

MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

BRUTEFORCE PASSWORD ATTACK USING
BURPSUITE

ASSIGNMENT 1

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 20, 2024

Contents

| | | |
|----------|---|-----------|
| 1 | Aim | 1 |
| 2 | Objectives | 1 |
| 3 | Theory | 1 |
| 3.1 | Burpsuite | 1 |
| 3.2 | Advantages | 1 |
| 3.3 | Disadvantages | 1 |
| 4 | Implementation | 2 |
| 4.1 | Launching Burpsuite | 2 |
| 4.2 | Opening Browser for Locally hosted Django Project | 3 |
| 4.3 | Entering Credentials and Interecepting | 3 |
| 4.4 | Setting Payloads by selecting Username and Password | 4 |
| 4.5 | Choosing Cluster Bomb | 5 |
| 4.6 | Setting Password Brute Force Attack lists | 6 |
| 4.7 | Setting Password Brute Force Attack lists | 7 |
| 4.8 | Setting Usernames list from brute forcer | 8 |
| 4.9 | Executing Attack | 9 |
| 4.10 | Executing Attack, as seen on django server console logs | 9 |
| 4.11 | Finding Correct password by noticing change in length | 10 |
| 4.12 | Correct password found | 10 |
| 5 | Platform | 10 |
| 6 | Conclusion | 11 |

1 Aim

To perform a brute force attack using Burpsuite.

2 Objectives

1. To learn about the Burpsuite tool.
2. To perform a brute force attack using Burpsuite.
3. To understand the concept of brute force attacks.

3 Theory

3.1 Burpsuite

Burp Suite is a leading cybersecurity tool that provides web application security testing. It is developed by PortSwigger, an IT security company based in the UK. Burp Suite is widely used by security professionals to perform various security testing tasks, such as scanning, crawling, and testing web applications for vulnerabilities.

3.2 Advantages

- BurpSuite provides a user-friendly interface, making it accessible to both beginners and experienced users.
- It offers a wide range of features for web application testing, including proxy, scanner, and intruder, among others.
- BurpSuite supports various platforms, including Windows, macOS, and Linux, enhancing its versatility and usability.
- The tool allows for easy customization and extension through the use of plugins, enabling users to tailor their testing environment according to their needs.
- BurpSuite provides detailed reports and logs, facilitating thorough analysis and documentation of test results.

3.3 Disadvantages

- While BurpSuite offers a free version, its full set of features is only available in the paid version, which may be a barrier for some users.
- Due to its extensive functionality, BurpSuite has a steep learning curve, requiring time and effort to master all of its features effectively.
- The tool's reliance on Java may lead to performance issues, especially when dealing with large-scale or complex testing scenarios.
- BurpSuite's automated scanning capabilities may produce false positives or miss certain vulnerabilities, requiring manual verification by users.

- The graphical user interface (GUI) of BurpSuite, while intuitive for many, may not be suitable for users who prefer command-line interfaces or scripted testing approaches.

4 Implementation

4.1 Launching Burpsuite



Figure 1: Launching Burpsuite

4.2 Opening Browser for Locally hosted Django Project

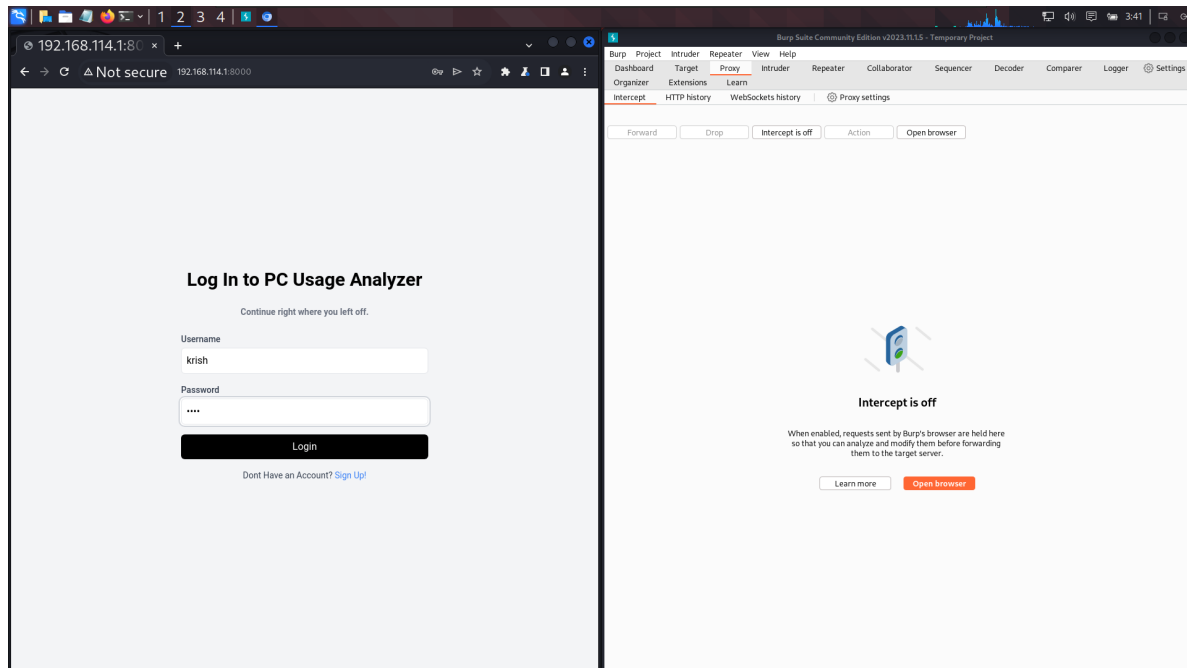


Figure 2: Opening Browser for Locally hosted Django Project

4.3 Entering Credentials and Interecepting

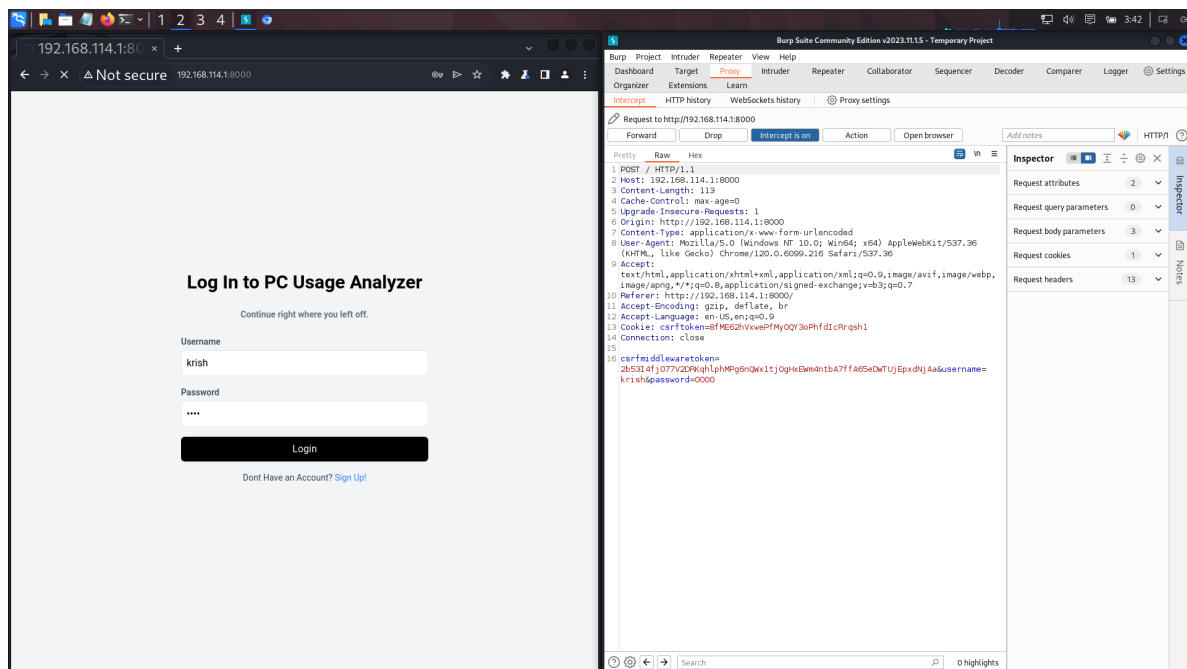


Figure 3: Entering Credentials and Interecepting

4.4 Setting Payloads by selecting Username and Password

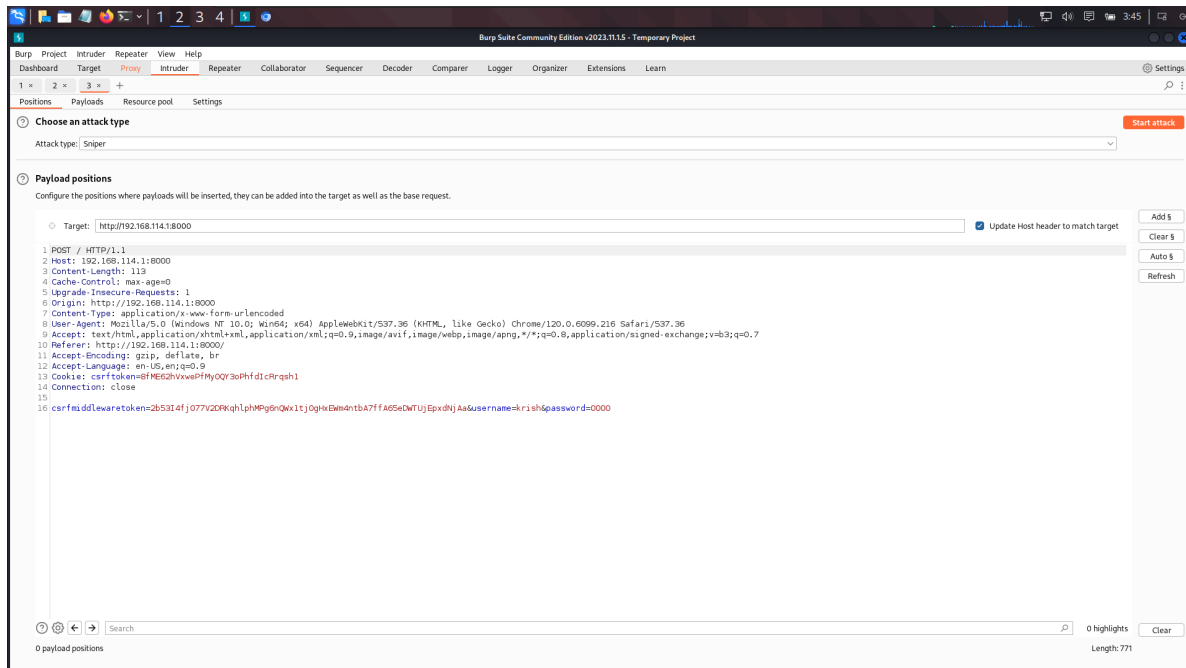


Figure 4: Setting Payloads by selecting Username and Password

4.5 Choosing Cluster Bomb

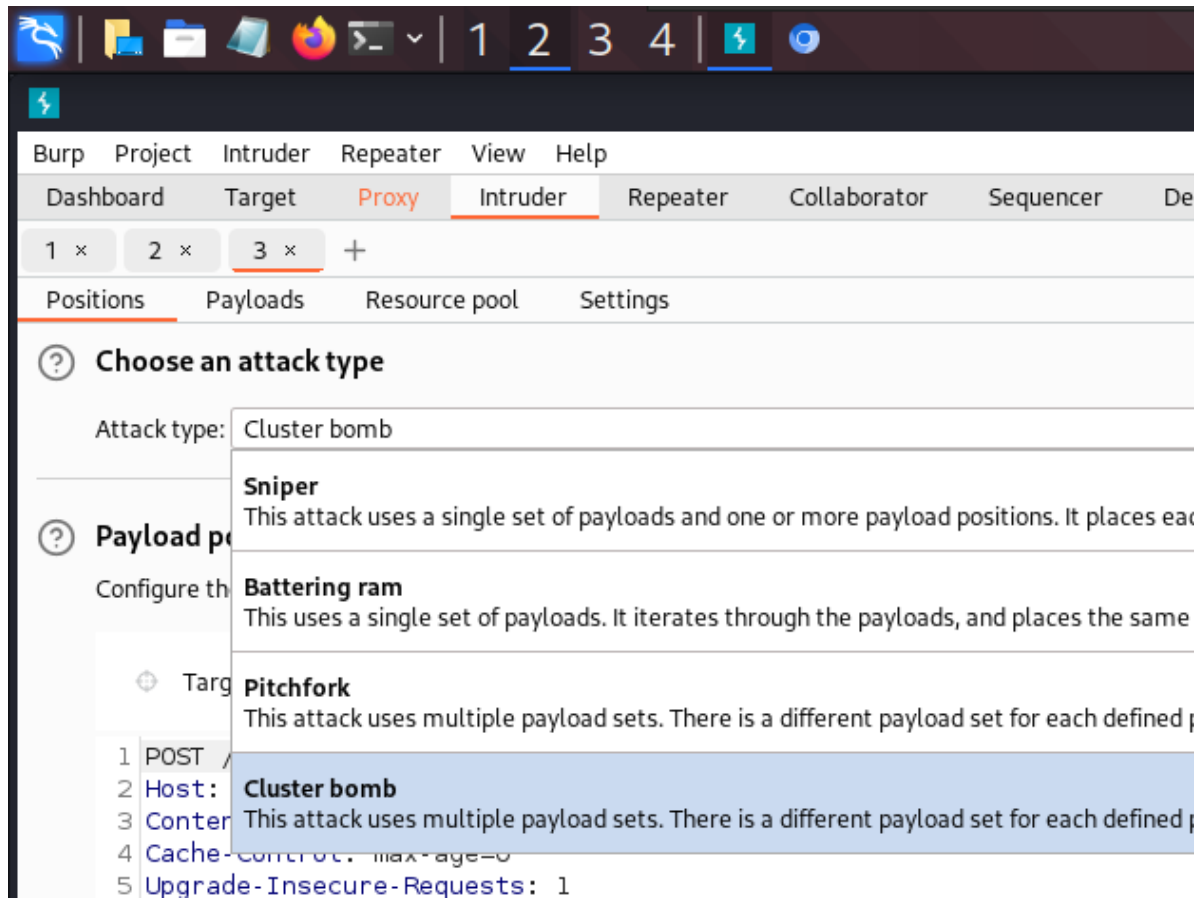


Figure 5: Choosing Cluster Bomb

4.6 Setting Password Brute Force Attack lists

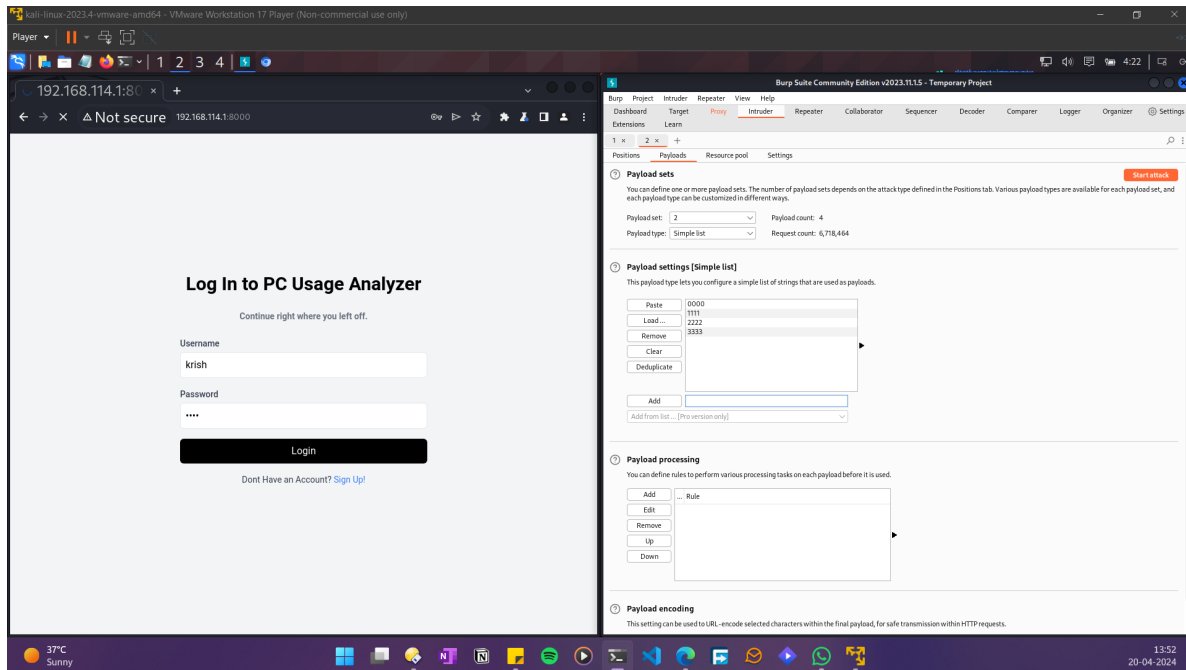


Figure 6: Setting Password Brute Force Attack lists

4.7 Setting Password Brute Force Attack lists

The screenshot shows the Burp Suite interface with the 'Payloads' tab selected. At the top, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. Below the tabs, the 'Payload sets' section is visible, containing a help icon, a title, a description, and configuration fields for 'Payload set' (value: 2), 'Payload count' (value: 4), 'Payload type' (value: Simple list), and 'Request count' (value: 6,718,464). Below this is the 'Payload settings [Simple list]' section, which includes a description, a list of payloads (0000, 1111, 2222, 3333), and buttons for 'Paste', 'Load ...', 'Remove', 'Clear', 'Deduplicate', 'Add', and 'Add from list ... [Pro version only]'.

1 x **2 x** +

Positions **Payloads** Resource pool Settings

? **Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type. Each payload type can be customized in different ways.

Payload set: 2 Payload count: 4

Payload type: Simple list Request count: 6,718,464

? **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste 0000

Load ... 1111

Remove 2222

Clear 3333

Deduplicate

Add

Add from list ... [Pro version only]

Figure 7: Setting Password Brute Force Attack lists

4.8 Setting Usernames list from brute forcer

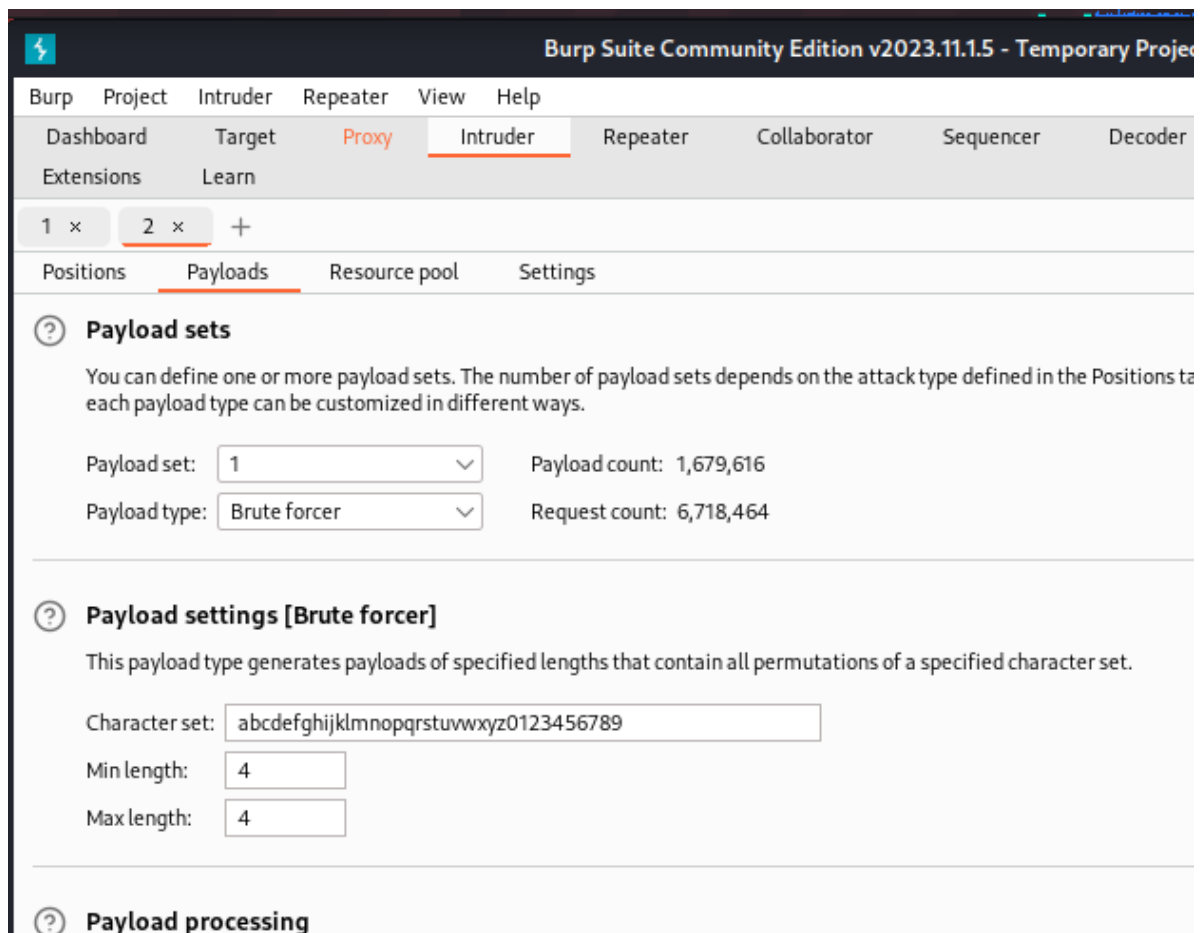


Figure 8: Setting Usernames list from brute forcer

4.9 Executing Attack

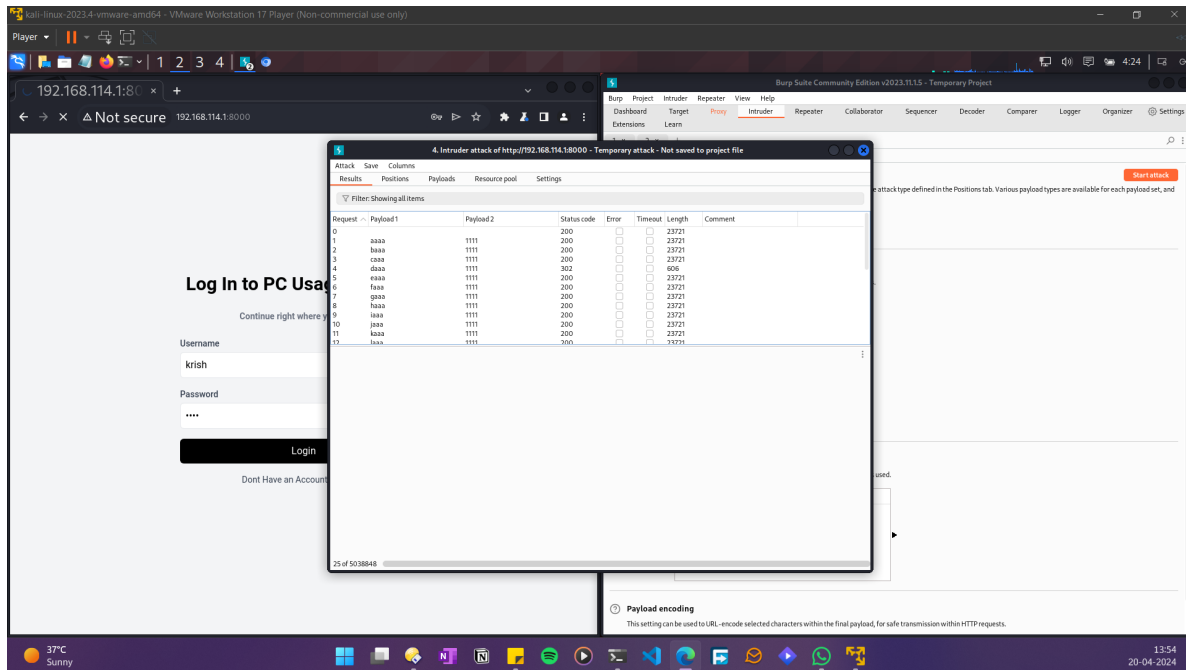


Figure 9: Executing Attack

4.10 Executing Attack, as seen on django server console logs

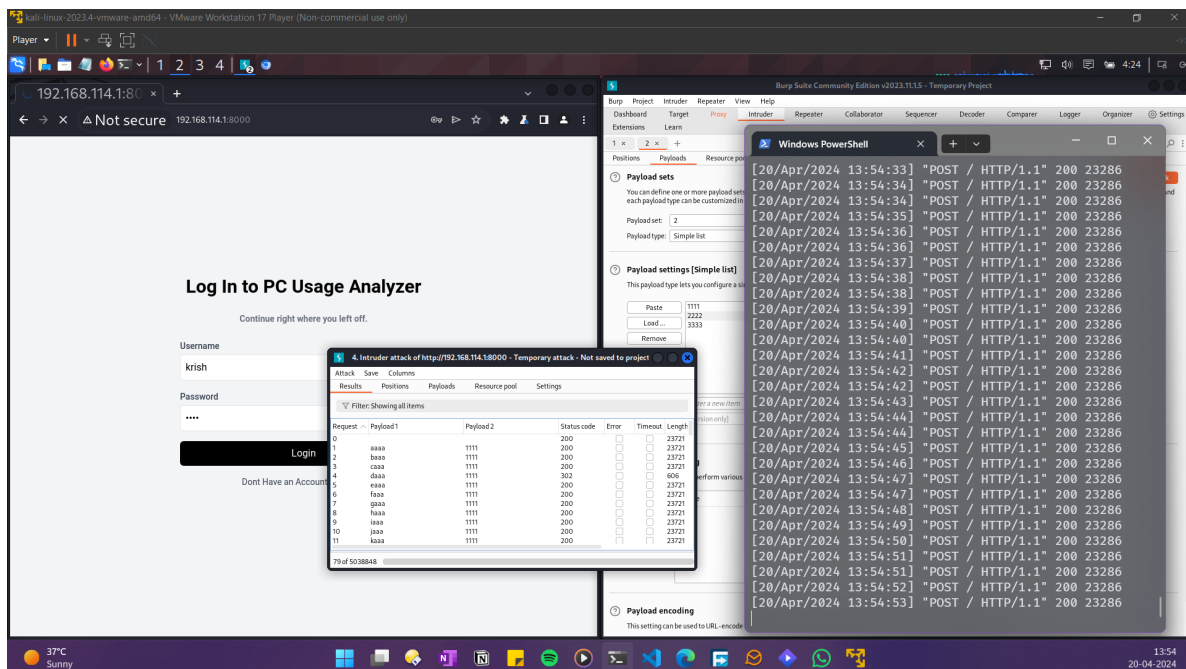


Figure 10: Executing Attack, as seen on django server console logs

4.11 Finding Correct password by noticing change in length

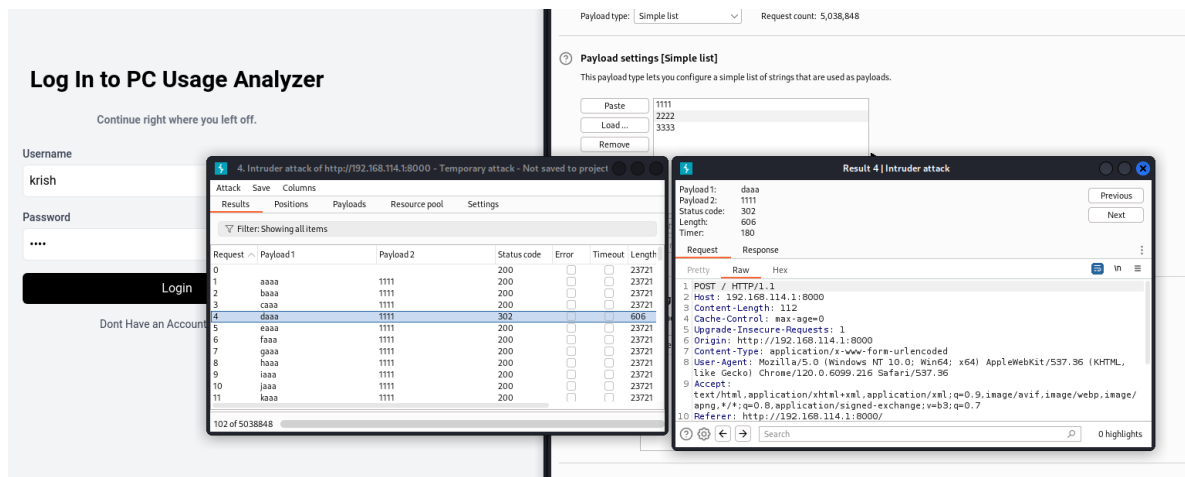


Figure 11: Finding Correct password by noticing change in length

4.12 Correct password found

| 4. Intruder attack of http://192.168.114.1:8000 - Temporary attack - Not saved to project | | | | | | | |
|---|-----------|-----------|-------------|--------------------------|--------------------------|--------|--|
| Attack Save Columns | | | | | | | |
| Results Positions Payloads Resource pool Settings | | | | | | | |
| Filter: Showing all items | | | | | | | |
| Request | Payload 1 | Payload 2 | Status code | Error | Timeout | Length | |
| 0 | | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 1 | aaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 2 | baaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 3 | caaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 4 | daaa | 1111 | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 606 | |
| 5 | aaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 6 | faaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 7 | gaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 8 | haaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 9 | iaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 10 | jaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |
| 11 | kaaa | 1111 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 23721 | |

Figure 12: Correct password found

5 Platform

Operating System: Arch Linux X8664

IDEs or Text Editors Used: Visual Studio Code

FAQs

1. Features of Burp Suite:

- Web vulnerability scanning
- Intercepting proxy
- Application scanning

2. Three versions of Burp Suite:

- Community Edition (free)
- Professional Edition (paid)
- Enterprise Edition (paid with additional team features)

3. Safety of Burp Suite:

- Burp Suite is safe for ethical hacking and security testing when used responsibly and legally.

4. Purpose of the proxy tab in Burp Suite:

- Allows intercepting and modifying HTTP/S requests and responses for analyzing and manipulating web traffic during security testing.

6 Conclusion

In this assignment, we learned about the Burpsuite tool and performed a brute force attack using Burpsuite. We set up the attack by intercepting the login request, setting up the payloads, and executing the attack. We observed the attack in action and found the correct password by noticing the change in the response length. This exercise helped us understand the concept of brute force attacks and how they can be used to compromise security.