
# IT APP. SEC. LAB FILE

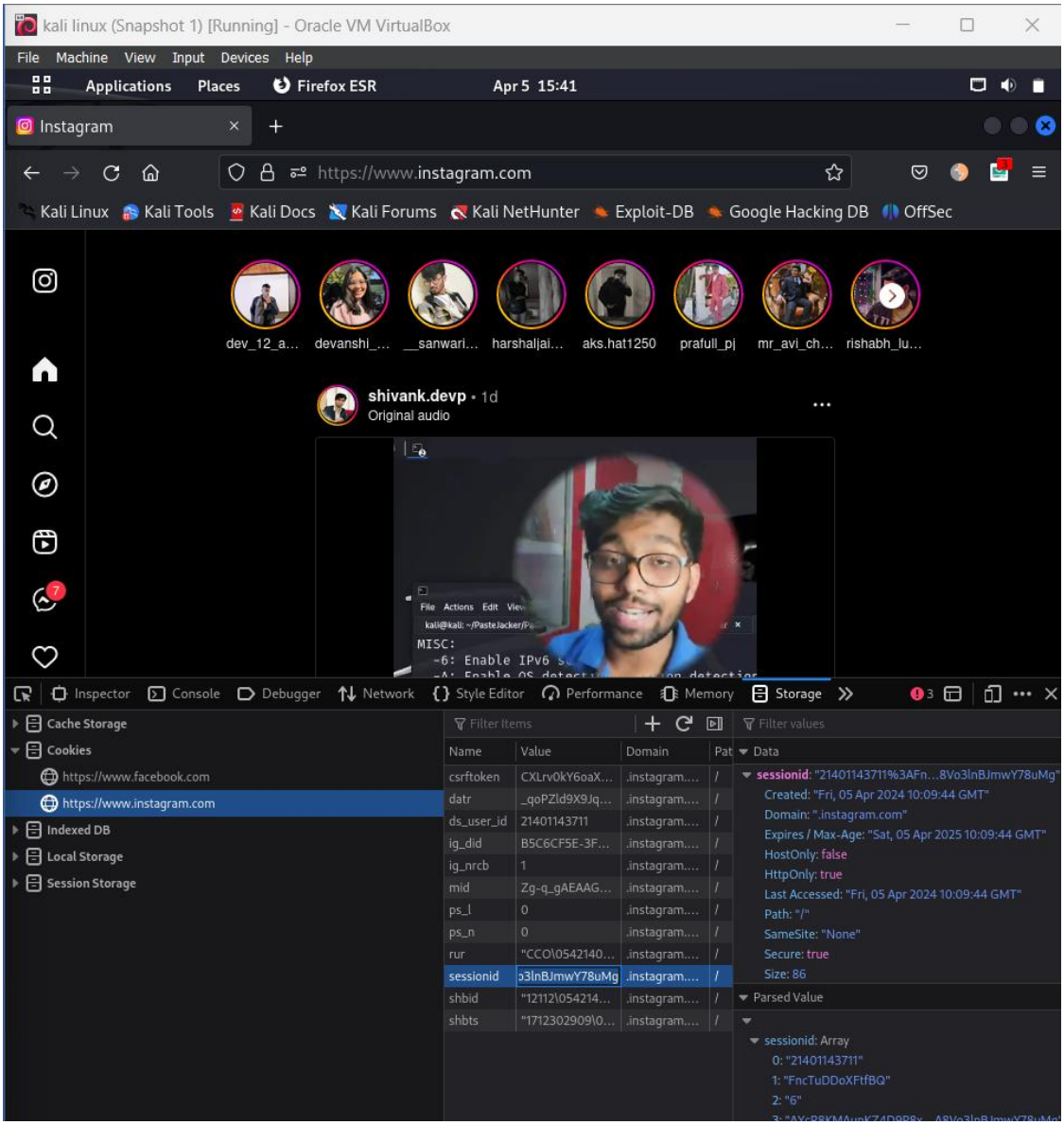
To- Dr. Gopal Rawat

**Name- Dhairya Jain**
**Sap ID- 500105432**
**Batch- CSF-B1**

Aim- Cookie replay

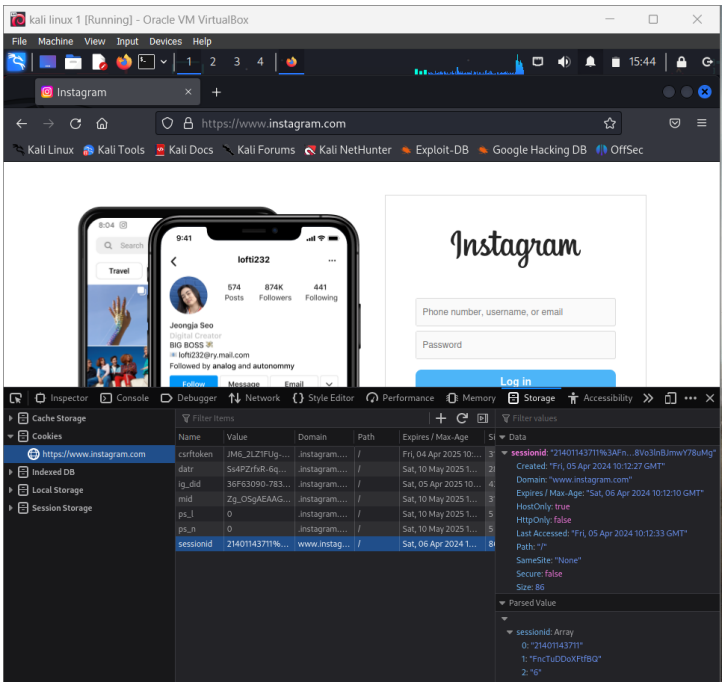
- **Instagram.com**

➢ Taking cookies from Instagram by inspecting the page then go to storage then cookie in cookie look for session id copy the session id from here

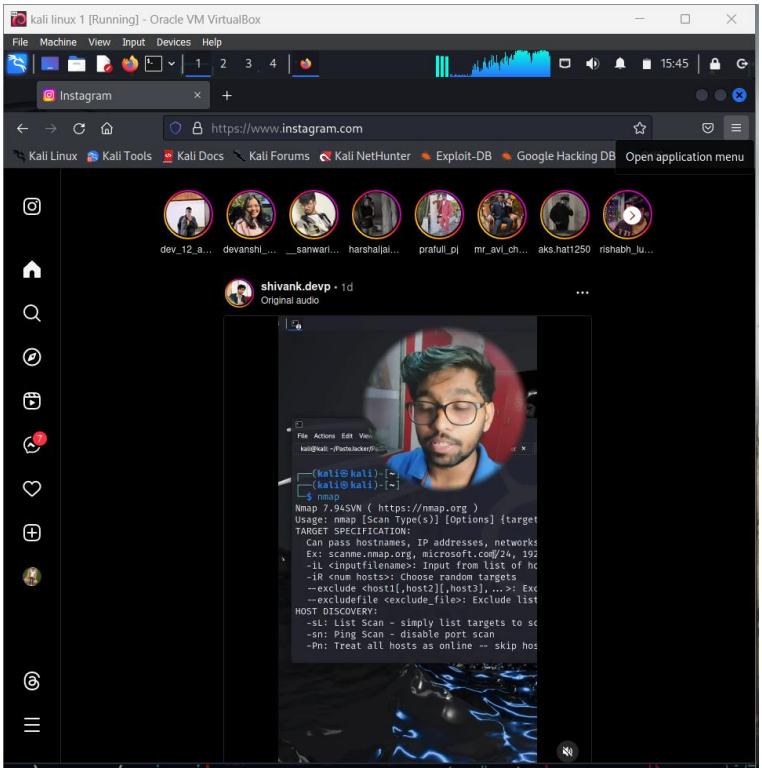



➢ Replaying cookie on different vm

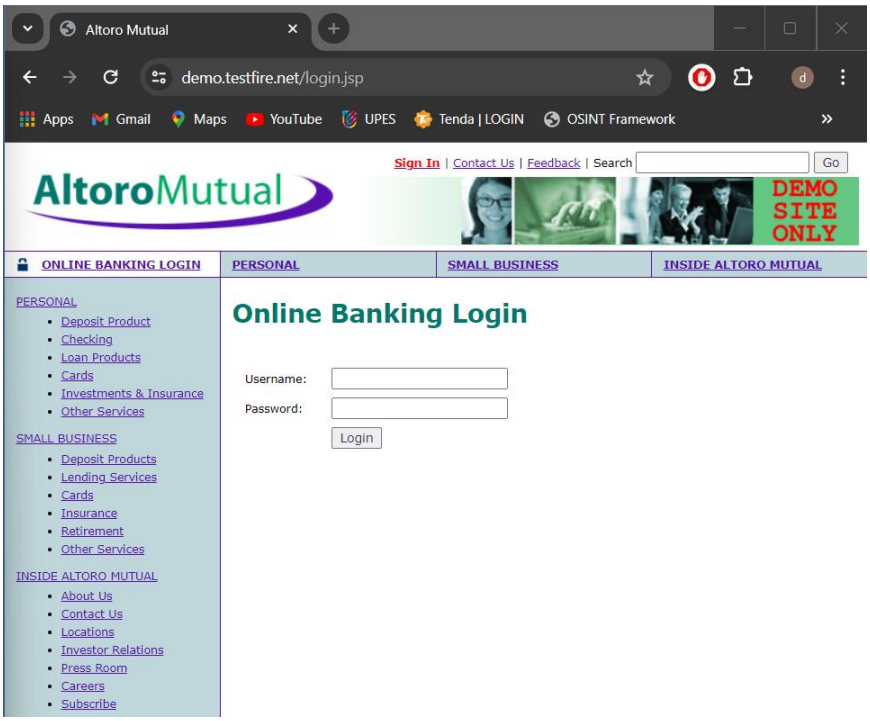
➢ Follow the same step as above at place of copying session id value, Create new instance and set name as sessionid and paste the copied or steeled cookie in value part

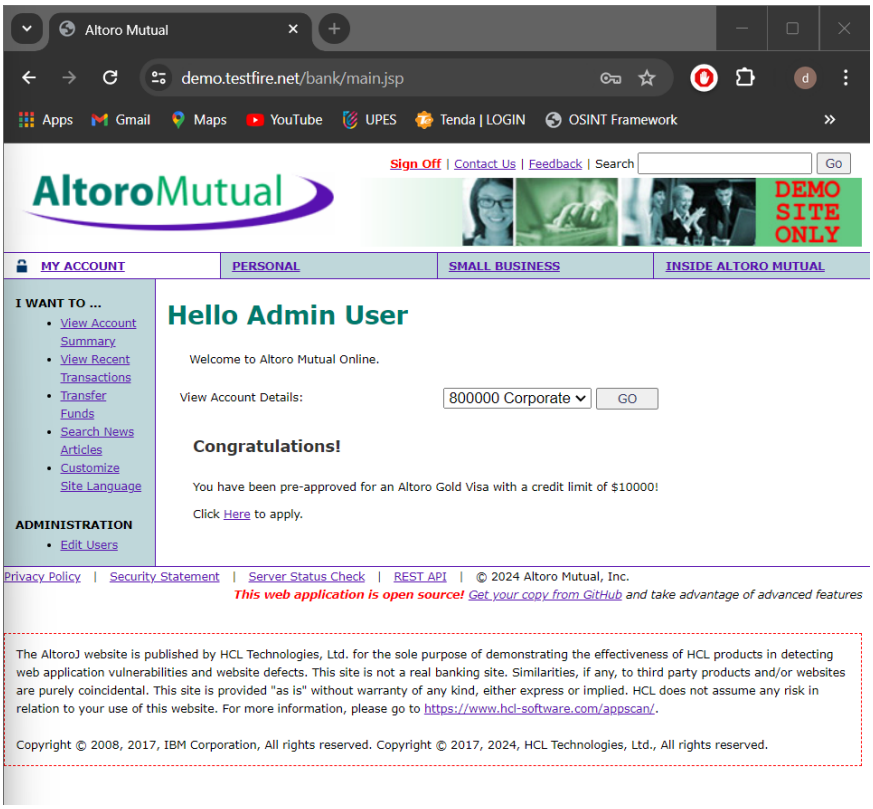



- Signed in without id password by replaying the cookie

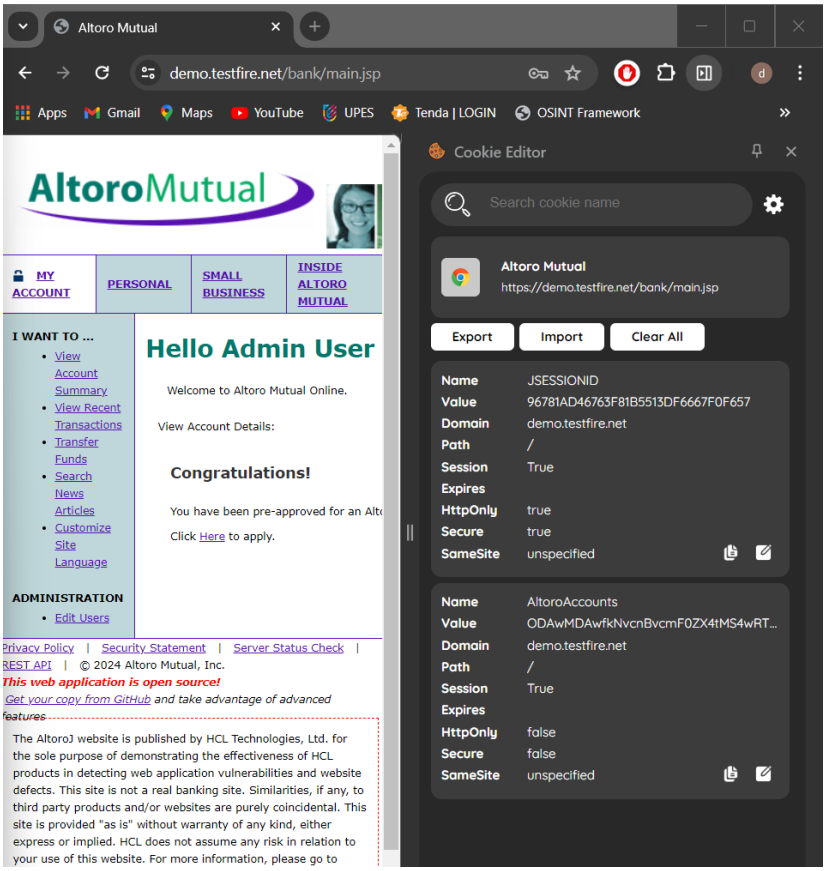


- https://demo.testfire.net/
  - Now we will capture the cookie from base machine(windows) and replay it on kali linux(vm) for https://demo.testfire.net/
  - Username-admin
  - Password-admin

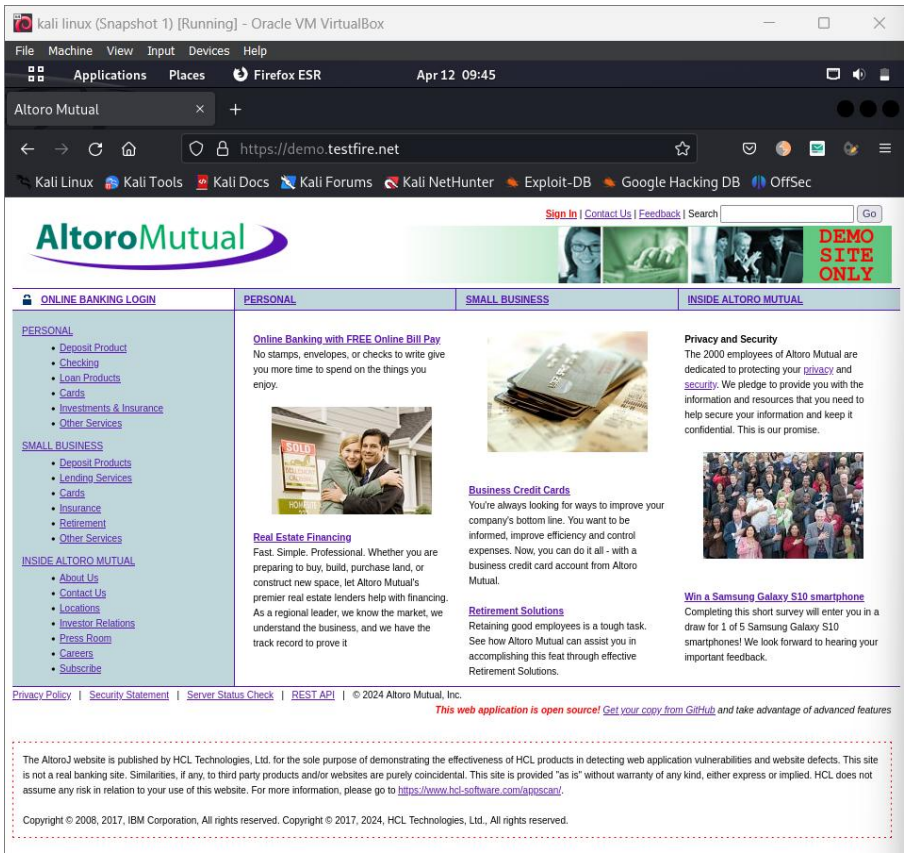


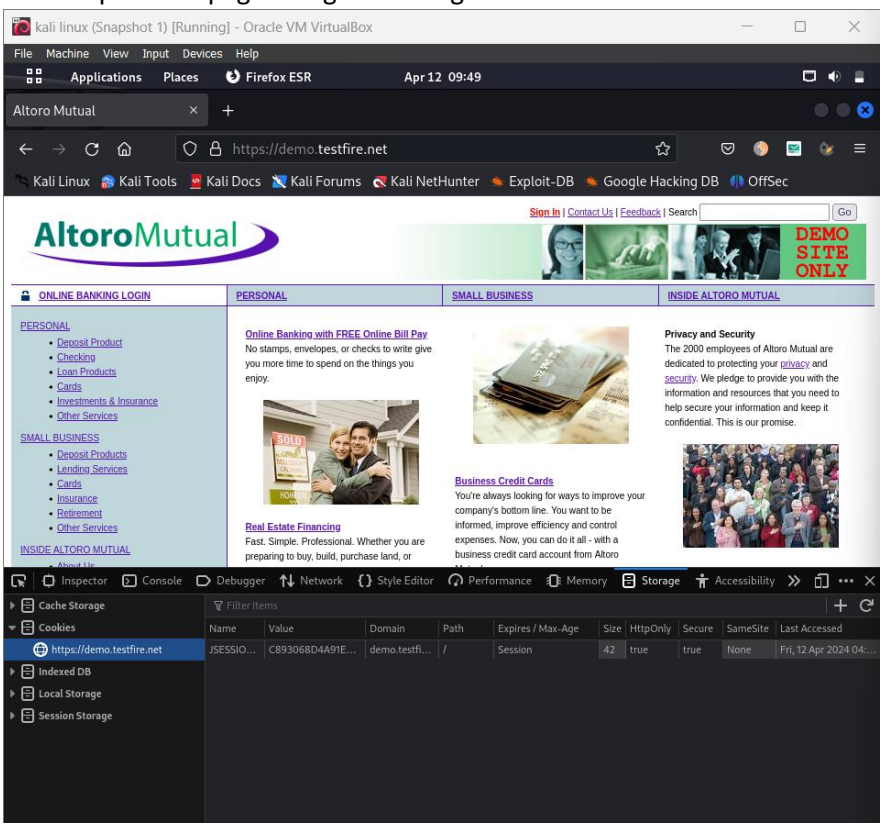
- After logging in capture cookie using extension cookie editor or you can also capture cookie from settings also



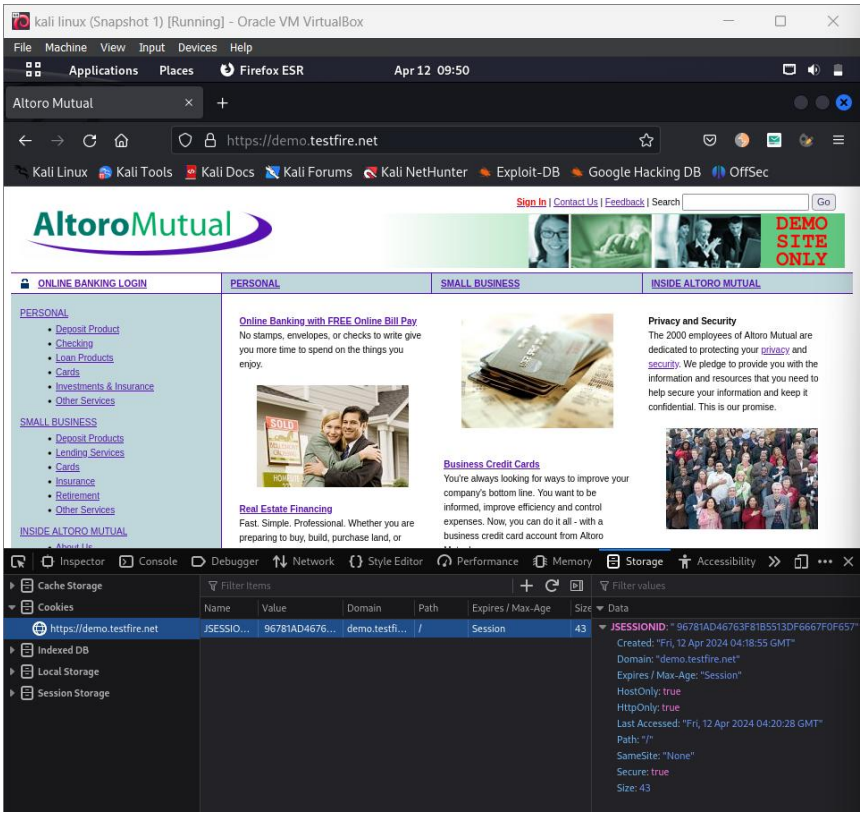

- Now go to kali linux and paste the capture cookie there for replaying



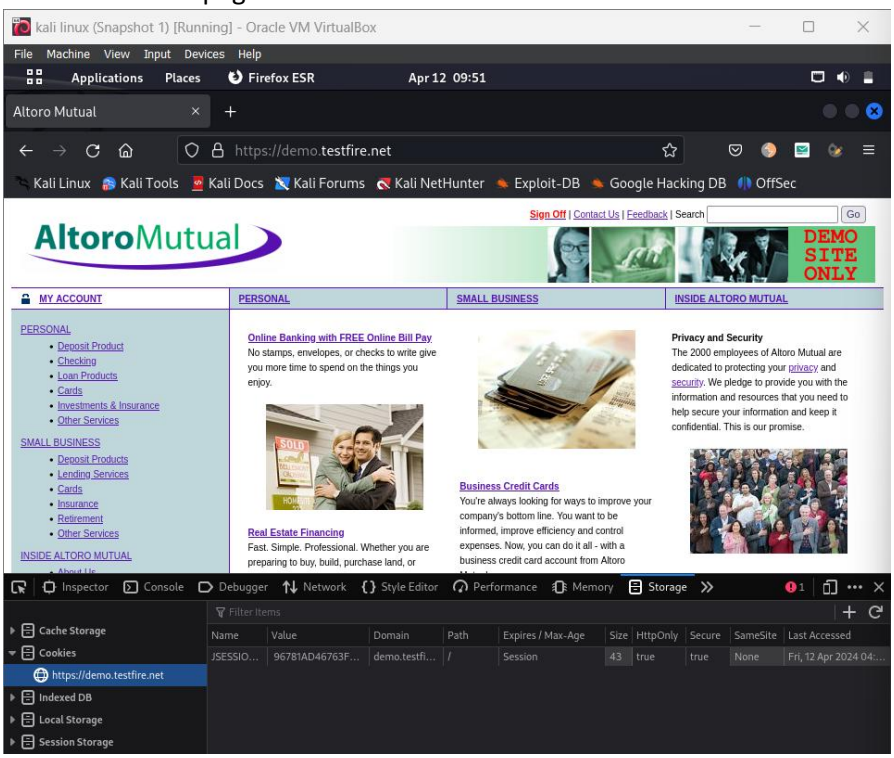
- Now inspect this page and go to storage then cookie the see for sessions




- Now edit the session value and paste the captured cookie there



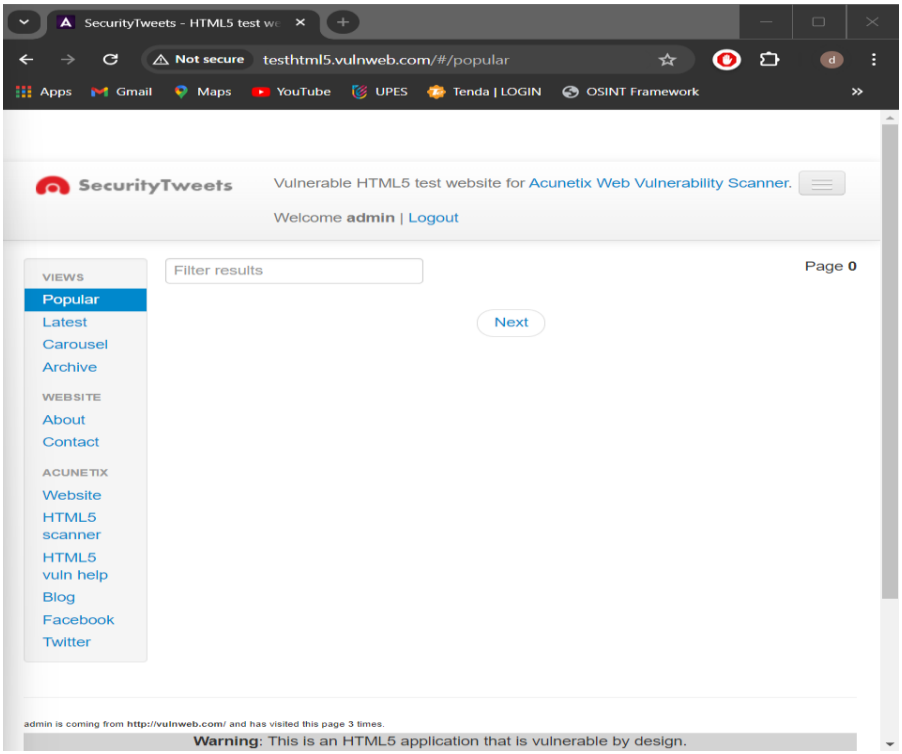
- Now refresh the page



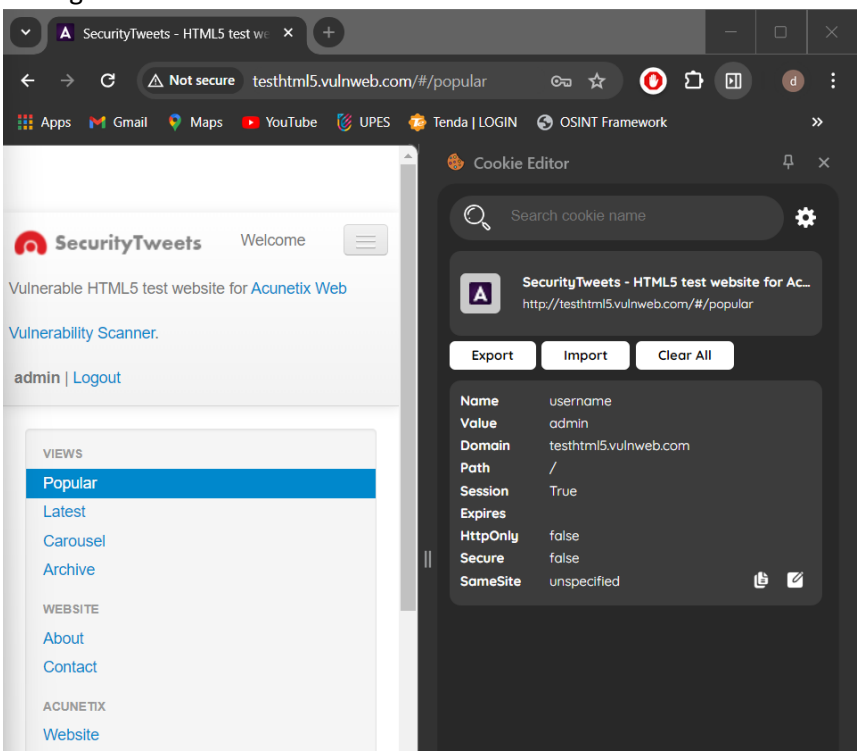

- After refreshing the page we found that we are signed in without entering id password by just replaying cookie

- Vulnweb.com

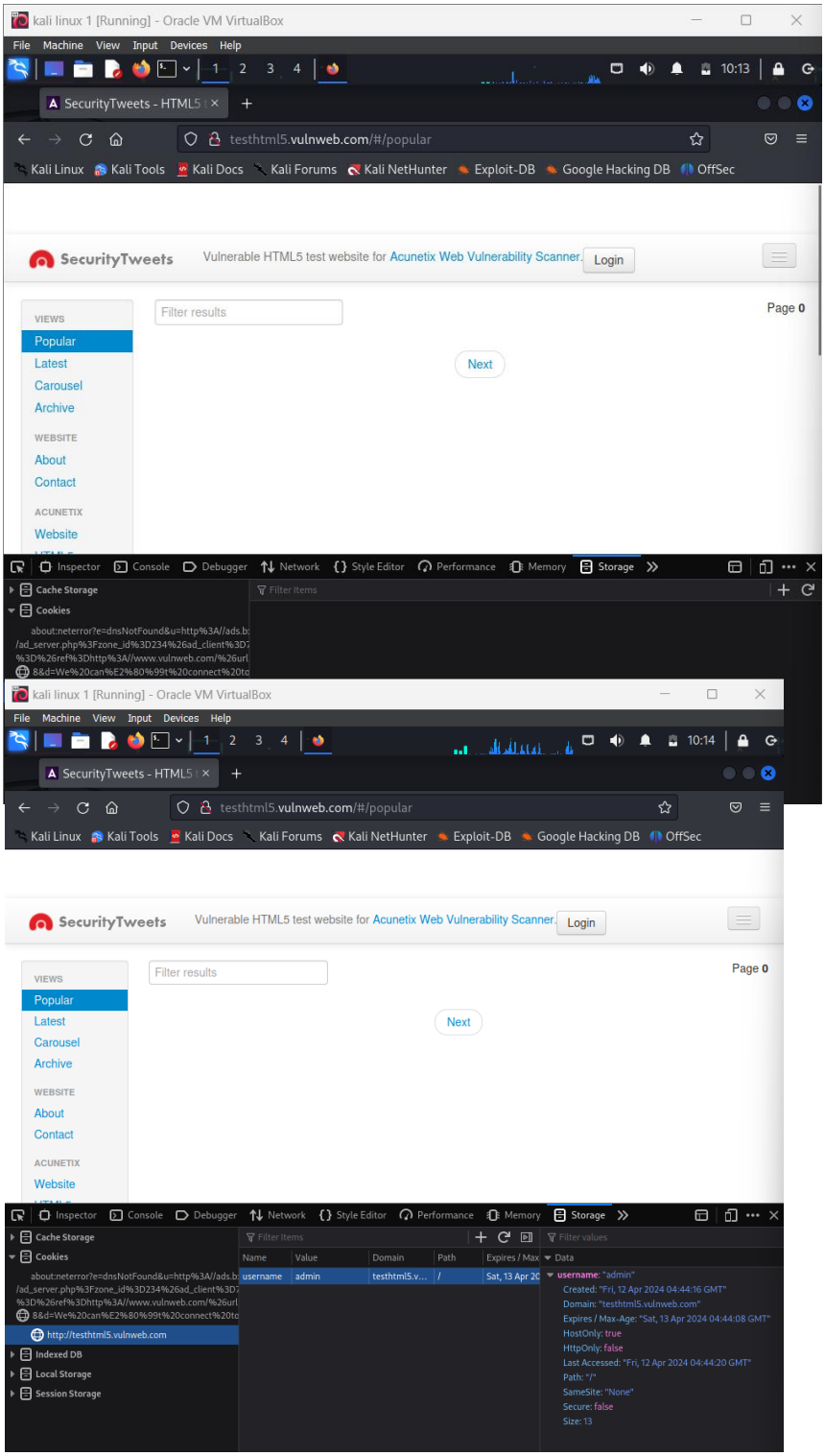
➢ Go to vulnweb.com open securityTweets and login by using id- admin password-123456



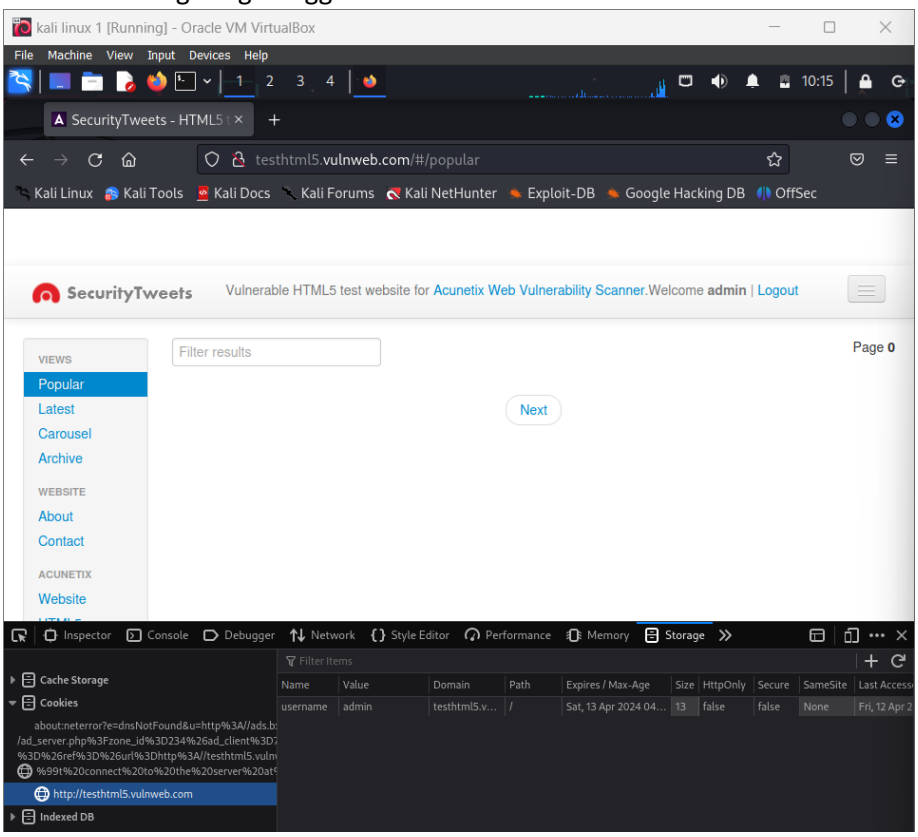

➢ After logging in capture cookie using extension cookie editor or you can also capture cookie from settings also



- Now go to kali linux and paste the capture cookie there for replaying
- Now inspect this page and go to storage then cookie Now add new instance and paste the captured cookie there then refresh the page



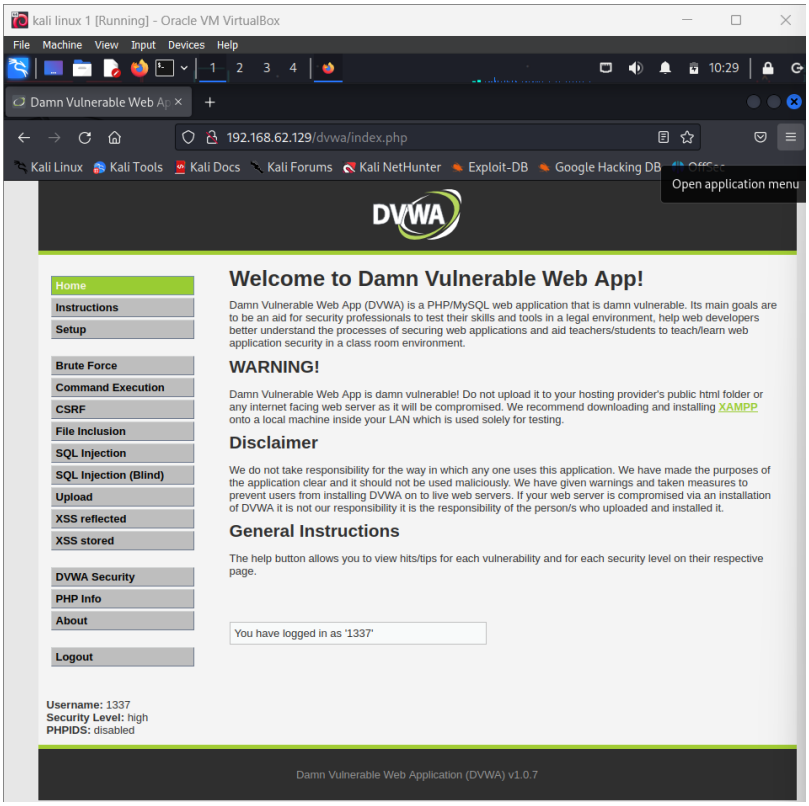
- After refreshing we get logged in



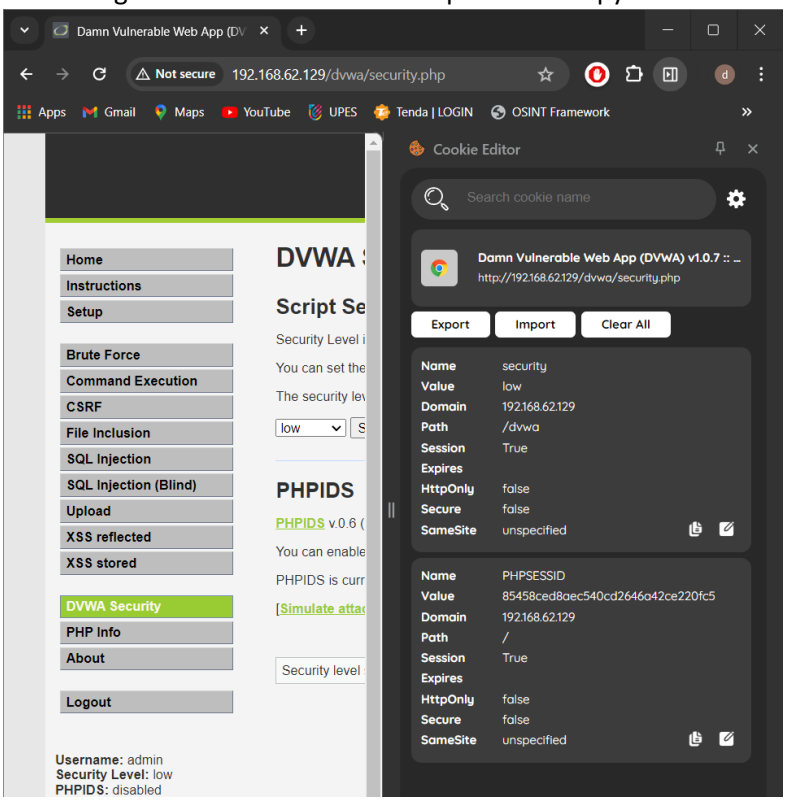
- **DVWA(for low)**

➢ Login the dvwa in windows with user name- admin and password-password at dvwa security low

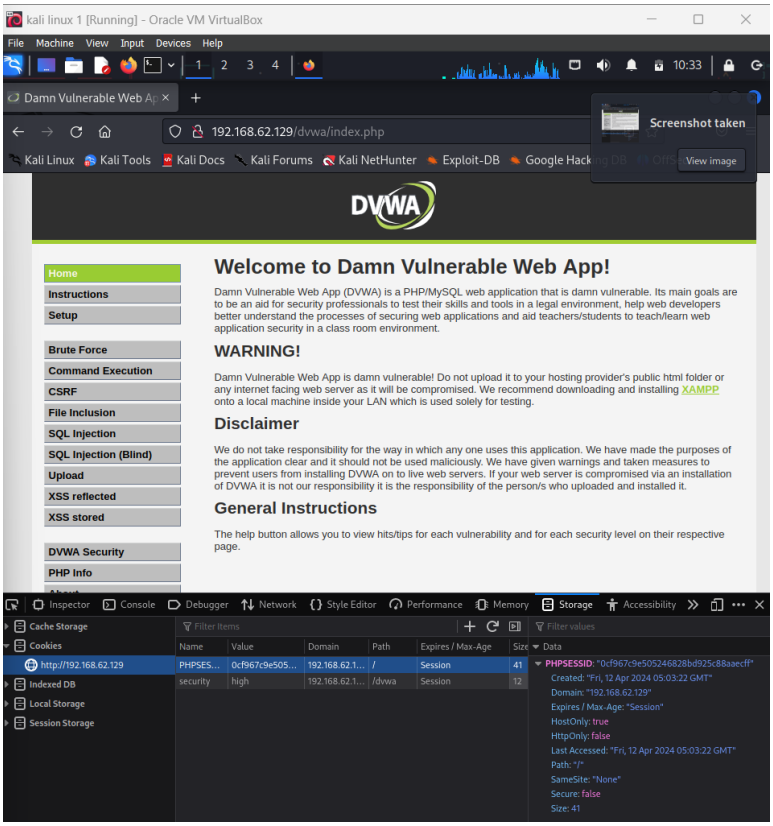

➢ And in linux login using id-1337 and password-charley



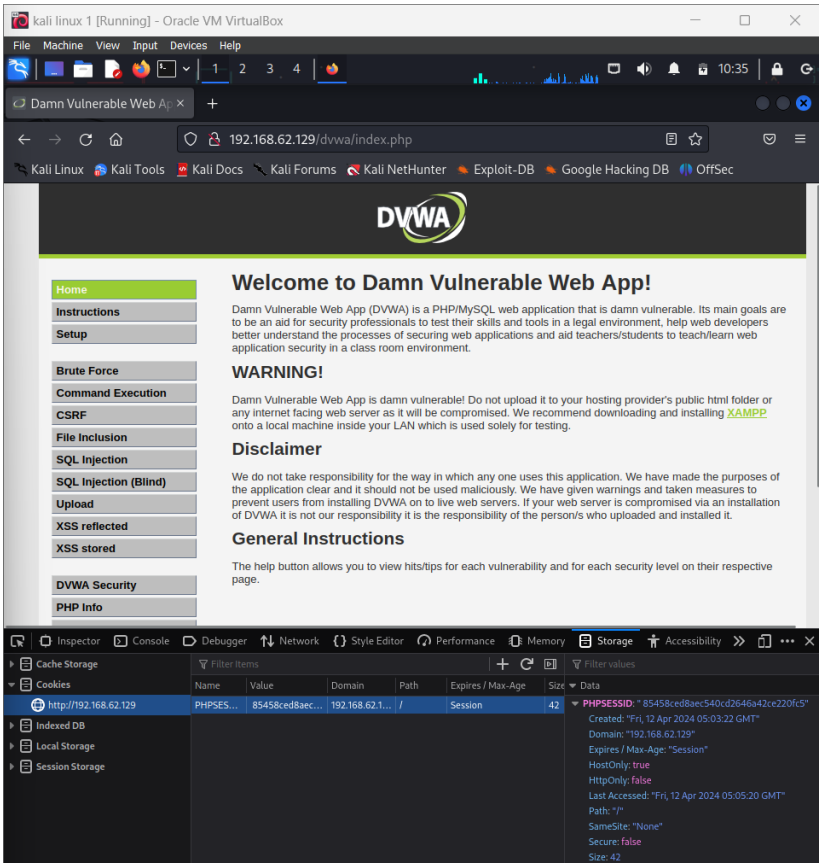
- Now using extension cookie editor capture and copy the cookie from there



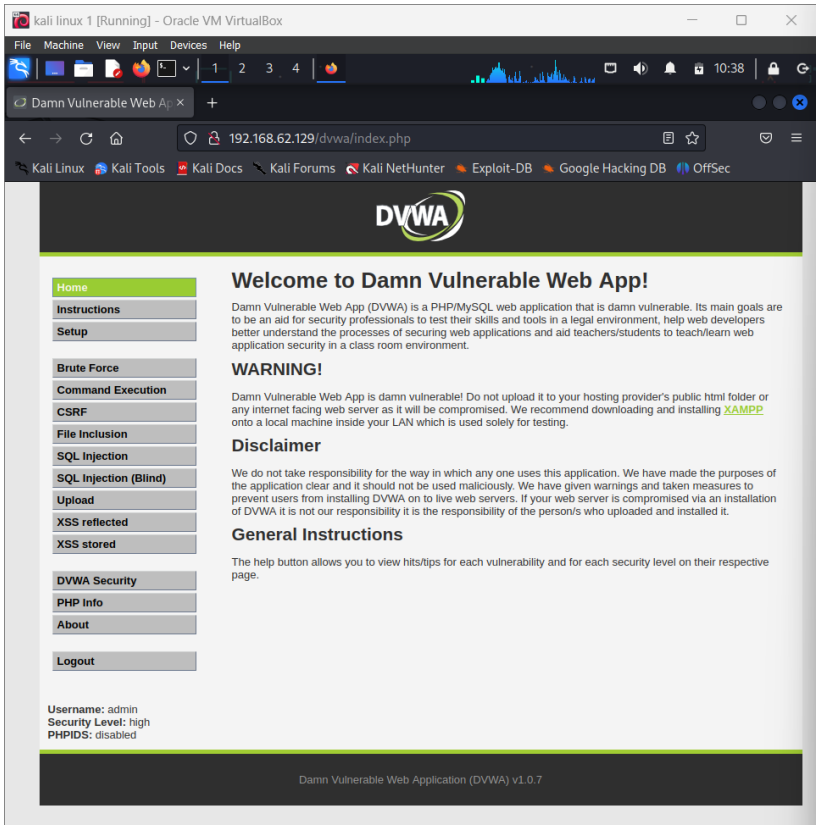

- Now go to linux and inspect the page and go to storage then cookie



- Now remove the security attribute and edit the phpsid and paste the cookie copied from windows

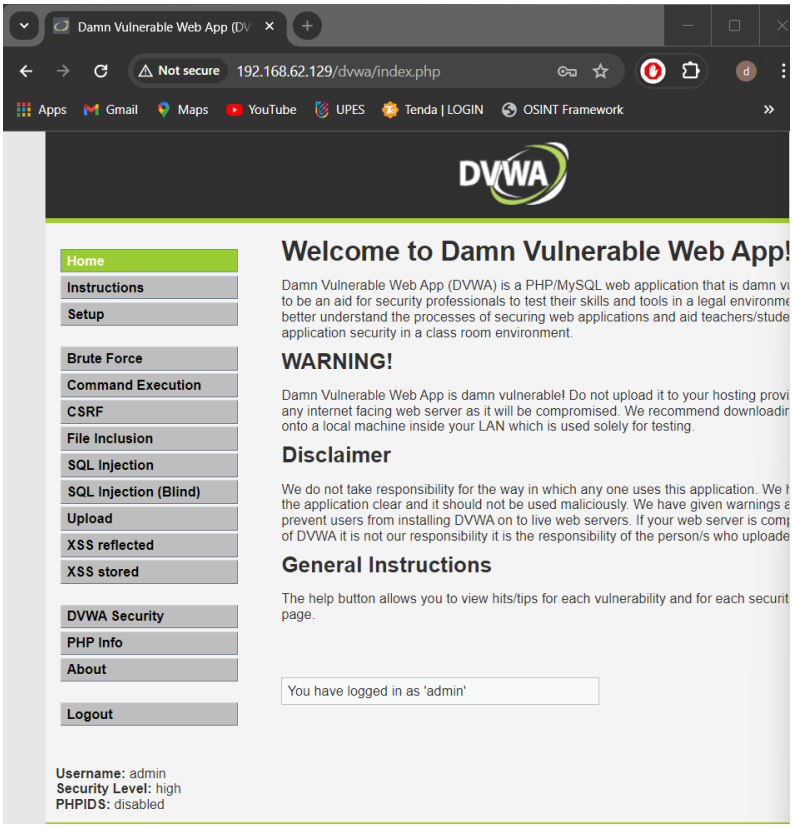



- Now refresh the page and you will notice you will be logged in as admin account as you have earlier logged in as 1337 that means we had successfully replayed the cookie

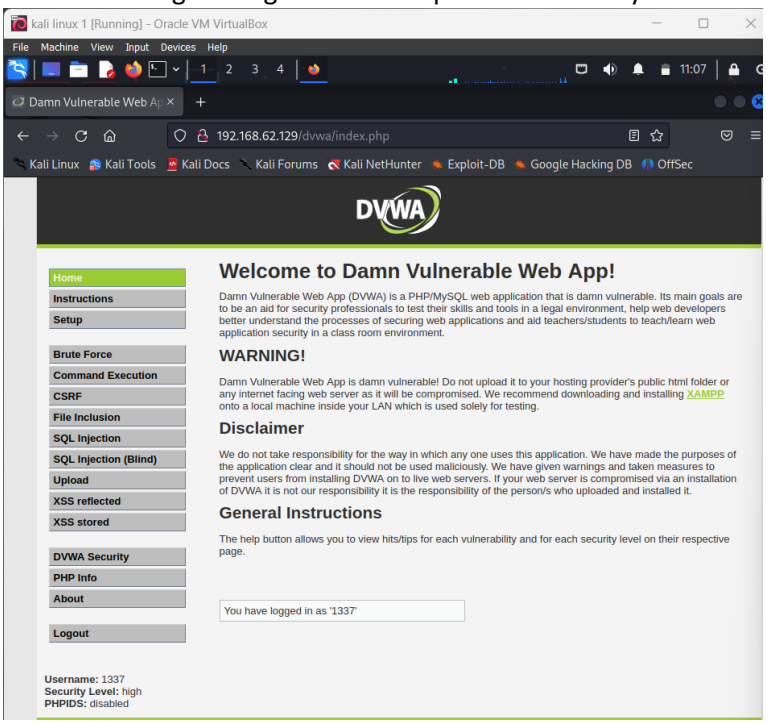


- **DVWA(for high)**

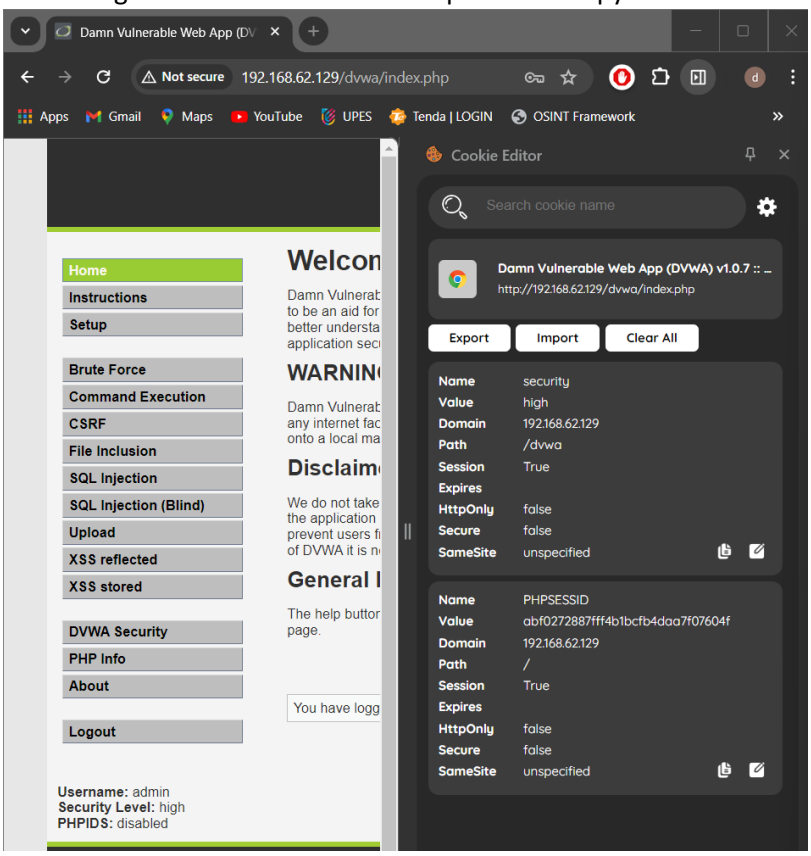
➢ Login the dvwa in windows with user name- admin and password-password at dvwa security high



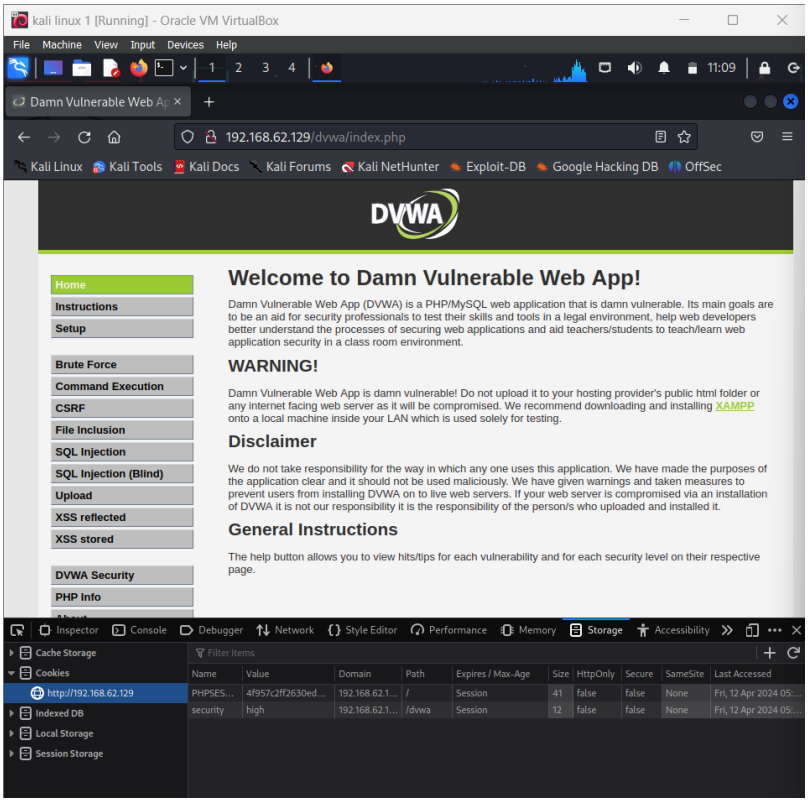

➢ And in linux login using id-1337 and password-charley



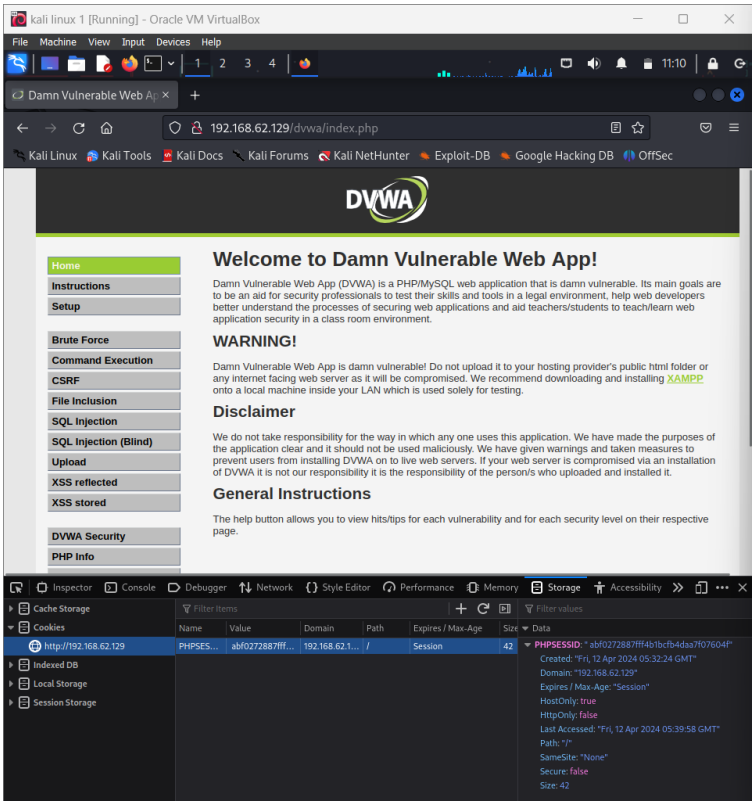
- Now using extension cookie editor capture and copy the cookie from there



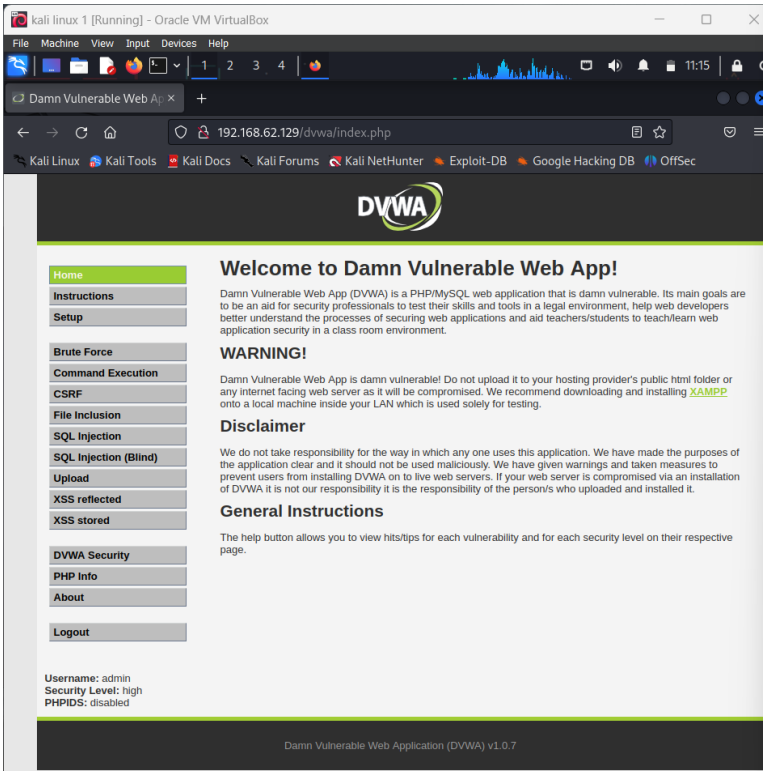

- Now go to linux and inspect the page and go to storage then cookie



- Now remove the security attribute and edit the phpsid and paste the cookie copied from windows



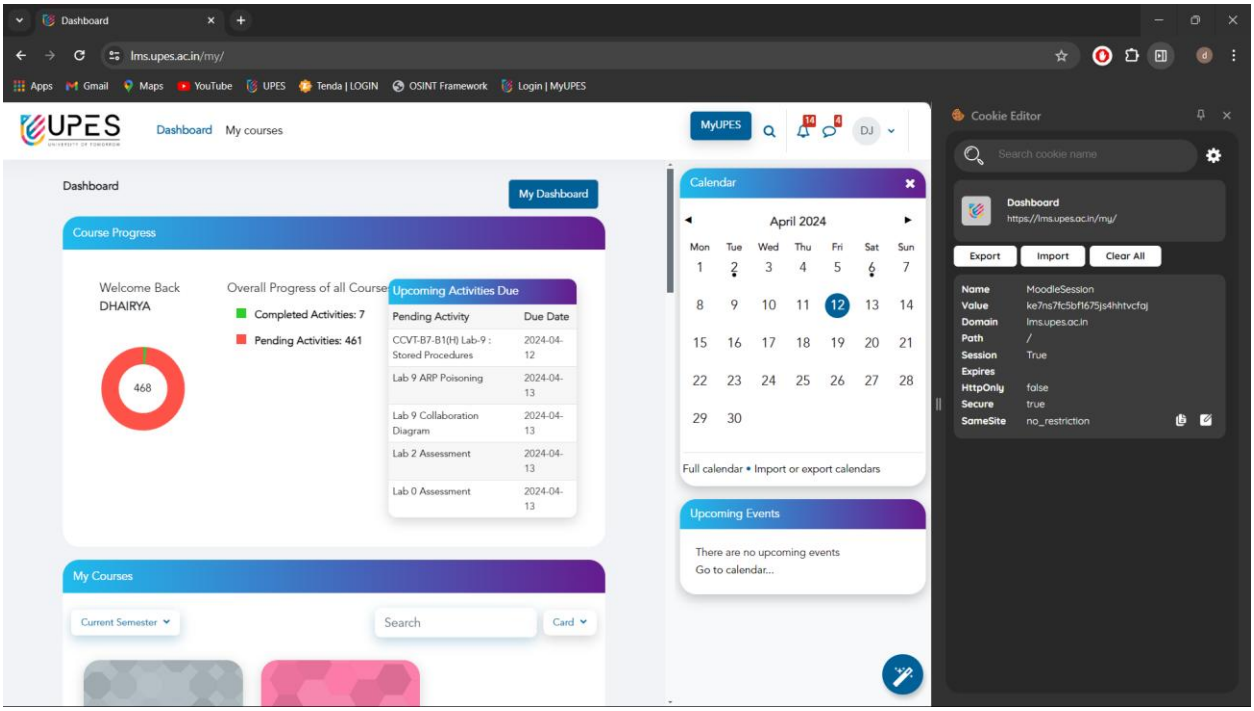

- Now refresh the page and you will notice you will be logged in as admin account as you have earlier logged in as 1337 that means we had successfully replayed the cookie



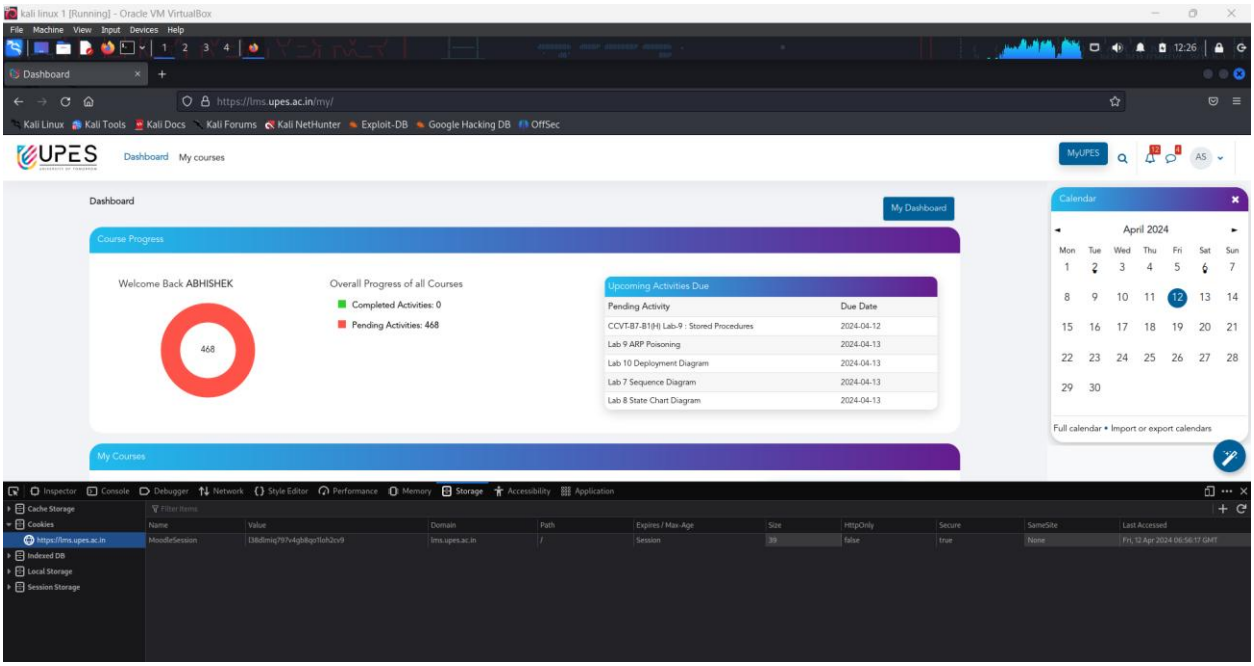
## Bonous-

# ➢ Upes lms

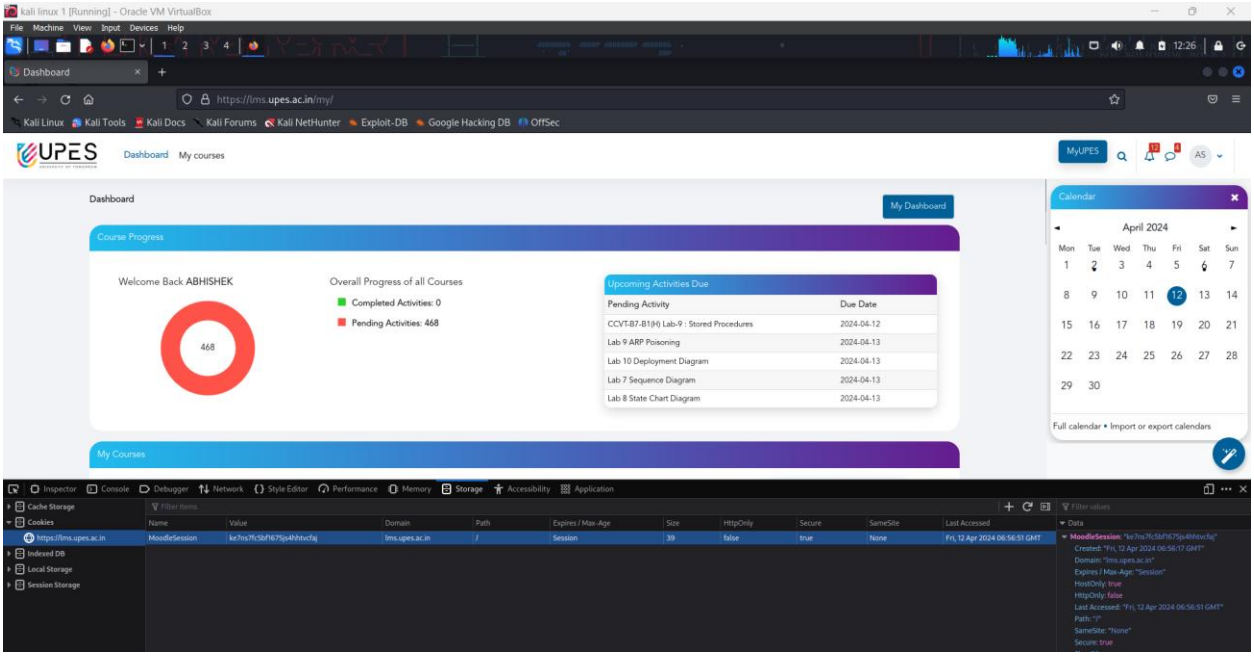
- ➢ On windows open upes student portel login in with my id dhairya.105432@stu.upes.ac.in
- ➢ open lms of upes student portal site and with the help of cookie editor extension capture and copy cookie



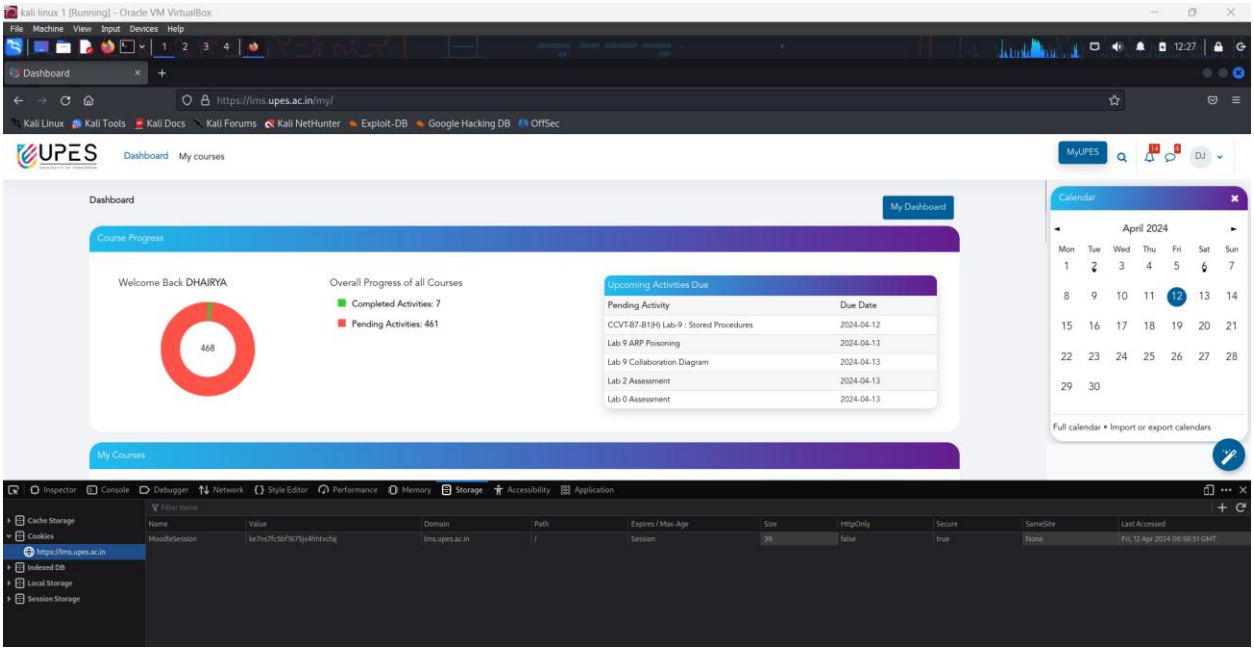

- ➢ on kali linux open upes student portal using your friends id, I am using abhishek id
- ➢ now go to lms then inspect page then go to storage and open cookie



- now edit cookie and paste cookie copied from windows in linux

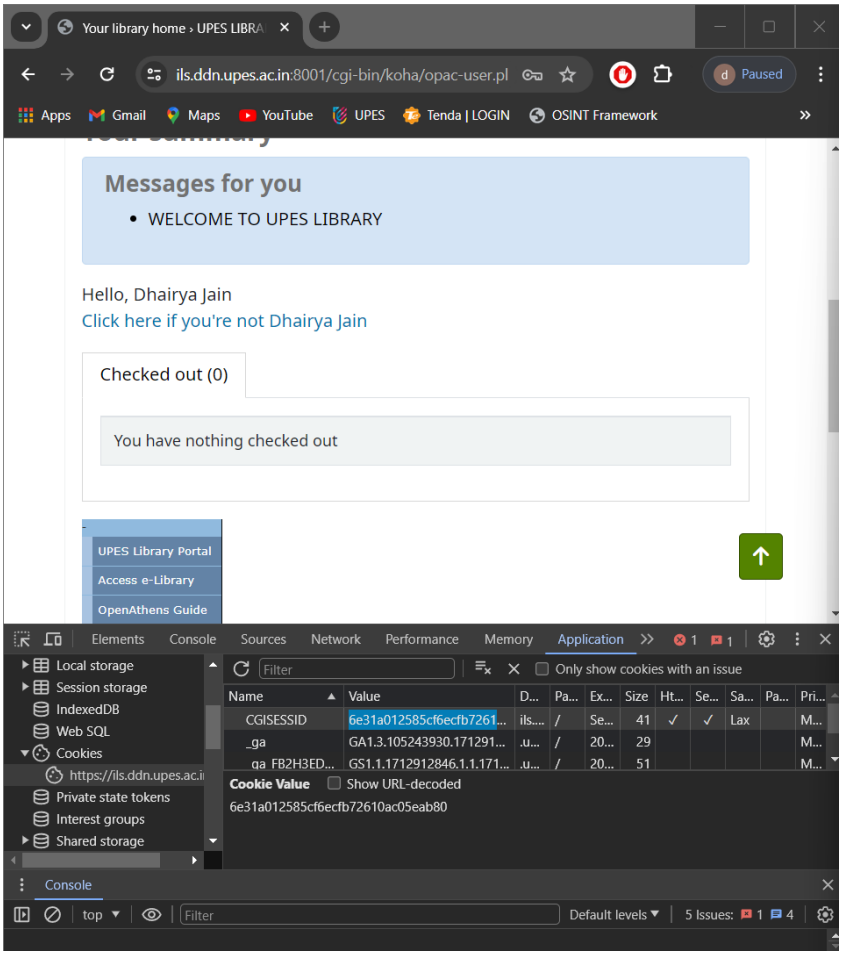



- now refresh the page you will find that your id is logged in instead of your friends id

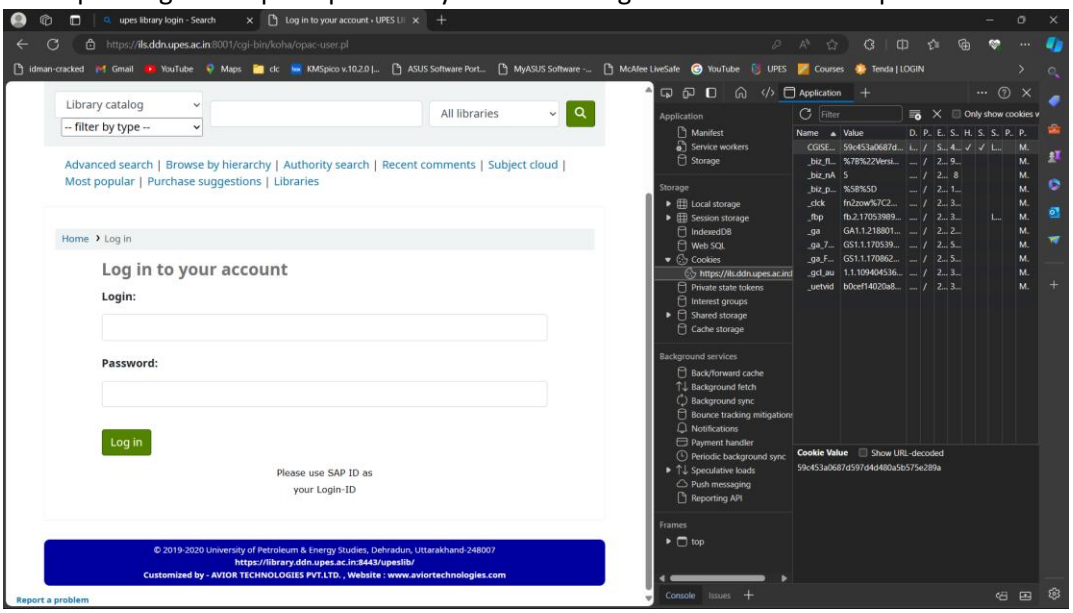


## ➢ upes library

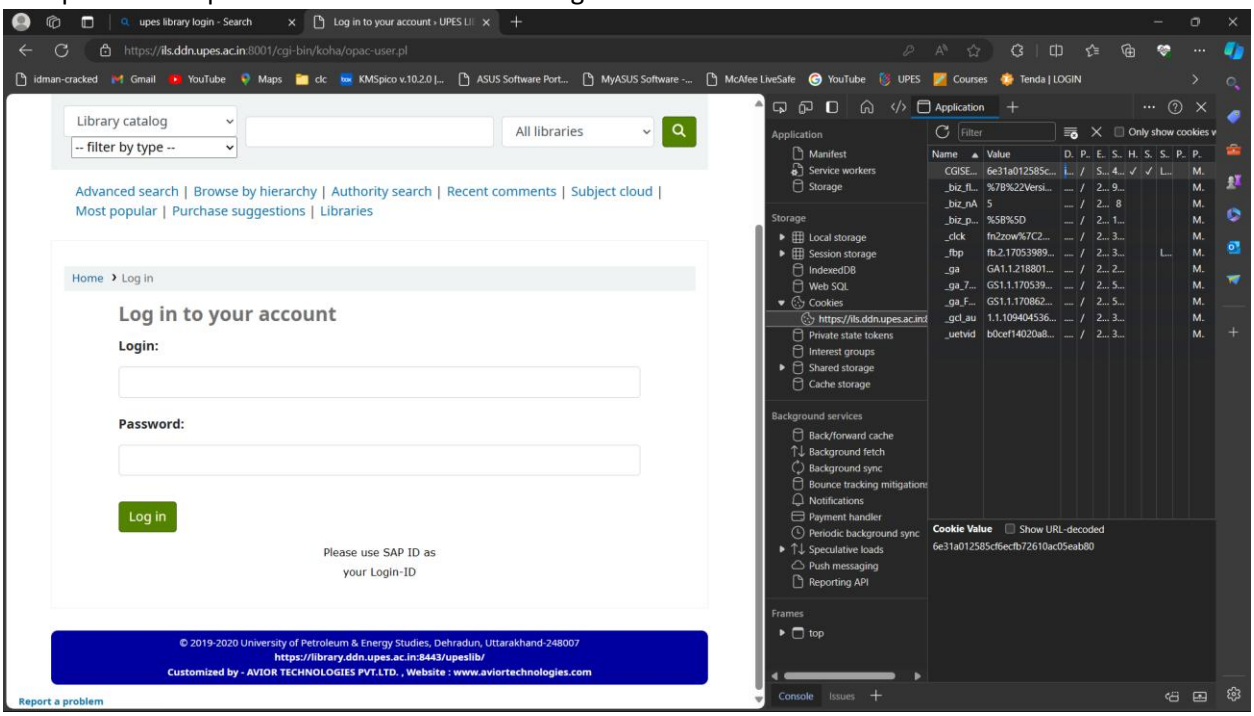
➢ open upes library site on chrome and login using your sapid and password and then inspect page and go to application and then go to cookie and copy cookie



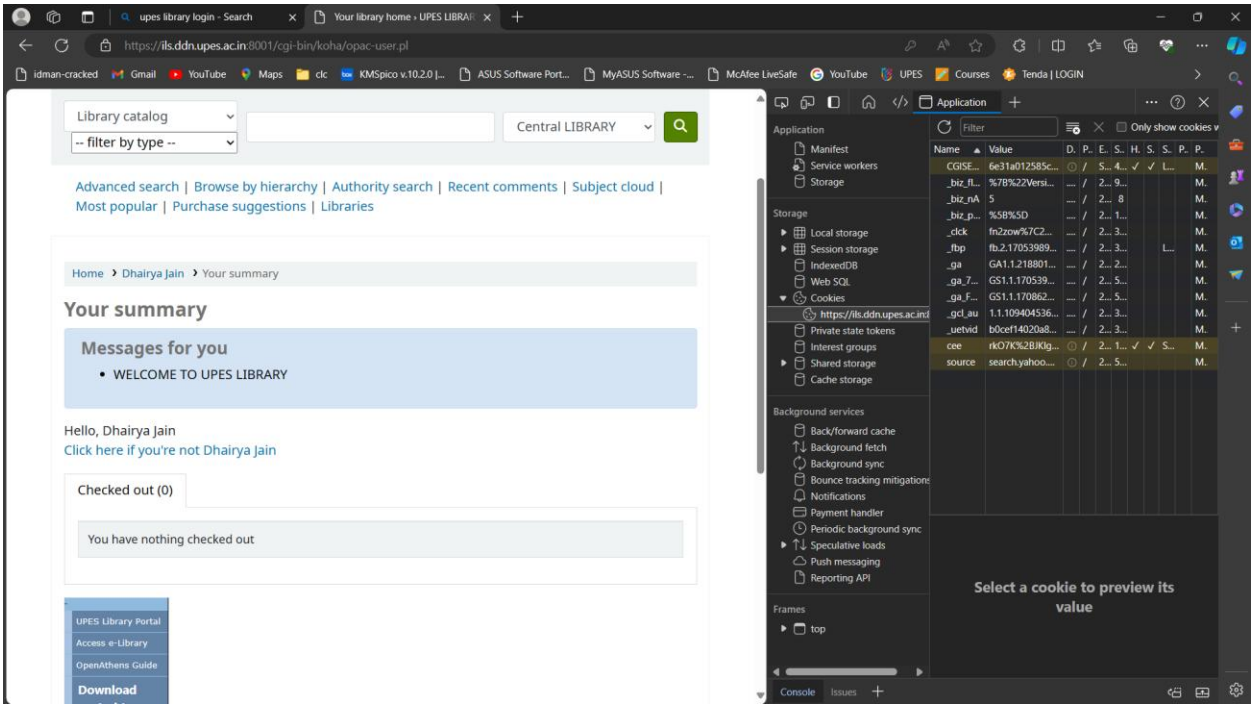

➢ now open edge and open upes library and do not login in this and also inspect and check cookie



- now paste the copied cookie from chrome in edge




- now refresh you will be logged in without id password



- **Countermeasure**
  - Session timeout after short interval of time
  - Encrypted communication channel ssl
  - Anti replay mechanishim