

AI for Cyber Security with IBM Qradar

Name: Prince Levin Panditi

Email: prince.21bce9648@vitapstudent.ac.in

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 analyse 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 behaviour 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 analyse 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 organisations 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. Unauthorised 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.

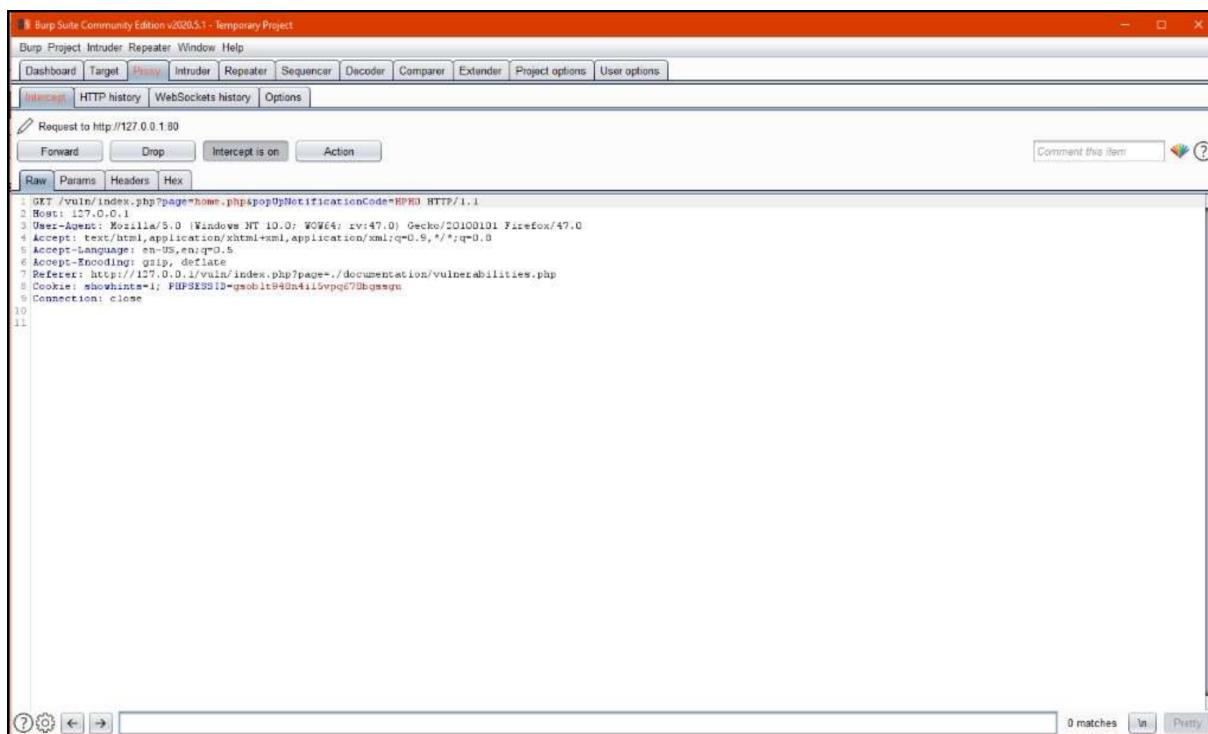
Test the vulnerabilities of testfire.net

Testing Environment:

1. Altoro Mutual [demo.testfire.net]

Tools Used:

1. Burp Suite



2. OWASP Zap Vulnerability Scanner

Cross Site Scripting (Reflected)

URL: http://127.0.0.1:8000/index.php?page=javascript%3Aalert%28%29%3D

Risk: **High**

Vulnerability: Medium

Parameter: page

Attack: javascript%3A...

CVE ID: 79

CWE ID: 79

Source: Active (40012 - Cross Site Scripting (Reflected))

Description:

Cross-site Scripting (XSS) is an attack technique that involves sending attacker-supplied code into a victim's browser instance. A browser cookie can be a constant web-based or a temporary object embedded in a cookie provided such as the browser while visiting, an RSS reader, or an email client. The code itself is usually written in HTML and JavaScript, but may also refer to JSON, XML, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zones) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive information.

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.)

The screenshot shows two windows. On the left is the 'Online Banking Login' page with fields for Username (' Or '1'='1') and Password ('*****'). On the right is the 'Hello Admin User' page, which displays a welcome message, account details (800000 Corporate), and a congratulatory message about pre-approval for a credit card.

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

The screenshot of Burp Suite shows the 'Request' tab containing the payload: 'GET /vuln/index.php?page=user-info.php&username=Shaswat&password=123456&user-info-php-submit-button=View+Account+Details HTTP/1.1'. The 'Response' tab shows the server's response, which includes the HTML code for the login page and the user's session information.

Burp Suite Community Edition v2020.5.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Proxy Target 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
```