# Burp Suite: Brute Force Attack

## Exp. No.: 2

**Aim:** To use Burp Suite to conduct brute force attack. **Apparatus Required:** Burp Suite, Foxy Proxy **Theory & Commands involved:**

## Brute Force:

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page.

It plays a vital role in web penetration testing because is the simplest method to gain access to a site or server by checking the correct username or password by calculating every possible combination that could generate a username or password.

## Brute Force in Burp Suite using Intruder:

Burp Suite is a set of tools used for penetration testing of web applications.

Burp Intruder is a tool for automating customized attacks against web applications.

The intruder is used for Brute-force attacks on password forms, pin forms, and other such forms.

Burp Intruder supports various attack types - these determine the way in which payloads are assigned to payload positions.

## Attack Types:

* 1. **Sniper**
     + This uses a single set of payloads. It targets each payload position in turn, and places each payload into that position in turn.
     + This attack type is useful for fuzzing a number of request parameters individually for common vulnerabilities.
     + The total number of requests generated in the attack is the product of the number of positions and the number of payloads in the payload set.

## Battering ram

* + - This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.
    - This attack type is useful where an attack requires the same input to be inserted in multiple places within the request (e.g., a username within a Cookie and a body parameter).
    - The total number of requests generated in the attack is the number of payloads in the payload set.

## Pitchfork

* + - This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, and places one payload into each defined position.
    - This attack type is useful where an attack requires different but related input to be inserted in multiple places within the request (e.g., a username in one parameter, and a known ID number corresponding to that username in another parameter).
    - The total number of requests generated in the attack is the number of payloads in the smallest payload set.

## Cluster bomb

* + - This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.
    - This attack type is useful where an attack requires different and unrelated or unknown input to be inserted in multiple places within the request (e.g., when guessing credentials, a username in one parameter, and a password in another parameter).
    - The total number of requests generated in the attack is the product of the number of payloads in all defined payload sets - this may be extremely large.

## Procedure:

**Exercise 1: Create a simple login website and perform the 4 different attacks. Login Website:**

A simple website is created in Flask or any technology (sample website screenshot is included in the following steps).

The directory contains

-- app.py

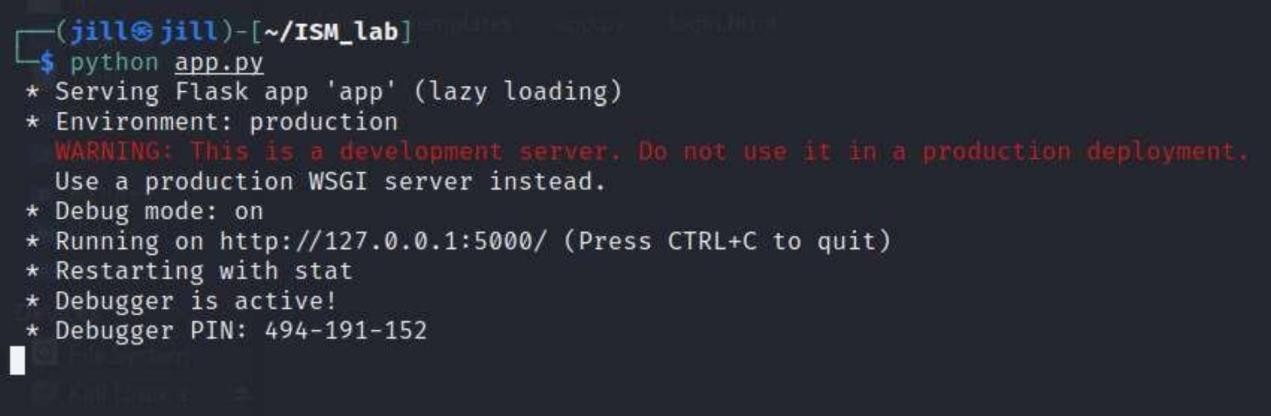
-- templates

-- login.html

-- home.html

To run the web application, execute the below command in the terminal.

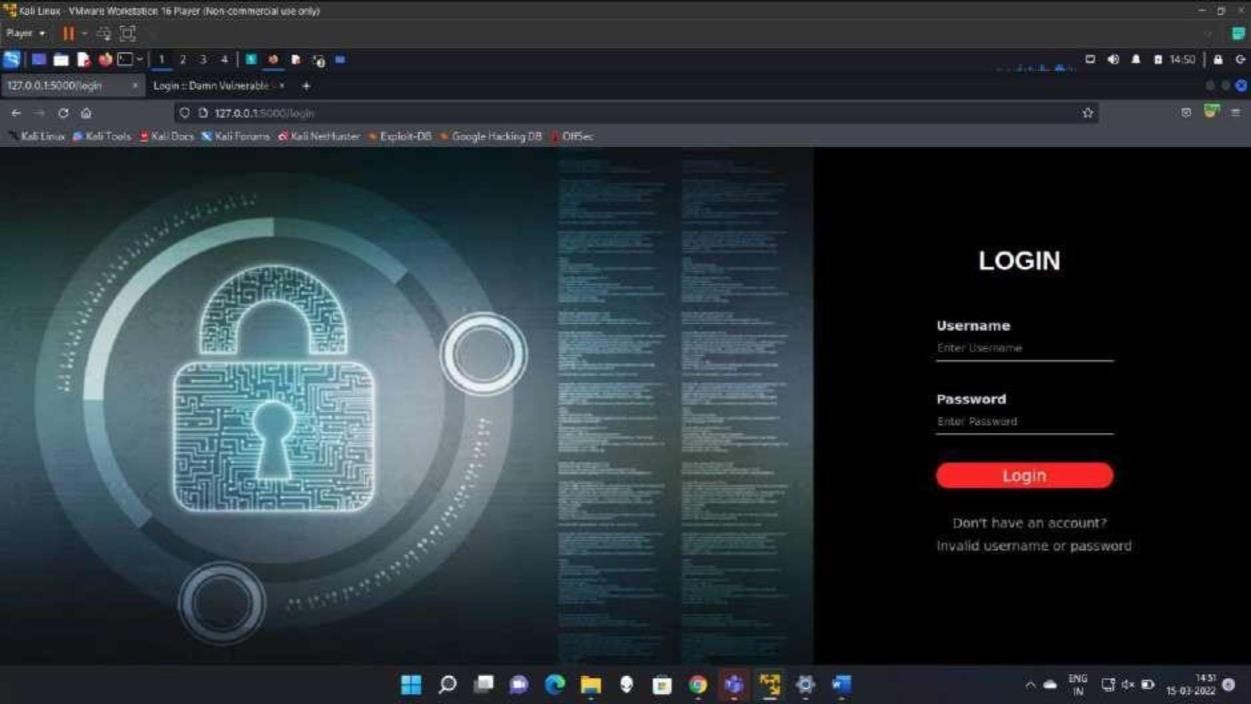
## python app.py



The website is running on the localhost.

Go to the browser and open http://127.0.0.1:5000/login.

The below page is displayed.



## Brute forcing using Intruder:

In the login page, enter any random username and password, and send the request to Burp Suite.

In the proxy section, right click the request and send it to intruder.

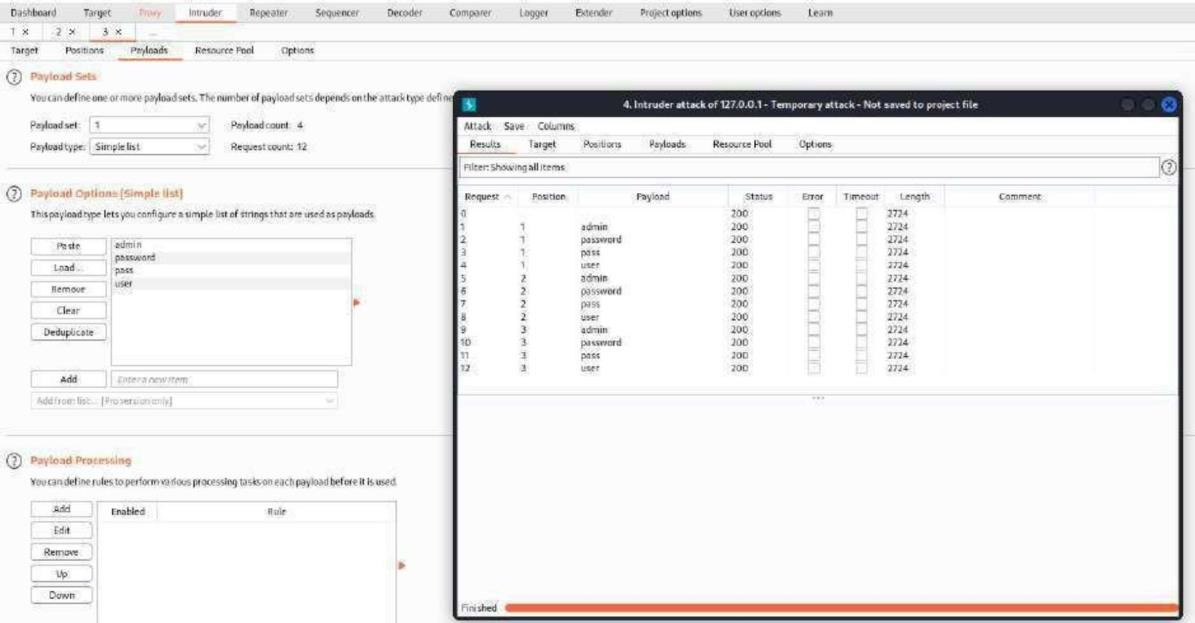


Add the payload positions only to username and passwd, and remove the payload for Cookie.

Choose different attack types as per need. The results of the same is shown next.

## Snipper Attack:

|  |  |
| --- | --- |
| **Payload set** | 1 |
| **Payload type** | Simple list |
| **Payload options** | admin password pass  user |

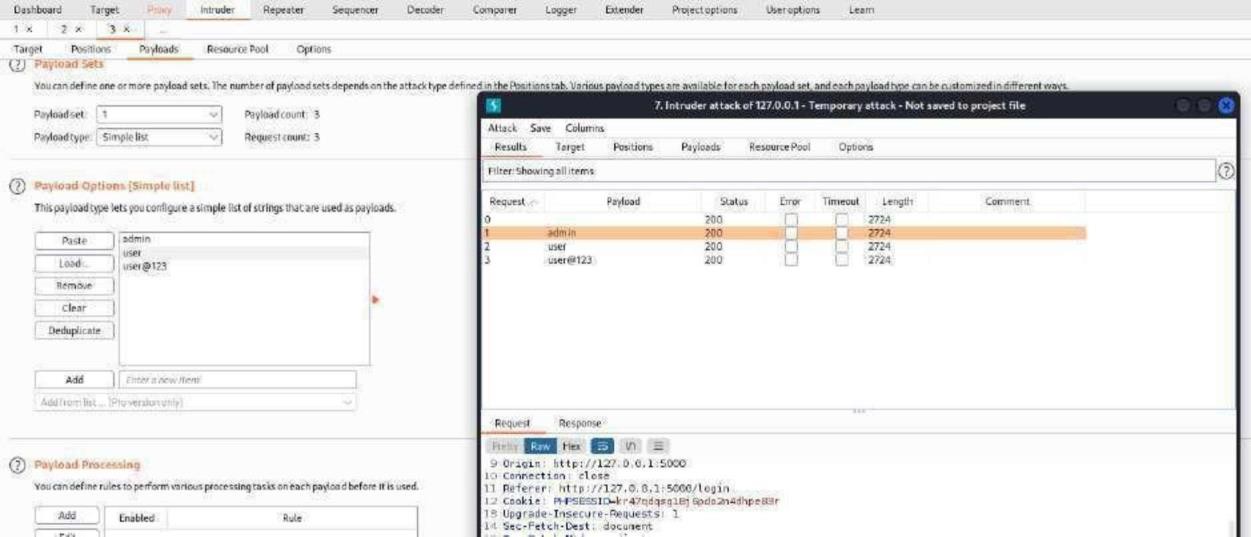


The length of all the response is the same. Hence the username and password were not found using this attack.

## Battering Ram:

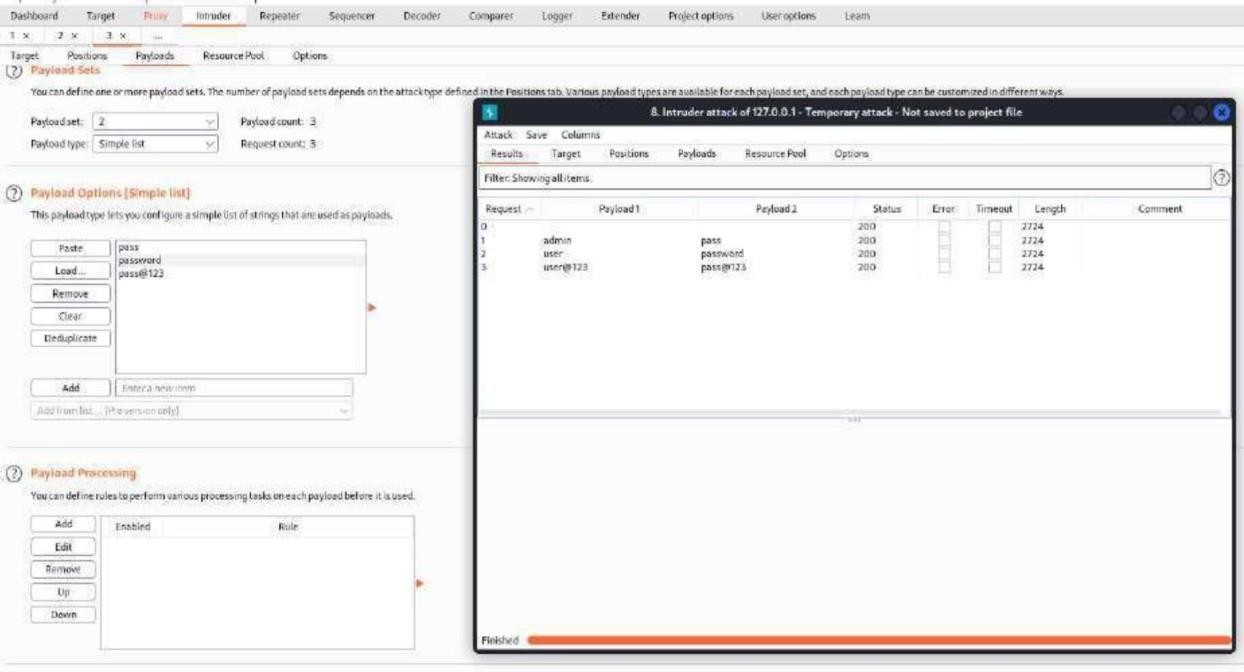
|  |  |
| --- | --- |
| **Payload set** | 1 |
| **Payload type** | Simple list |
| **Payload options** | admin  user user@123 |

The length of all the response is the same. Hence the username and password were not found using this attack.



## Pitchfork:

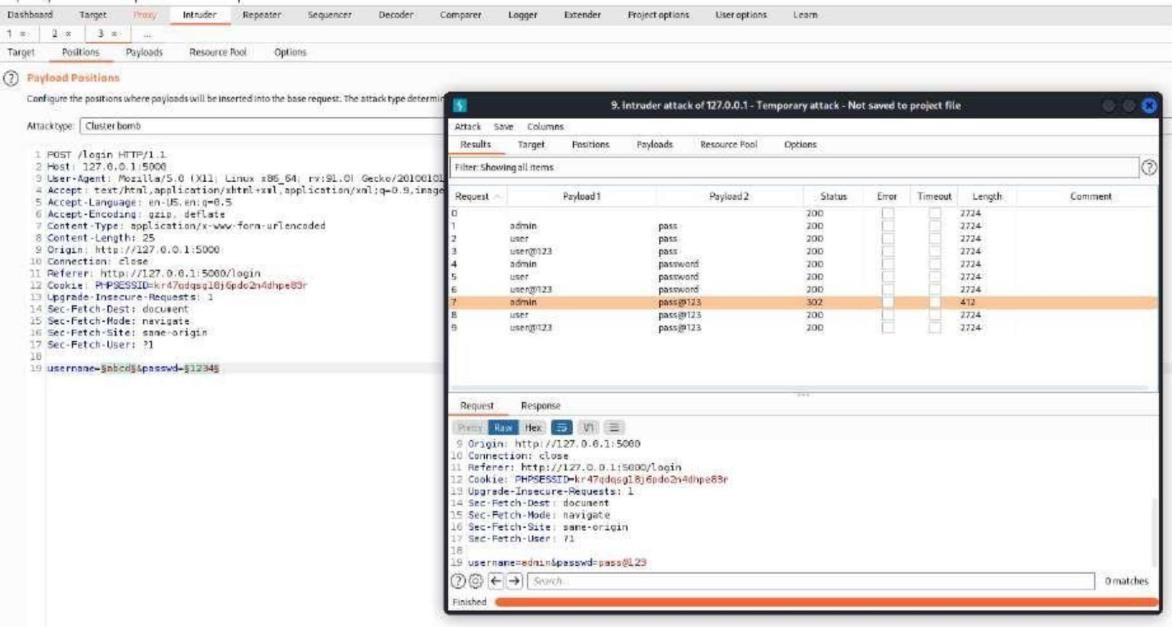
|  |  |  |
| --- | --- | --- |
| **Payload set** | 1 | 2 |
| **Payload type** | Simple list | Simple list |
| **Payload options** | admin  user user@123 | pass  password pass@123 |



The length of all the response is the same. Hence the username and password were not found using this attack.

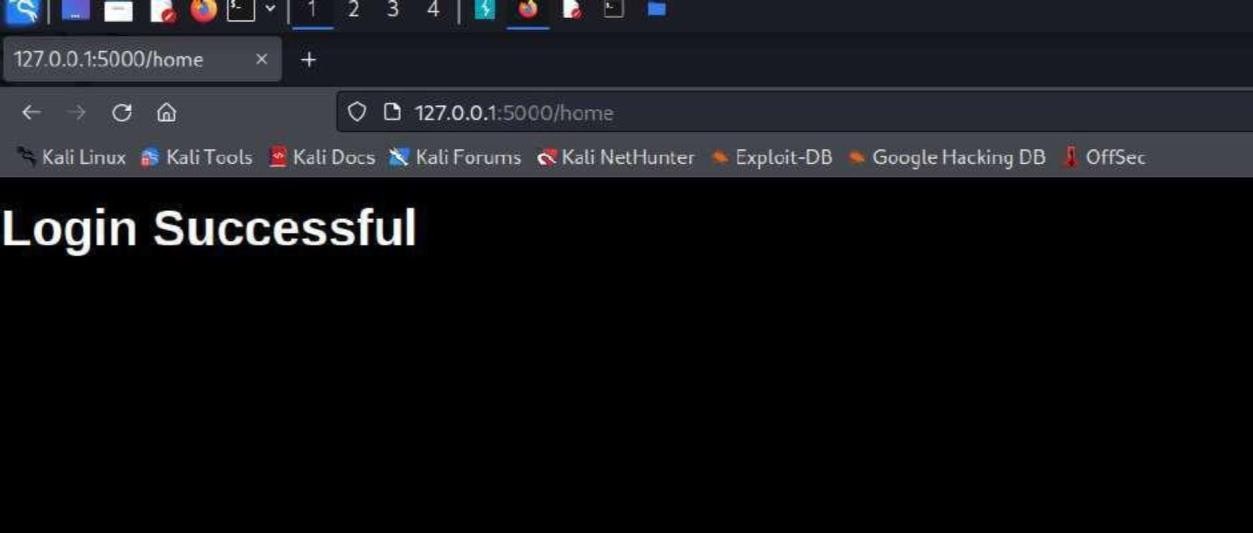
## Cluster bomb:

|  |  |  |
| --- | --- | --- |
| **Payload set** | 1 | 2 |
| **Payload type** | Simple list | Simple list |
| **Payload options** | admin  user user@123 | pass  password pass@123 |



The request-7 whose username and password were **admin** and **pass@123** respectively has the response length different that the other.

Trying this combination in the website, gives the below result:



## Conclusion:

Hence the username and password of the website was found using brute force attack.