

[illegible]

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:~#
```

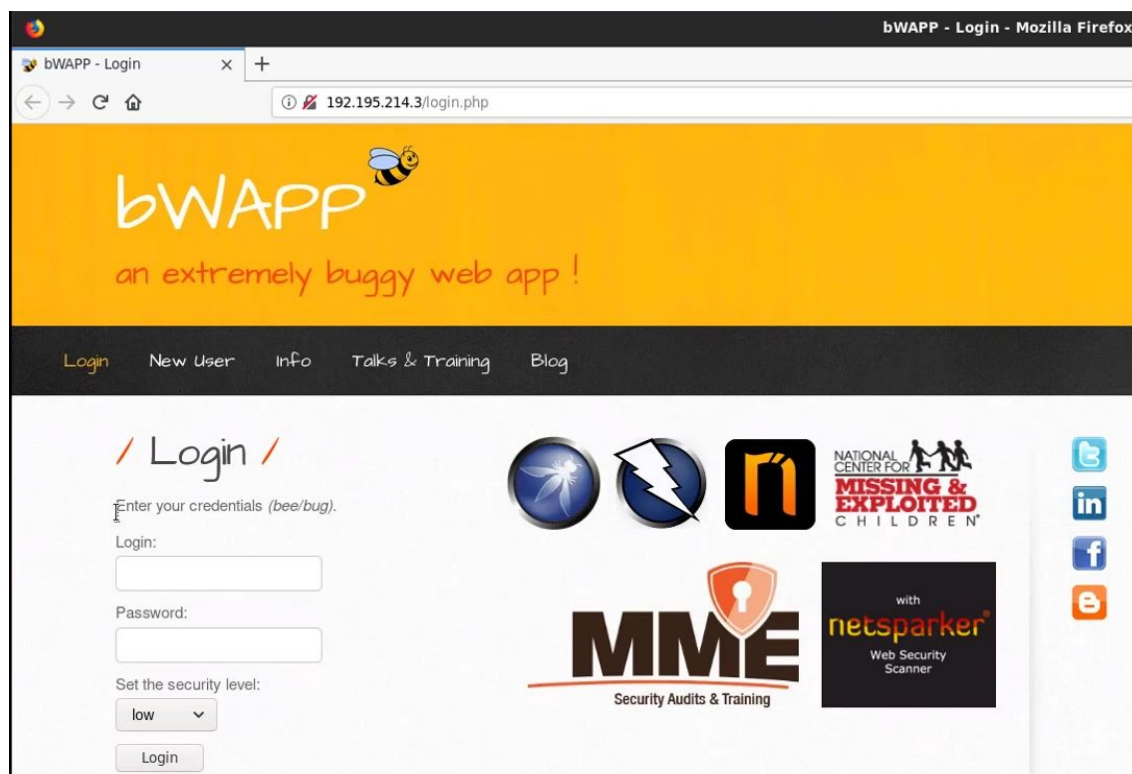
Step 2: Run a nmap scan against the target IP.

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)

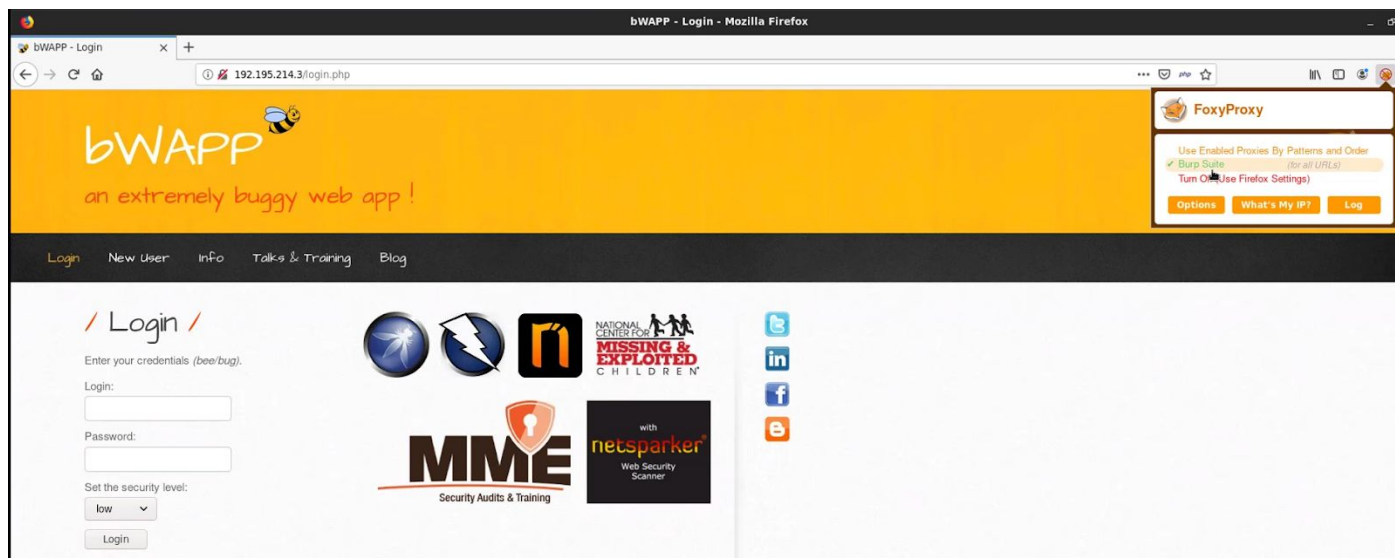
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

Step 3: Open the target webportal in the browser.

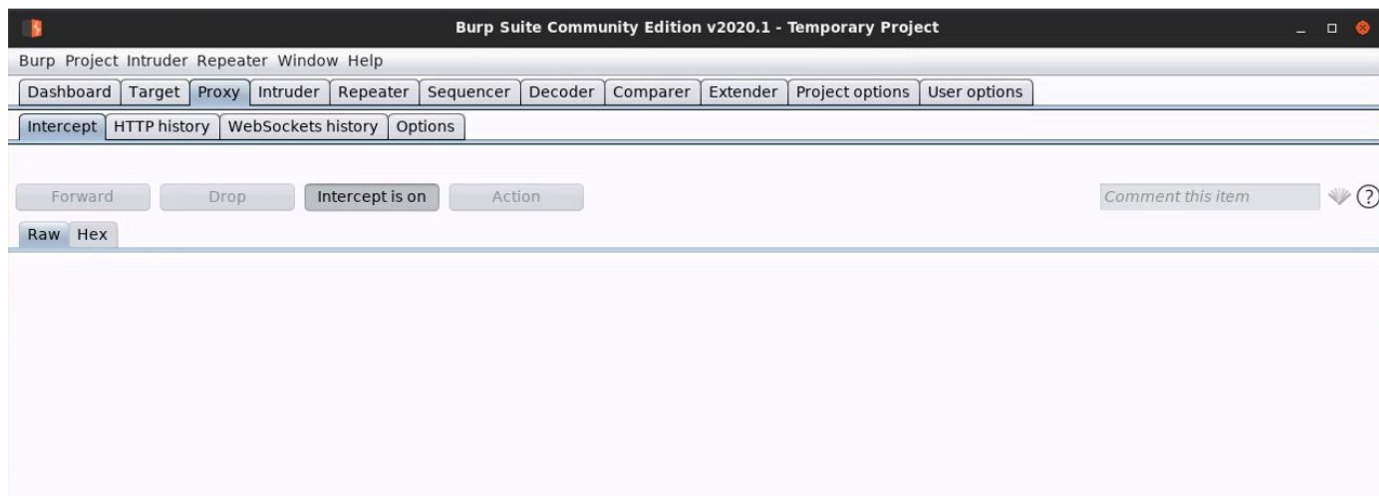


The bWAPP web application is running on the target machine.

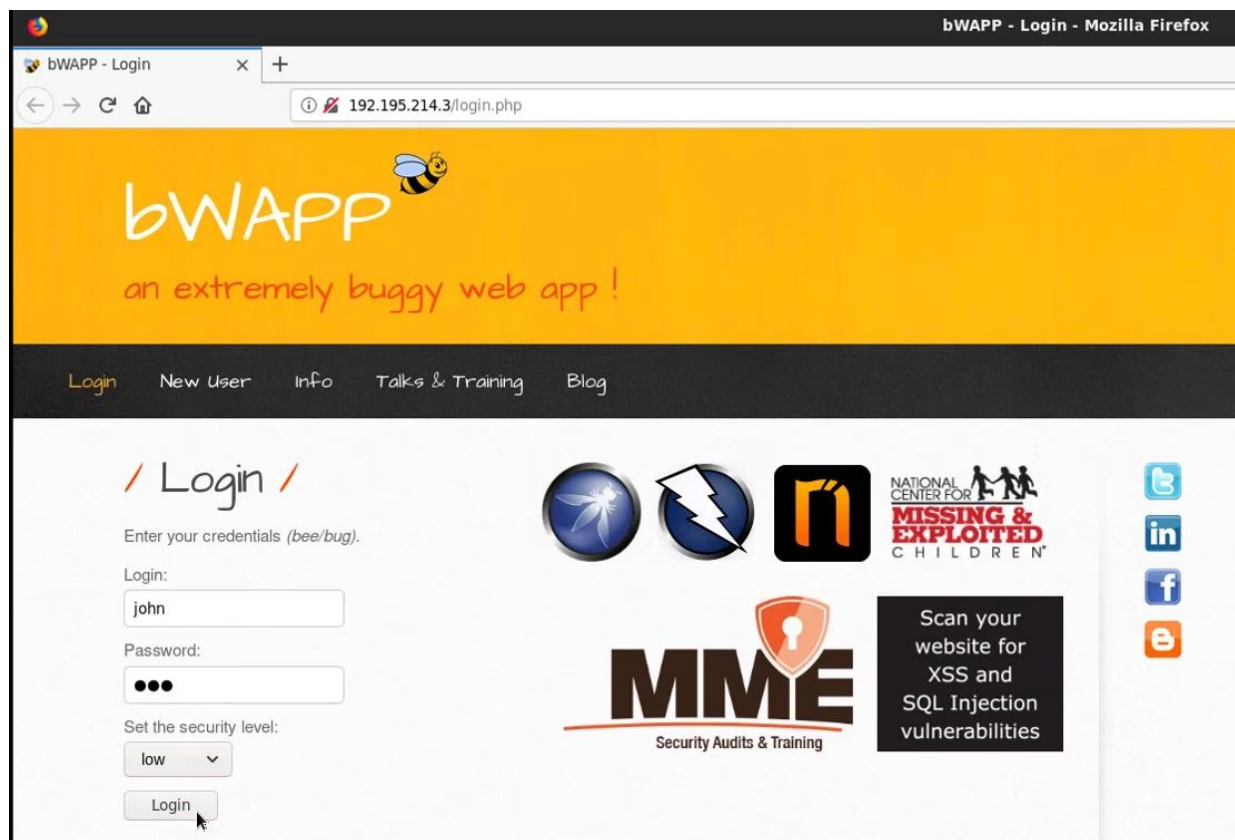
Step 4: Select burp proxy from the “Foxyproxy” options.



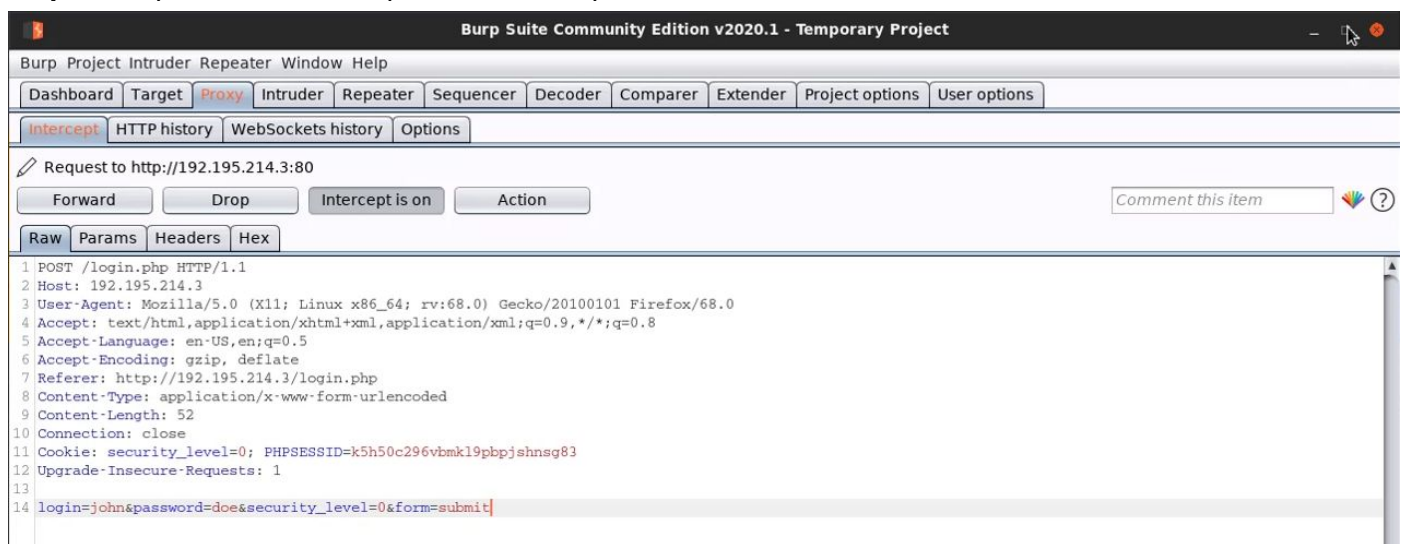
Step 5: Start Burp Suite in interception mode.



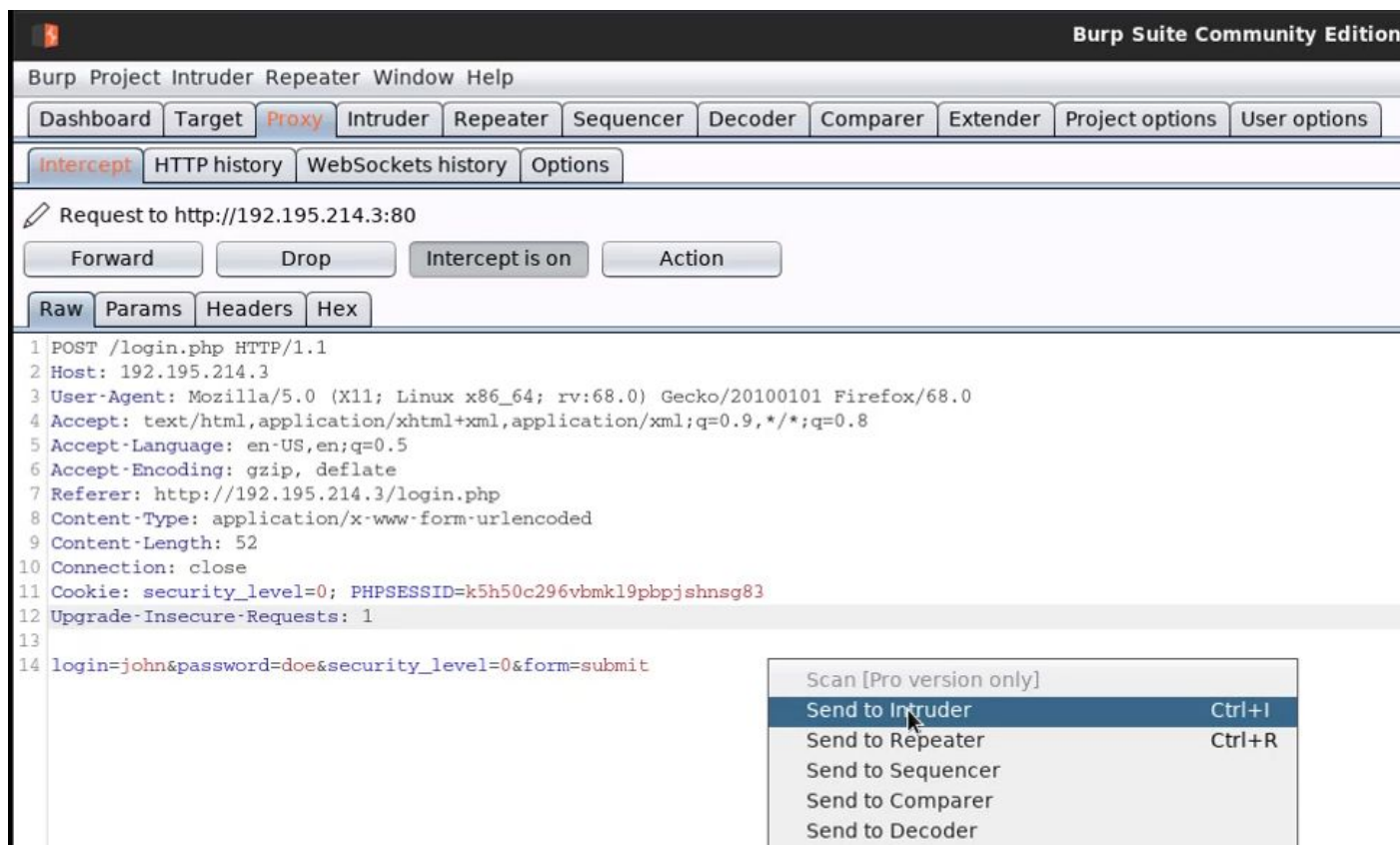
Step 6: Enter dummy credentials in the login page and press 'login'.



Step 7: Burp suite will intercept the POST request.



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



Burp Suite Community Edition

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://192.195.214.3:80

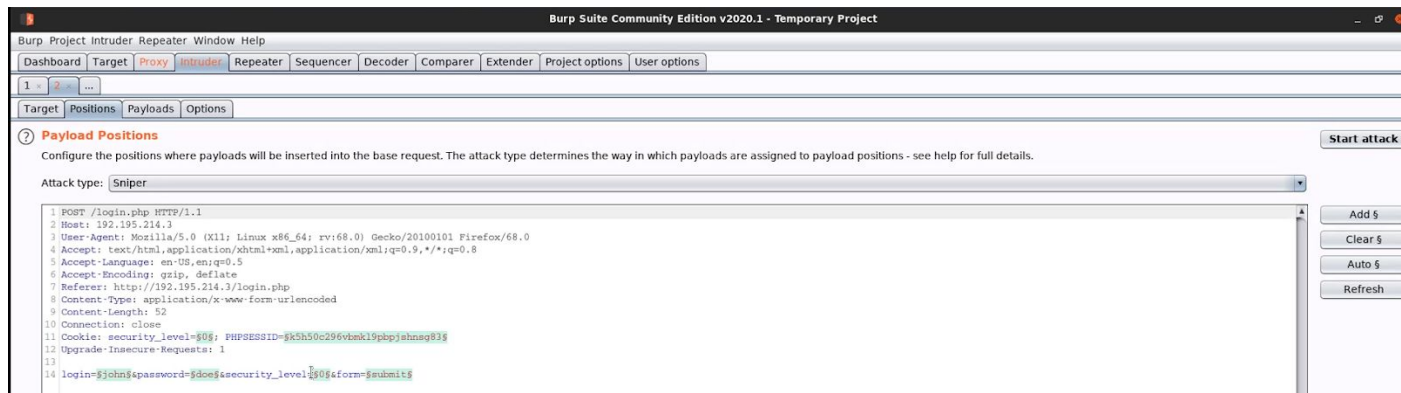
Forward Drop Intercept is on Action

Raw Params Headers Hex

```
1 POST /login.php HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.195.214.3/login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 52
10 Connection: close
11 Cookie: security_level=0; PHPSESSID=k5h50c296vbmkl9pbpjshnsg83
12 Upgrade-Insecure-Requests: 1
13
14 login=john&password=doe&security_level=0&form=submit
```

Scan [Pro version only]
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder

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



Burp Suite Community Edition v2020.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Target Positions Payloads Options

① Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

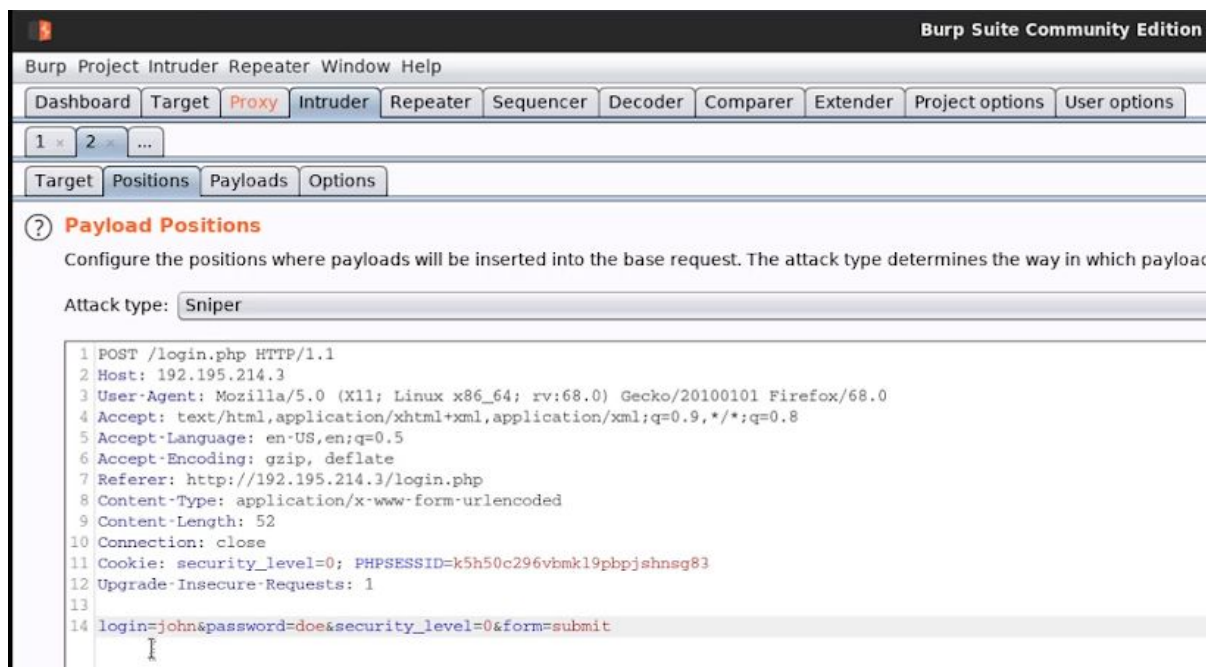
Attack type: Sniper

```
1 POST /login.php HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.195.214.3/login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 52
10 Connection: close
11 Cookie: security_level=$0$, PHPSESSID=$k5h50c296vbmkl9pbpjshnsg83$
12 Upgrade-Insecure-Requests: 1
13
14 login=$john$&password=$doe$&security_level=$0$&form=$submit$
```

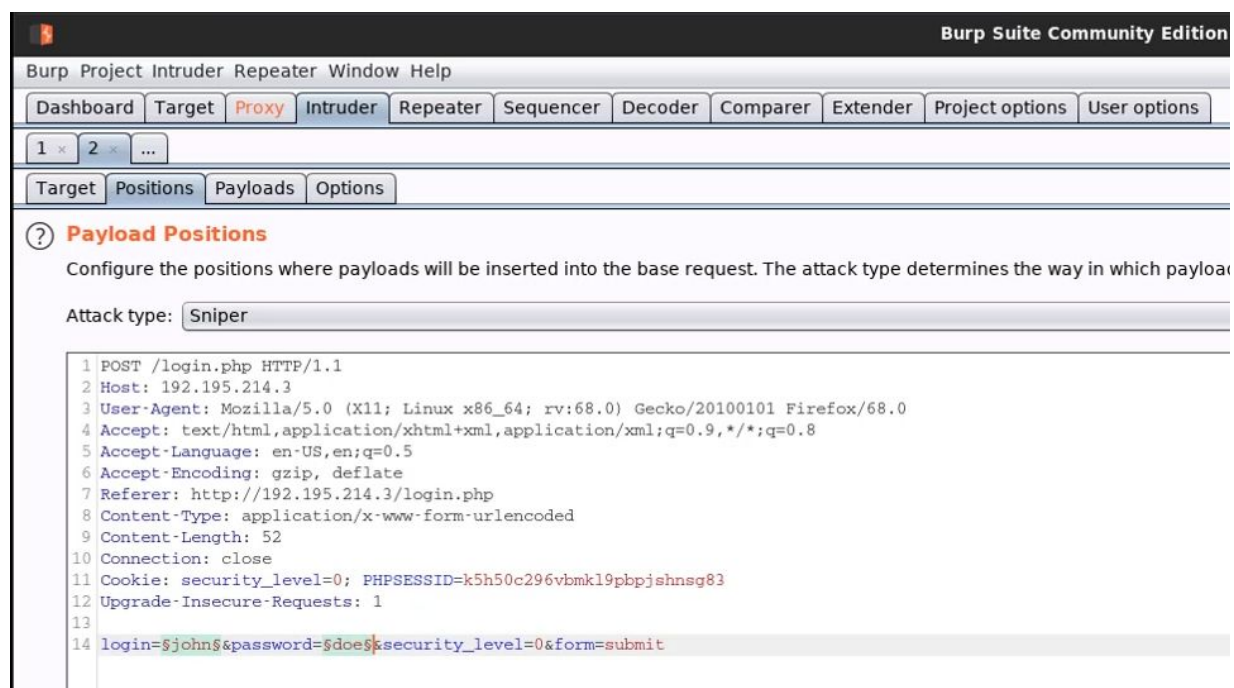
Add \$
Clear \$
Auto \$
Refresh

Start attack

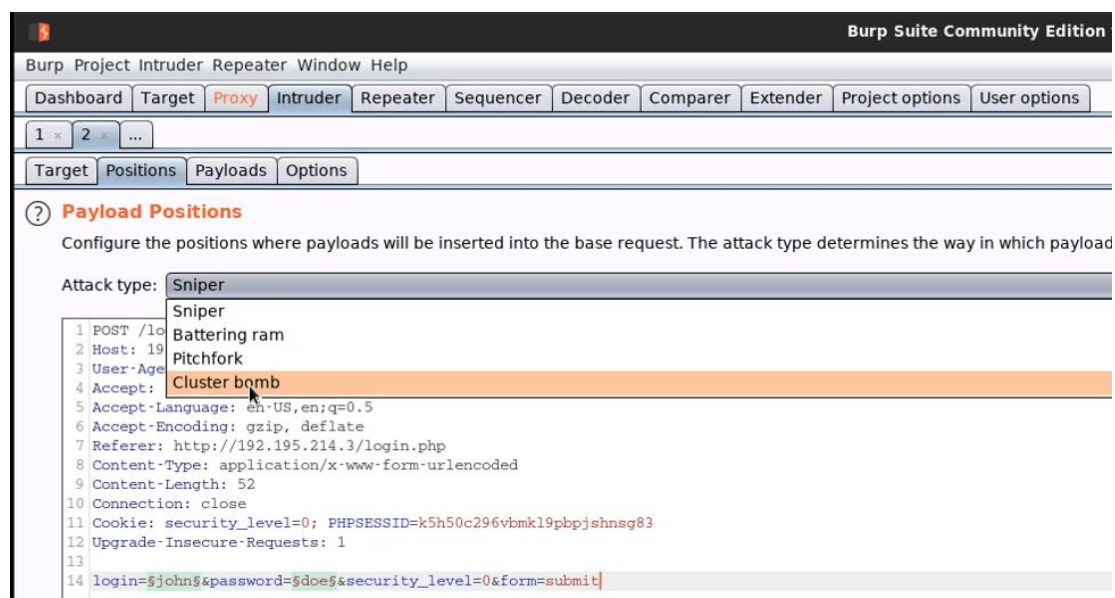
Step 10: Clear all payload positions by clicking on 'clear' button.



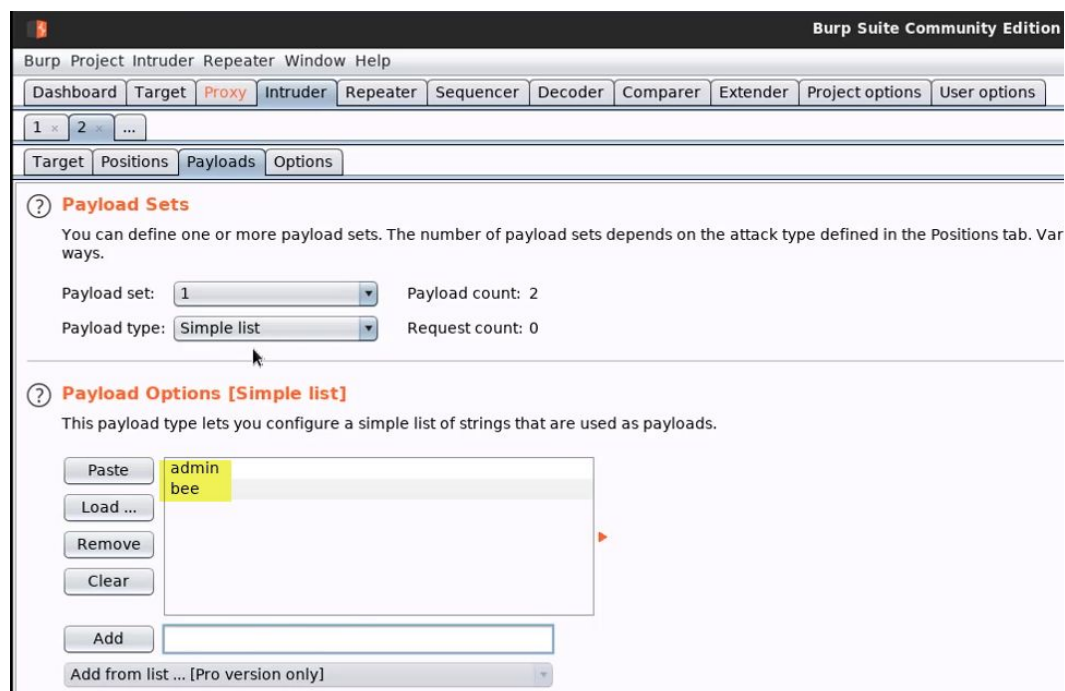
Step 11: Now, mark values of login and password as payload positions.



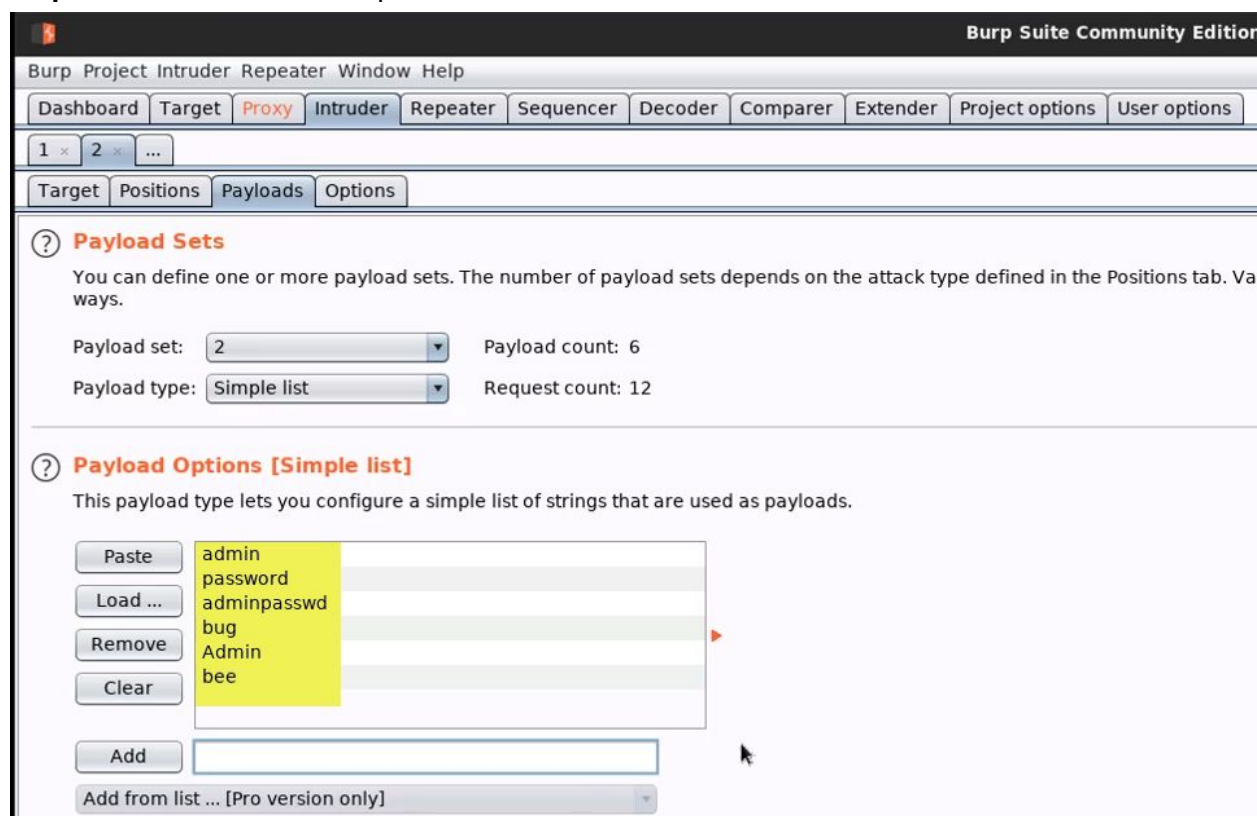
Step 12: Select “cluster bomb” feature.



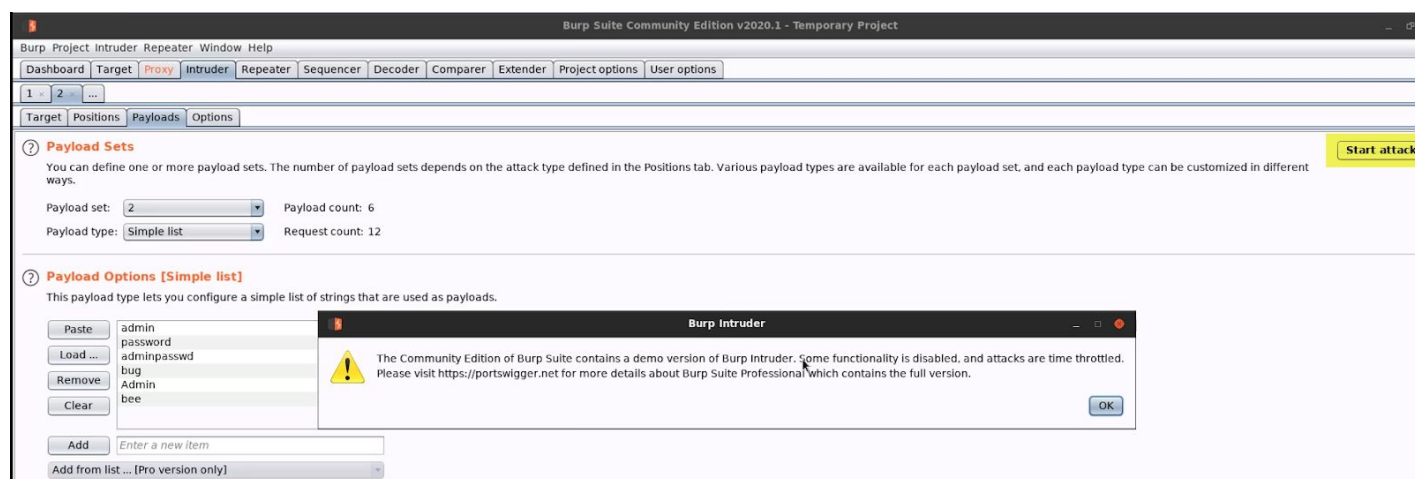
Step 13: Add first list for usernames.



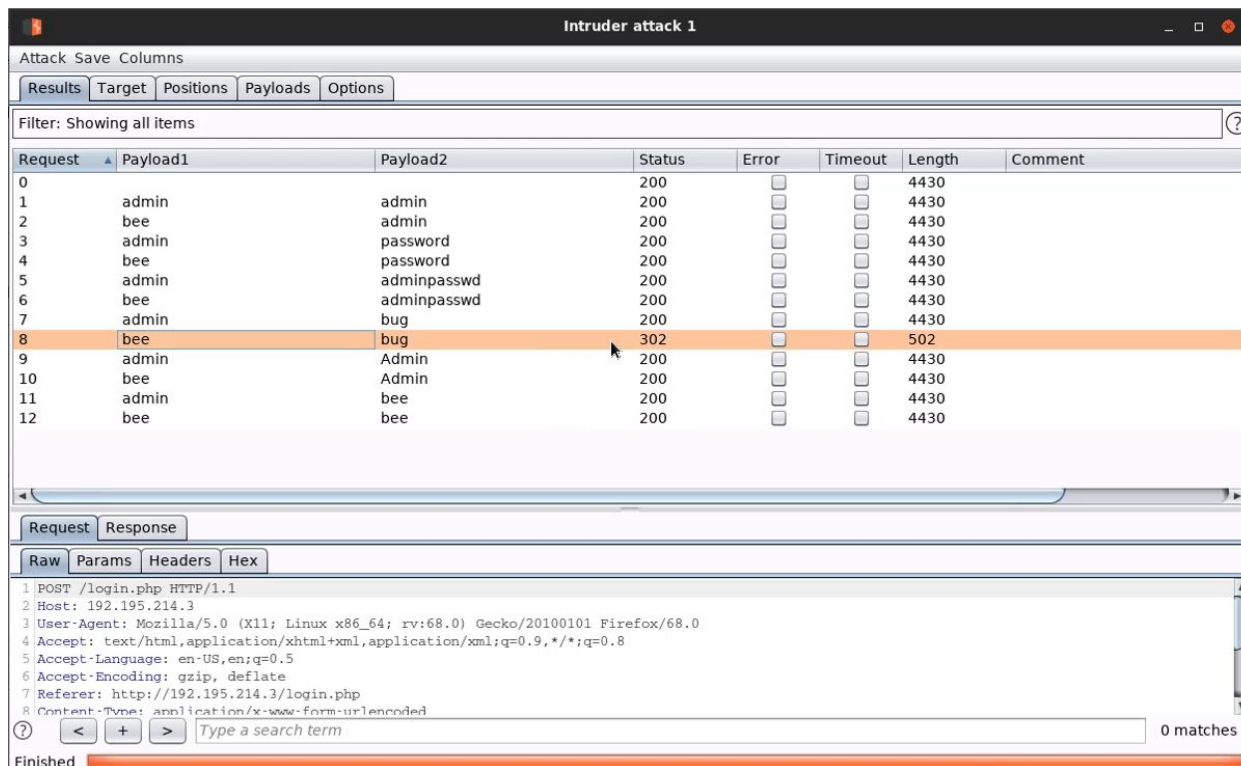
Step 14: Add second list for passwords.



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.



Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
2	bee	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
3	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
4	bee	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
5	admin	adminpasswd	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
6	bee	adminpasswd	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
7	admin	bug	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
8	bee	bug	302	<input type="checkbox"/>	<input type="checkbox"/>	502	
9	admin	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
10	bee	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
11	admin	bee	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	
12	bee	bee	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	

Request Response

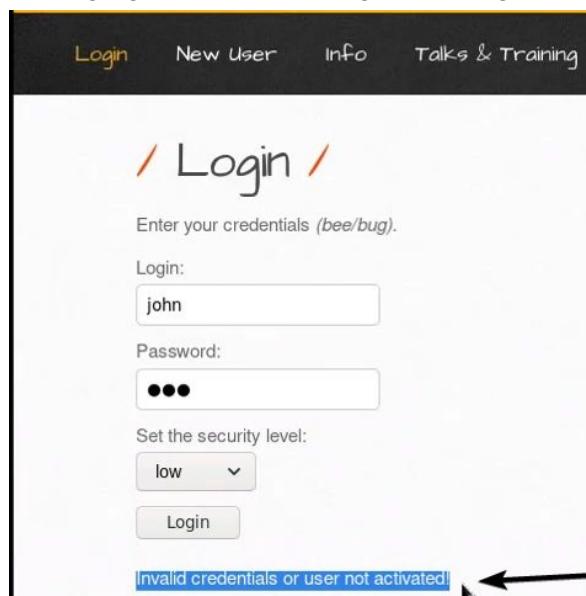
Raw Params Headers Hex

```
1 POST /login.php HTTP/1.1
2 Host: 192.195.214.3
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.195.214.3/login.php
8 Content-Type: application/x-www-form-urlencoded
```

0 matches

Finished

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



Login New User Info Talks & Training

/ Login /

Enter your credentials (bee/bug).

Login:

Password:

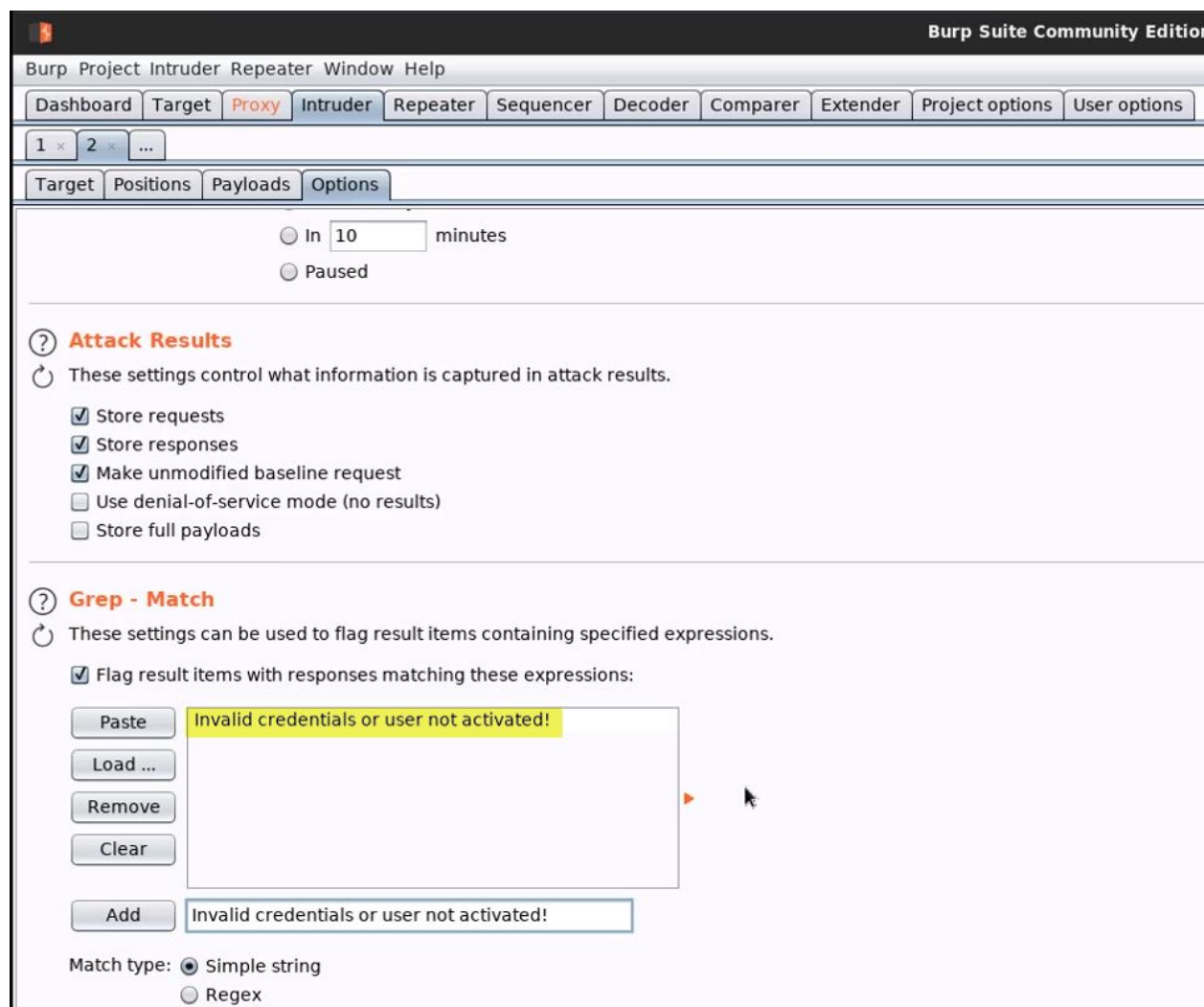
Set the security level:

low

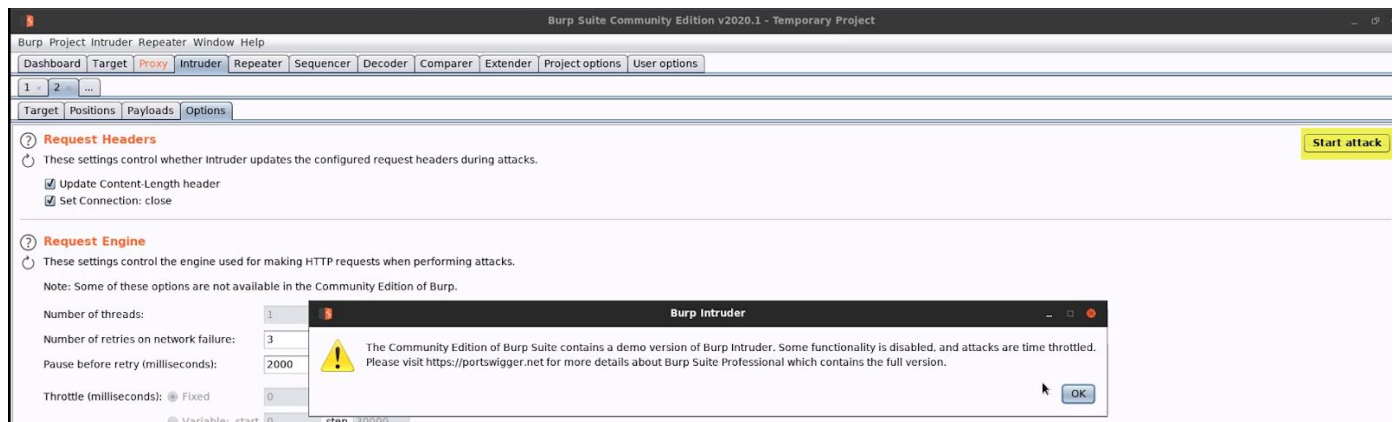
Login

Invalid credentials or user not activated!

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.

Intruder attack 2

Attack Save Columns

Results


Target

Positions

Payloads

Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Invalid... 
8	bee	bug	302	<input type="checkbox"/>	<input type="checkbox"/>	502	<input type="checkbox"/>
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
2	bee	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
3	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
4	bee	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
5	admin	adminpasswd	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
6	bee	adminpasswd	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
7	admin	bug	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
9	admin	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
10	bee	Admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
11	admin	bee	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>
12	bee	bee	200	<input type="checkbox"/>	<input type="checkbox"/>	4430	<input checked="" type="checkbox"/>

Hence, the correct credentials are:

Username: bee

Password: bug