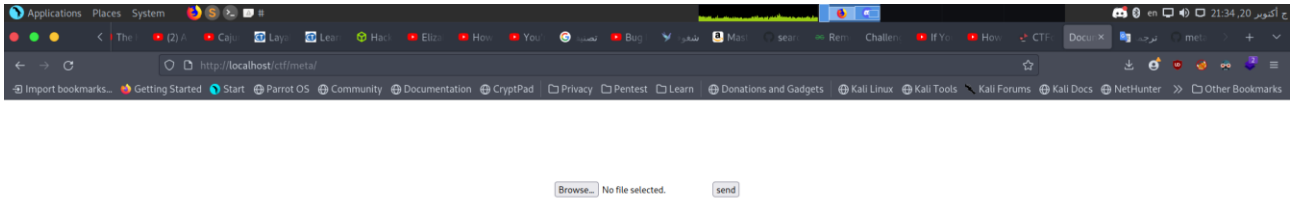
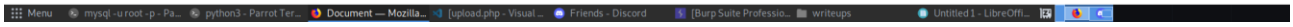
meta challenge | hard title

Reported By:
AZZAM AL DUYULI

Reported To:
Academy of learning

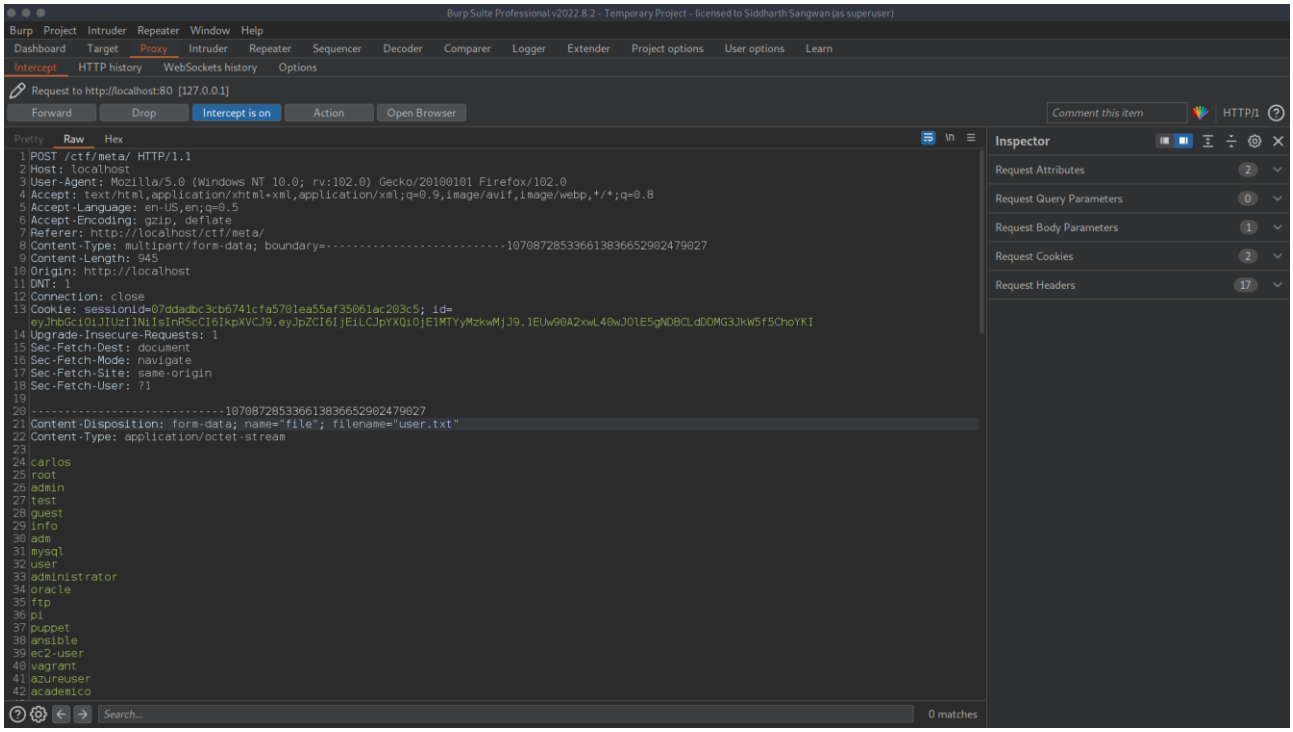




.

When I started challenge I saw input for upload file so I think it’s file upload vulnerablity so I try to upload file then I serach about upload directory but I didn’t found any directory but I found file called upload.php and when I go inside it I see the name for my file in it so without extention so I thind this maybe sql injection in the name for the file so come back to home page and choose file to upload it and intercept the request by using burp suite and this is the request.

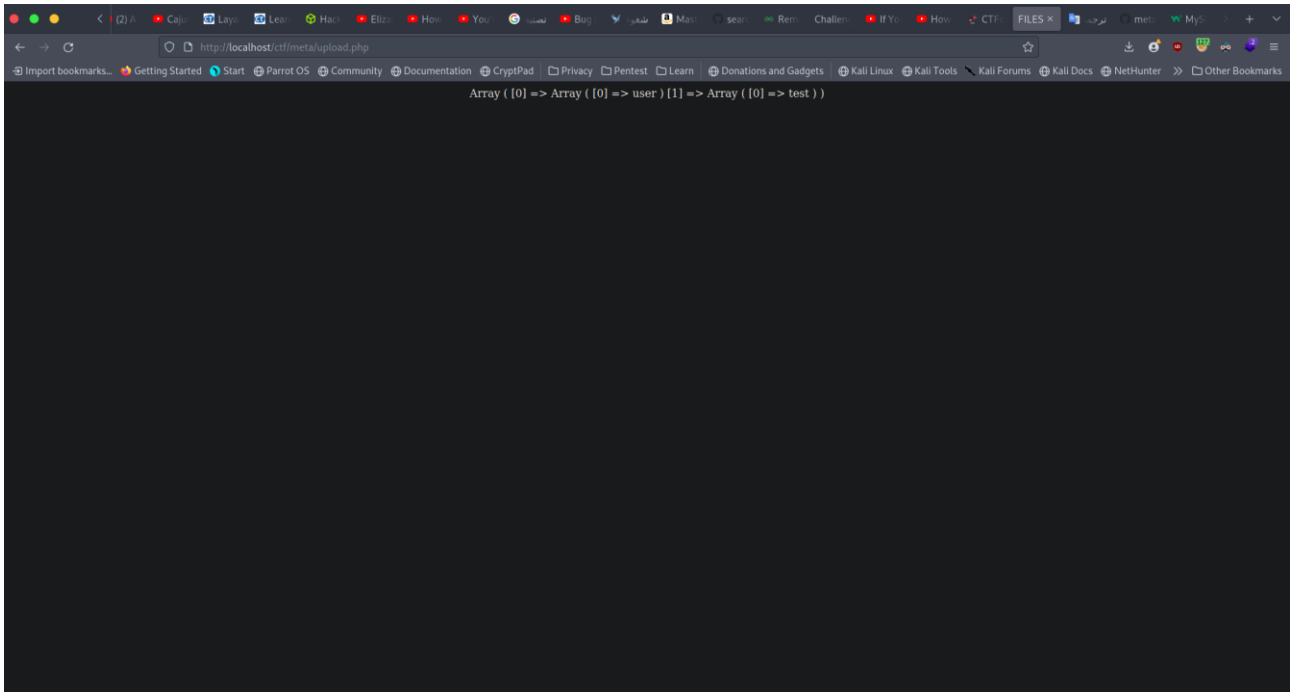
.



.

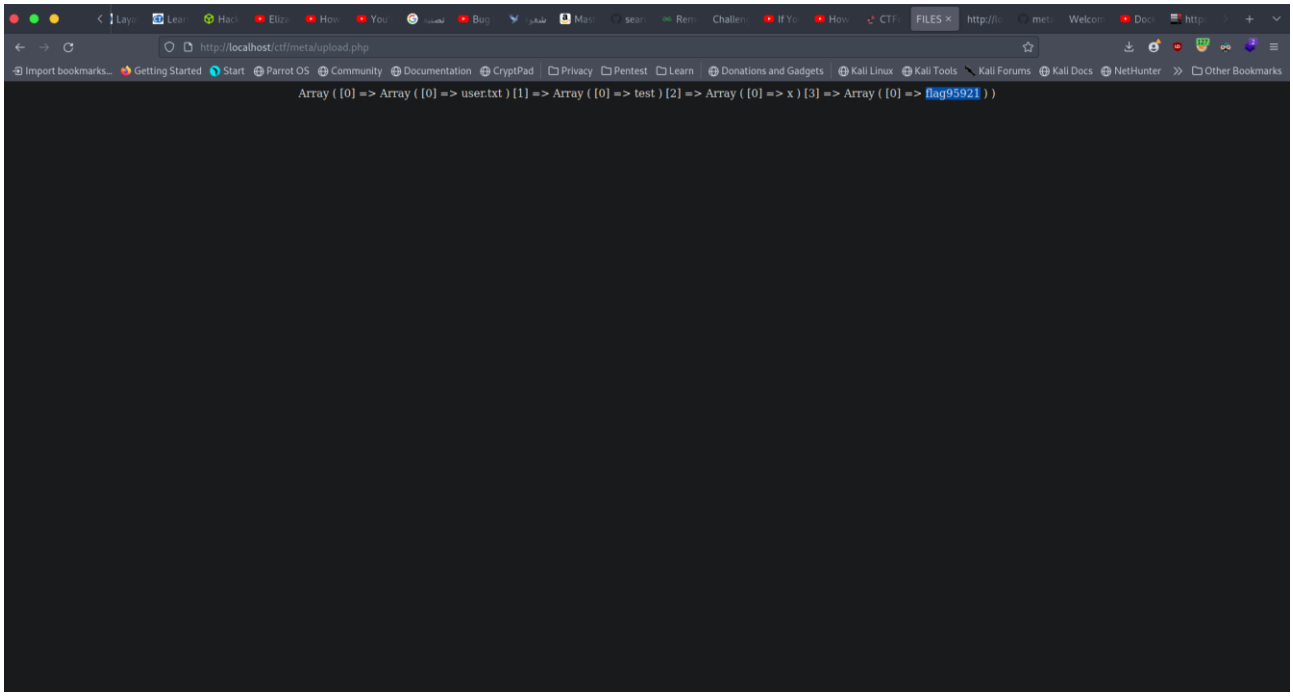
The name for my file is user.txt so we can see this name in the request in the Content-Disposition: exactly in the filename. So if I change the value in filename to test.txt and upload file and then go to upload.php pgae I will see test.txt like this

.



.

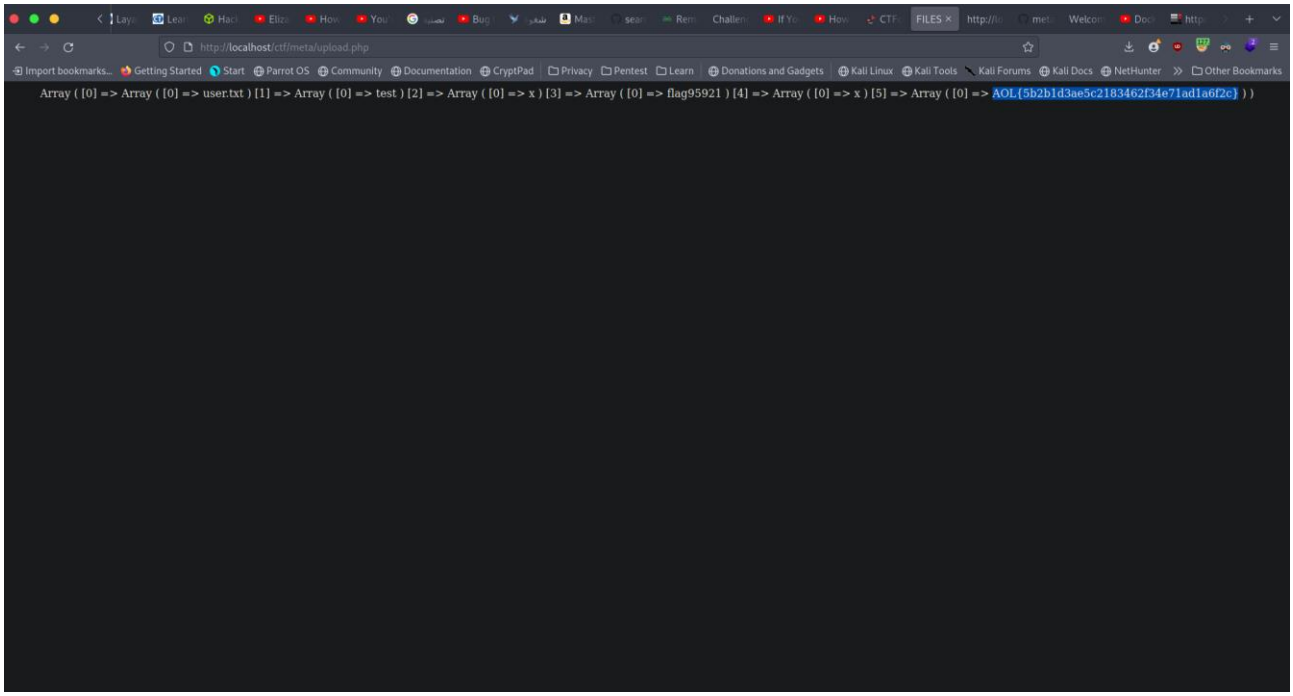
So I will upload file again but I will intercept the request and send it to repeater in burp suite and I will change the filename to test'.txt and send it and in upload.php page I didn't see it.So I think maybe it's sql injection . So I come back to repeater in burp suite and put this payload in the filename to exploit the sql injection I enter this payload → x'),((select TABLE_NAME from information_schema.tables where table_name like '%flag%'))#.txt
This payload to find any table in this in this database contain in his name the flag word
then in the upload page I see this



.

I see table has name flag95921 so I write this payload to read the data in this table (flag95921)
- > x'),((select * from flag95921))#.txt

And I see the flag



.

This is the end of the report