

Name : SAIRAM B  
Reg no: 21BLC1468

## ASSIGNMENT - 4

### **Burp Suite :-**

A popular web vulnerability scanner and security testing tool used by cybersecurity professionals and ethical hackers to assess the security of web applications. It's developed by PortSwigger and provides a wide range of features for web application security testing, assessment, and penetration testing.

### **Why Burp Suite:-**

- Burp Suite is widely used in the field of web application security because of its robust set of features and userfriendly interface.
- It allows security professionals to identify, analyze, and exploit security vulnerabilities in web applications, helping organizations improve their security posture.
- Burp Suite is highly customizable and extensible, making it suitable for various types of web application testing scenarios.
- It provides detailed reports and logs that help security teams understand and address vulnerabilities effectively.

### **Key Features of Burp Suite:-**

**Proxy:** Burp Suite acts as an intercepting proxy, allowing you to inspect and modify HTTP requests and responses between your browser and the web application. This is useful for understanding how the application behaves and identifying potential vulnerabilities.

**Scanner:** Burp Scanner is an automated vulnerability scanner that identifies common security issues, such as SQL injection, cross-site scripting (XSS), and more. It helps in identifying vulnerabilities quickly.

**Spider:** The Spider tool crawls through a web application to map out its structure and discover hidden or unlinked pages, potentially uncovering additional attack surfaces.

**Repeater:** Repeater allows you to repeat and modify specific requests to the web application, making it useful for testing and exploiting vulnerabilities.

**Intruder:** The Intruder tool is used for performing automated attacks on web applications. It can help with tasks like password guessing, parameter fuzzing, and more.

**Decoder:** Decoder assists in decoding and encoding data using various encoding schemes, which is valuable for understanding how input data is processed by the application.

**Comparer:** This tool helps you compare two requests or responses, making it easier to spot differences and potential vulnerabilities.

**Extensions:** Burp Suite supports extensions and has an active community that develops add-ons to enhance its functionality. You can create custom extensions to tailor the tool to your specific needs.

**Session Management:** Burp Suite includes tools for managing user sessions, cookies, and authentication mechanisms, making it easier to test authenticated areas of a web application.

Testing on testfire.net :

Sign In | Contact Us | Feedback | Search [Go]

**AltoroMutual**

DEMO SITE ONLY

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

**Online Banking Login**

Username:

Password:

**PERSONAL**

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

**SMALL BUSINESS**

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

**INSIDE ALTORO MUTUAL**

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

Intercept HTTP history WebSockets history Proxy settings

Request to http://testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action Open browser

Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
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
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 42
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=C53963122ED135FD3598C3BC9F55814B; AltoroAccounts=ODAwMDAwfKMvcnBvcnF0ZX41LjI0MDE1MzQ2MUU3fDgwMDAwMX5DaGVja2luZ34xMTQyODIuNDR8
13 Upgrade-Insecure-Requests: 1
14
15 uid=veekshitha&passw=admin&btnSubmit=Login
```

**Inspector**

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 2

Request headers 12

When we login in our website, burp suite has captured the login details ,it has also captured cookie id, j session id,  
By poisoning them we can perform session hijacking attack as well as man in the middle attack.

**Adding payloads :**

?

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type and the payload type can be customized in different ways.

Payload set: 1

Payload count: 5

Payload type: Simple list

Request count: 0

?

**Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

veekshitha

admin

veekshitha@admin

21bce8943

Add

Enter a new item

Add from list ... [Pro version only]

## Payload positions :

Target: http://testfire.net

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

POST /doLogin HTTP/1.1

Host: testfire.net

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 42

Origin: http://testfire.net

Connection: close

Referer: http://testfire.net/login.jsp

Cookie: JSESSIONID=\$C53963122ED135FD3598C3BC9F55814B5; AltoroAccounts=\$0DAwMDAwfKvNcnBvcf0ZX41LjI0MDE1MzQ2MUU3fDgwMDAwMX5DaGVja2luZ34xMTQyODIuNDR8\$

Upgrade-Insecure-Requests: 1

uid=\$veekshitha&passw=\$admin&btnSubmit=\$Login\$

## Attack :

2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file

Attack

Save

Columns

Results

Positions

Payloads

Resource pool

Settings

Filter: Showing all items

Request	Position	Payload	Status code	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	126	
1	1		302	<input type="checkbox"/>	<input type="checkbox"/>	201	
2	1	veekshitha	302	<input type="checkbox"/>	<input type="checkbox"/>	201	
3	1	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	201	
4	1	veekshitha@admin	302	<input type="checkbox"/>	<input type="checkbox"/>	201	
5	1	21bce8943	302	<input type="checkbox"/>	<input type="checkbox"/>	201	
6	2		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
7	2	veekshitha	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
8	2	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
9	2	veekshitha@admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
10	2	21bce8943	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
11	3		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
12	3	veekshitha	302	<input type="checkbox"/>	<input type="checkbox"/>	126	

Finished

## HTTPS History :

Intercept HTTP history WebSockets history | Proxy settings

▼ Filter: Hiding CSS, image and general binary content

[illegible]