ATTACK DEFENSE

by PentesterAcademy

Name	Attacking HTTP Login Form with Burp Suite
URL	https://attackdefense.com/challengedetails?cid=1898
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

In this lab exercise, we will take a look at how to use Burp Suite to attack HTTP Login forms.

Objective: Perform Dictionary Attack on the bWAPP login page.

Solution:

Step 1: Finding the IP address.

Command: ip addr

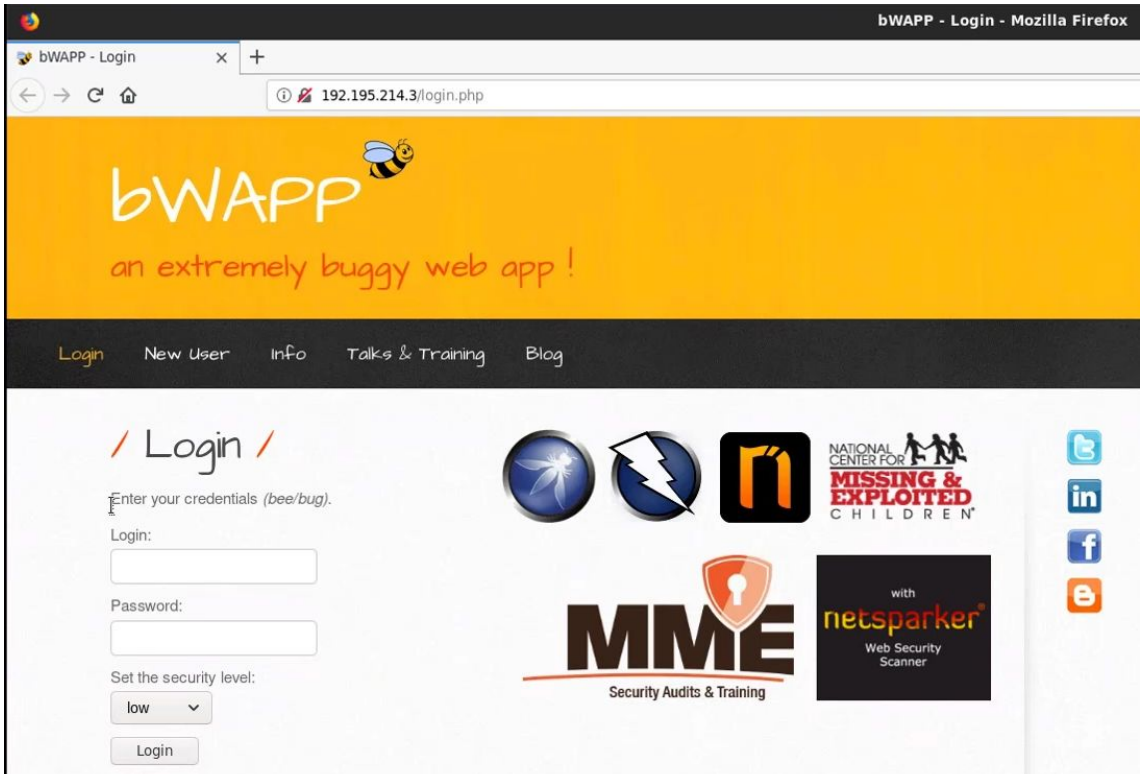
```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
25090: eth0@if25091: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
25093: eth1@if25094: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:c3:d6:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.195.214.2/24 brd 192.195.214.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run a nmap scan against the target IP.

Command: nmap 192.195.214.3

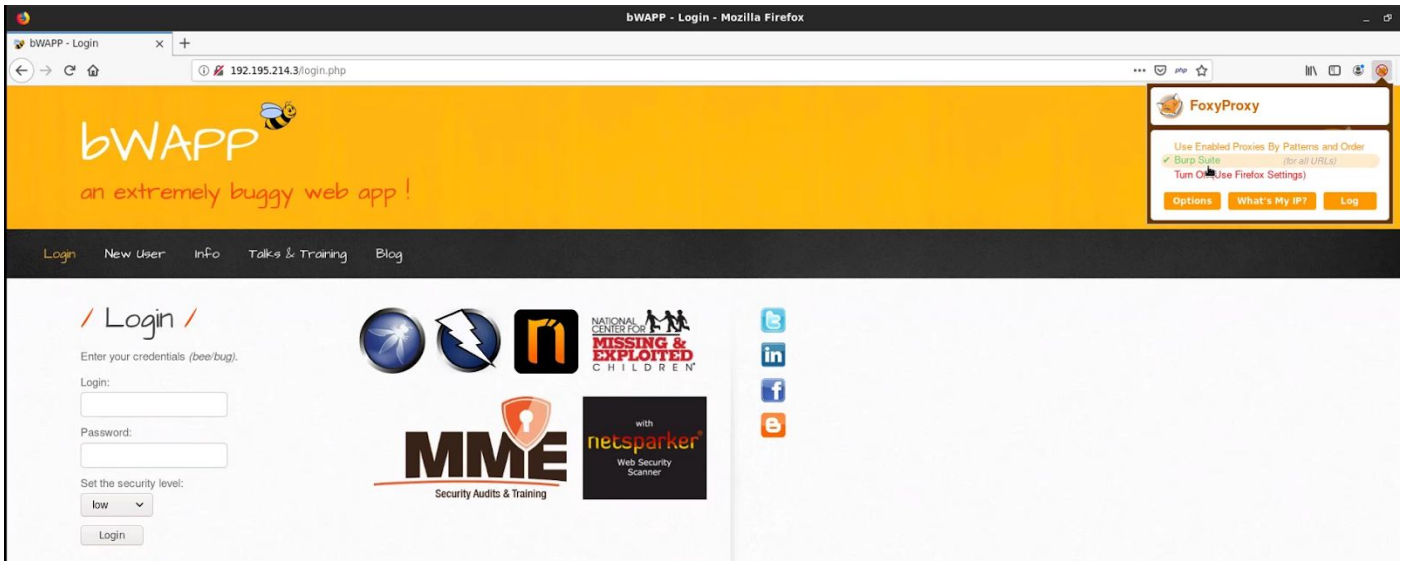
```
root@attackdefense:~# nmap 192.195.214.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-21 04:50 IST
Nmap scan report for target-1 (192.195.214.3)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:C3:D6:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

Step 3: Open the target webportal in the browser.



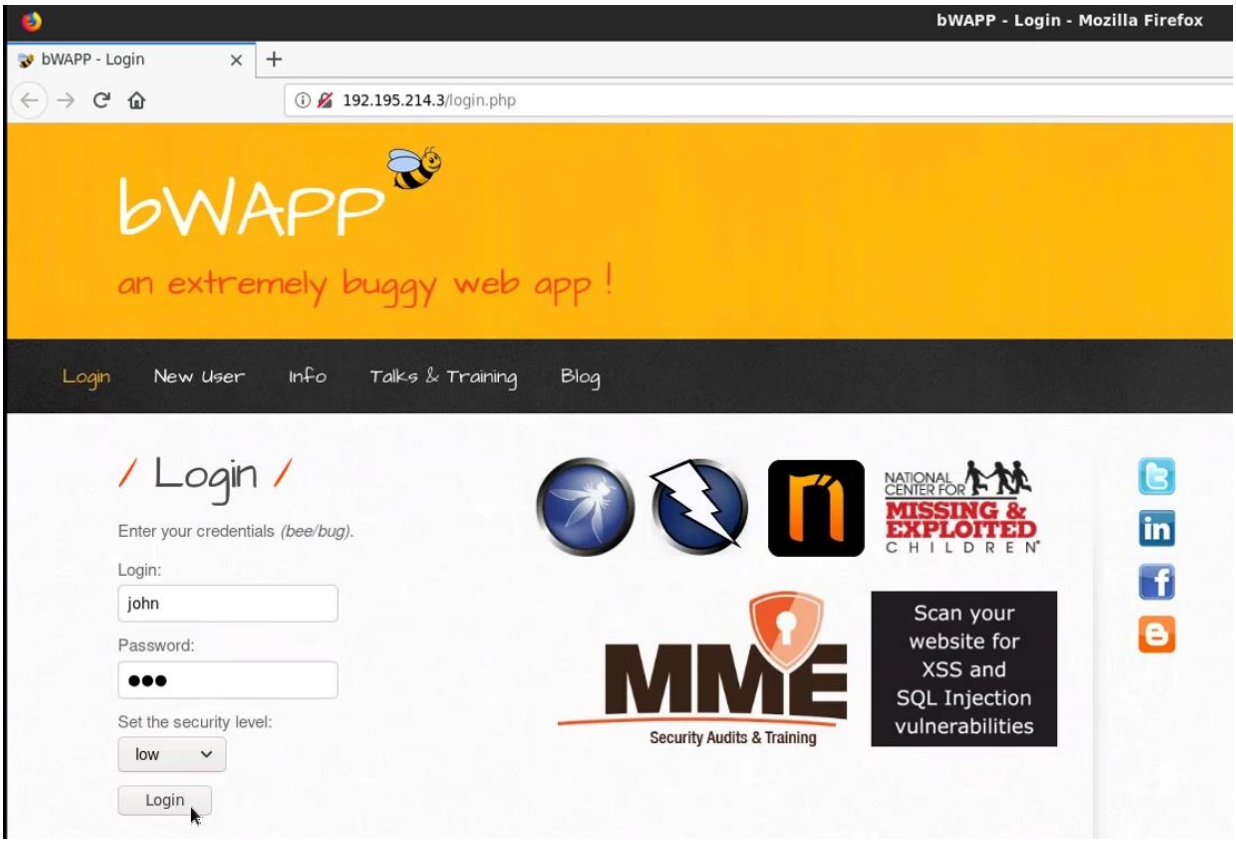
The bWAPP web application is running on the target machine.

Step 4: Select burp proxy from the “Foxyproxy” options.

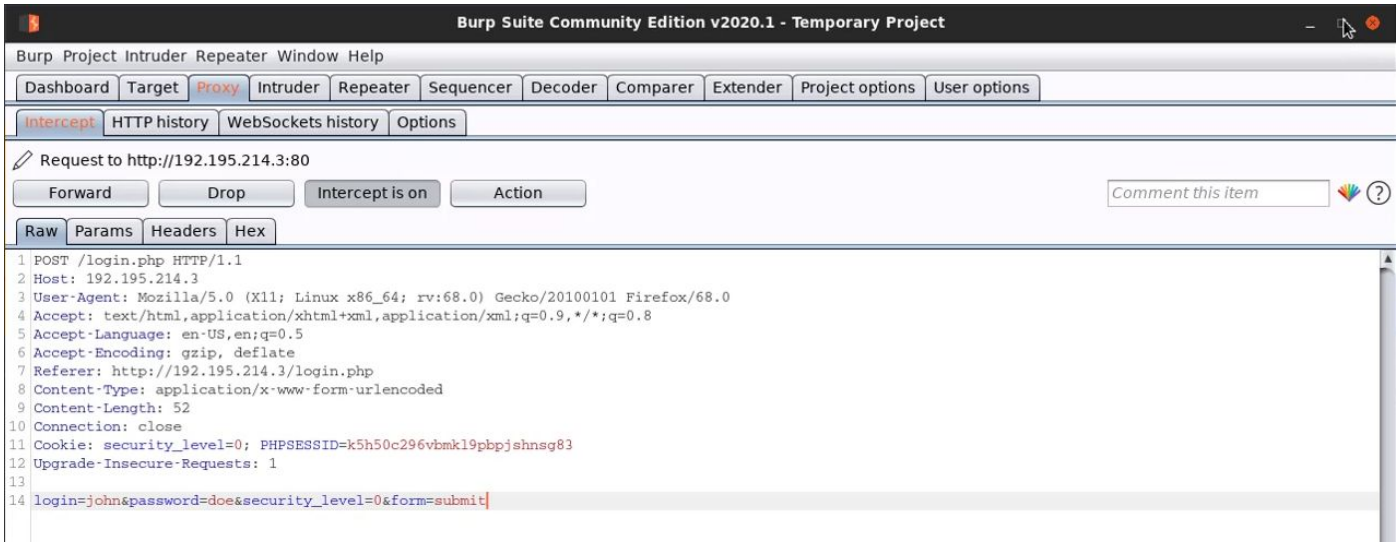


Step 5: Start Burp Suite in interception mode.

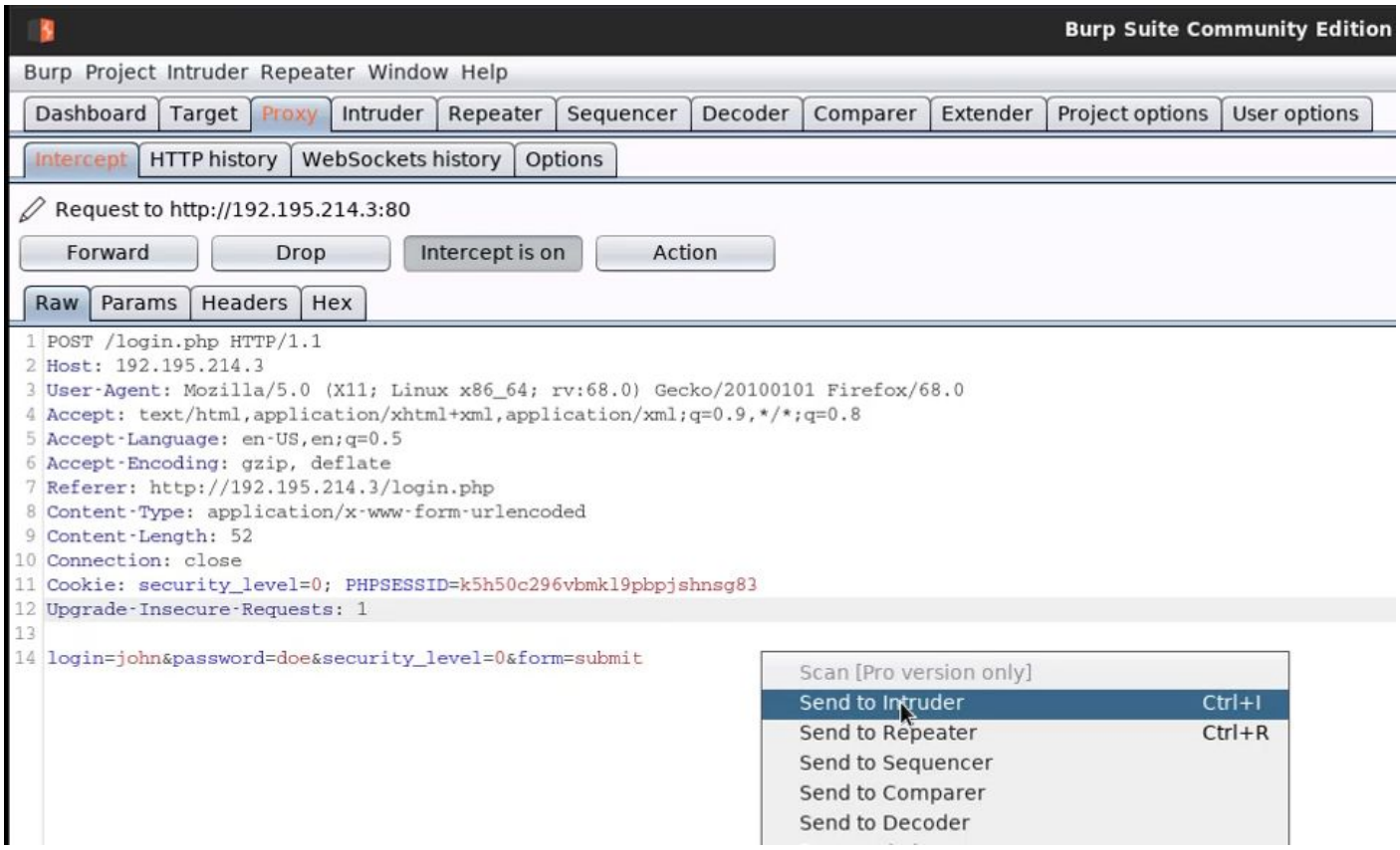
Step 6: Enter dummy credentials in the login page and press ‘login’.



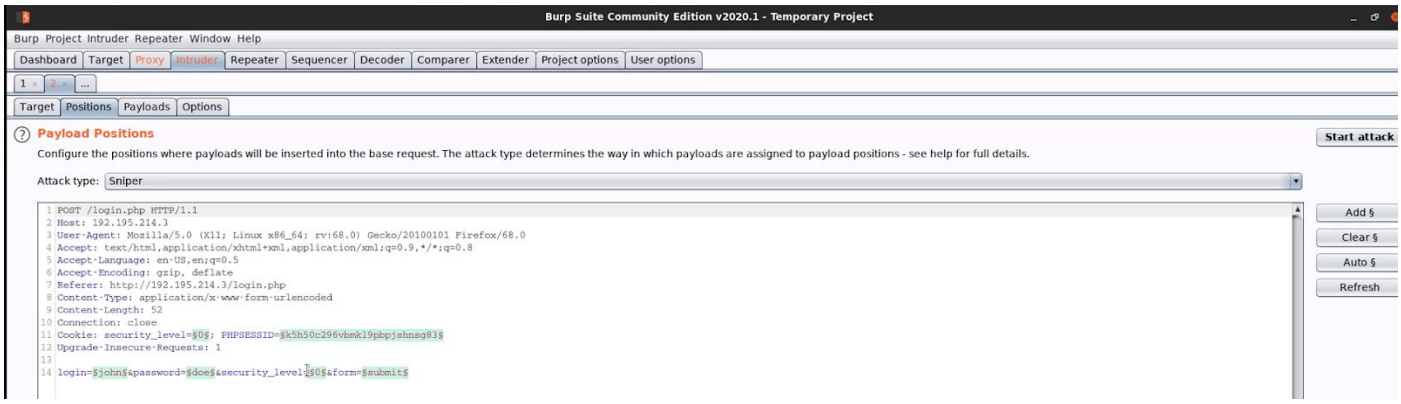
Step 7: Burp suite will intercept the POST request.



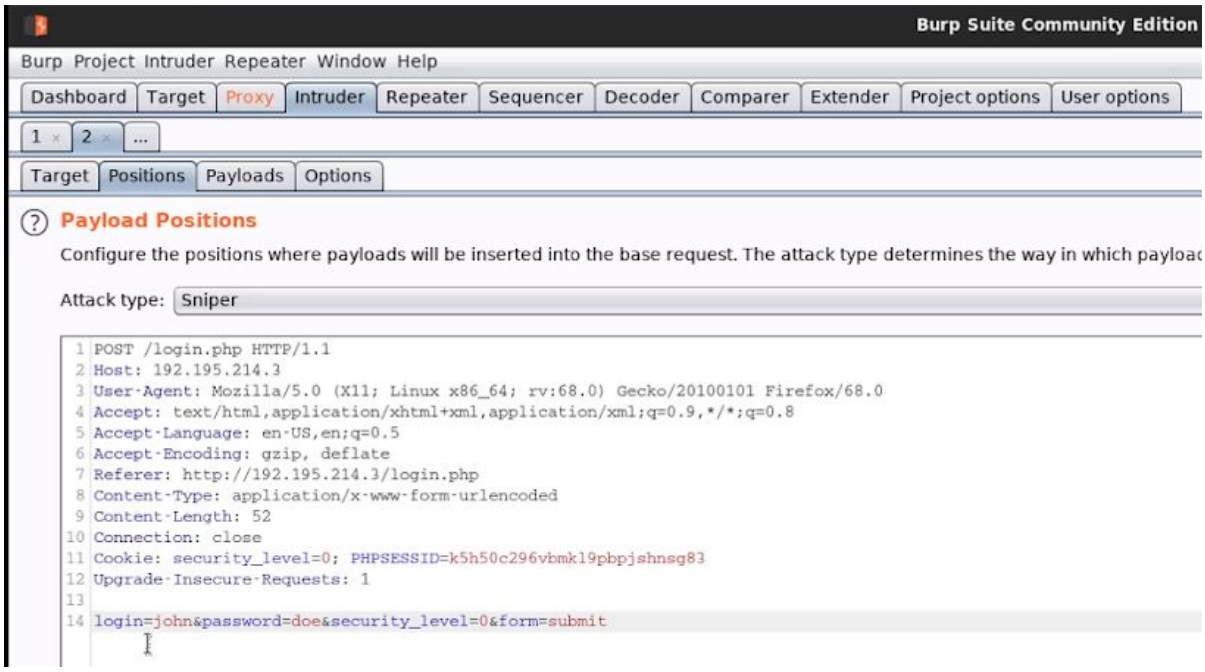
Step 8: Send the captured request to intruder (i.e. Burp Suite intruder module) .



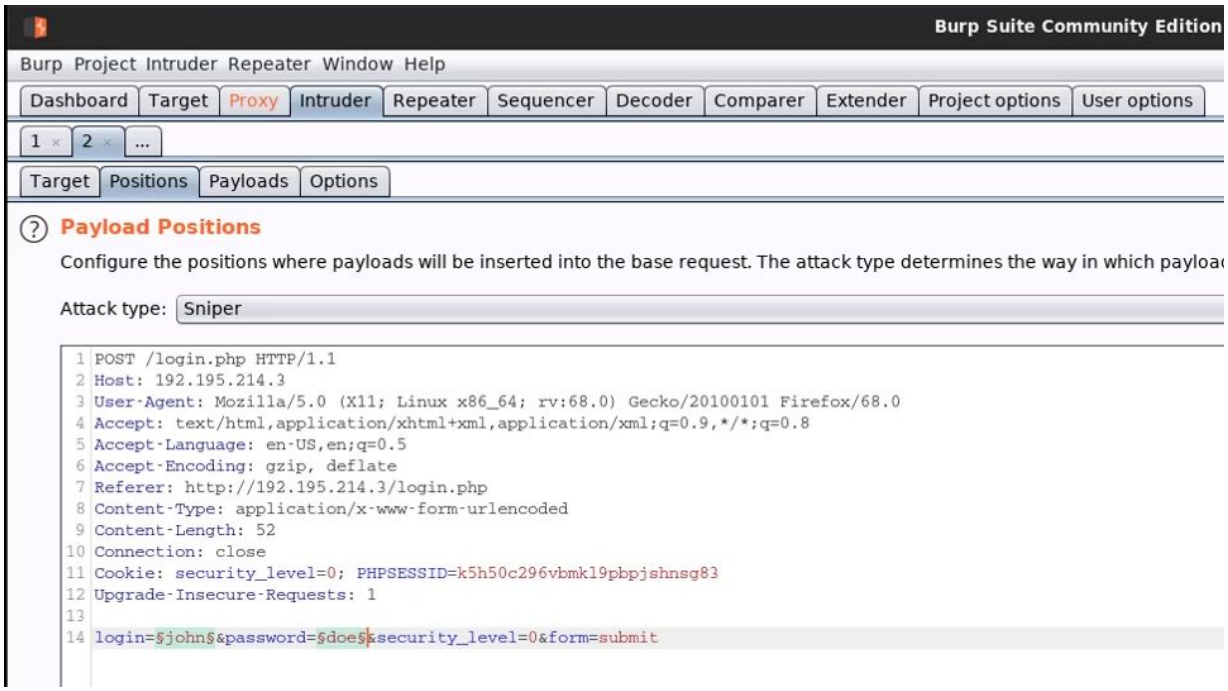
Step 9: Burp suite automatically marks all the payload positions.



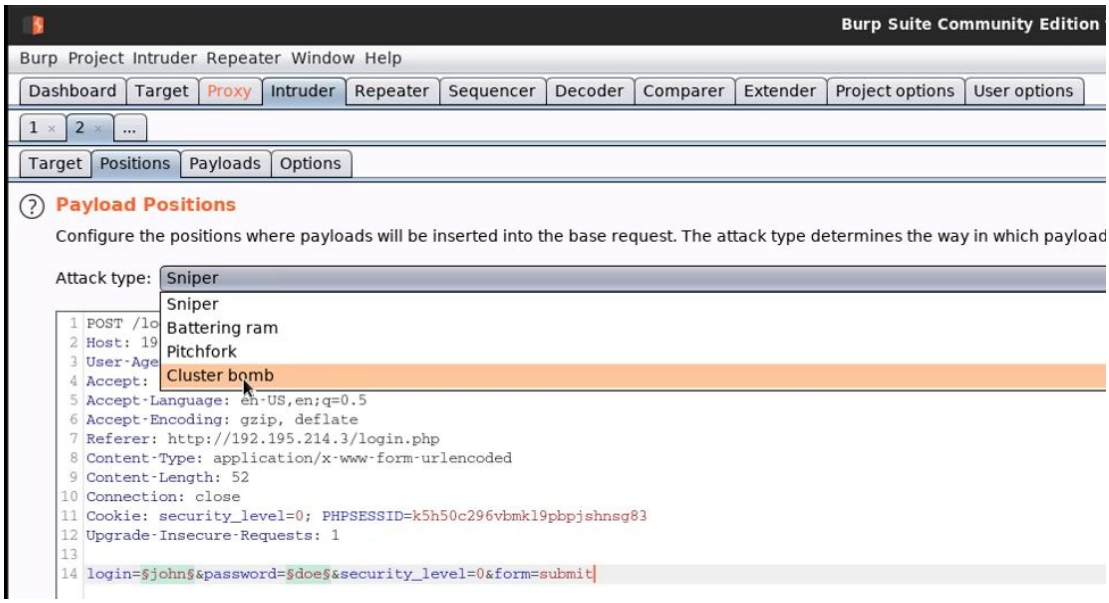
Step 10: Clear all payload positions by clicking on ‘clear’ button.



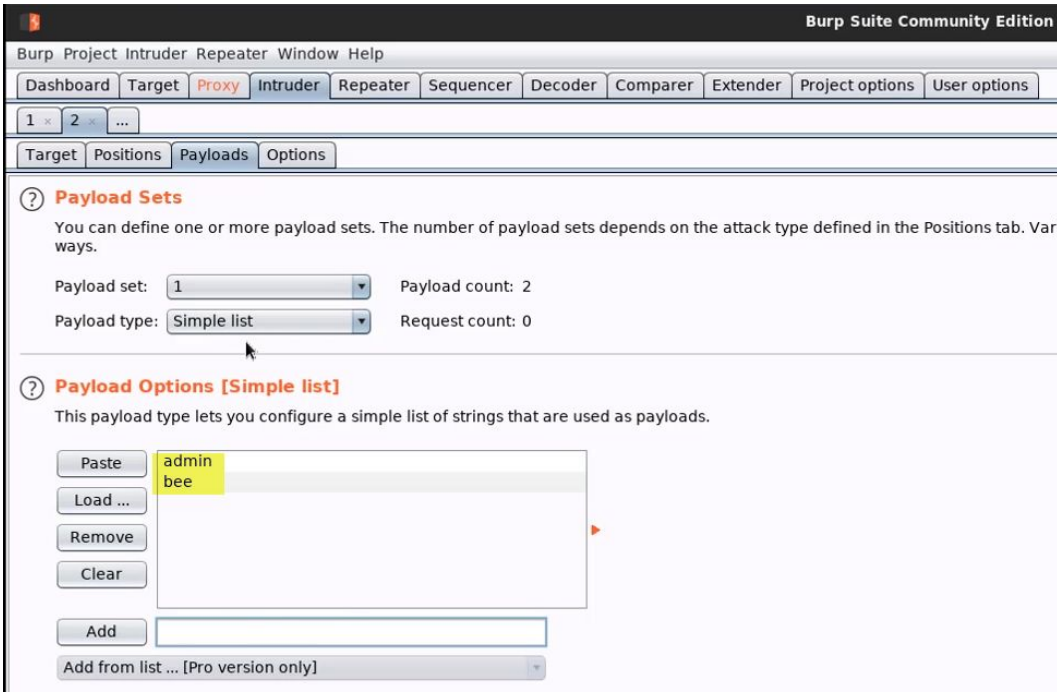
Step 11: Now, mark values of login and password as payload positions.



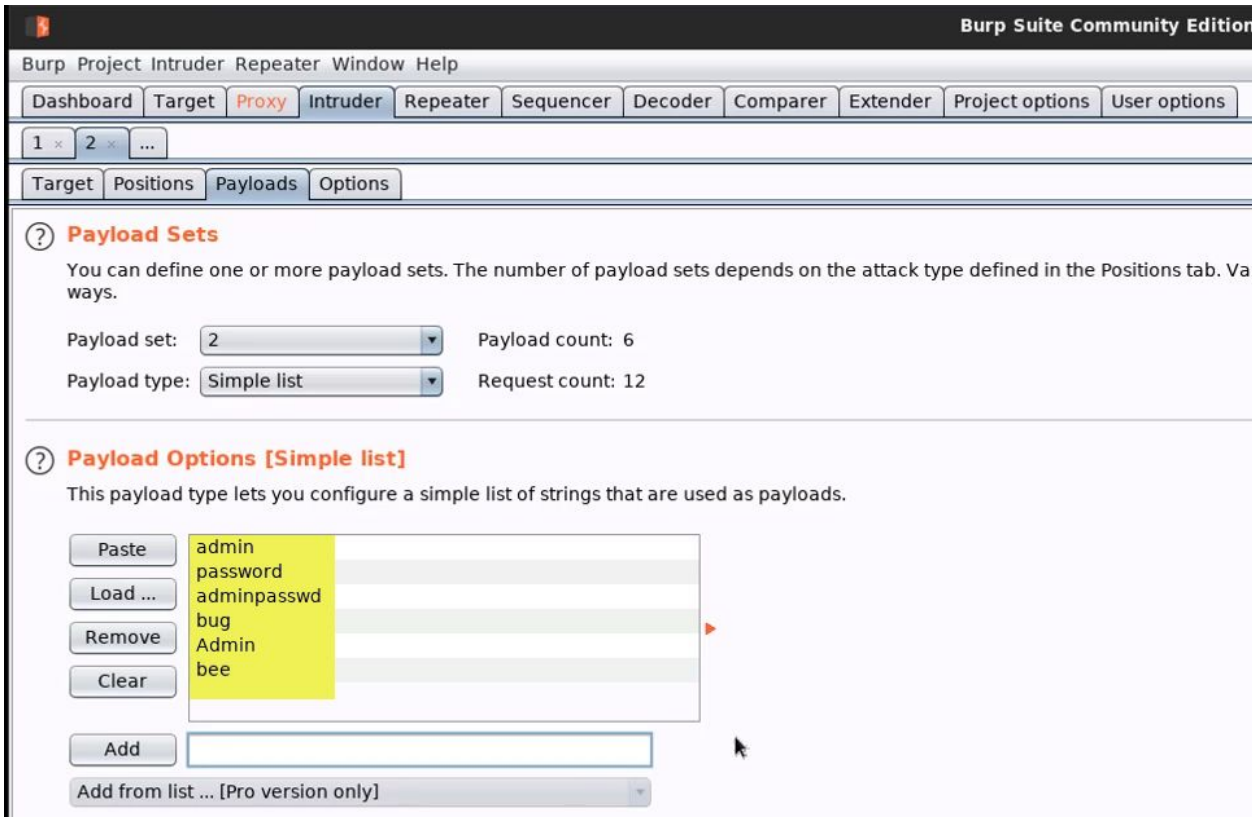
Step 12: Select “cluster bomb” feature.



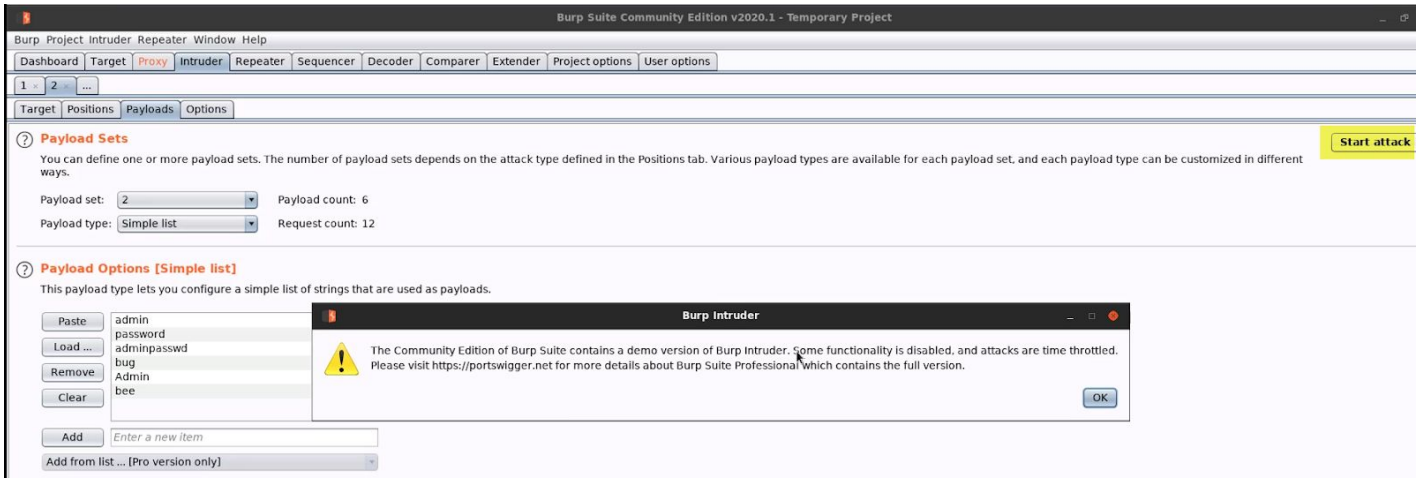
Step 13: Add first list for usernames.



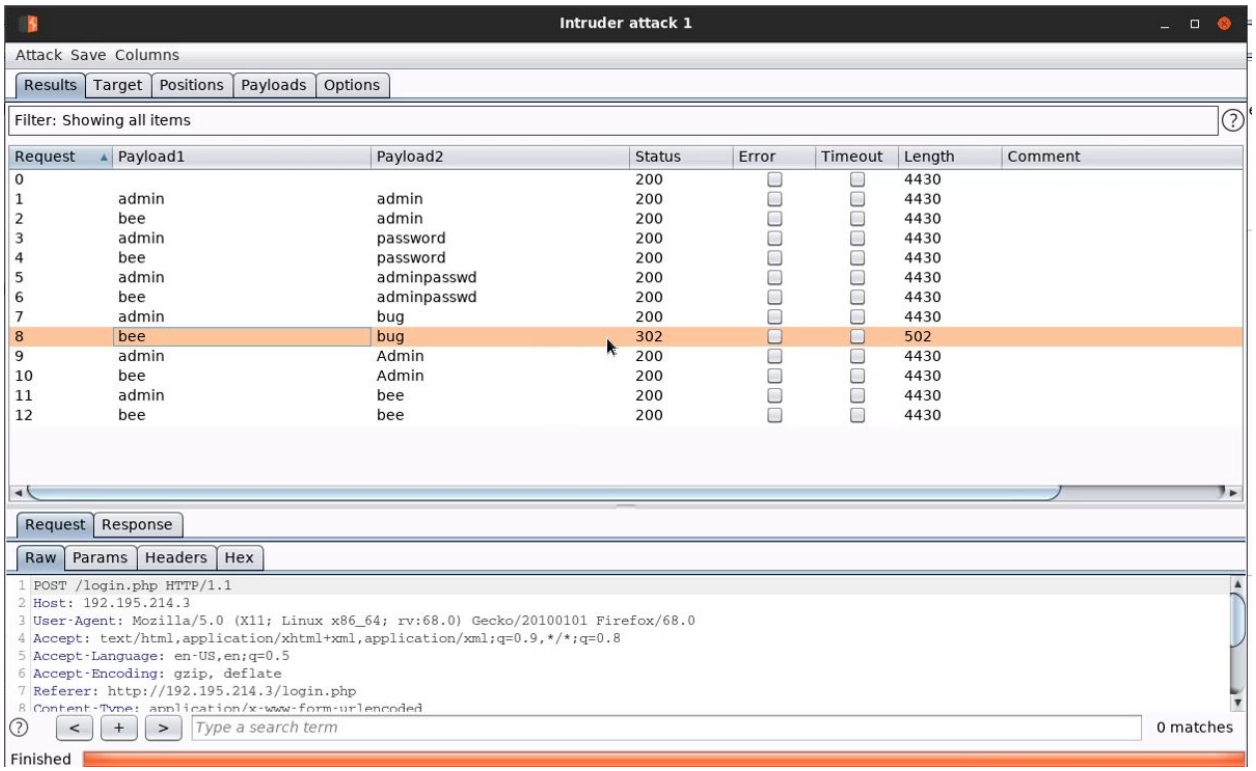
Step 14: Add second list for passwords.



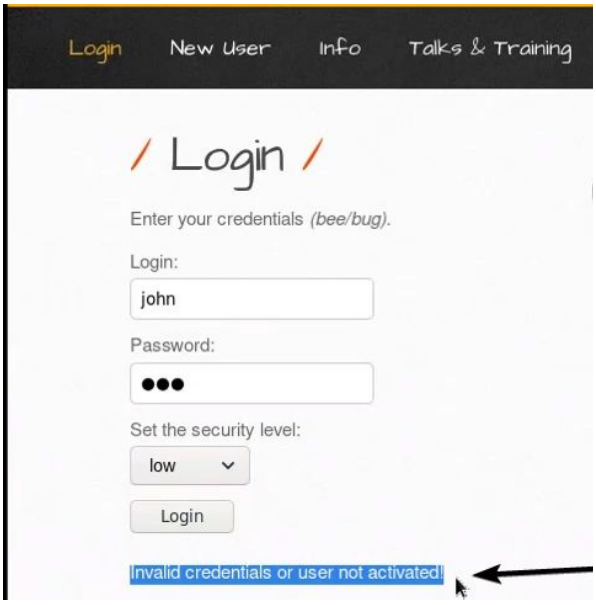
Step 15: Start the attack by clicking “Start Attack” button and pressing “OK” the pop-up.



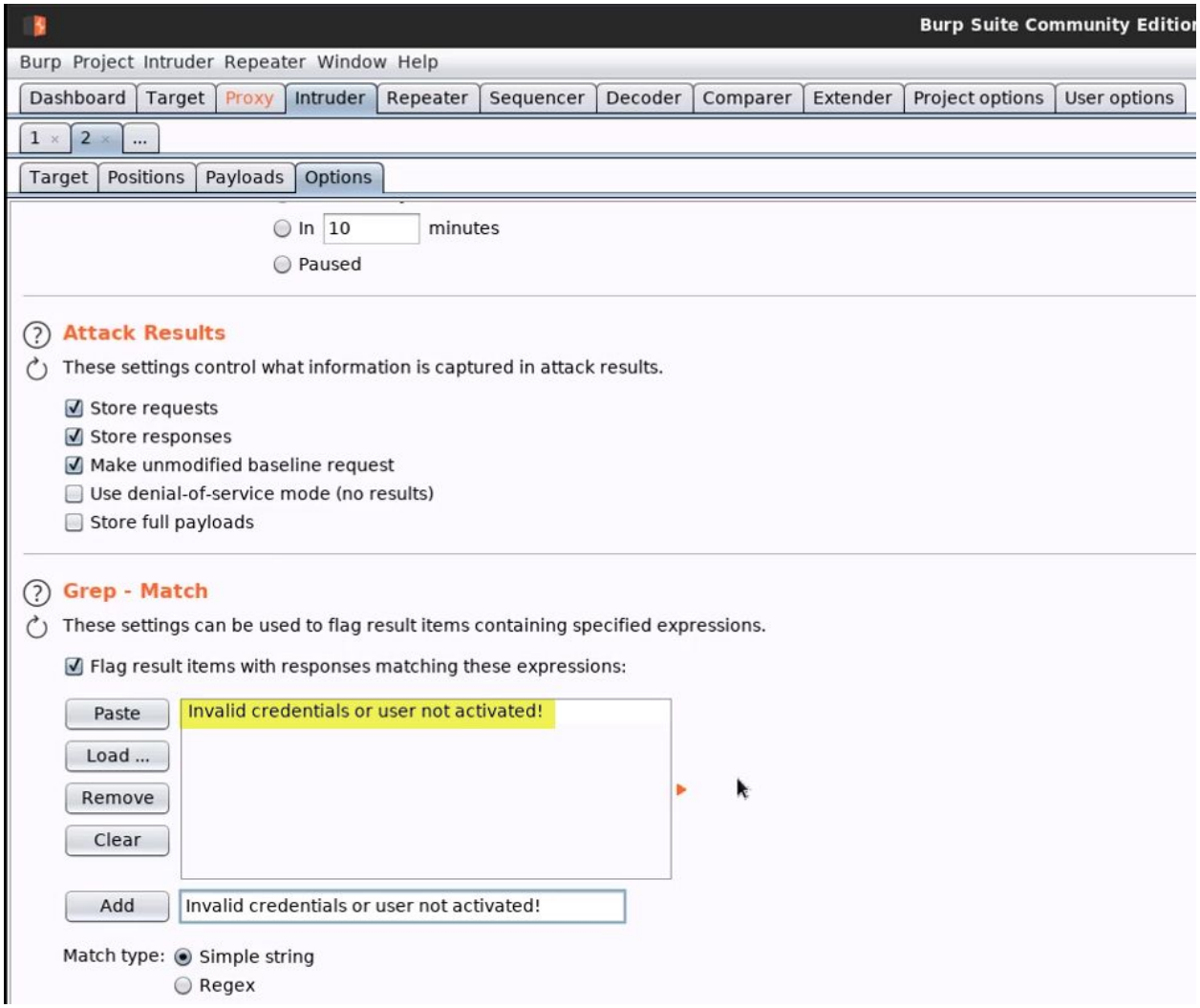
Step 16: The response with username “bee” and password “bug” returned 302.



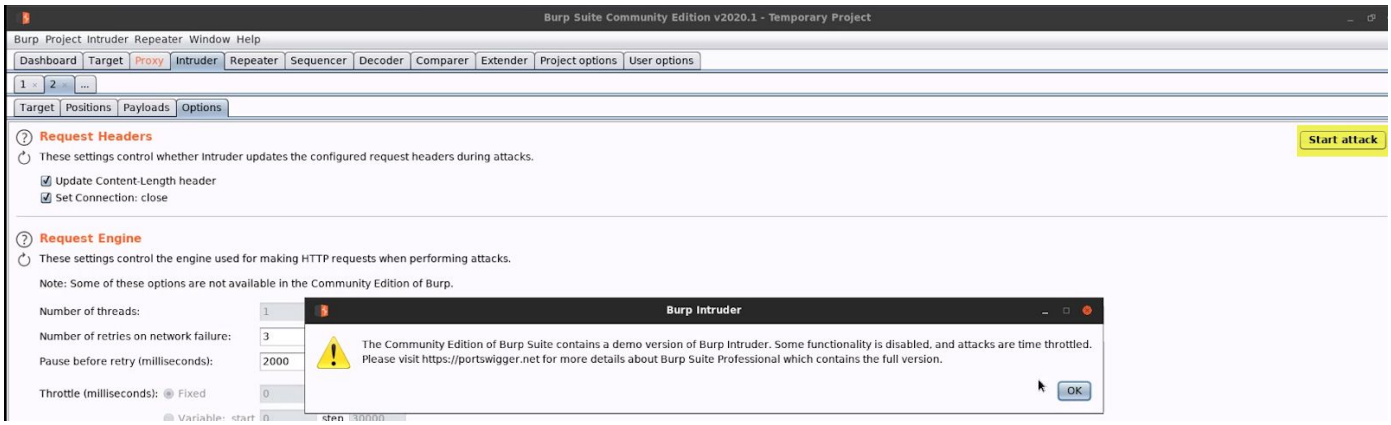
Step 17: Copy the error message given on the wrong/invalid login attempt.



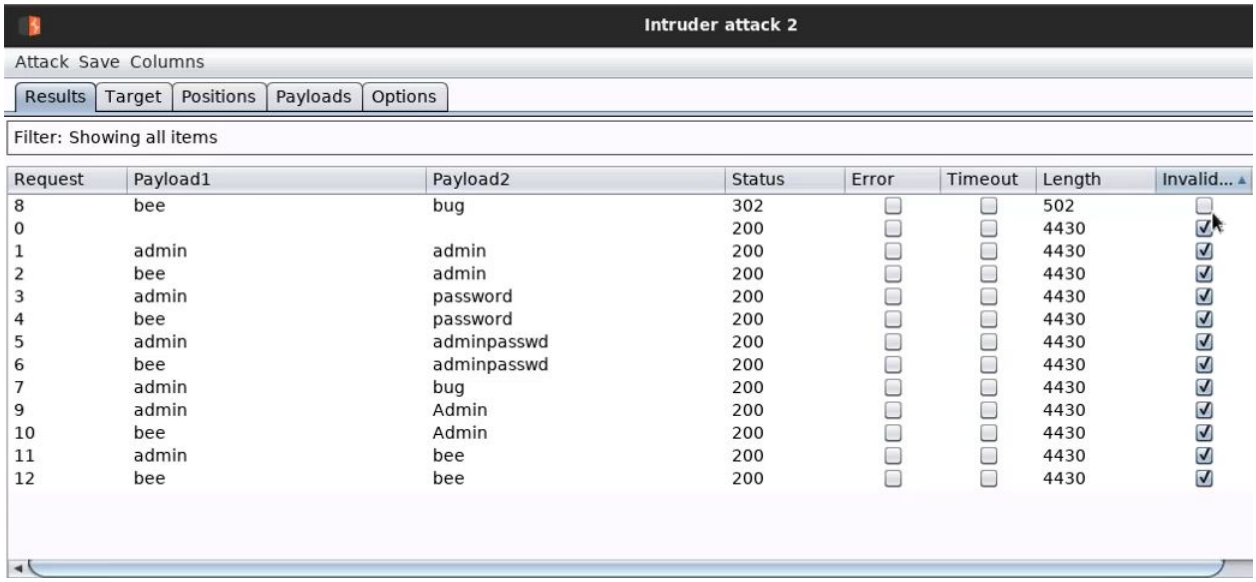
Step 18: Add the copied error message into Grep-Match option.



Step 19: Start the attack by clicking “Start Attack” button and pressing “OK” the pop-up.



Step 20: This time Burp is also showing if the response consists of the defined error message string or not. In this one too, the username 'bee' and password 'bug' doesn't have a response consisting the error message.



Request	Payload1	Payload2	Status	Error	Timeout	Length	Invalid...
8	bee	bug	302	☐	☐	502	☐
0			200	☐	☐	4430	☑
1	admin	admin	200	☐	☐	4430	☑
2	bee	admin	200	☐	☐	4430	☑
3	admin	password	200	☐	☐	4430	☑
4	bee	password	200	☐	☐	4430	☑
5	admin	adminpasswd	200	☐	☐	4430	☑
6	bee	adminpasswd	200	☐	☐	4430	☑
7	admin	bug	200	☐	☐	4430	☑
9	admin	Admin	200	☐	☐	4430	☑
10	bee	Admin	200	☐	☐	4430	☑
11	admin	bee	200	☐	☐	4430	☑
12	bee	bee	200	☐	☐	4430	☑

Hence, the correct credentials are:

Username: bee
Password: bug