

ASSIGNMENT-4

NAME: P. MONISH

Reg No: 21BCE9517

Q. What is burp suite and explain its features.

Burp Suite is a popular cybersecurity tool designed for web application security testing and penetration testing. Developed by PortSwigger, Burp Suite is widely used by security professionals, ethical hackers, and developers to identify and address security vulnerabilities in web applications. It provides a comprehensive set of features for web security assessment, including:

1. Scanning and Crawling: Burp Suite can crawl websites to discover all accessible pages and analyze the web application's structure. It helps identify various components, such as forms, links, and parameters.

2. Web Application Scanning: Burp Suite can automatically scan web applications for common security vulnerabilities, including SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and more. It tests the application's inputs and behavior to find potential security flaws.

3. Manual Testing: One of the key features of Burp Suite is its Proxy tool, which allows security professionals to intercept and modify web traffic between the browser and the web application. This enables manual testing of inputs, requests, and responses, making it easier to identify and exploit vulnerabilities.

4. Intruder: Burp Suite's Intruder tool facilitates automated attacks on web applications, helping identify vulnerabilities through various attack payloads and techniques. It can be used for tasks like brute force attacks, fuzzing, and parameter manipulation.

5. Repeater: The Repeater tool allows users to manipulate and replay individual HTTP requests, making it useful for testing specific functionalities and verifying the impact of changes on the application.

6. Sequencer: Burp Suite's Sequencer tool is used to analyze the randomness and quality of tokens or session identifiers, which can be crucial for understanding the security of authentication mechanisms.

7. Extensibility: Burp Suite can be extended using custom plugins and scripts. This extensibility allows security professionals to create their own tools or integrate with other security testing frameworks.

8. Reporting: After testing, Burp Suite generates detailed reports that highlight identified vulnerabilities, potential risks, and recommended remediation steps. These reports are valuable for communicating security findings to development and security teams.

Burp Suite is available in both free and commercial versions. The free version, known as "Burp Suite Community Edition," provides basic functionality and is often used by individuals for educational and personal purposes. The commercial version, "Burp Suite Professional," offers advanced features and is commonly used by organizations for professional security testing and assessment of their web applications.

It's important to note that Burp Suite should be used responsibly and within the boundaries of legal and ethical guidelines. Unauthorized and malicious use of such tools on websites and applications without proper authorization is illegal and unethical. Security professionals and ethical hackers should always obtain proper permissions before conducting security assessments using Burp Suite or similar tools.

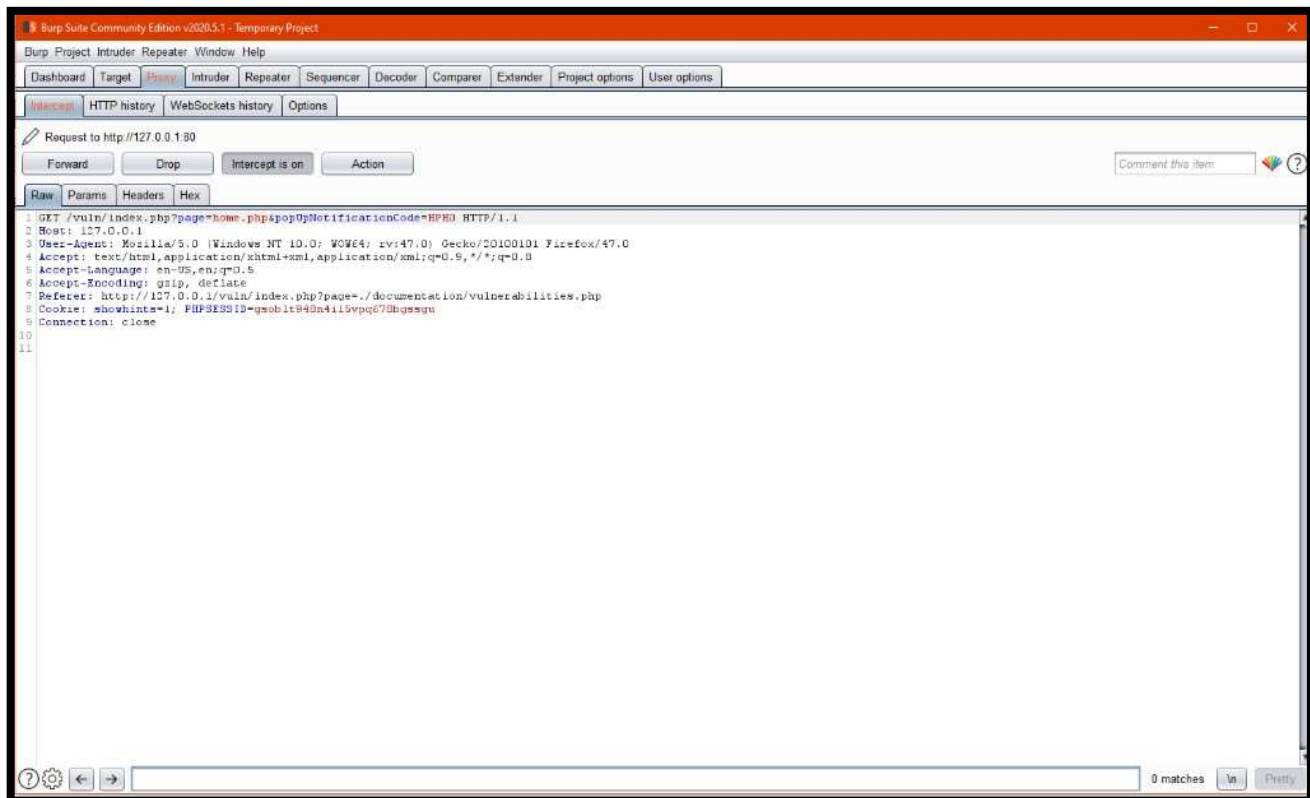
Test the vulnerabilities of testfire.net

Testing Environment:

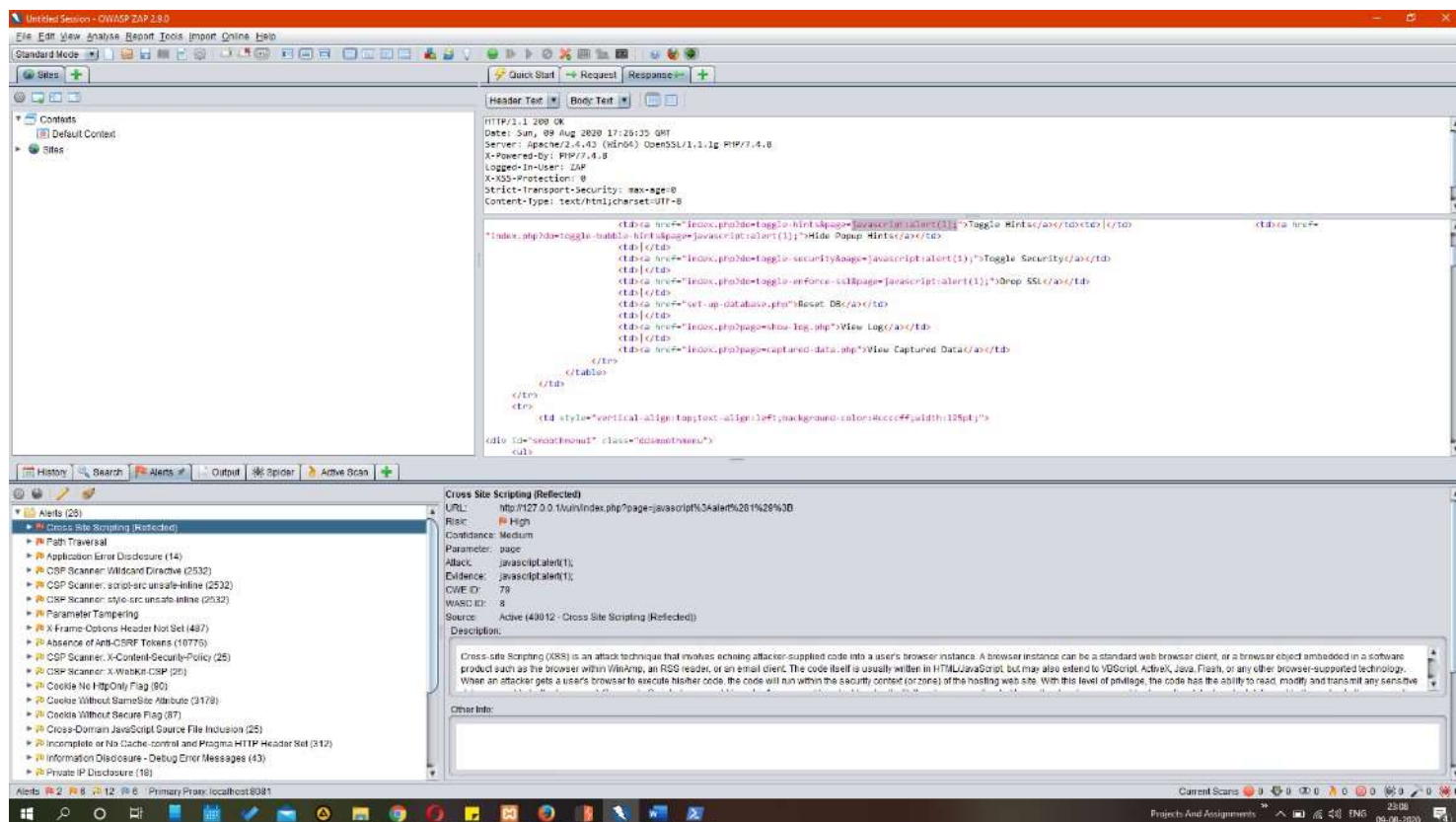
1. Altoro Mutual [demo.testfire.net]

Tools Used:

1. Burp Suite



2. OWASP Zap Vulnerability Scanner



Location / URL - <http://demo.testfire.net/login.jsp>



Steps and Description.

I was able to easily get through the login page of demo.testfire.net, accessible at <http://demo.testfire.net/login.jsp> by using the payload ' Or '1'=1.

(Ignored the ' after the last character of the payload, as it was found as already being added by the web app.)

Online Banking Login

Username:

Password:

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of €8799.02!

Click [Here](#) to apply.

1. We take the request and forward it to the repeater.

The screenshot shows the Burp Suite Community Edition v2020.5.1 interface. The 'Repeater' tab is active, displaying a request and its corresponding response.

Request:

```
1 GET /vuln/index.php?page=user-info.php&username=Shaswat&password=123456&user-info-php-submit-button=View+Account+Details HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://127.0.0.1/vuln/index.php?page=user-info.php
8 Cookie: showhints=1; PHPSESSID=da9n02oi2o54f0ikm9cqrjdmko
9 Connection: close
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Fri, 07 Aug 2020 14:17:45 GMT
3 Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.8
4 X-Powered-By: PHP/7.4.8
5 Logged-In-User:
6 X-XSS-Protection: 0
7 Strict-Transport-Security: max-age=0
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10 Content-Length: 54258
11
12 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www
13 <html>
14 <head>
15 <link rel="shortcut icon" href="./images/favicon.ico" type="image/x-ic
16 <link rel="stylesheet" type="text/css" href="./styles/global-styles.cs
17 <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/dd
18 <link rel="stylesheet" type="text/css" href="./styles/ddsmoothmenu/dd
19
20 <script type="text/javascript" src="./javascript/ddsmoothmenu/ddsmooth
21 </script>
22 <script type="text/javascript" src="./javascript/ddsmoothmenu/jquery.m
23 </script>
24 <script type="text/javascript">
25 ddsmoothmenu.init({
26   mainmenuid: "smoothmenu1", //menu DIV id
27   orientation: 'v', //Horizontal or vertical menu: Set to "h" or "v"
28   classname: 'ddsmoothmenu', //class added to menu's outer DIV
29   //customtheme: ["#cccc44", "#cccccc"],
30   contentsource: "markup" // "markup" or ["container_id", "path_to_me
31 });
32 </script>
33 <script type="text/javascript">
34 $(function() {
35   $('[ReflectedXSSExecutionPoint]').attr("title", "");
36   $('[ReflectedXSSExecutionPoint]').balloon();
37   $('[CookieTamperingAffectedArea]').attr("title", "");
38   $('[CookieTamperingAffectedArea]').balloon();
39 });
40 </script>
```

The status bar at the bottom indicates "Done" and "54,553 bytes | 624 millis".

1

Burp Suite Community Edition v2020.5.1 - Temporary Project

Burp

Project

Intruder

Repeater

Window

Help

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

User options

Intercept

HTTP history

WebSockets history

Options

Request to http://127.0.0.1:80

Forward

Drop

Intercept is on

Action

Comment this item

Raw

Params

Headers

Hex

1

GET /vuln/index.php?page=user-info.php&username=Shaswat&password=123456&user-info-php-submit-button=View+Account+Details HTTP/1.1

2

Host: 127.0.0.1

3

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0

4

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

5

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

6

Accept-Encoding: gzip, deflate

7

Referer: http://127.0.0.1/vuln/index.php?page=user-info.php

8

Cookie: showhints=1; PHPSESSID=da9n02oi2o54f0ikm9cqrjdmko

9

Connection: close

10

11