Experiment2.3

Student Name: RAJDEEP JAISWAL. **UID: 20BCS2761**
Branch: CSE **Section/Group: 902-B**
Semester: 5th
Subject Name: WMS LAB **Subject Code: 20CSP-338**

1. **Aim:** Implementation of Session hijacking attack on http-enabled website

2. **Objective:** To Identify vulnerable session cookies.

3. **Software/Hardware Requirements:** Windows 7 & above

4. **Tools to be used:** Burpsuite

5. **Introduction:** **Session Hijacking:**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

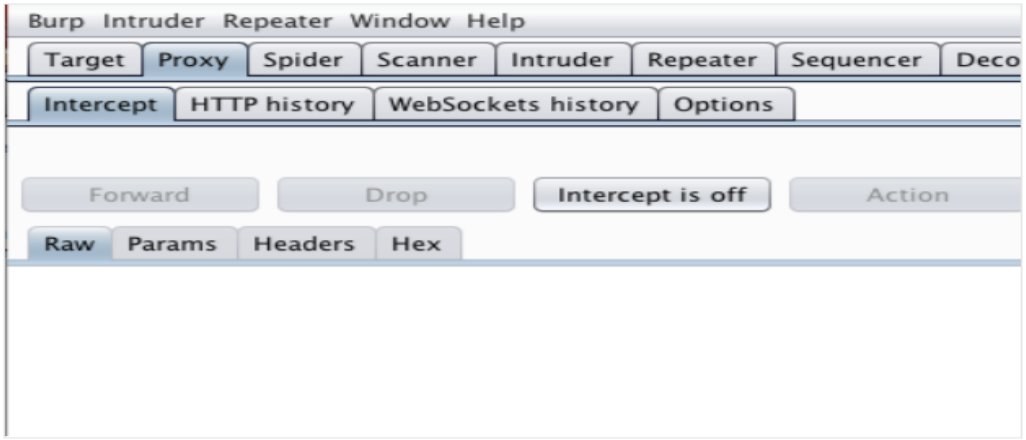
The session token could be compromised in different ways; the most common are:

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
- Man-in-the-middle attack
- Man-in-the-browser attack

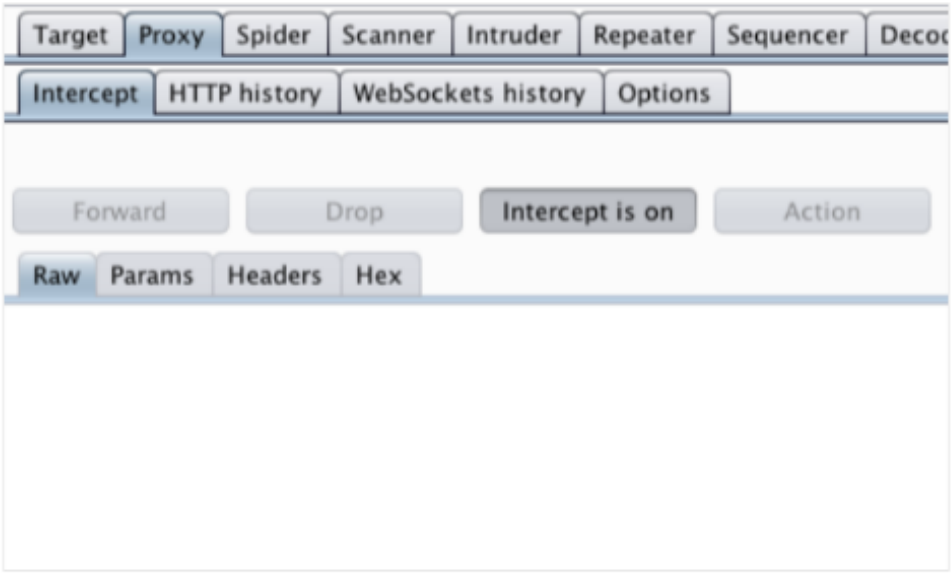
6. Steps/Method/Coding:

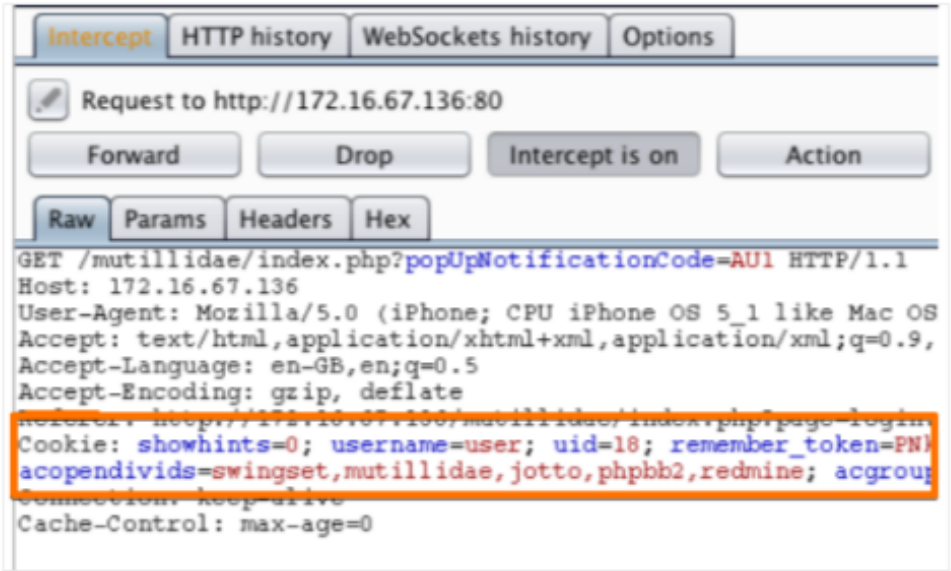
- First, ensure that Burp is correctly configured with your browser.
- With intercept turned off in the Proxy "Intercept" tab, visit the login page of the application you are testing in your browser.
- Log in to the application you are testing.
- You can log in using the credentials user:user.
- Return to Burp.
- In the Proxy "Intercept" tab, ensure "Intercept is on".
- Refresh the page in your browser.
- The request will be captured by Burp, it can be viewed in the Proxy "Intercept" tab.
- Cookies can be viewed in the cookie header.
- We now need to investigate and edit each individual cookie.
- Right click anywhere on the request and click "Send to Repeater".
- Go to the Repeater tab.
- The cookies in the request can be edited easily in the "Params" tab.
- By removing cookies from the request we can ascertain the function of each cookie.
- The response from the server can be viewed in the "Response" panel in Repeater.

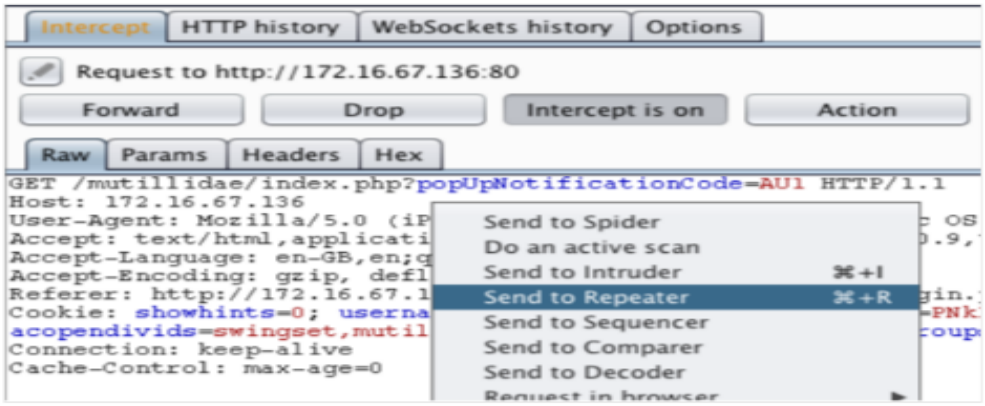
7. Output:

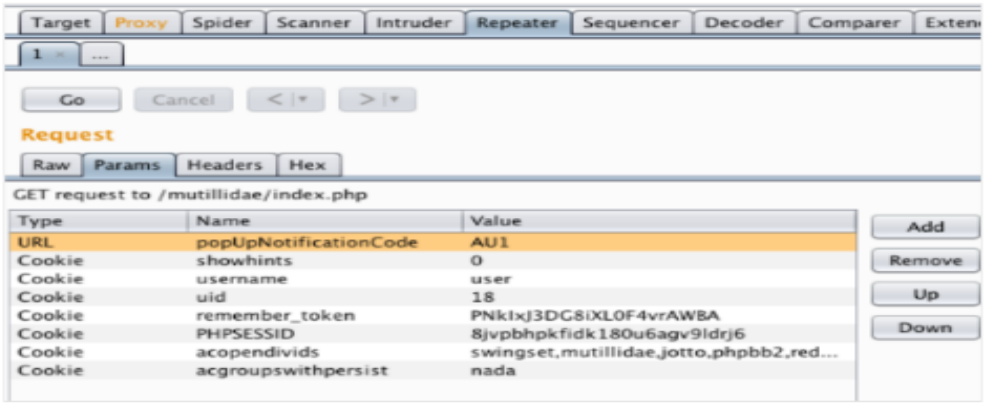

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Deco
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Raw Params Headers Hex

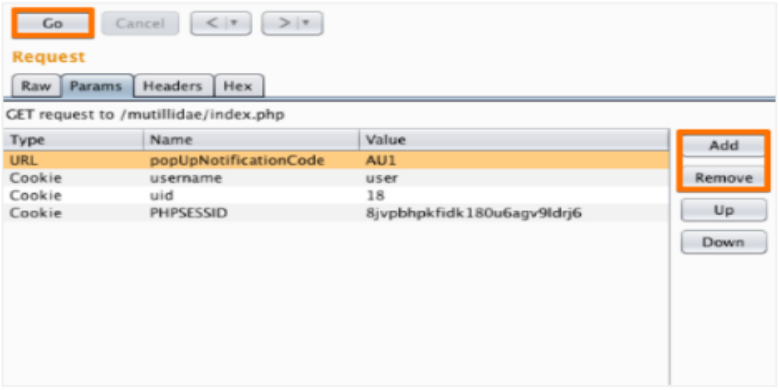

ack
Help Me!
Please sign-in
Name
user
Password
Login
Dont have an account? Please register here

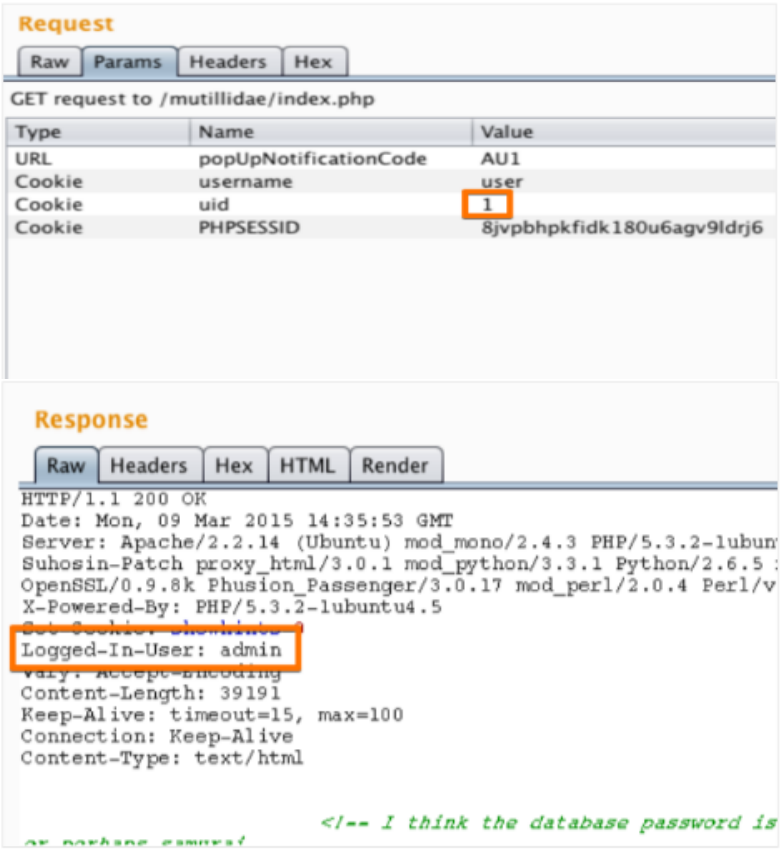

Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex


Intercept
HTTP history
WebSockets history
Options
Request to http://172.16.67.136:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=0; username=user; uid=18; remember_token=PN
acopendivids=swingset,mutillidae,jotto,phpbb2,redmine; acgrou
Cache-Control: max-age=0


Intercept
HTTP history
WebSockets history
Options
Request to http://172.16.67.136:80
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET /mutillidae/index.php?popUpNotificationCode=AU1 HTTP/1.1
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iP
Accept: text/html,applicati
Accept-Language: en-GB,en;q
Accept-Encoding: gzip, defl
Referer: http://172.16.67.1
Cookie: showhints=0; userna
acopendivids=swingset,mutil
Connection: keep-alive
Cache-Control: max-age=0
Send to Spider
Do an active scan
Send to Intruder ⌘+I
Send to Repeater ⌘+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
1
Go
Cancel
Request
Raw
Params
Headers
Hex
GET request to /mutillidae/index.php
Type
Name
Value
URL
popUpNotificationCode
AU1
Cookie
showhints
0
Cookie
username
user
Cookie
uid
18
Cookie
remember_token
PNkIxJ3DG8iXL0F4vrAWBA
Cookie
PHPSESSID
8jvpbhpkfidk180u6agv9ldrj6
Cookie
acopendivids
swingset,mutillidae,jotto,phpbb2,red...
Cookie
acgroupswithpersist
nada
Add
Remove
Up
Down





Learning Outcomes:

- Learnt to implement session hijacking.
- Learnt to use burpsuite to perform session hijacking.