

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**

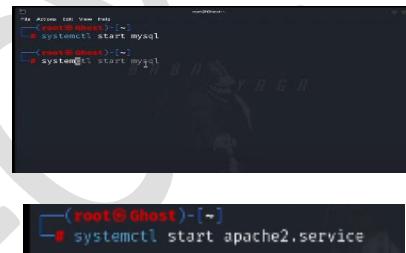
With the stolen session token, the attacker can impersonate the user and access their account, perform unauthorized actions, or steal sensitive information.

- **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.

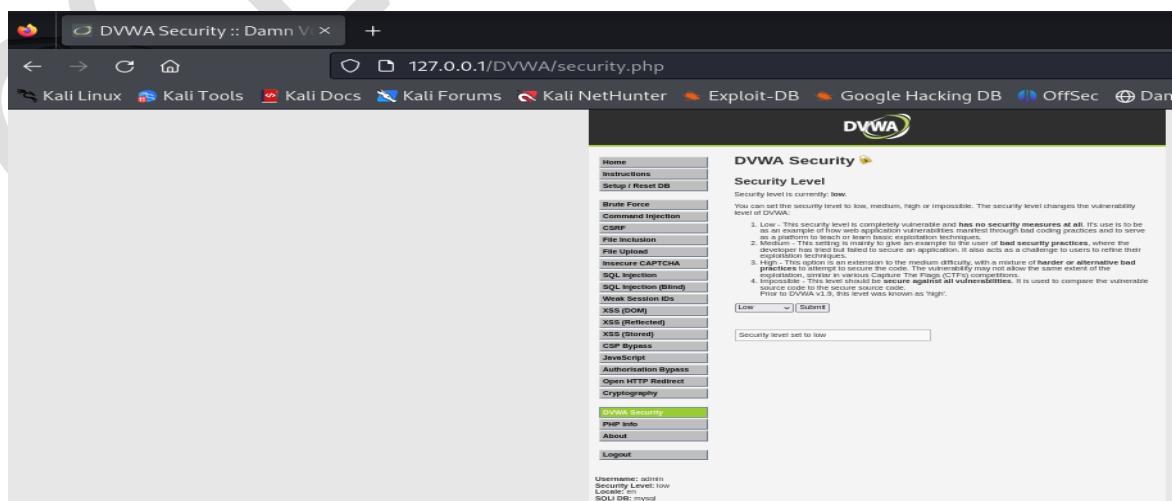
Session hijacking is a significant and growing threat to web application security. It can lead to privacy breaches, unauthorized transactions, and other security concerns.

Steps:



```
root@Ghost:~# systemctl start mysql
root@Ghost:~# systemctl start apache2.service
```

Step1: Open DVWA and set the security level as LOW



DVWA Security :: Damn Vulnerable Web Application

Security Level

Security level is currently: **Low**

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of the application.

3. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be used as a platform to teach or learn basic exploitation techniques.

2. Medium - This security level is moderately vulnerable and has some basic security practices, where the developer has tried or failed to secure an application. It also acts as a challenge to users to refine their penetration testing skills.

3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad guys. It's used to test the user's skills against more advanced security measures, similar to various Capture The Flag (CTF) competitions.

4. Impossible - This security level is completely secure and has no vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Submit

Security level set to

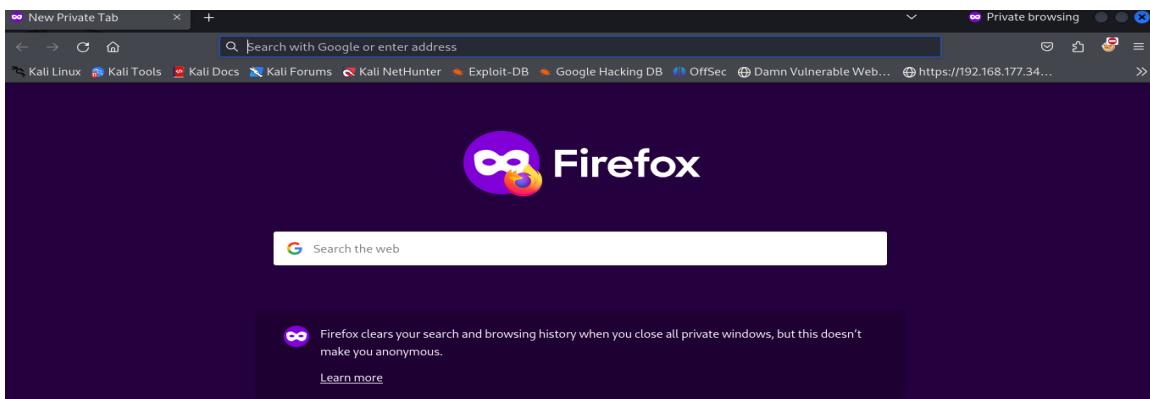
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Java Deserialization
Authorization Bypass
Open HTTP Redirect
Cryptography

DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: low
Locally Served
SQL DB: mysql

Advanced Cyber Security

Open new private window



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

ID	First Name	Surname	Update
5	Bob	Smith	[Update]
4	Pablo	Picasso	[Update]
3	Hack	Me	[Update]
2	Gordon	Brown	[Update]
1	admin	admin	[Update]

Logout from the normal window

ID	First Name	Surname	Update
5	Bob	Smith	[Update]
4	Pablo	Picasso	[Update]
3	Hack	Me	[Update]
2	Gordon	Brown	[Update]
1	admin	admin	[Update]

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

Advanced Cyber Security

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer

Intercept HTTP history WebSockets history | Proxy settings

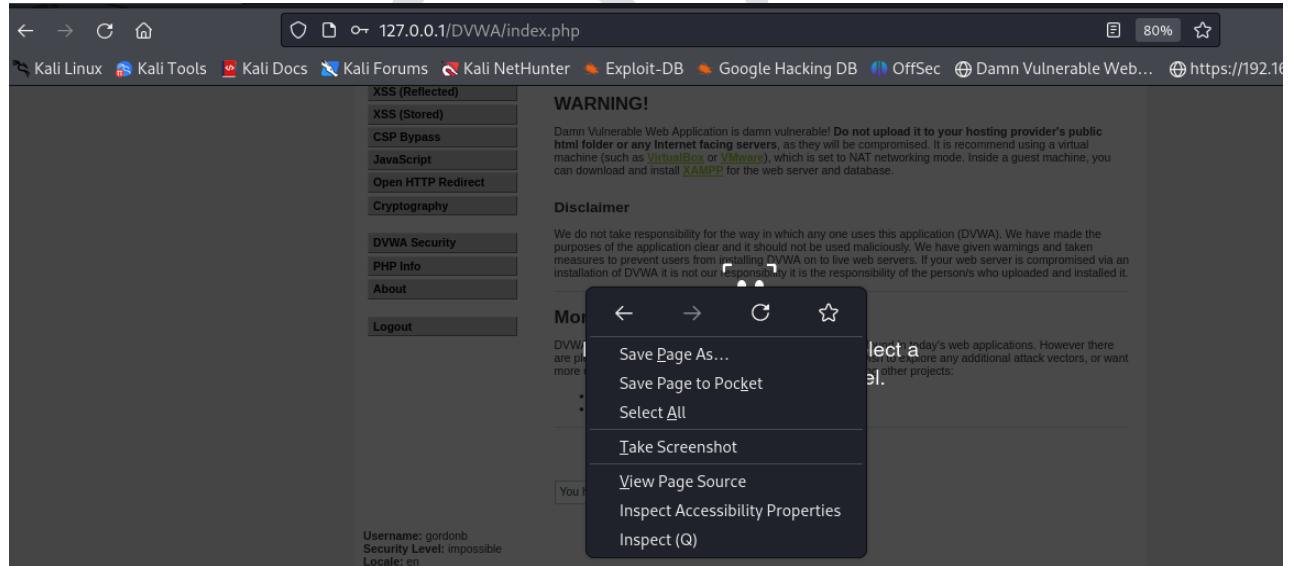
Request to http://127.0.0.1:80

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=14sopfvn05oajlp95qgfuo0mpq
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=7c2bcealfccf7f0a53ac01bc8350b79b
```

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



Advanced Cyber Security

Go to storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	p37n0kis6i2jkn1f418bf2iv	127.0.0.1	/	Fri, 06 Dec 2024 17:57:07 GMT	35	true	false	Strict	Thu, 05 Dec 2024 18:10:06 GMT
security	impossible	127.0.0.1	/	Session	18	true	false	None	Thu, 05 Dec 2024 18:10:06 GMT

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