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

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

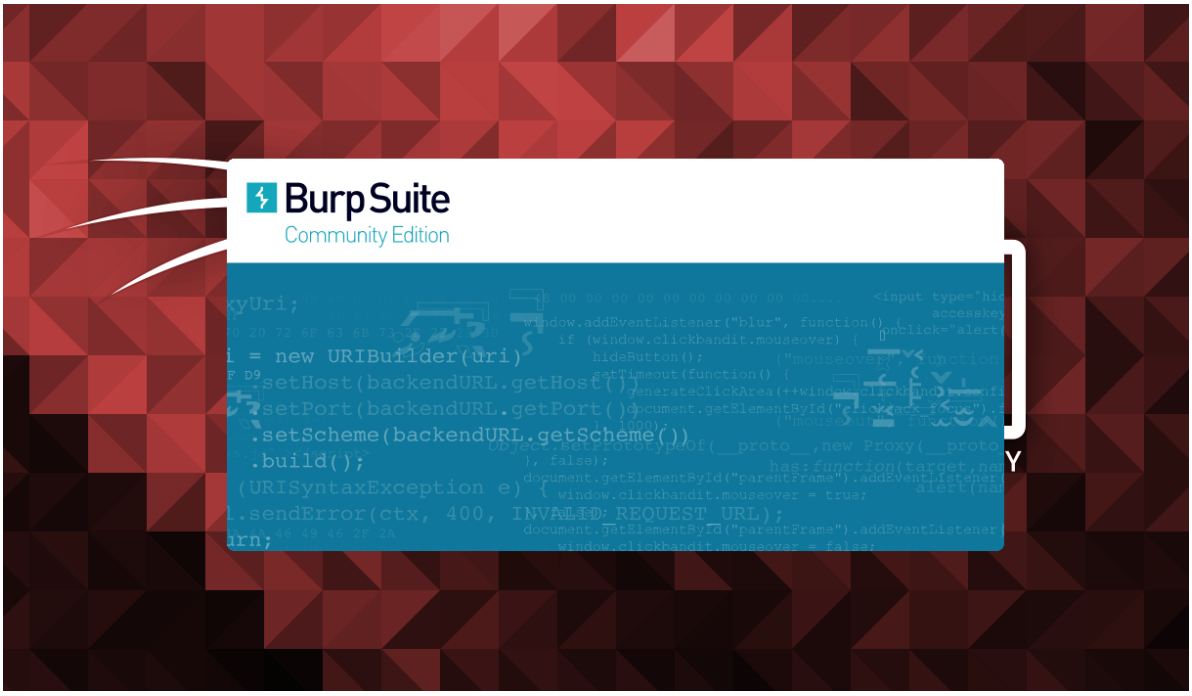

Figure 1: Launching Burpsuite

4.2 Opening Browser for Locally hosted Django Project

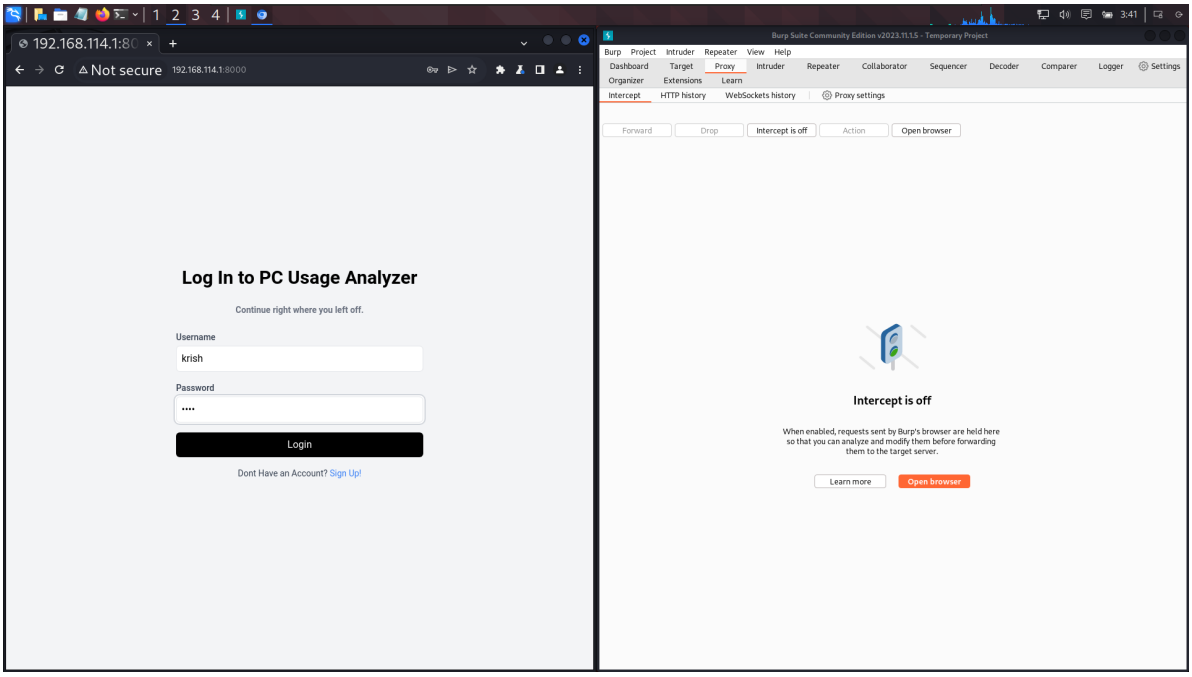

Figure 2: Opening Browser for Locally hosted Django Project

4.3 Entering Credentials and Interecepting

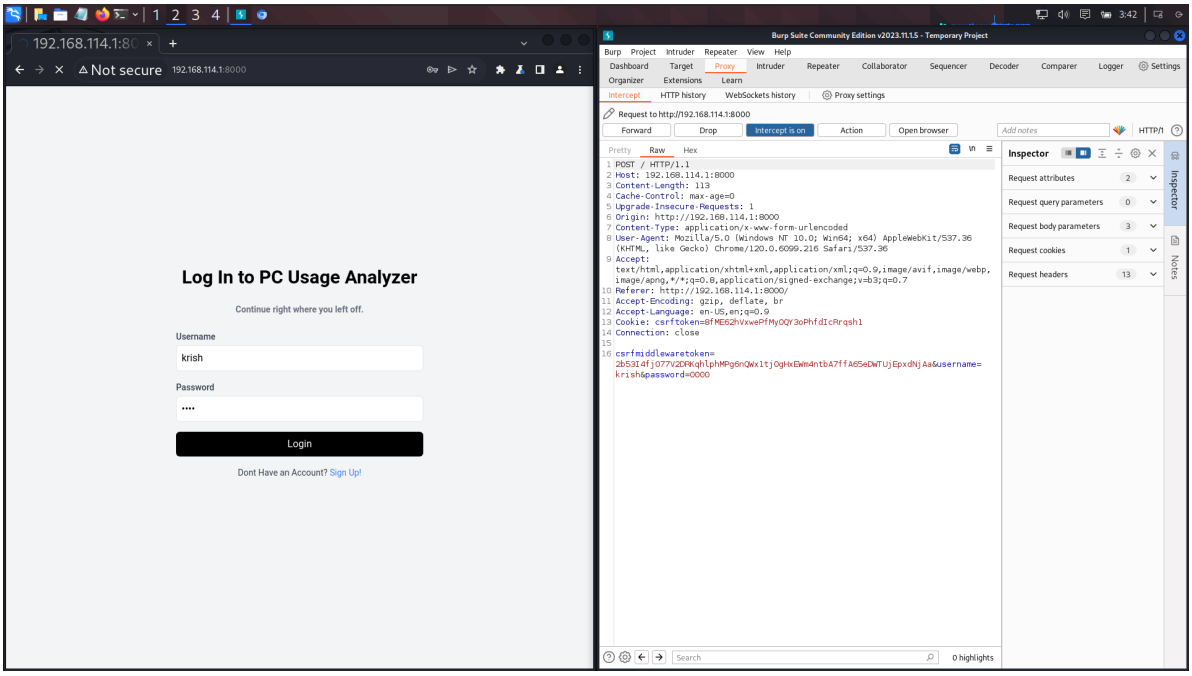

Figure 3: Entering Credentials and Interecepting

4.4 Setting Payloads by selecting Username and Password

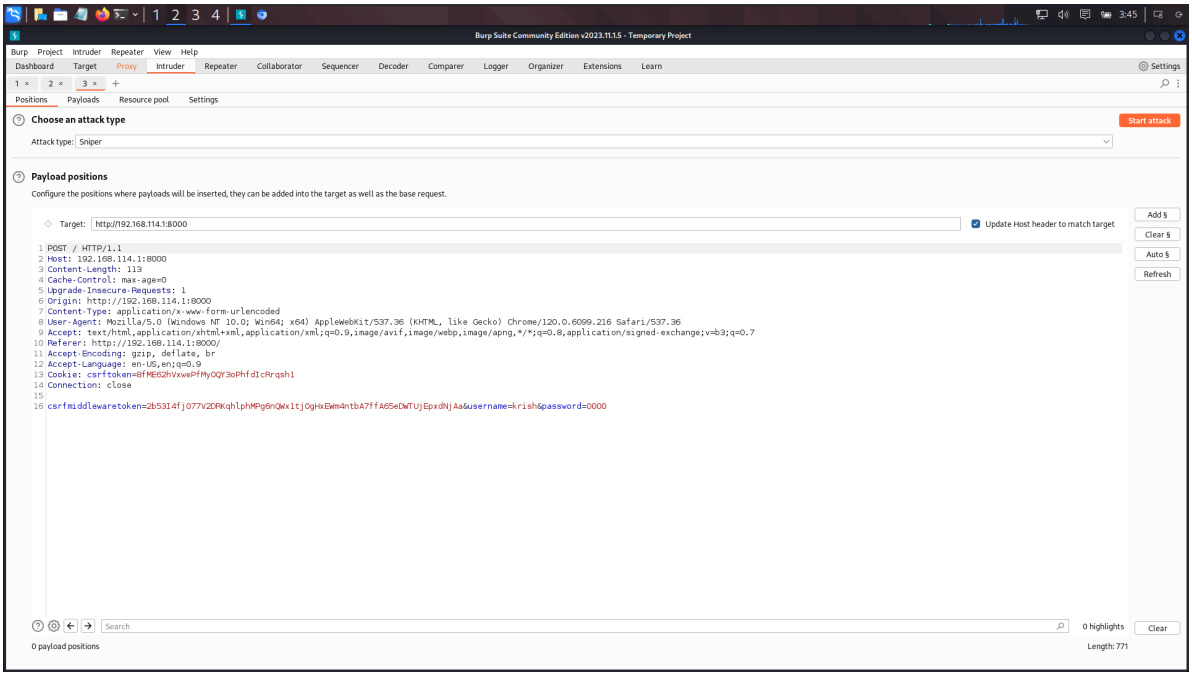

Figure 4: Setting Payloads by selecting Username and Password

4.5 Choosing Cluster Bomb

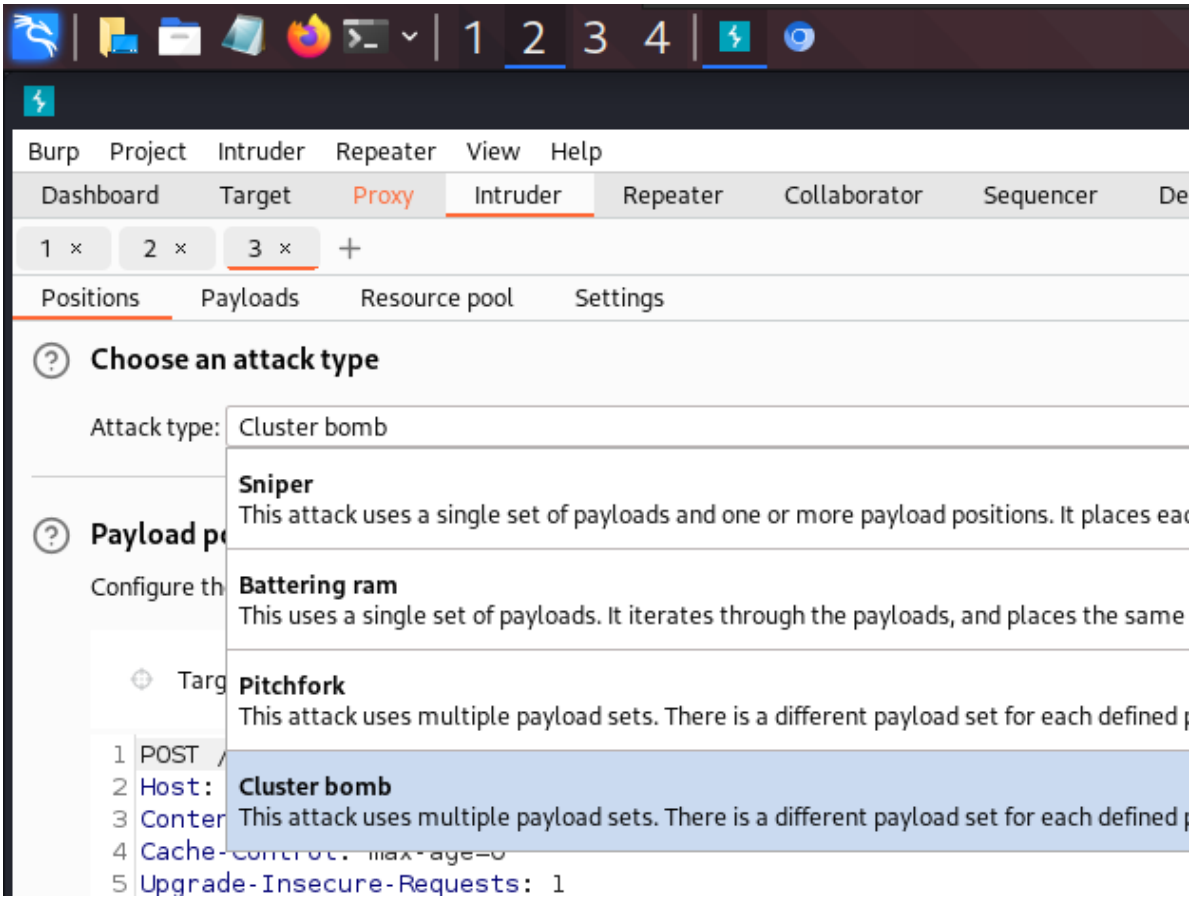

Figure 5: Choosing Cluster Bomb

4.6 Setting Password Brute Force Attack lists

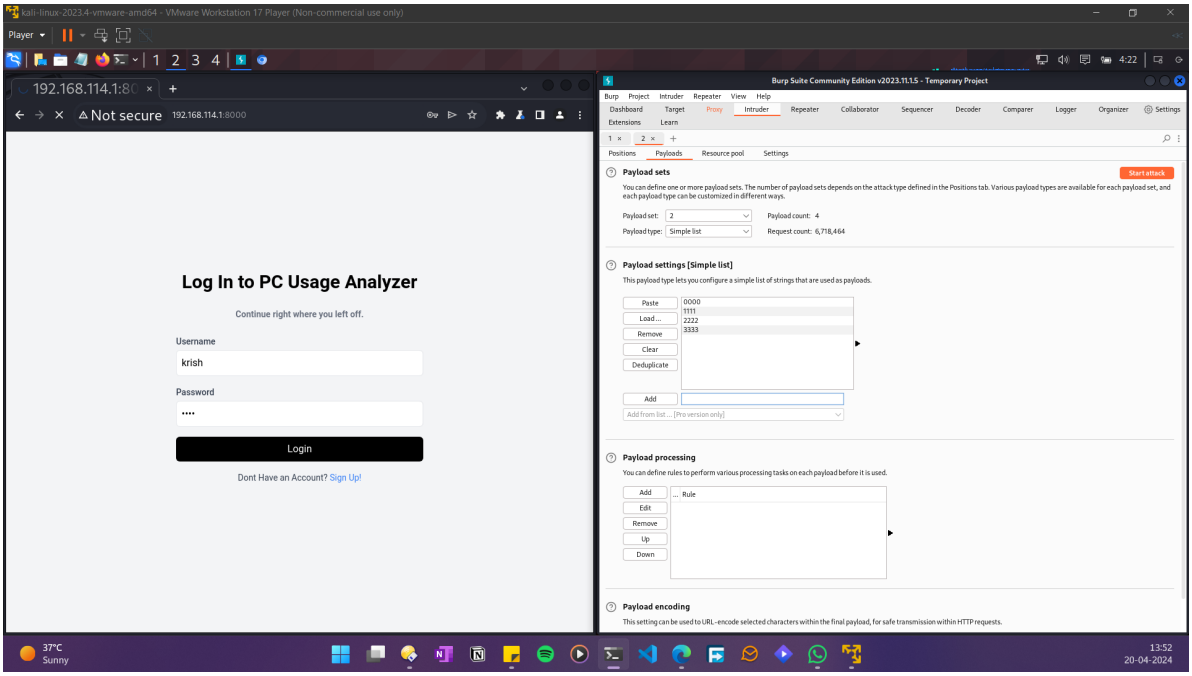

Figure 6: Setting Password Brute Force Attack lists

4.7 Setting Password Brute Force Attack lists

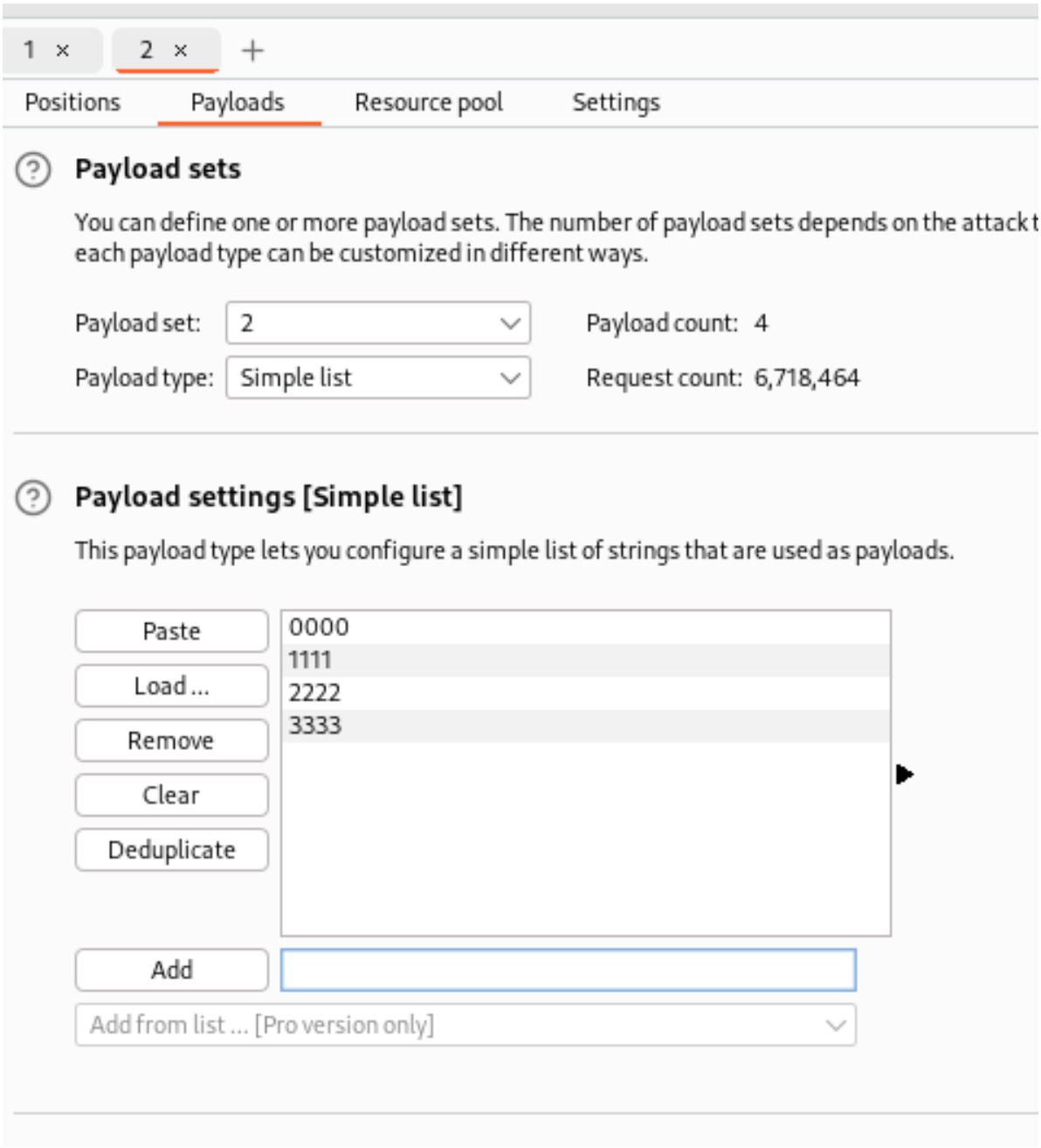

Figure 7: Setting Password Brute Force Attack lists

4.8 Setting Usernames list from brute forcer

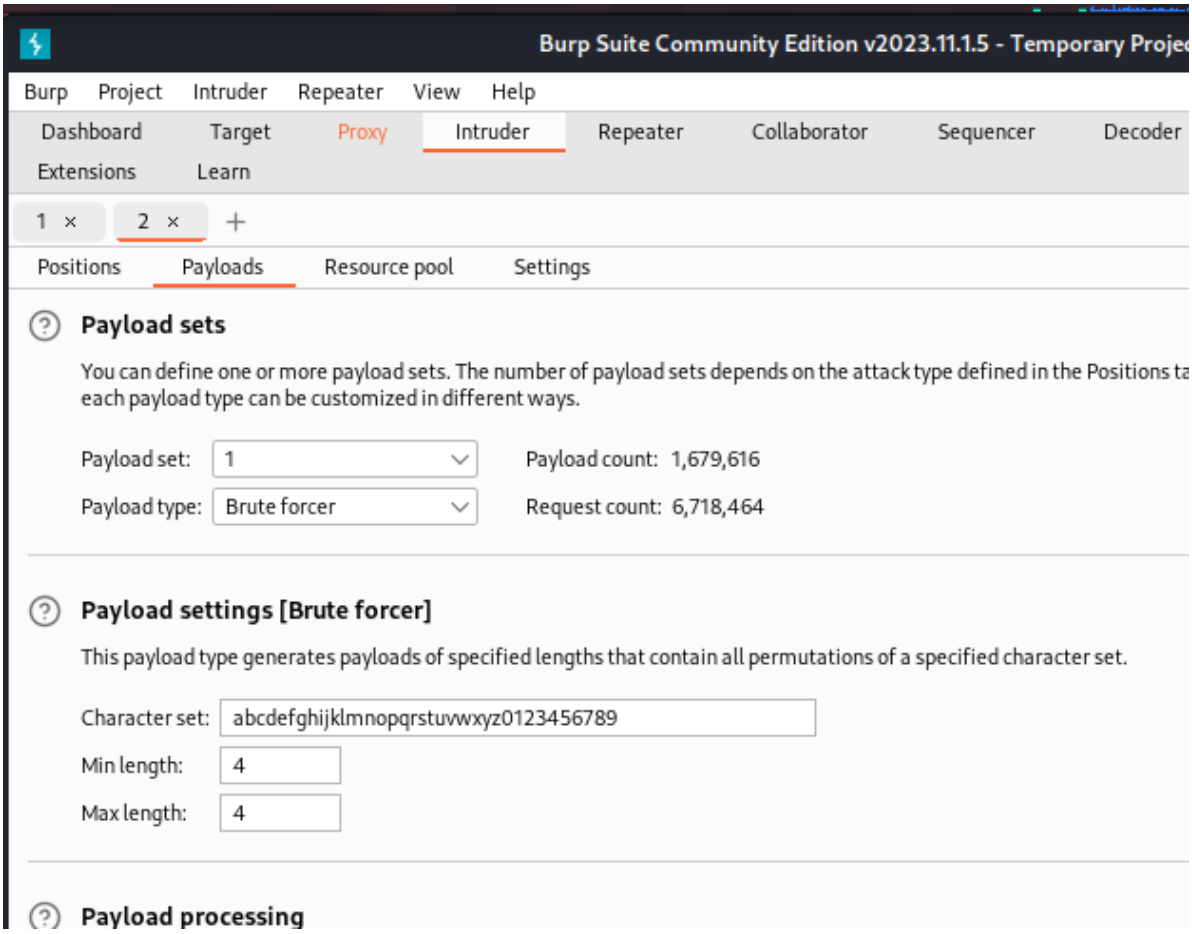

Figure 8: Setting Usernames list from brute forcer

4.9 Executing Attack

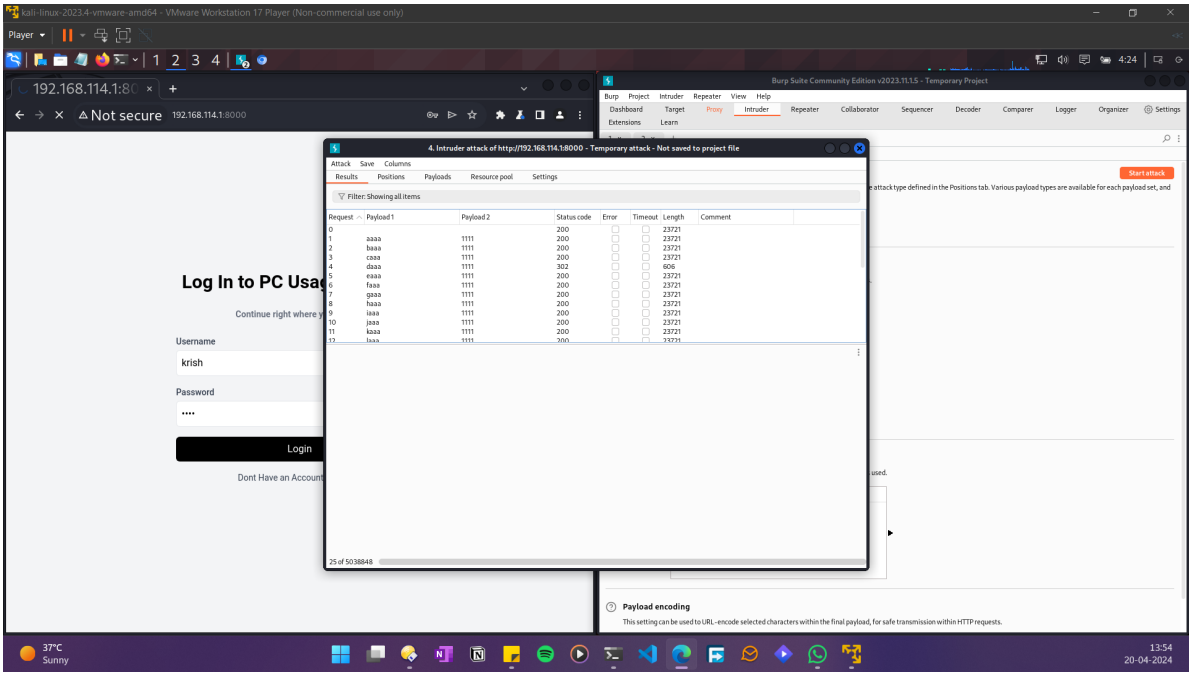

Figure 9: Executing Attack

4.10 Executing Attack, as seen on django server console logs

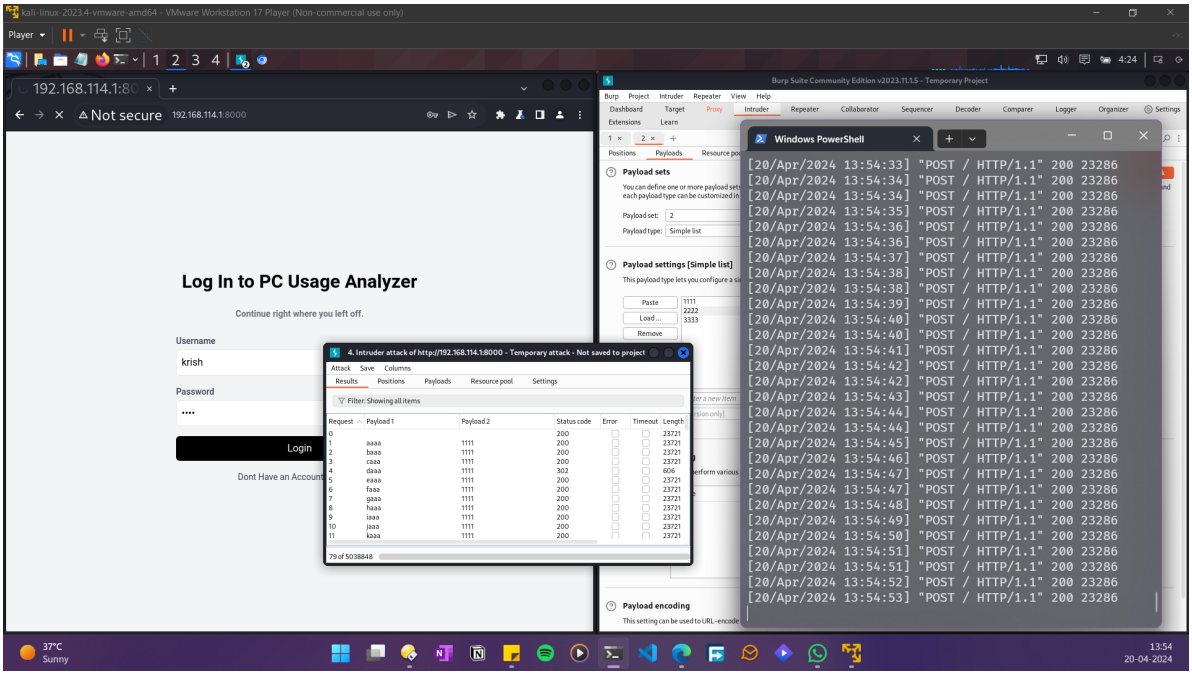

Figure 10: Executing Attack, as seen on django server console logs

4.11 Finding Correct password by noticing change in length

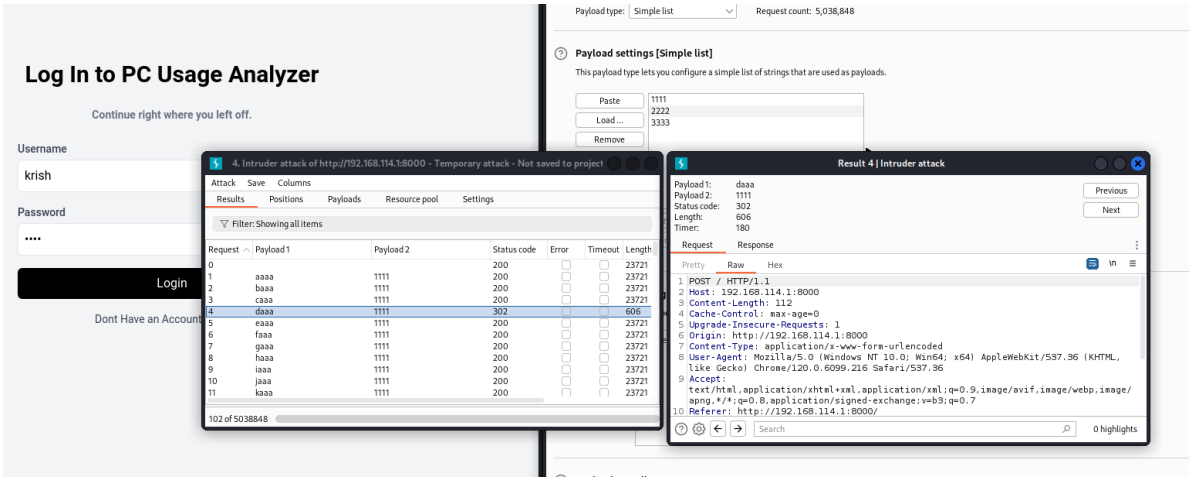

Figure 11: Finding Correct password by noticing change in length

4.12 Correct password found

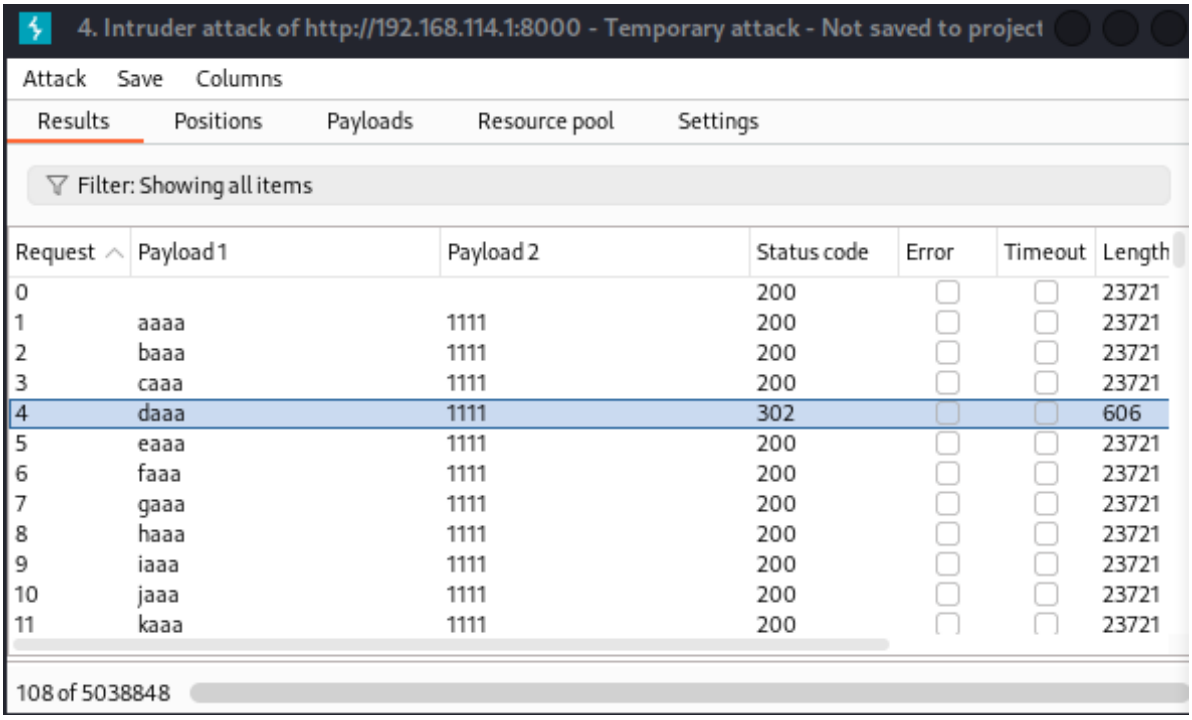

Figure 12: Correct password found

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.