

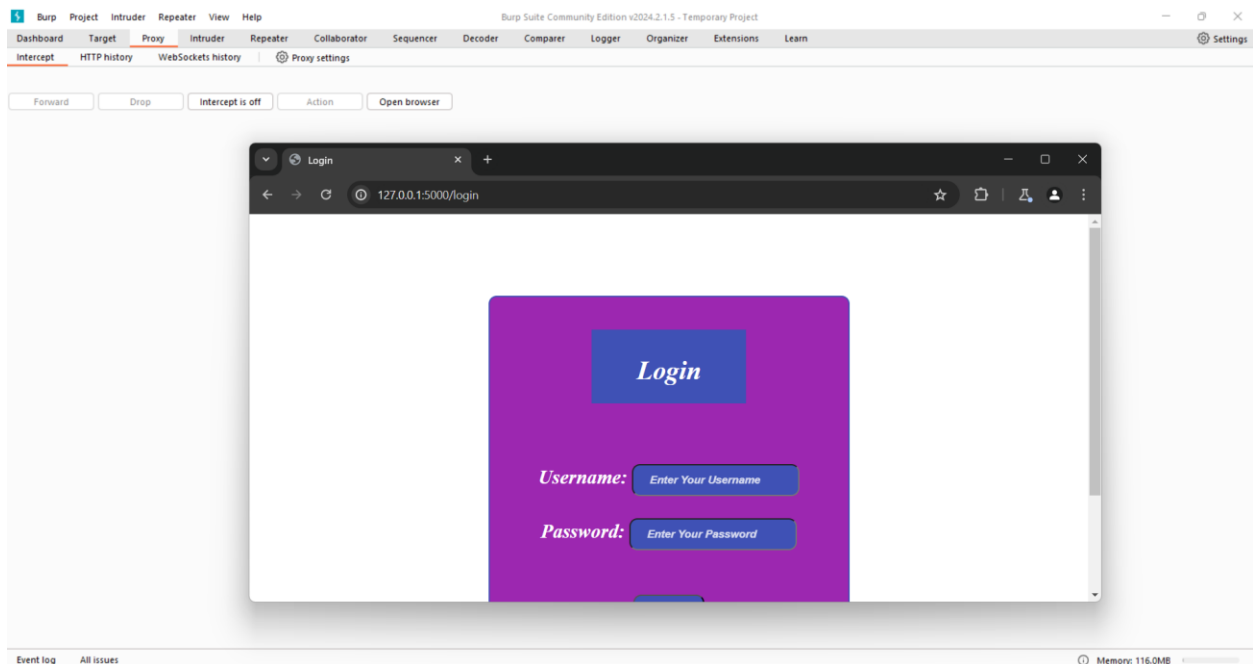
# Step-by-Step Guide: Using Burp Suite for Brute Forcing website

## Introduction

Brute forcing an HTTP website involves systematically attempting different combinations of usernames and passwords to gain unauthorized access. Burp Suite offers powerful tools to automate this process efficiently. This guide will walk you through the steps to set up and execute a brute force attack on an HTTP website using Burp Suite.

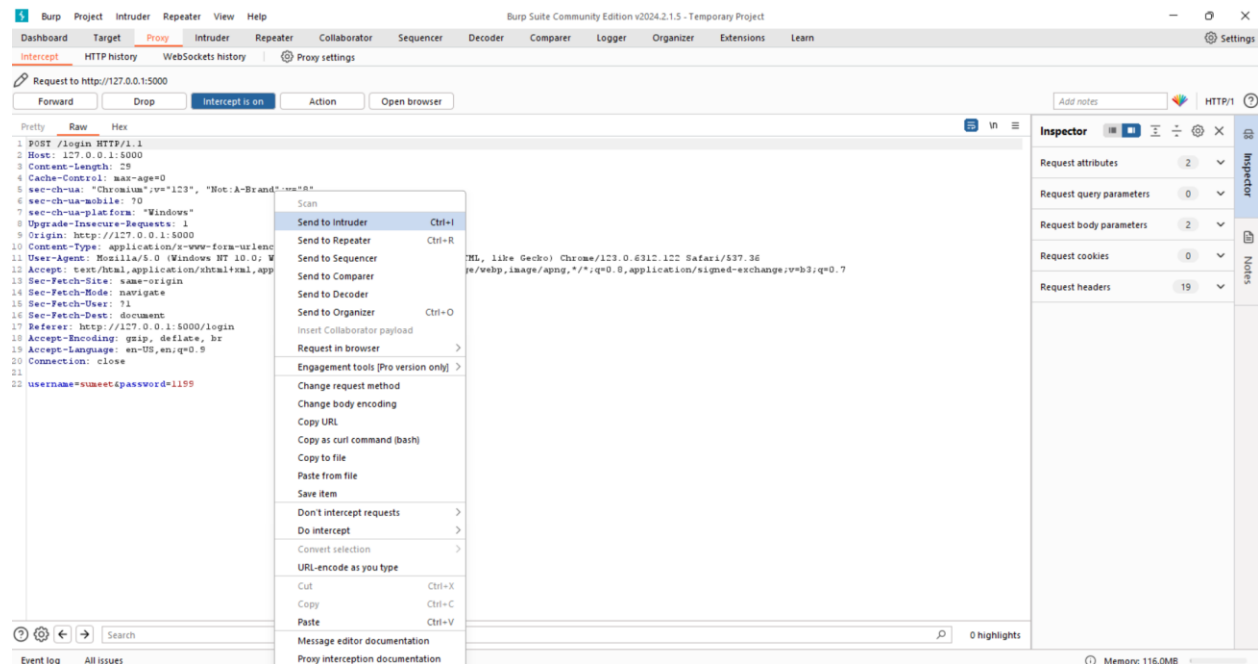
## Step 1: Configure Burp Suite

1. Launch Burp Suite on your system.
2. Go to the "Proxy" tab and ensure the "Intercept is on" button is toggled off.
3. Navigate to the "Intruder" tab, where you will perform the brute force attack.



## Step 2: Import Target

1. Open your web browser and navigate to the login page of the HTTP website.
2. Enter any invalid username and password combination and submit the form.
3. In Burp Suite, go to the "Proxy" tab and locate the intercepted login request.
4. Right-click on the request and select "Send to Intruder" to import it into the Intruder tool.



## Step 3: Configure Intruder

1. In the Intruder tab, go to the "Positions" sub-tab.
2. Identify the parameters corresponding to the username and password fields in the login request.
3. Highlight each parameter and click "Add S" to mark them as attack targets.
4. Go to the "Payloads" sub-tab.
5. Load your wordlist containing potential usernames and passwords as payloads.
6. Configure the payload positions for the username and password fields accordingly.

1 x2 x+

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

Settings

PositionsPayloadsResource poolSettings

Choose an attack type

Attack type: Cluster bomb

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1:5000

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

1 POST /login HTTP/1.1

2 Host: 127.0.0.1:5000

3 Content-Length: 29

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium";v="123", "Not:A-Brand";v="8"

6 sec-ch-ua-mobile: ?0

7 sec-ch-ua-platform: "Windows"

8 Upgrade-Insecure-Requests: 1

9 Origin: http://127.0.0.1:5000

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36

12 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

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: http://127.0.0.1:5000/login

18 Accept-Encoding: gzip, deflate, br

19 Accept-Language: en-US,en;q=0.9

20 Connection: close

21

22 username=\$username&password=\$password

Search

2 highlights

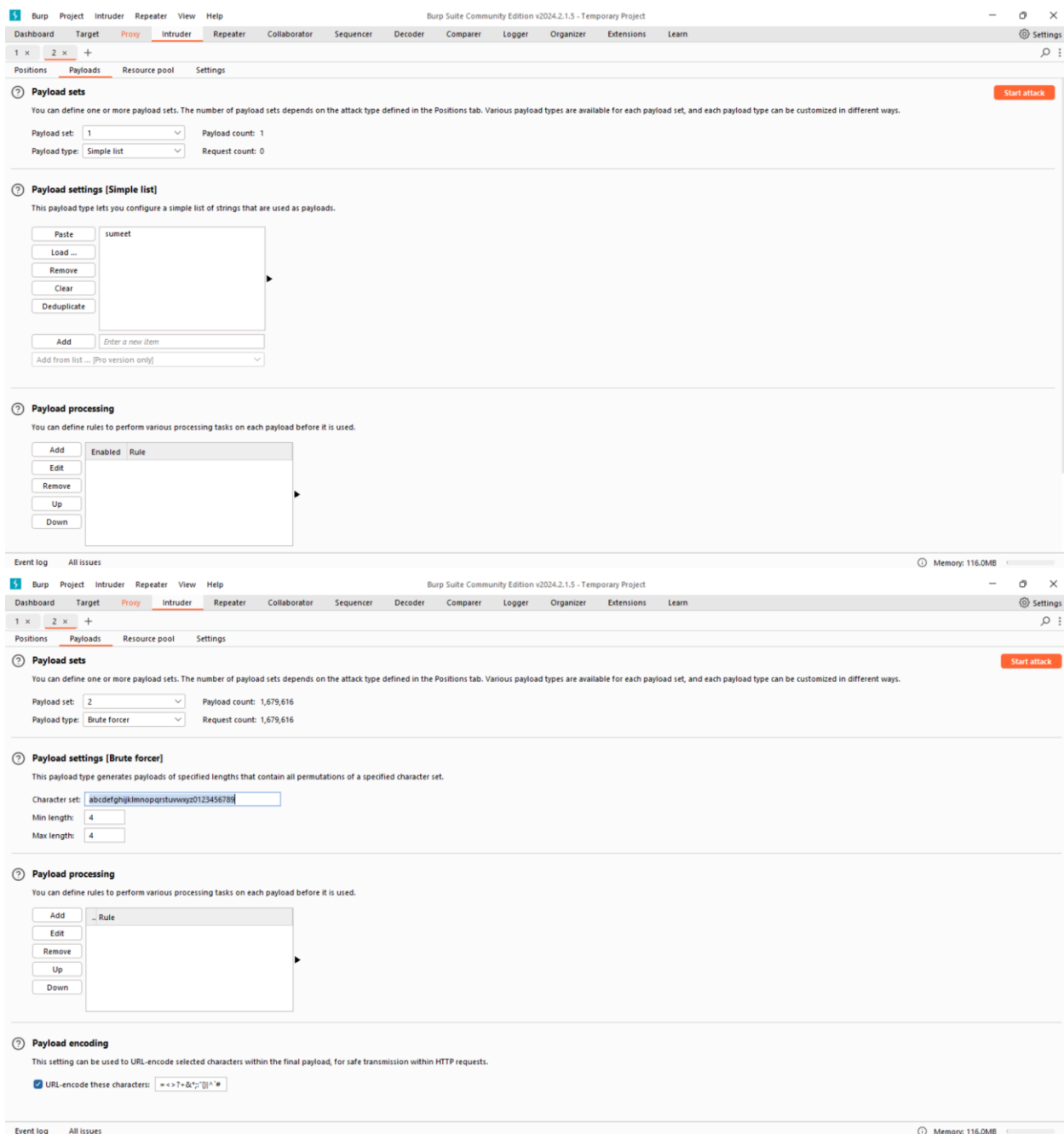
Clear

2 payload positions

Length: 842

Event logAll issues

Memory: 116.0MB



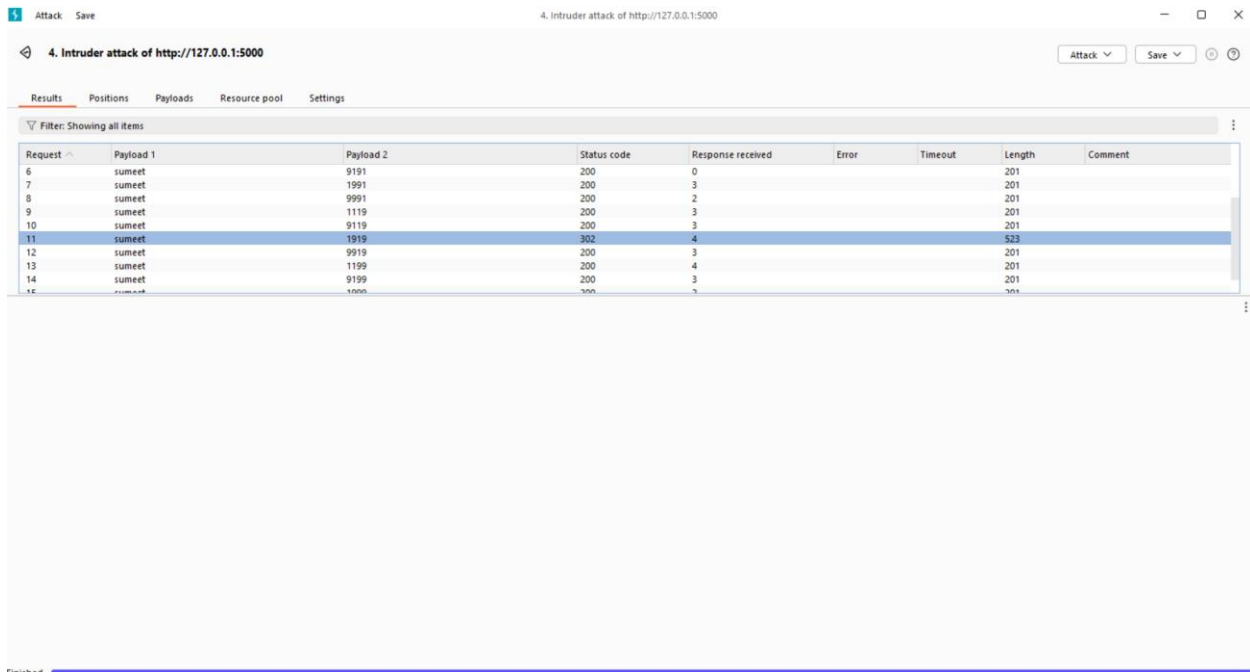
## Step 4: Start Brute Force Attack

1. Go to the "Options" sub-tab within the Intruder tool.
2. Configure the attack settings, such as the number of concurrent connections and timeout values.
3. Go back to the "Positions" sub-tab and ensure everything is set up correctly.

4. Click on the "Start attack" button to initiate the brute force attack.

## Step 5: Analyze Results

1. Monitor the progress of the brute force attack in the "Intruder" tab.
2. As valid username/password combinations are found, they will be highlighted in the "Results" sub-tab.
3. Review the results to identify successful login attempts and valid credentials.



Attack Save 4. Intruder attack of http://127.0.0.1:5000

4. Intruder attack of http://127.0.0.1:5000 Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload 1 | Payload 2 | Status code | Response received | Error | Timeout | Length | Comment |
|---------|-----------|-----------|-------------|-------------------|-------|---------|--------|---------|
| 6       | sumeet    | 9191      | 200         | 0                 |       |         | 201    |         |
| 7       | sumeet    | 1991      | 200         | 3                 |       |         | 201    |         |
| 8       | sumeet    | 9991      | 200         | 2                 |       |         | 201    |         |
| 9       | sumeet    | 1119      | 200         | 3                 |       |         | 201    |         |
| 10      | sumeet    | 9119      | 200         | 3                 |       |         | 201    |         |
| 11      | sumeet    | 1919      | 302         | 4                 |       |         | 523    |         |
| 12      | sumeet    | 9919      | 200         | 3                 |       |         | 201    |         |
| 13      | sumeet    | 1199      | 200         | 4                 |       |         | 201    |         |
| 14      | sumeet    | 9199      | 200         | 3                 |       |         | 201    |         |
| 15      | sumeet    | 1999      | 200         | 3                 |       |         | 201    |         |

Finished

## Step 6: Take Action

1. Once valid credentials are identified, you can use them to log in to the HTTP website.
2. Take appropriate actions based on the results of the brute force attack, such as securing accounts with stronger passwords or implementing additional security measures.

## Conclusion

By following this step-by-step guide, you can leverage Burp Suite to conduct brute force attacks on HTTP websites efficiently. However, it's essential to use this knowledge responsibly and ethically, ensuring that you have proper authorization before attempting any security testing.