10. Session Hijacking and Fixation

Objective: To learn how session hijacking and fixation attacks work

Tools: DVWA, Burp Suite, Browser developer tools

Session hijacking is a cyber attack where an attacker gains control of a user's online activity by stealing or manipulating their session token:

- **How it works**

  When a user logs into a website, the server assigns a session token to the user's browser. The attacker then intercepts the session token, which can be done by eavesdropping on network traffic or exploiting vulnerabilities.

- **Impact**

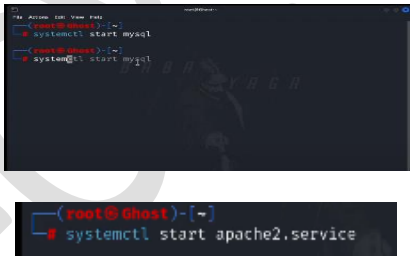
  With the stolen session token, the attacker can impersonate the user and access their account, perform unauthorized actions, or steal sensitive information.

- **Prevention**

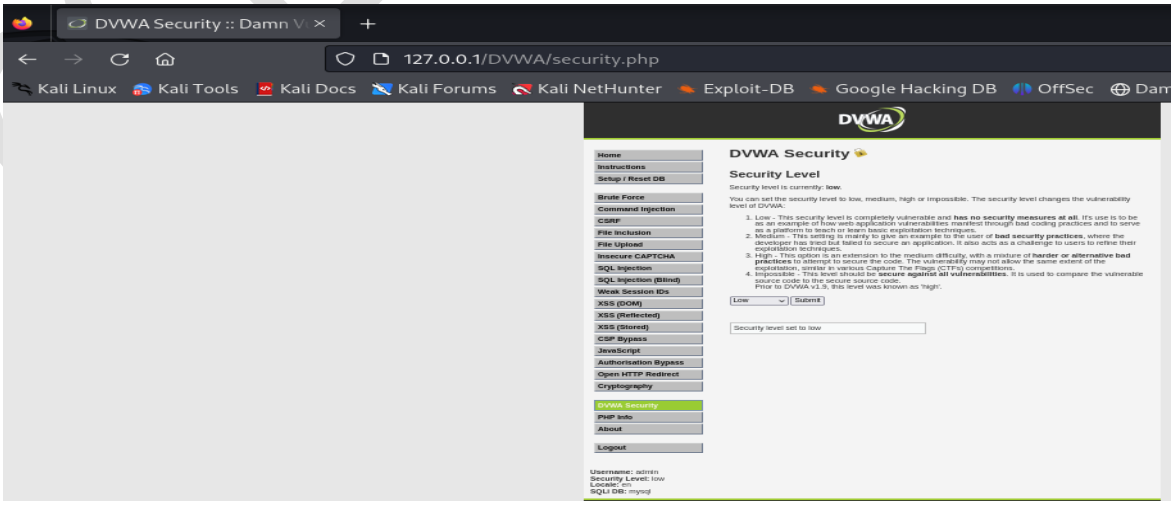
  Website owners can prevent session hijacking by using HTTPS and strengthening session management. Users can prevent session hijacking by logging out of websites, enabling multi-factor authentication, and being cautious of links they click.

  Session hijacking is a significant and growing threat to web application security. It can lead to privacy breaches, unauthorized transactions, and other security concerns.

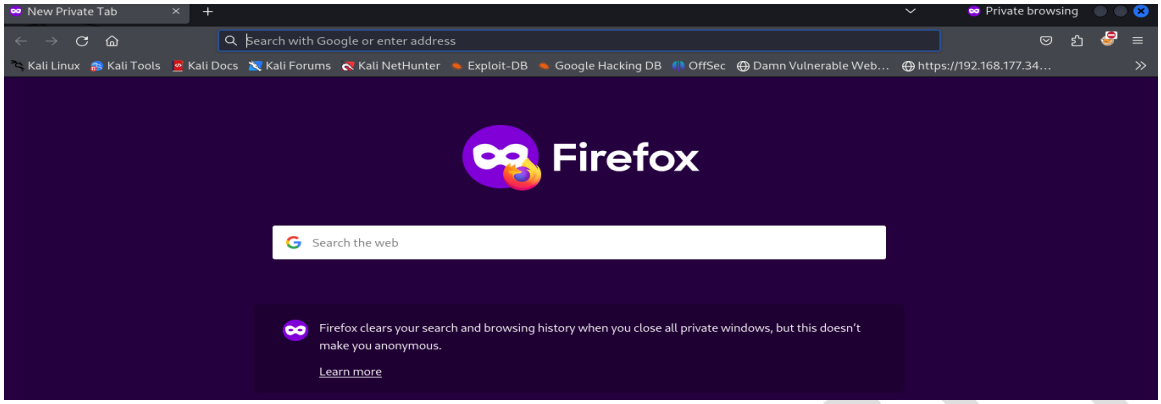
Steps:



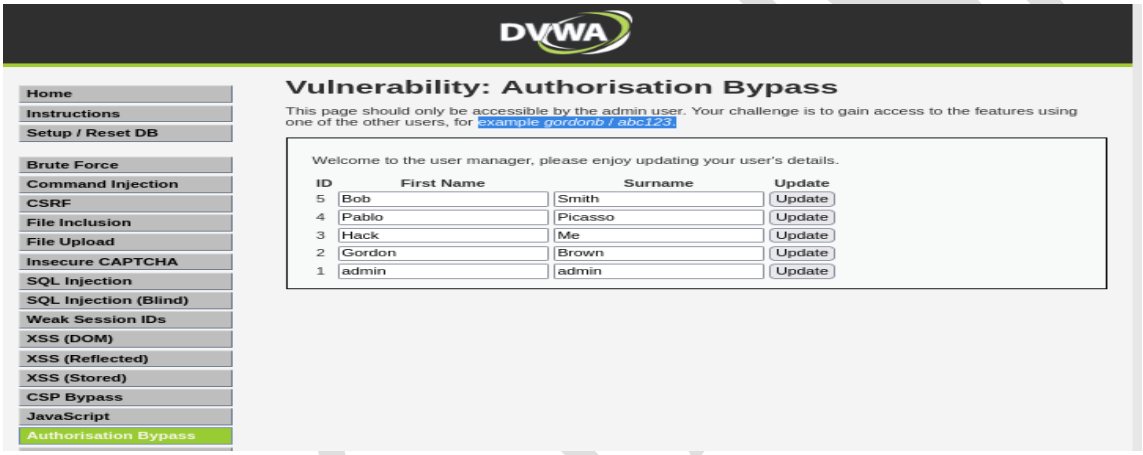
Step1: Open **DVWA** and **set the security level as LOW**



Open new private window



Step2**: login to DVWA** with username: **gordonb and password: abc123** in the private window



Logout from the normal window

Step3: Start the burp suit and capture the target, login in the normal window and enable the foxyproxy

Now we got the **PHP SESSID** and

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history Proxy settings

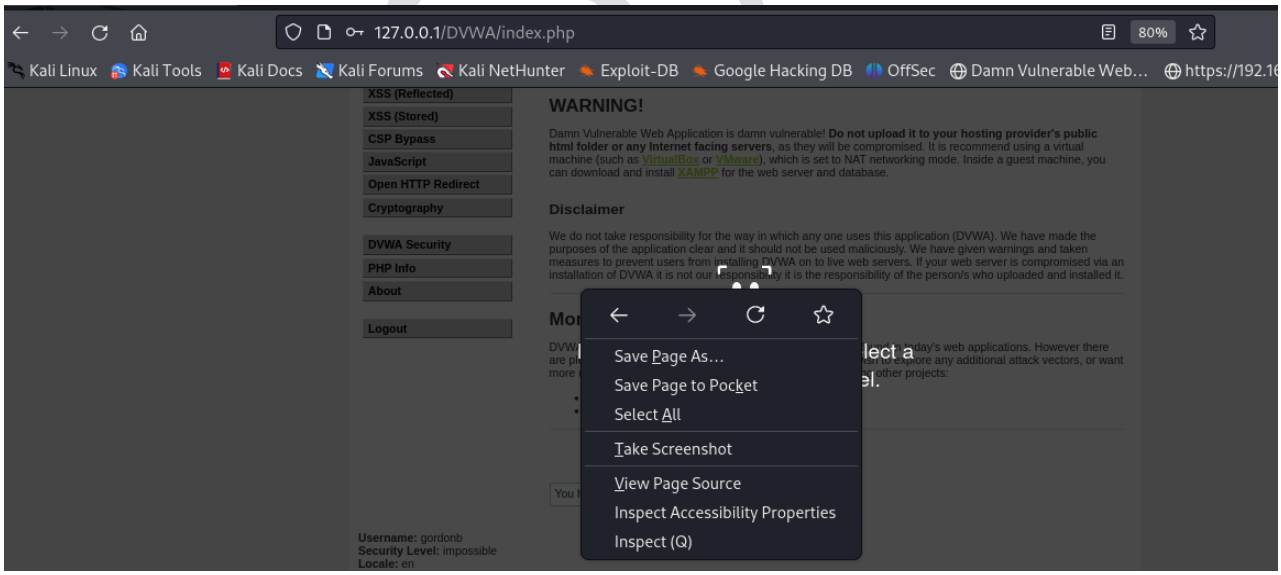
Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

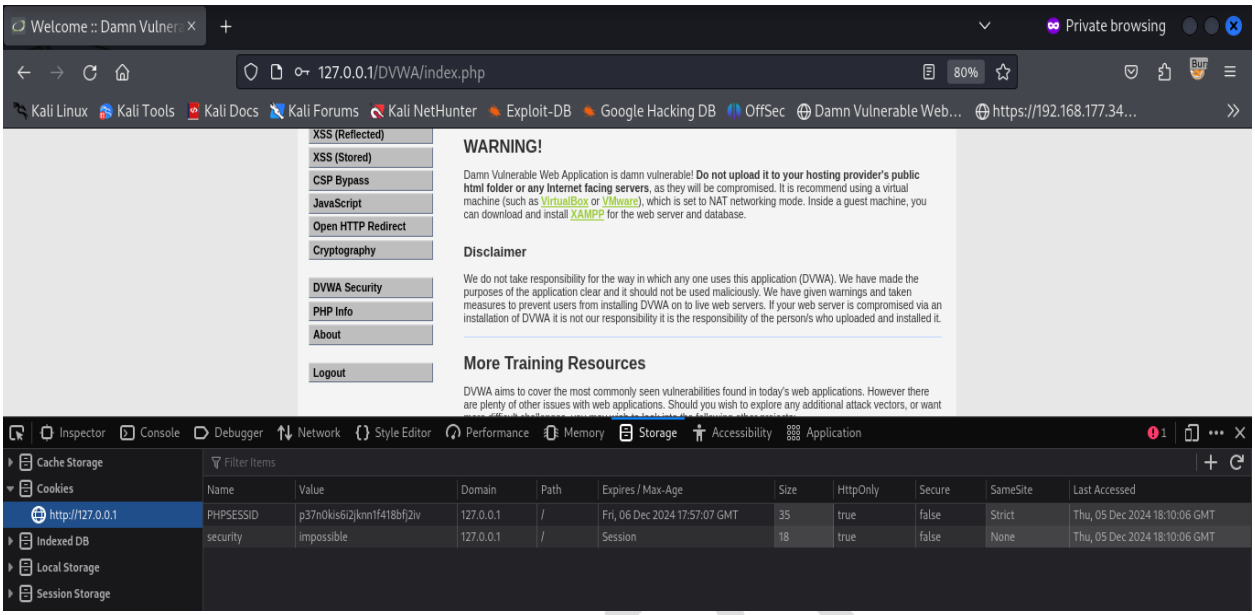
Pretty Raw Hex

```
1  POST /DVWA/login.php HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 88
9  Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: security=low; PHPSESSID=14sopfvn05oaqlp95qgfuo0mpq
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=admin&password=password&Login=Login&user_token=7c2bcea1fccf7f0a53ac01bc8350b79b
```

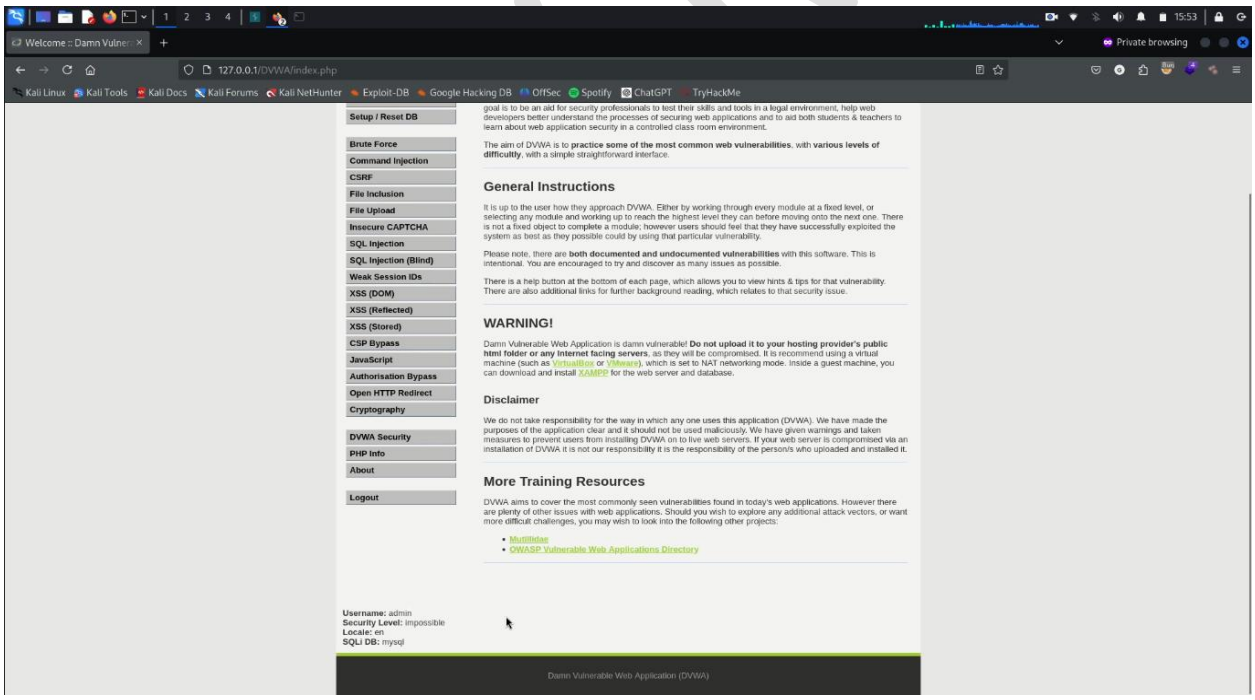
Step4: then go to private window and inspect the fetch by mouse right



Go to storage



Step5: Refresh the page will show as admin user



Link:

https://www.youtube.com/watch?v=zblBWf_8TGg&list=PL0JHrE_bOMXjC2VnKpFLp1scjWMPf6cxW&index=1&ab_channel=MaCT