3. Insecure Direct Object Reference(IDOR)

Objective: To identify and exploit IDOR vulnerabilities
Tools: Burpsuit, DVWA, custom web application

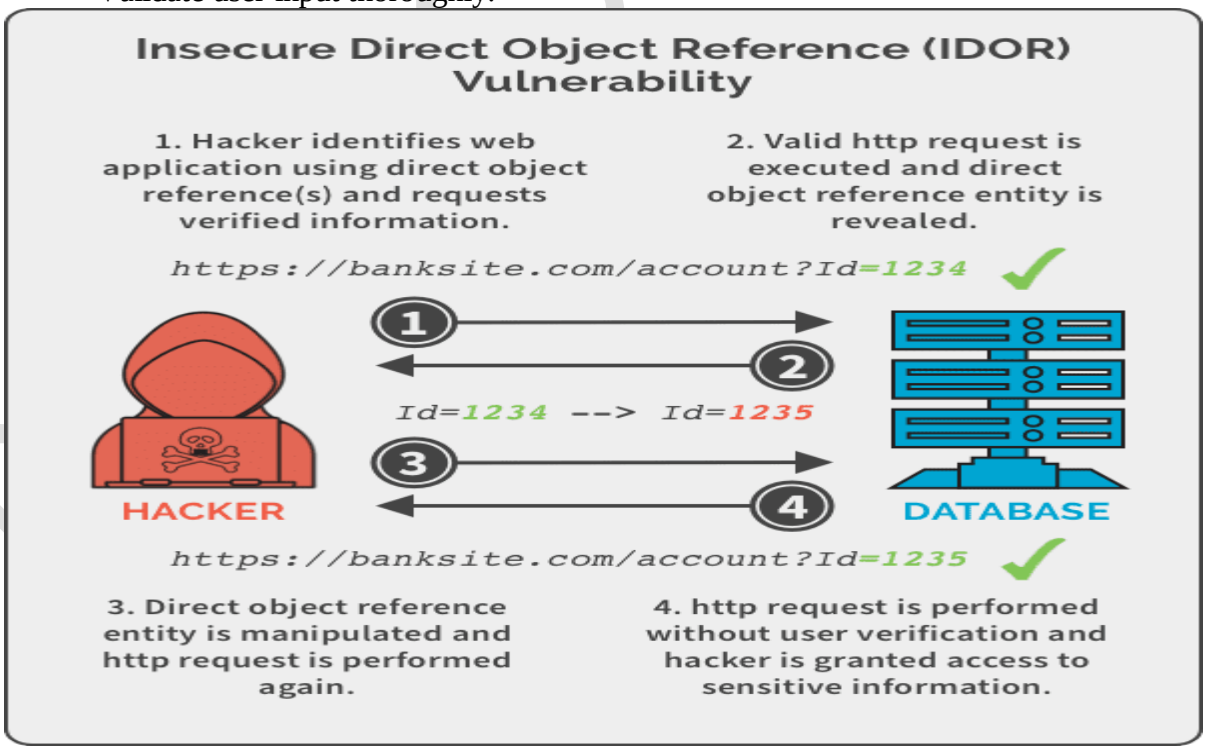
Insecure Direct Object Reference (IDOR) is a web application security vulnerability that occurs when an application exposes internal object identifiers to users without proper access controls. This allows attackers to manipulate these identifiers and gain unauthorized access to sensitive data.

Here are some examples of IDOR:

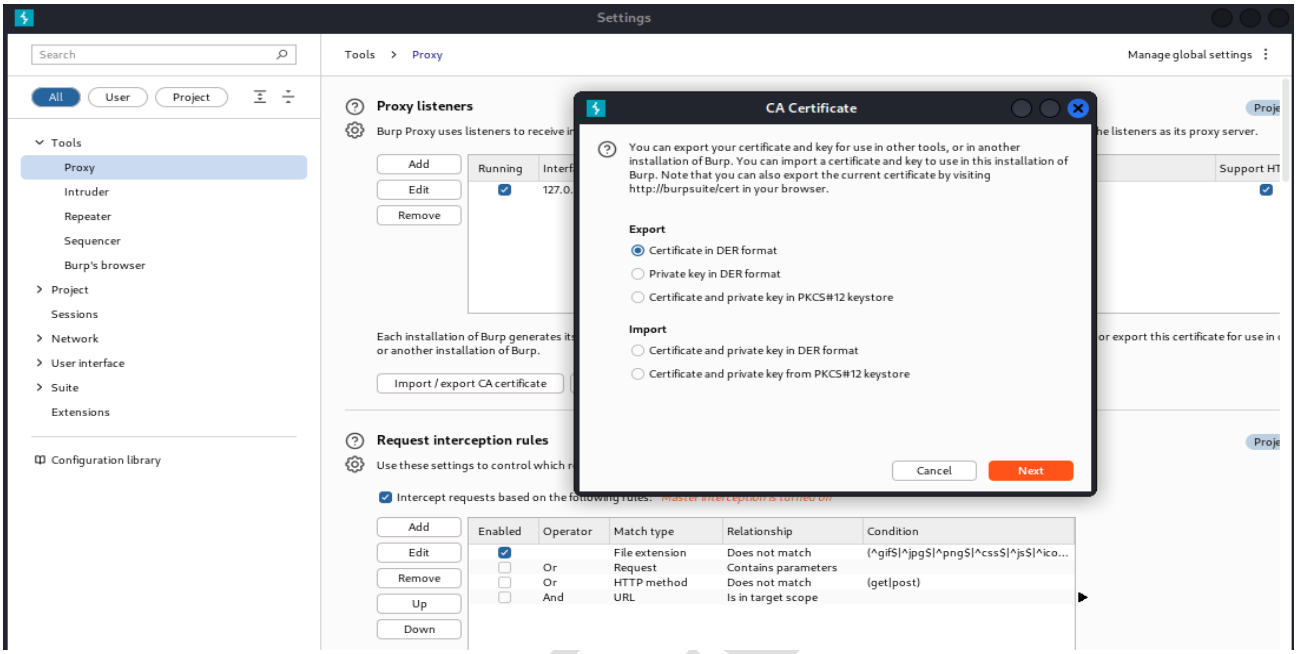
- Direct reference to database objects: An attacker can modify a customer number value to bypass access controls and view other customers' records.
- Substituting a parameter value: A malicious hacker can substitute a parameter value in a URL with a similar value that belongs to another user.

To prevent IDOR, you can:

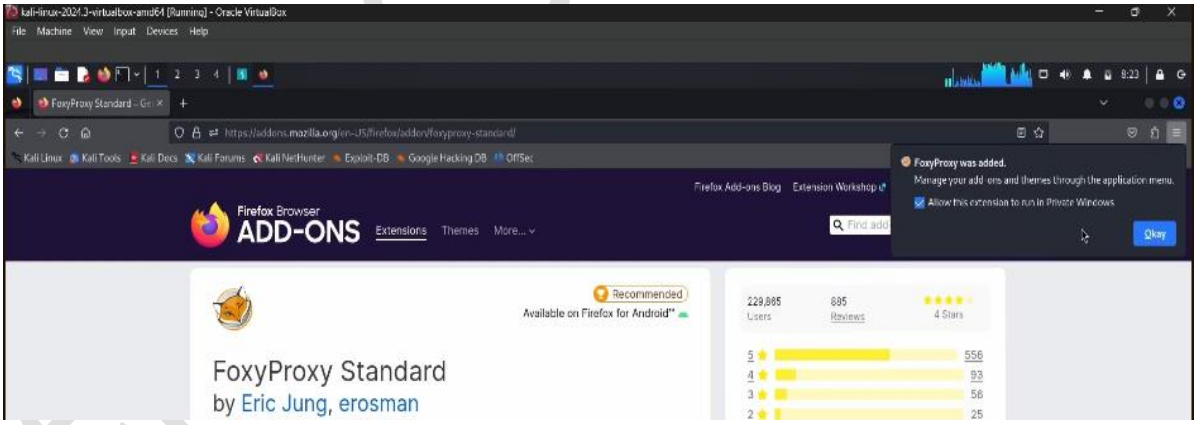
- Use a UUID instead of a direct user ID in a URL.
- Use Role-Based Access Control (RBAC) to define specific roles and permissions for different users.
- Enforce strict authentication requirements like multi-factor authentication (MFA) or strong password policies.
- Validate user input thoroughly.



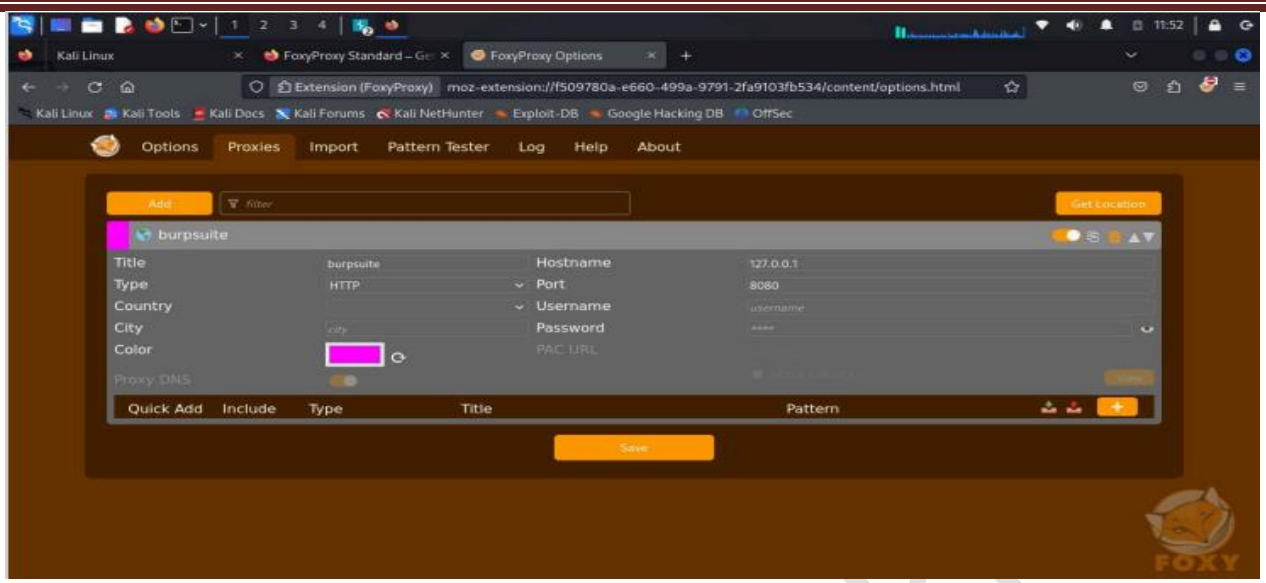
Step1: Open the burp suit in kali, navigate to setting in burp and click on to import/export button.
In export select first option and click on next and select the file, place it on desktop with cert file name. Now certificate is successfully exported



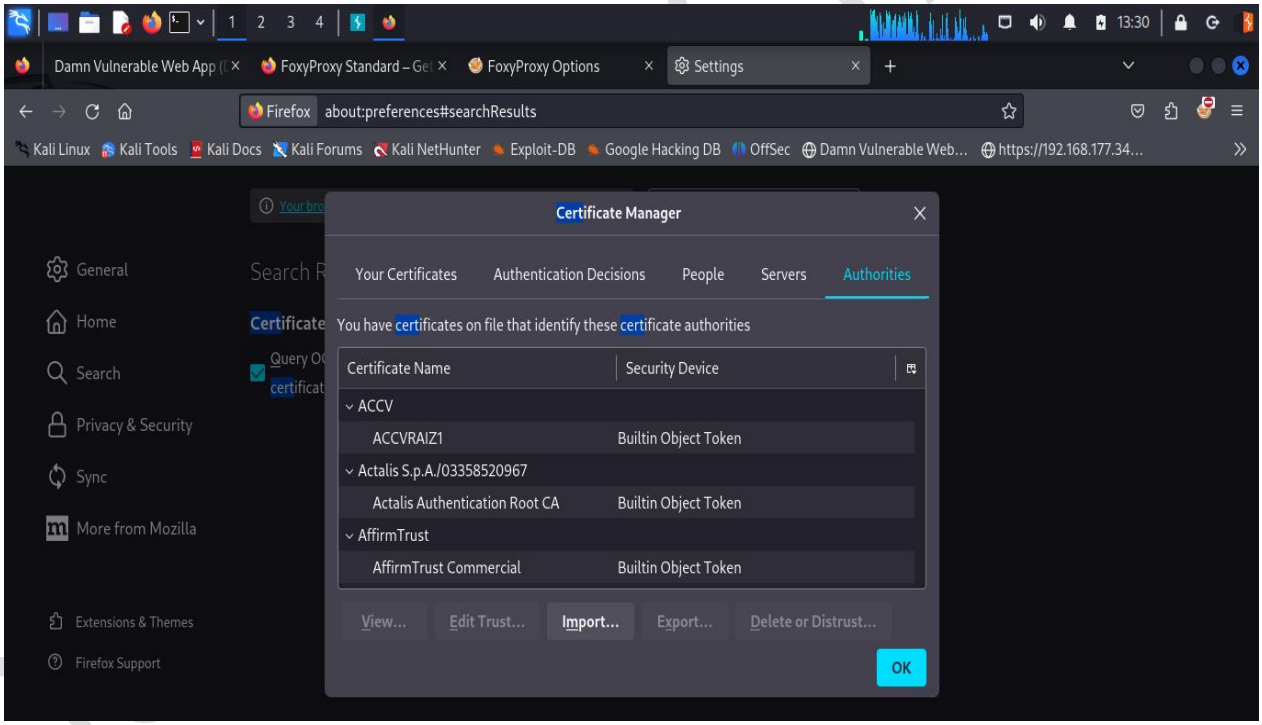
Step2: Go to the Firefox browser in kali, search for the extension **foxyproxy** in google and click on add Firefox button. Then go to tool bar and add foxyproxy
https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/



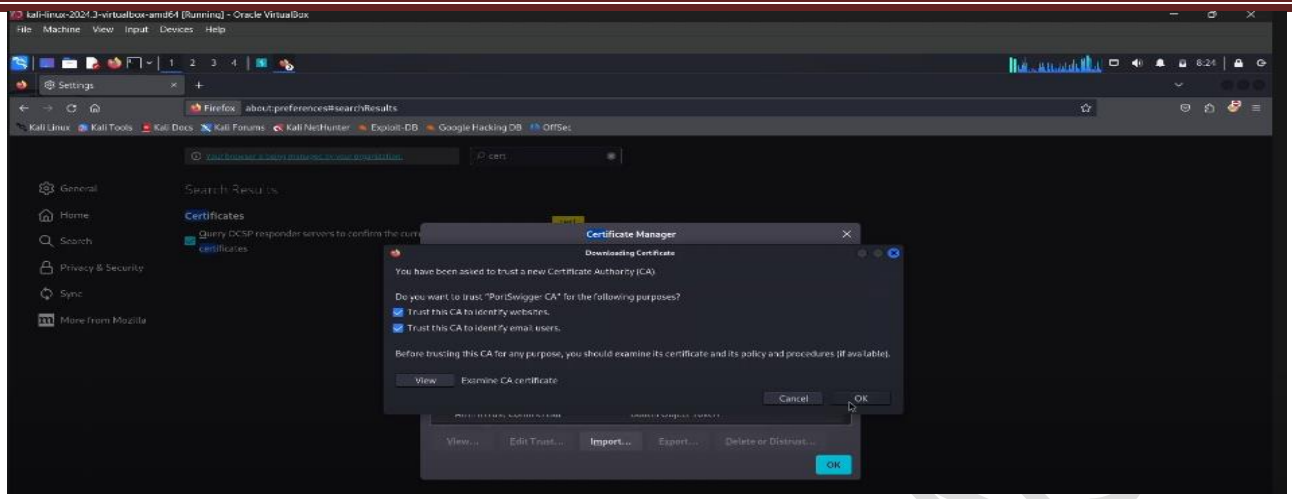
Step3: Go to new tab in browser, click on foxyproxy and click on options, click on proxies click on add button and fill the information like below



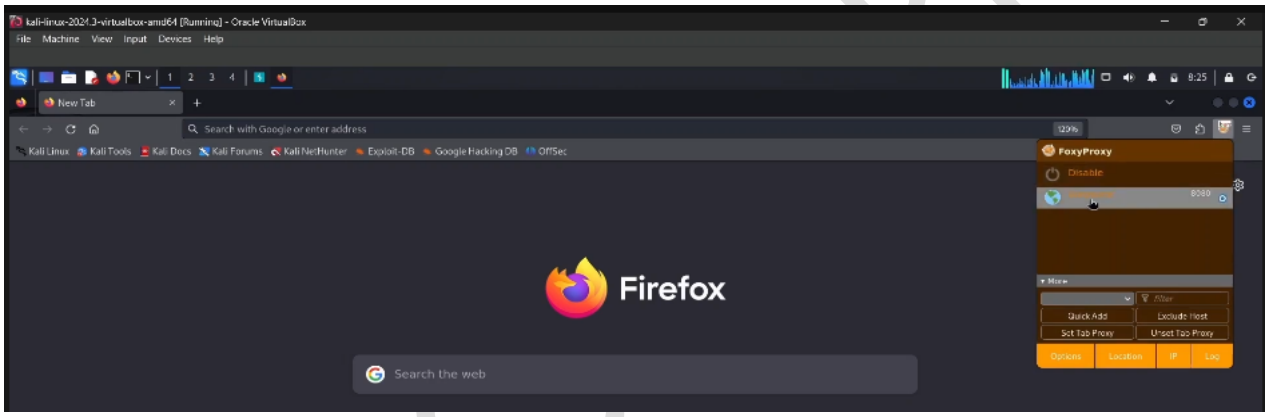
Step4: Open new tab and navigate to firefox setting, search for **cert.** Click on view certificate button Then click on **import button** and select the downloaded certificate.



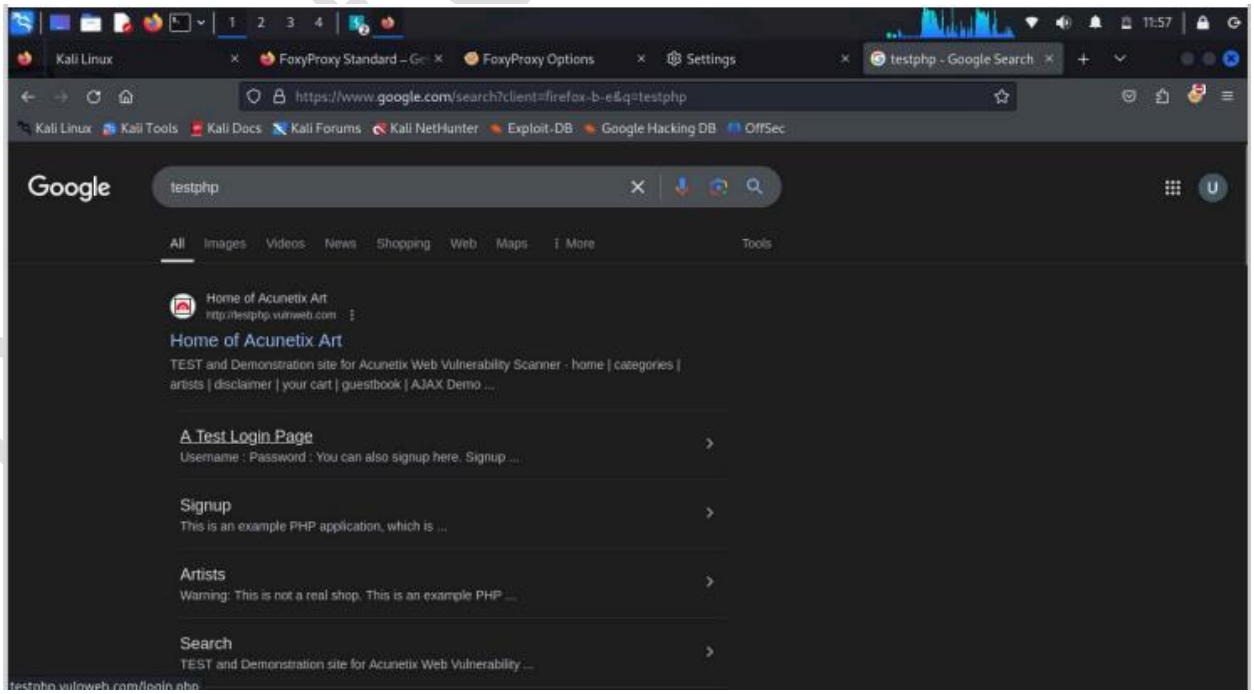
After that click on two checkboxes, now burpsuit is ready.



Step5: Goto new tab and enable the extension

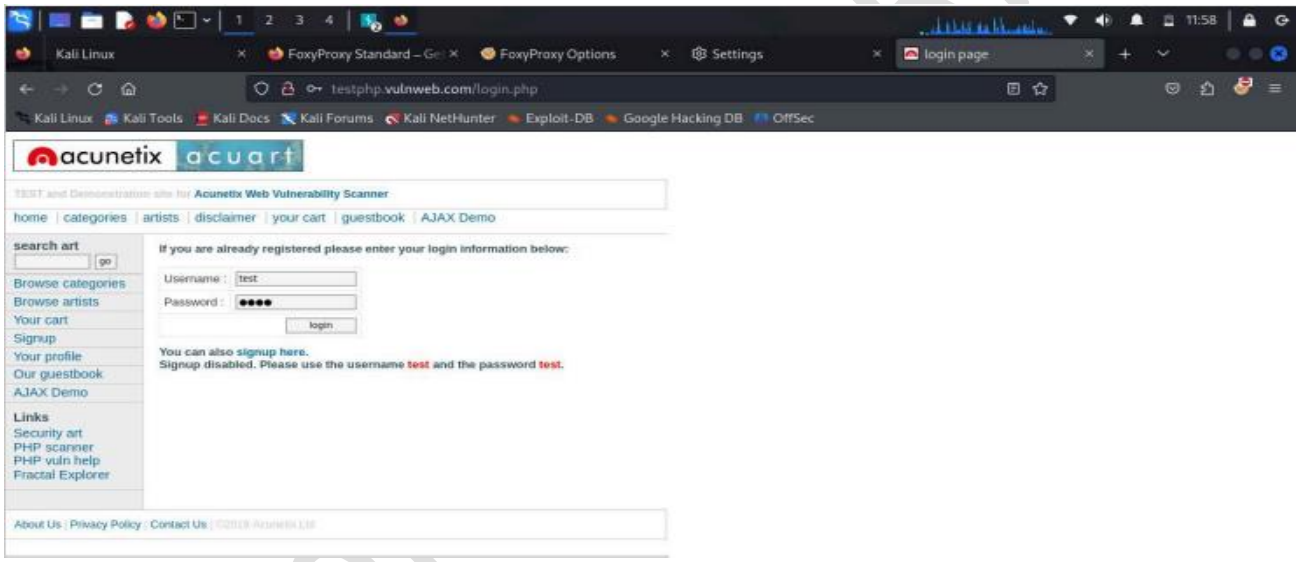


Step6: Goto browser search for **Testphp**

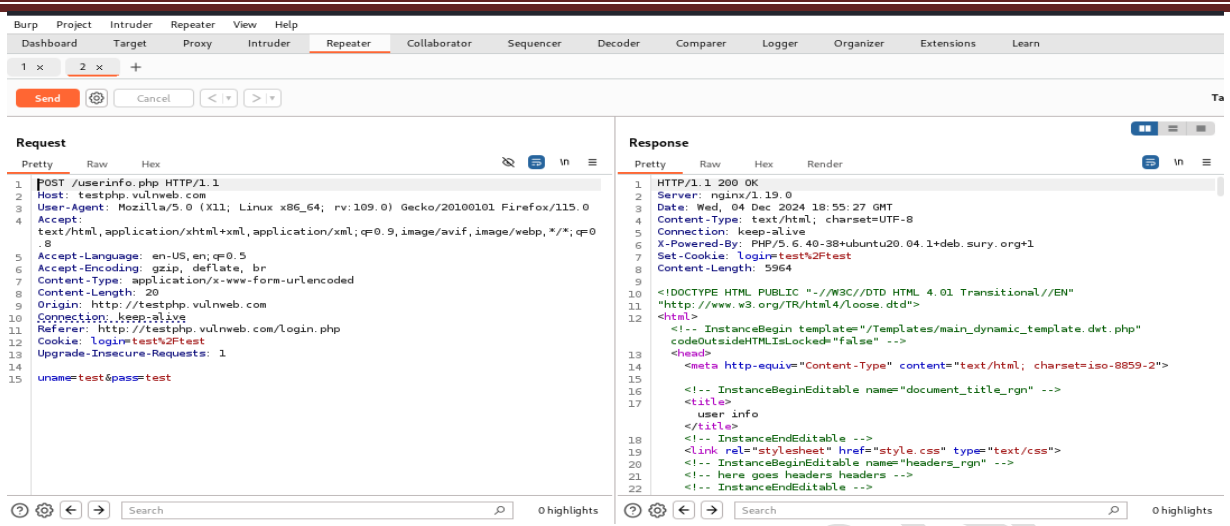


Open the first link, before providing the credentials the burpsuit should be on

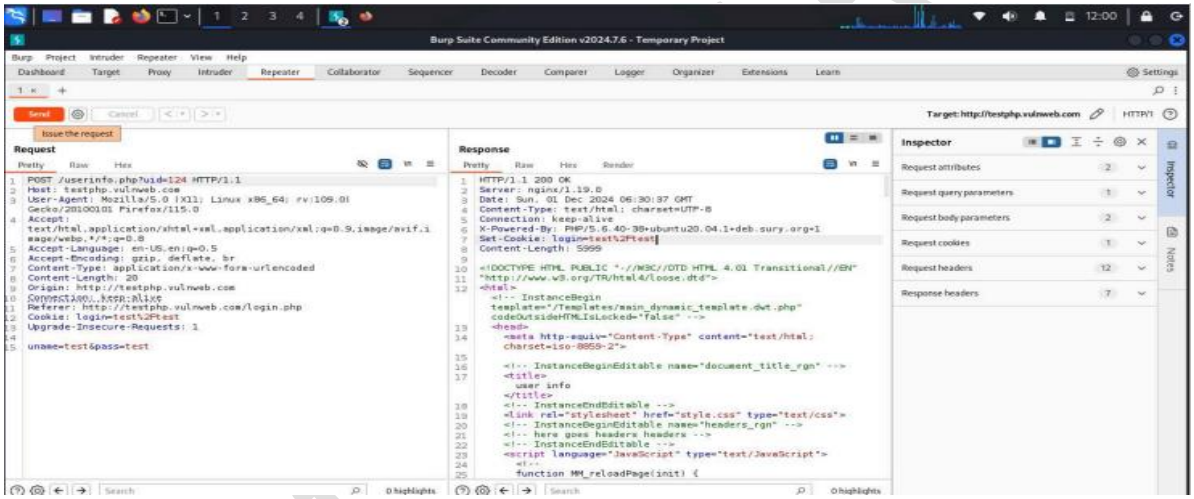
User name is **test** and password is **test**



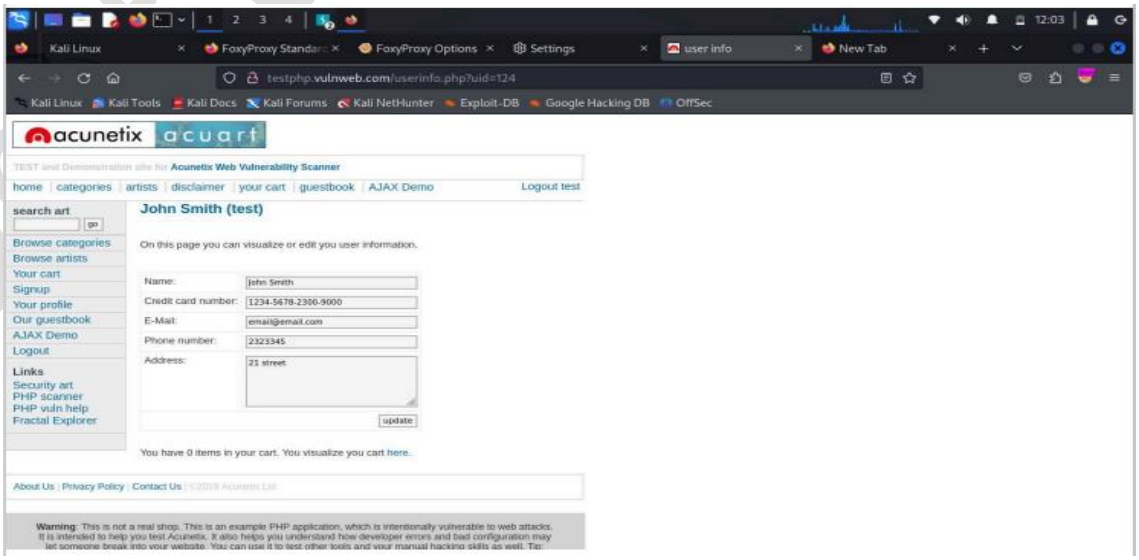
The traffic captured by burp sent to **repeater,** then click on to forward/send. Next turn off the interceptor.



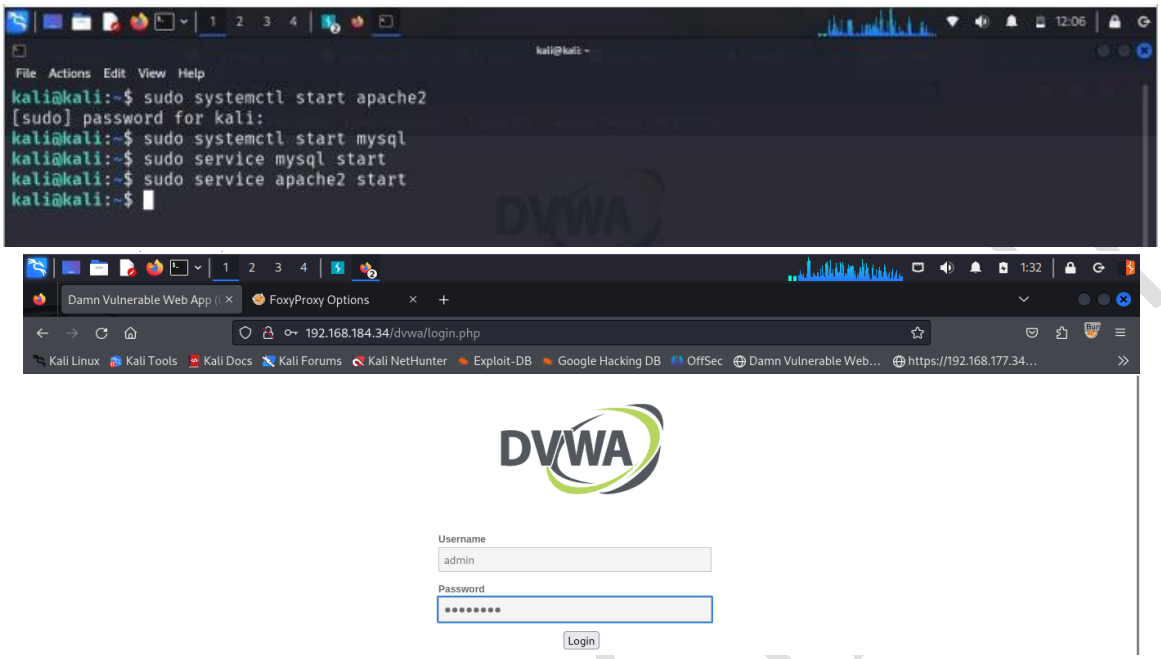
Step7: go to repeater and add code to first line with **? uid=124** ,then click on send.



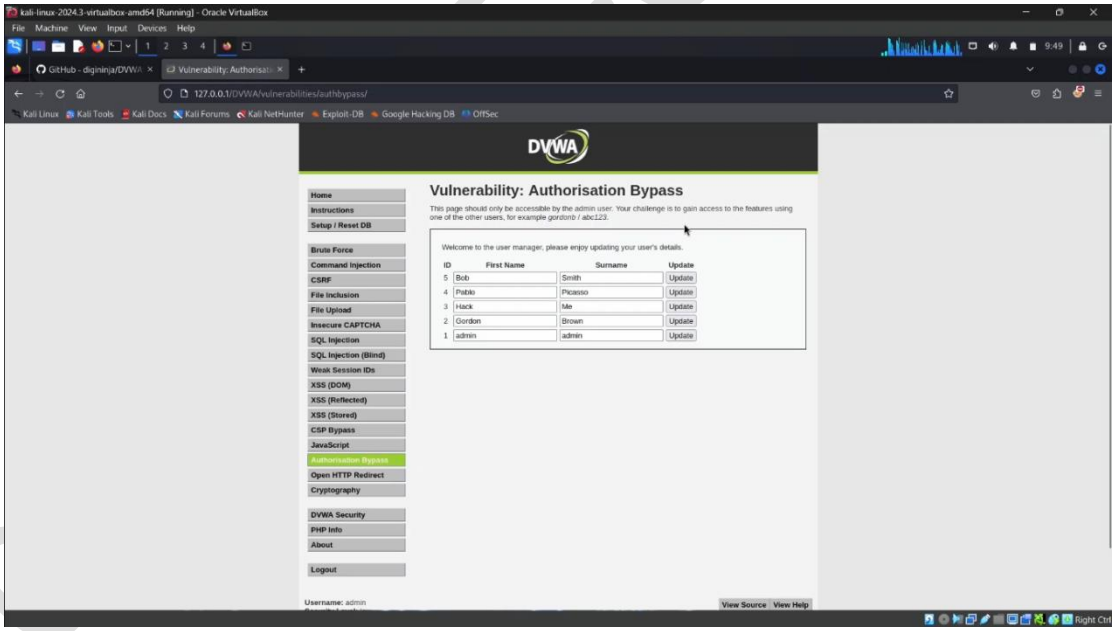
Now in response section click on **show response in the browser option,** then copy the link-burp suit is done.



Step 8: Open DVWA

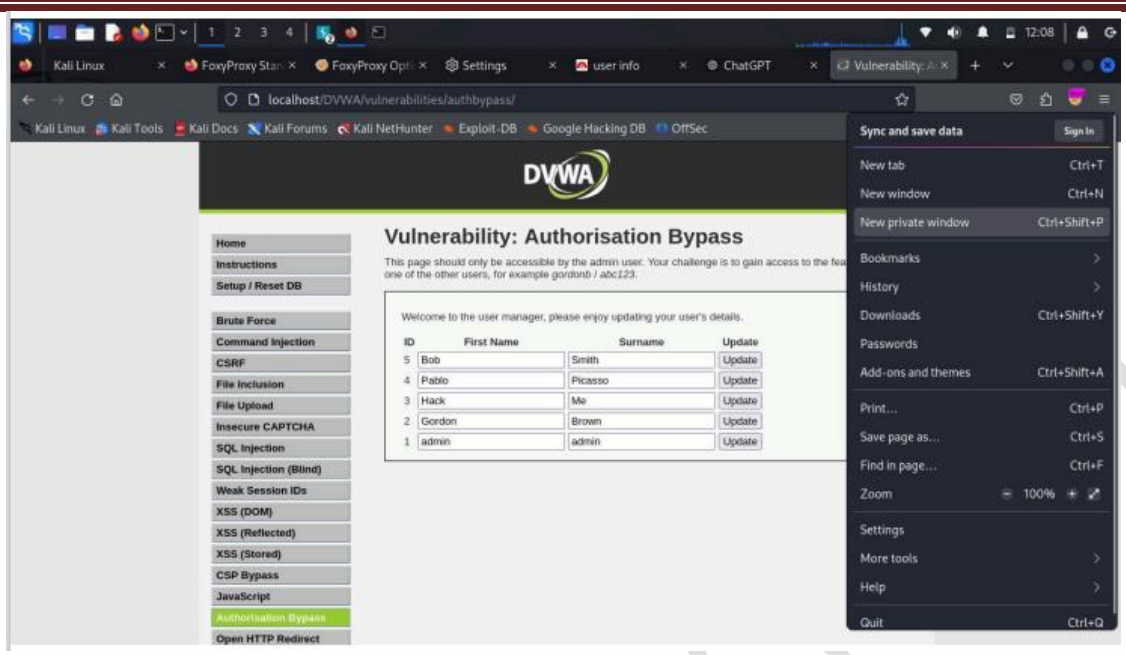


We are at admin credentials:

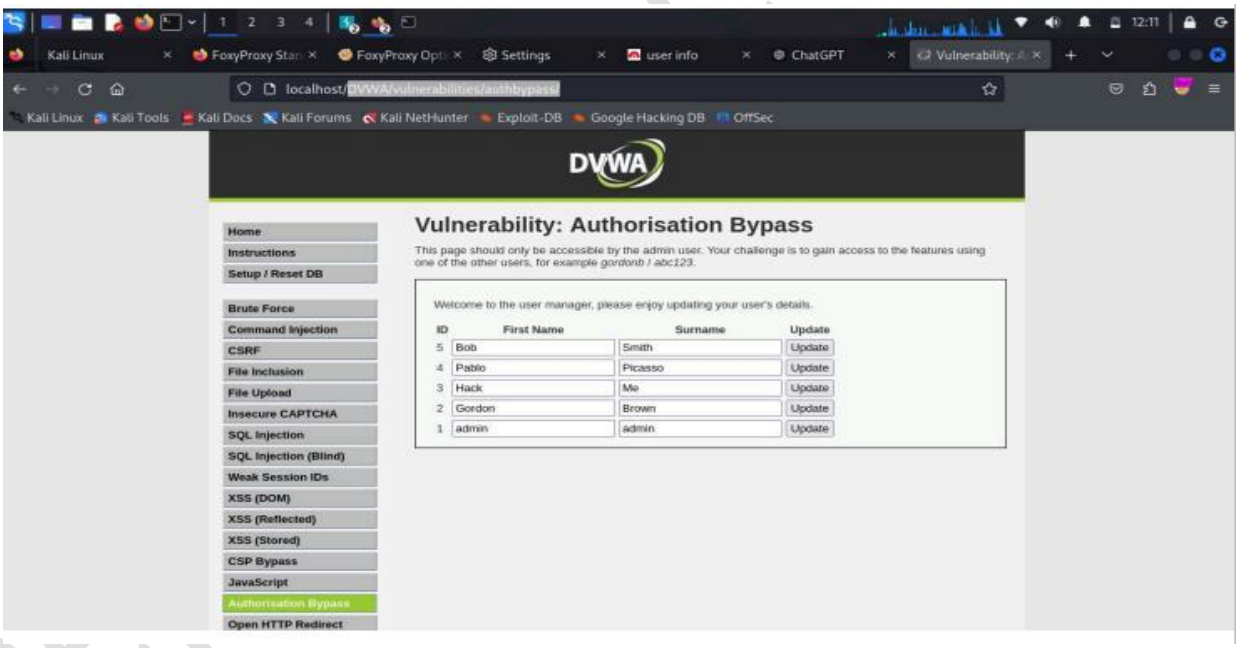


Authentication Bypass→low level

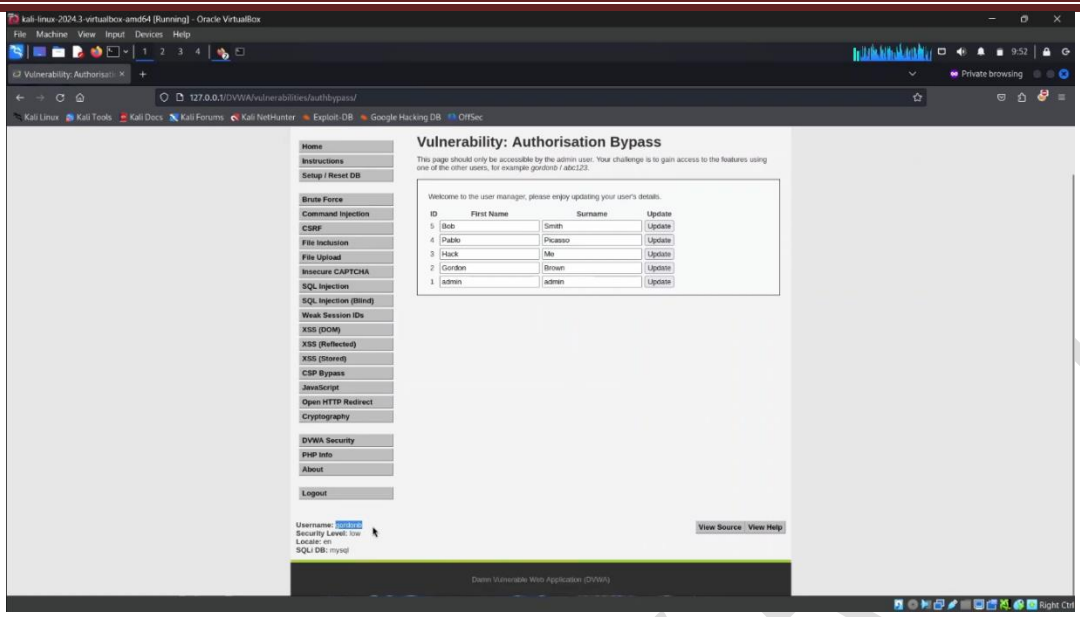
Open up a new private window



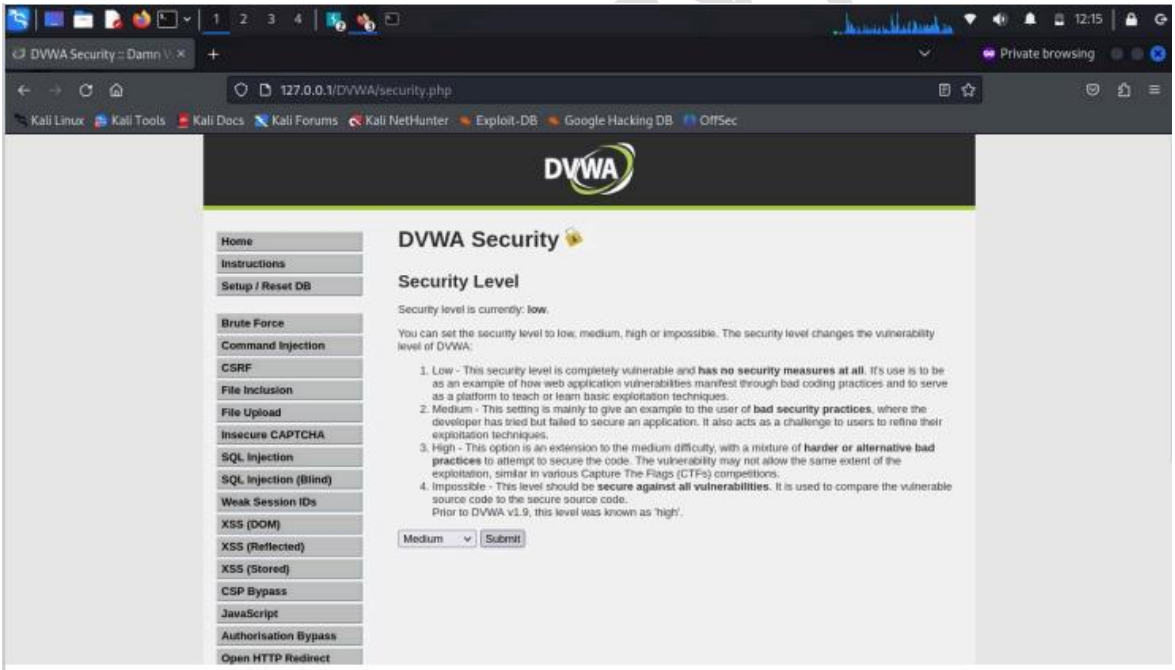
Then navigate to local host DVWA 127.0.0.1 try to login user **gordonb** and password **abc123**
Copy the marked URL from **admin** and paste it into **new private window**

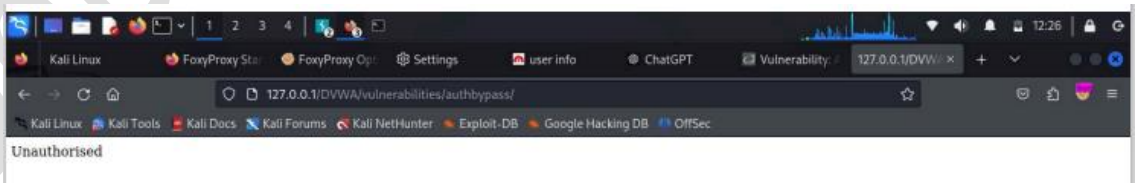


New private window looks like, we **got admin access**

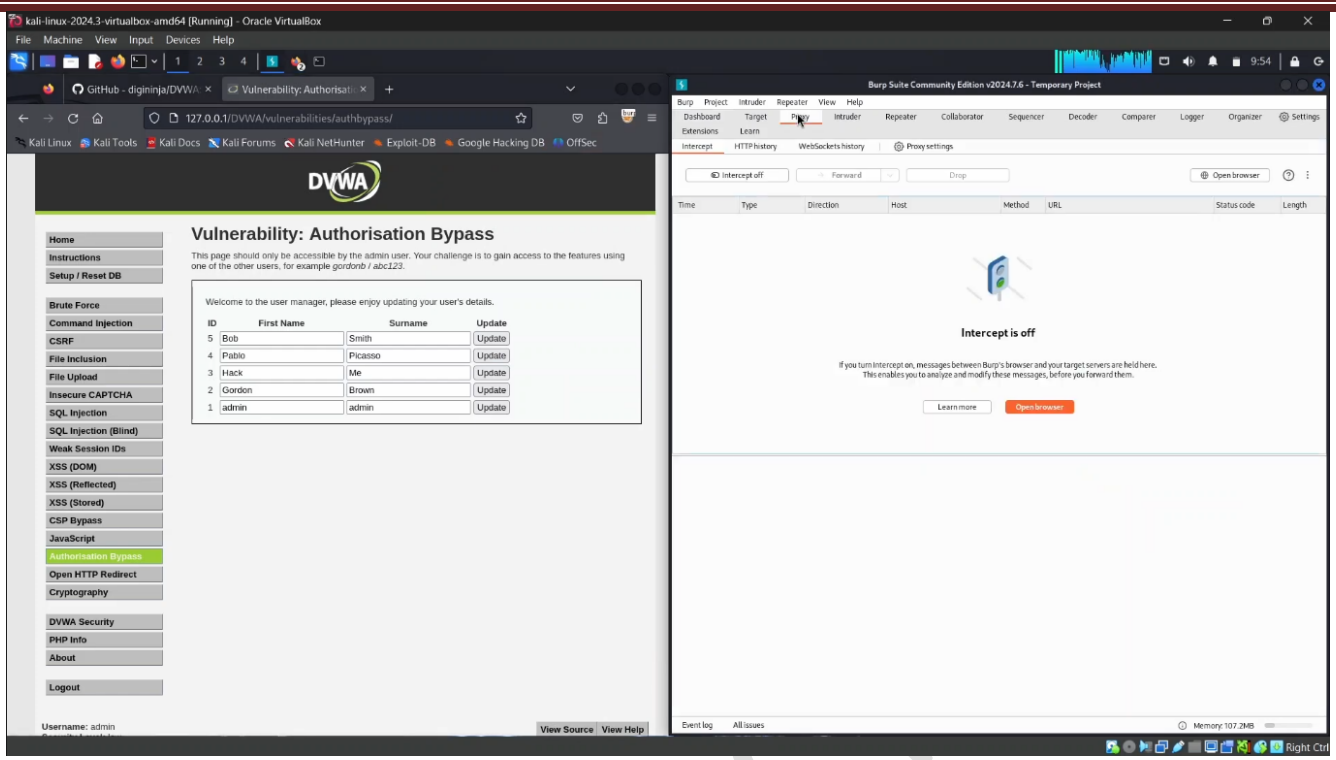


Enumerate for the medium level , then it will show like unauthorized

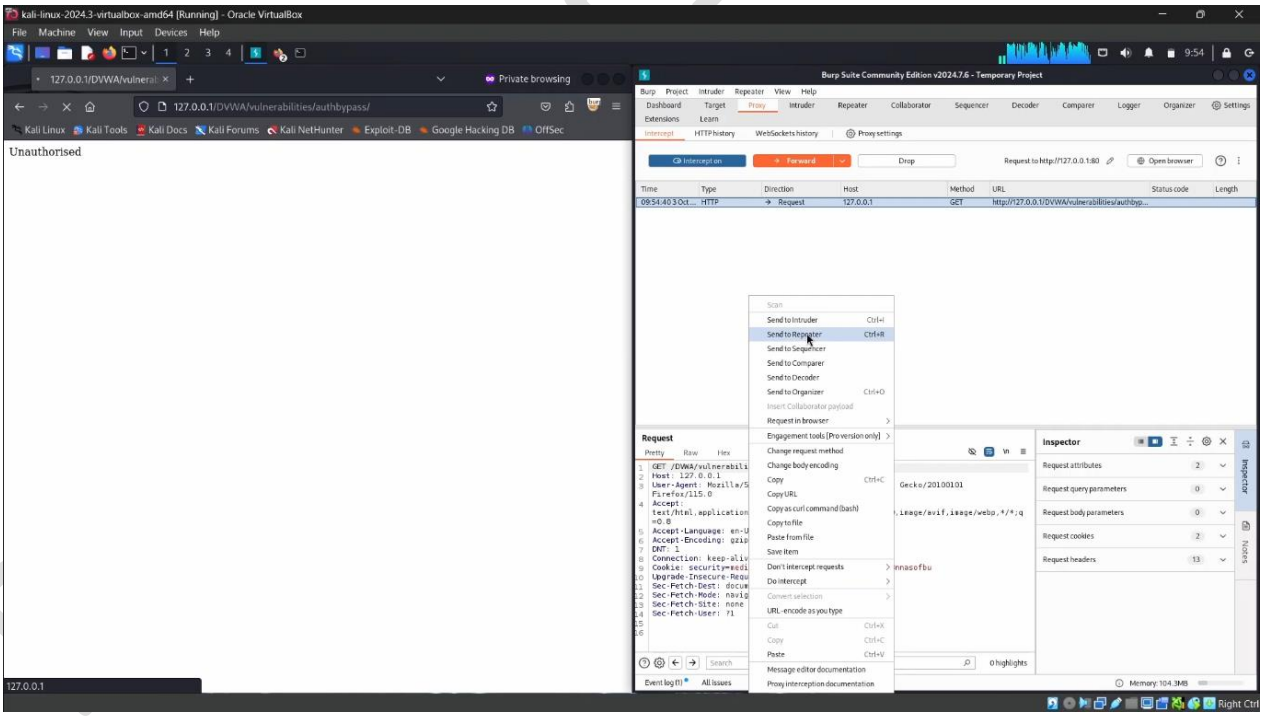


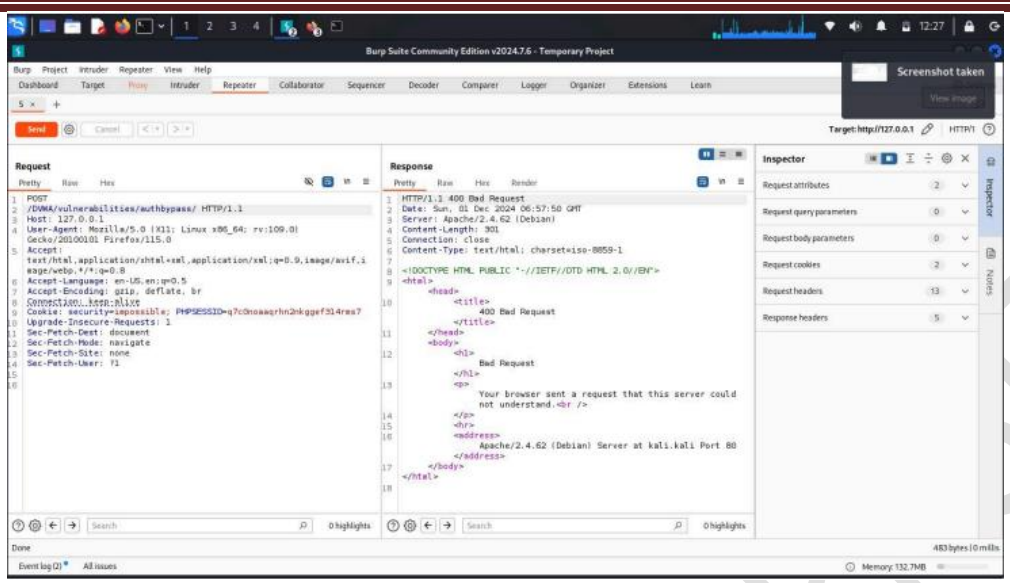


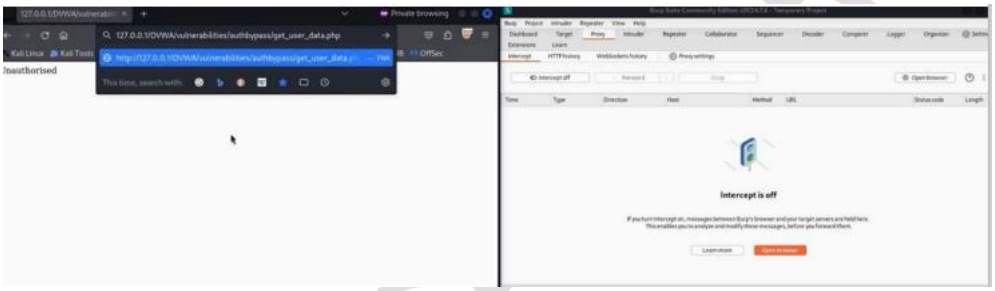
Step9: Open burp suit, in browser turn on burpsuit

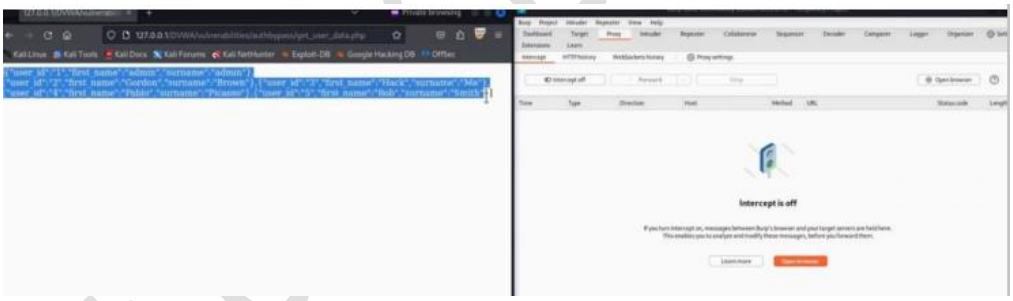


Turn on the **interceptor** and **refresh** the unauthorized page









Link: https://www.youtube.com/watch?v=0G08ydvmmYY&ab_channel=MaCT