ASSIGNMENT 4

Overview of the Assignment: Write about Burp Suite, state its uses, and elaborate on its features. Try the burp suite on testfire.net to identify any vulnerabilities.

What is BURPSUITE?

Burp Suite is a popular cybersecurity tool used for testing the security of web applications. It is developed by PortSwigger and is widely used by security professionals, penetration testers, and web developers to identify and fix vulnerabilities in web applications. Some of the key features and components of the burp suite include:

1. Proxy: Burp Suite acts as a proxy server that sits between your browser and the target web application. It allows you to intercept and inspect HTTP requests and responses, making it easier to identify security issues.

2. Scanner: Burp Suite includes an automated scanner that can crawl a web application and automatically identify common security vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It helps in identifying potential vulnerabilities quickly.

3. Repeater: This feature allows you to manually manipulate and resend individual HTTP requests. It is useful for testing the impact of different input values on a web application and analyzing how it responds.

4. Intruder: Burp Suite's Intruder tool is used for automating custom attacks against web applications. It can be configured to perform various types of brute force or parameter-based attacks to discover vulnerabilities.

5. Sequencer: The Sequencer tool is used for analyzing the quality of randomness in tokens and session identifiers generated by web applications. This can help in identifying vulnerabilities related to weak or predictable session management.

6. Decoder: Burp Suite includes various encoding and decoding functions for analyzing and manipulating data in different formats, such as URL encoding, base64 encoding, and more.

7. Extensibility: Burp Suite can be extended with custom plugins, which allows security professionals to add new functionality and automate specific tasks. Many community-contributed plugins are available.

8. Target and Site Map: These features help you organize and visualize the information gathered during scanning and testing sessions. They provide a structured view of the target application and its vulnerabilities.

9. Reporting: After conducting security assessments, Burp Suite can generate detailed reports that include identified vulnerabilities, their severity, and recommendations for mitigation.

Its various components and features make it valuable for a range of tasks related to assessing the security of web applications and services. Here are some common uses of Burp Suite:

- Web Application Scanning: Burp Suite's automated scanner can crawl a web application, identify vulnerabilities, and provide detailed reports. It is commonly used to find issues like SQL injection, cross-site scripting (XSS), and other security vulnerabilities.

- Manual Testing: Security professionals use Burp Suite's proxy and interception capabilities to manually inspect and manipulate HTTP requests and responses. This allows for the discovery of vulnerabilities that automated tools might miss.

- Session Management Analysis: Burp Suite's session handling tools can help analyze how a web application manages user sessions, including the predictability of session tokens and the effectiveness of session timeout mechanisms.

- Parameter Manipulation: The Intruder tool in Burp Suite is used to automate parameter-based attacks, such as brute force and fuzzing, to identify vulnerabilities that may arise from improper input validation or filtering.

- Web Services Testing: It can be employed to test the security of SOAP and RESTful web services, including the examination of XML and JSON payloads.

- Authentication Testing: Burp Suite can be used to test the security of login mechanisms, including username and password enumeration and brute force attacks.

- Client-Side Testing: Security professionals can analyze and test JavaScript code, cookies, and other client-side components for security vulnerabilities like DOM-based XSS.

- Custom Plugin Development: Security professionals can extend Burp Suite's functionality by developing custom plugins to automate specific tasks or integrate with other tools.

- Penetration Testing: Burp Suite is often used as part of penetration testing engagements to identify and demonstrate security weaknesses in web applications and APIs.

It is important to note that Burp Suite should be used only on web applications and services for which you have explicit authorization or legal permission to test. Unauthorized or irresponsible use of such tools can have legal and ethical implications.

Example of implementation of Burpsuite on testfire.net :

http://testfire.net/index.jsp [content parameter]

Summary

Severity:	**High**
Confidence:	**Firm**
Host:	**http://testfire.net**
Path:	**/index.jsp**

Issue detail

The value of the **content** request parameter is copied into the HTML document as plain text between tags. The payload **jftw8<a b=c>kg4p3** was submitted in the content parameter. This input was echoed unmodified in the application's response.

This behavior demonstrates that it is possible to inject new HTML tags and attributes into the returned document. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript but this was not successful. You should manually examine the application's behavior and attempt to identify any unusual input validation or other obstacles that may be in place.

Request 1

```
GET /index.jsp?content=inside.htmjftw8%3ca%20b%3dc%3ekg4p3 HTTP/1.1
Host: testfire.net
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: JSESSIONID=B8CFF6745F9E8C6109A3016DAEA32E49
Upgrade-Insecure-Requests: 1
Referer: http://testfire.net/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response 1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6930
Date: Mon, 25 Sep 2023 07:09:44 GMT
Connection: close


<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.
...[SNIP]...
<p>Failed due to The requested resource (/static/inside.htmjftw8<a b=c>kg4p3) is not available</p>
...[SNIP]...
```