SHASHIBHUSHAN DAS
21BCE0515

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 willdelve 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 andstrengthen 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 itseffectiveness in identifying and mitigating web application vulnerabilities. Hereare some key reasons why Burp Suite is a go-to choice for security professionals:

1. Vulnerability Detection: Burp Suite excels in identifying various web applicationvulnerabilities, 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 andcomes 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, whichcan 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 attackscenarios.

5. Reporting: Burp Suite generates detailed reports that provide a comprehensiveoverview 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 providesa 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. Thisis 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 scansweb 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 requeststo 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 onweb applications. It allows users to define attack payloads and positions within requests, making it a valuable asset for identifying vulnerabilities like brute forcelogin attempts.

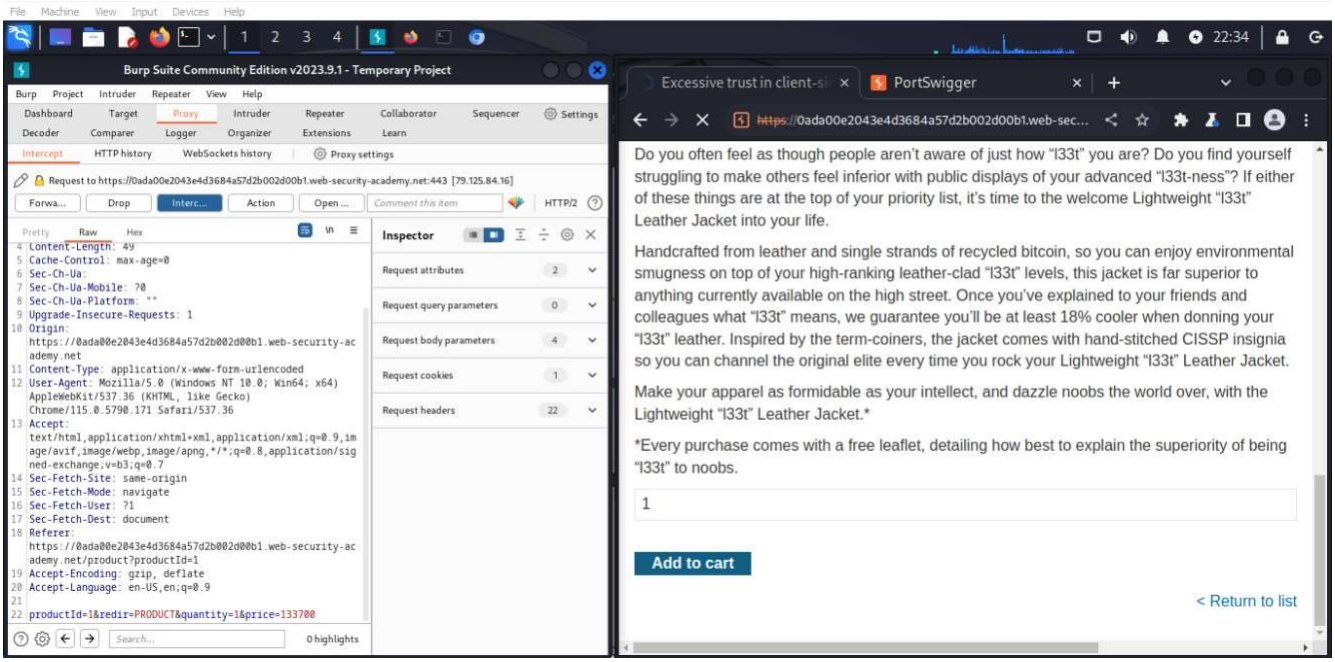
6. Sequencer: The Sequencer tool helps assess the quality of randomness intokens and session identifiers, which can be critical for understanding and exploiting vulnerabilities related to insecure randomness.

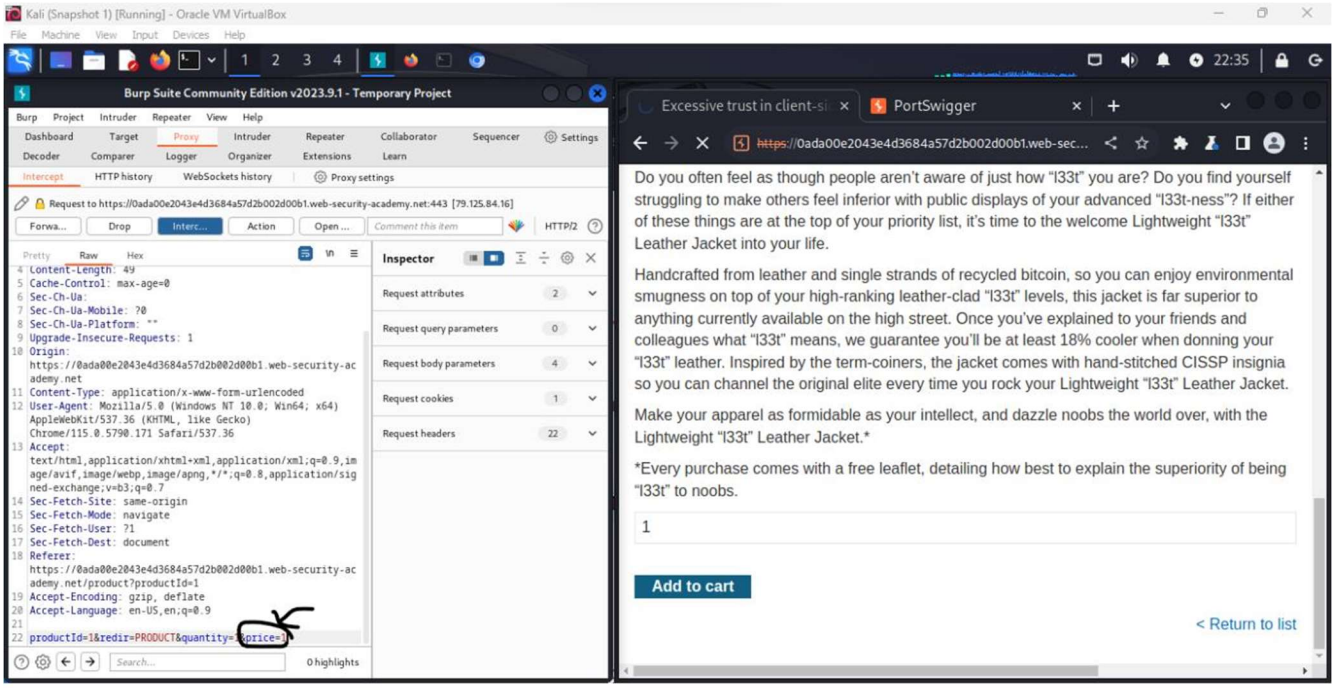
7. Decoder: Burp Suite includes various decoders for encoding and decoding data, which can be handy when working with encoded input, such as Base64 orURL encoding.

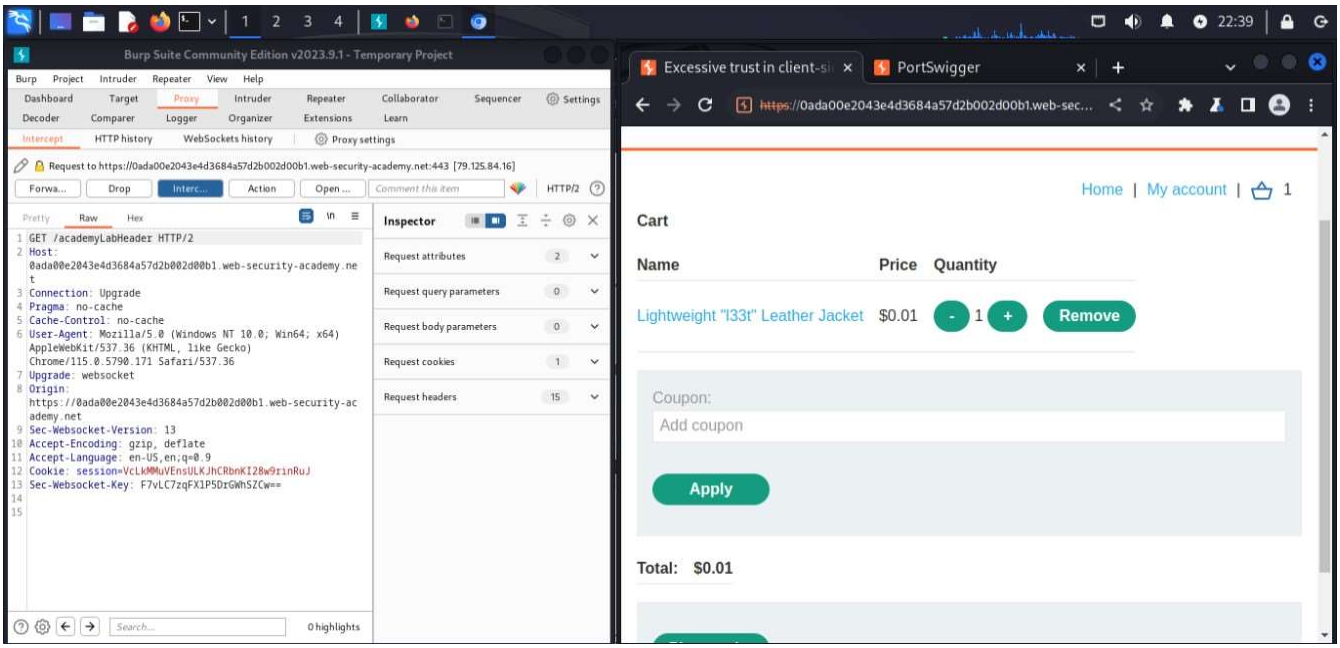
8. Comparer: The Comparer tool allows users to compare two requests or responses, making it easier to spot differences that might indicate vulnerabilitiesor security issues.

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 functionalityand tailor the tool to their specific needs.

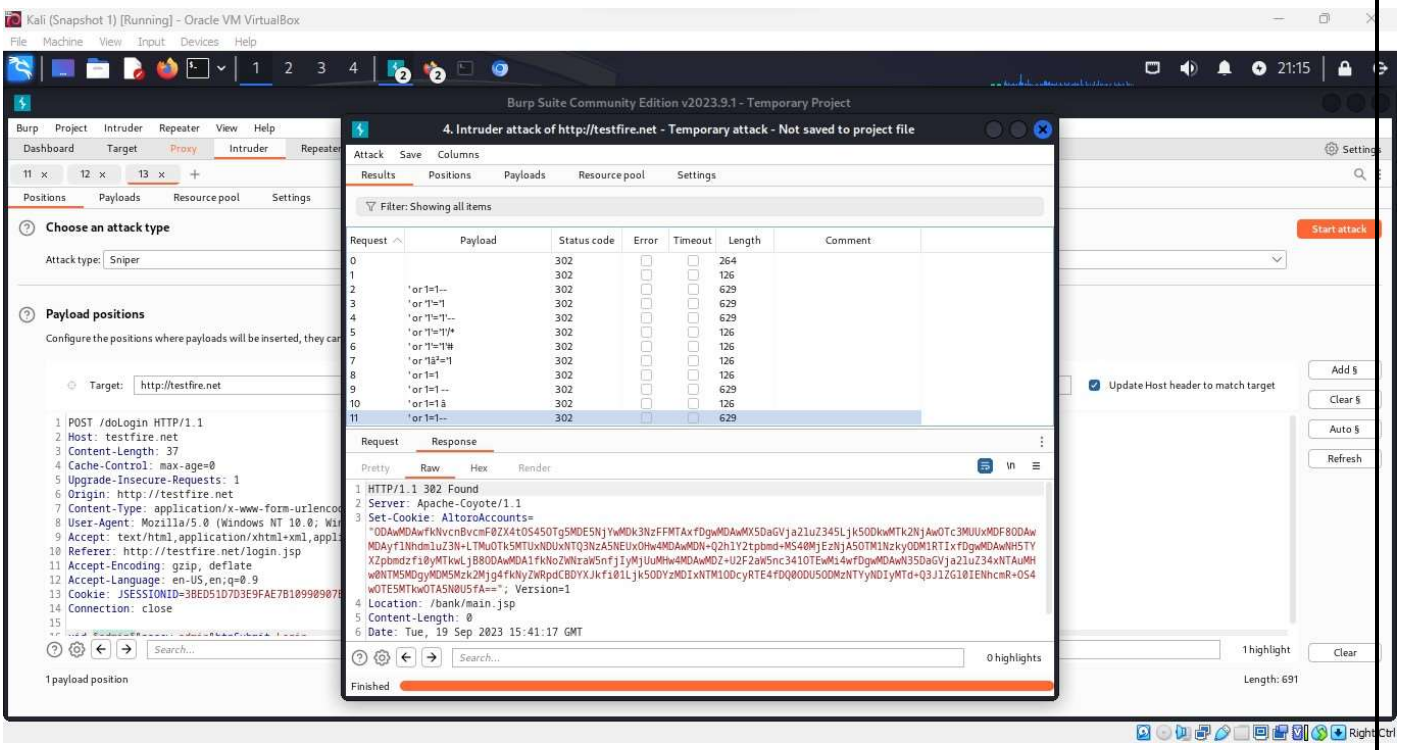
Attack 1:

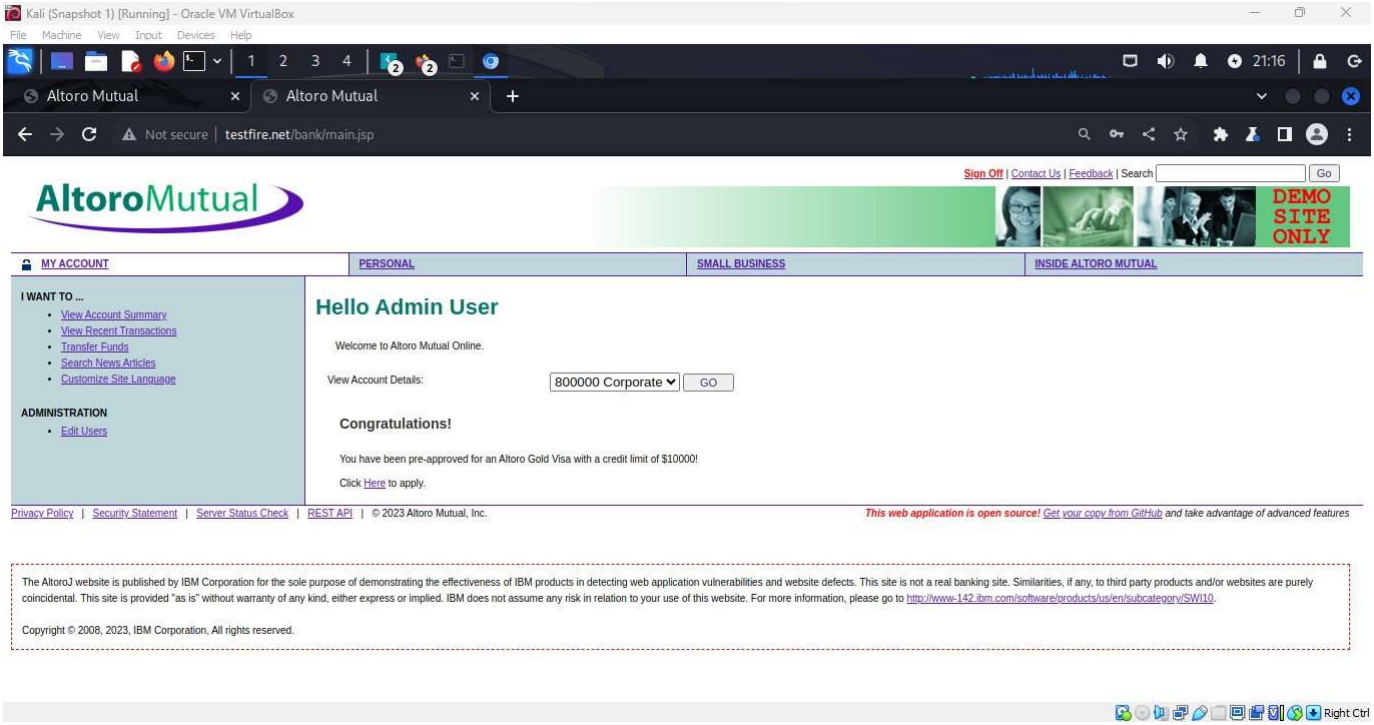

Burp Suite Community Edition v2023.9.1 - Temporary Project
Excessive trust in client-si
PortSwigger
Do you often feel as though people aren't aware of just how "l33t" you are? Do you find yourself struggling to make others feel inferior with public displays of your advanced "l33t-ness"? If either of these things are at the top of your priority list, it's time to the welcome Lightweight "l33t" Leather Jacket into your life.
Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "l33t" levels, this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "l33t" means, we guarantee you'll be at least 18% cooler when donning your "l33t" leather. Inspired by the term-coiners, the jacket comes with hand-stitched CISSP insignia so you can channel the original elite every time you rock your Lightweight "l33t" Leather Jacket.
Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "l33t" Leather Jacket.*
*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "l33t" to noobs.
1
Add to cart
< Return to list


Kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2023.9.1 - Temporary Project
Excessive trust in client-si
PortSwigger
Do you often feel as though people aren't aware of just how "l33t" you are? Do you find yourself struggling to make others feel inferior with public displays of your advanced "l33t-ness"? If either of these things are at the top of your priority list, it's time to the welcome Lightweight "l33t" Leather Jacket into your life.
Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "l33t" levels, this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "l33t" means, we guarantee you'll be at least 18% cooler when donning your "l33t" leather. Inspired by the term-coiners, the jacket comes with hand-stitched CISSP insignia so you can channel the original elite every time you rock your Lightweight "l33t" Leather Jacket.
Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "l33t" Leather Jacket.*
*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "l33t" to noobs.
1
Add to cart
< Return to list


Burp Suite Community Edition v2023.9.1 - Temporary Project
Request to https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net:443 [79.125.84.16]
GET /academyLabHeader HTTP/2
Host: 0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
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
Upgrade: websocket
Origin: https://0ada00e2043e4d3684a57d2b002d00b1.web-security-academy.net
Sec-Websocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=VcLkMMuVEnsULKJhCRbnKI28w9rinRuJ
Sec-Websocket-Key: F7vLC7zqFX1P5DrGWhSZCw==
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Excessive trust in client-si
PortSwigger
Home | My account | 1
Cart
Name
Price
Quantity
Lightweight "l33t" Leather Jacket
$0.01
Remove
Coupon:
Add coupon
Apply
Total: $0.01

Attack 2:


Kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2023.9.1 - Temporary Project
4. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Choose an attack type
Payload positions
Start attack
Update Host header to match target
Request
Response
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: /bank/main.jsp
Content-Length: 0
Date: Tue, 19 Sep 2023 15:41:17 GMT
Finished


Kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Altoro Mutual
testfire.net/bank/main.jsp
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
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/us/en/subcategory/SWI10.
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, eachhighlighting 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. Thishands-on experience helped us identify vulnerabilities and understand web applications better.

Attack 2 utilized the Intruder tool, allowing us to automate and customize attackson the web application with precision. This experience underscored Burp Suite'seffectiveness 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. BurpSuite demonstrates technology's effectiveness in identifying vulnerabilities and strengthening defenses against evolving cyber threats.