PROJECT : 7

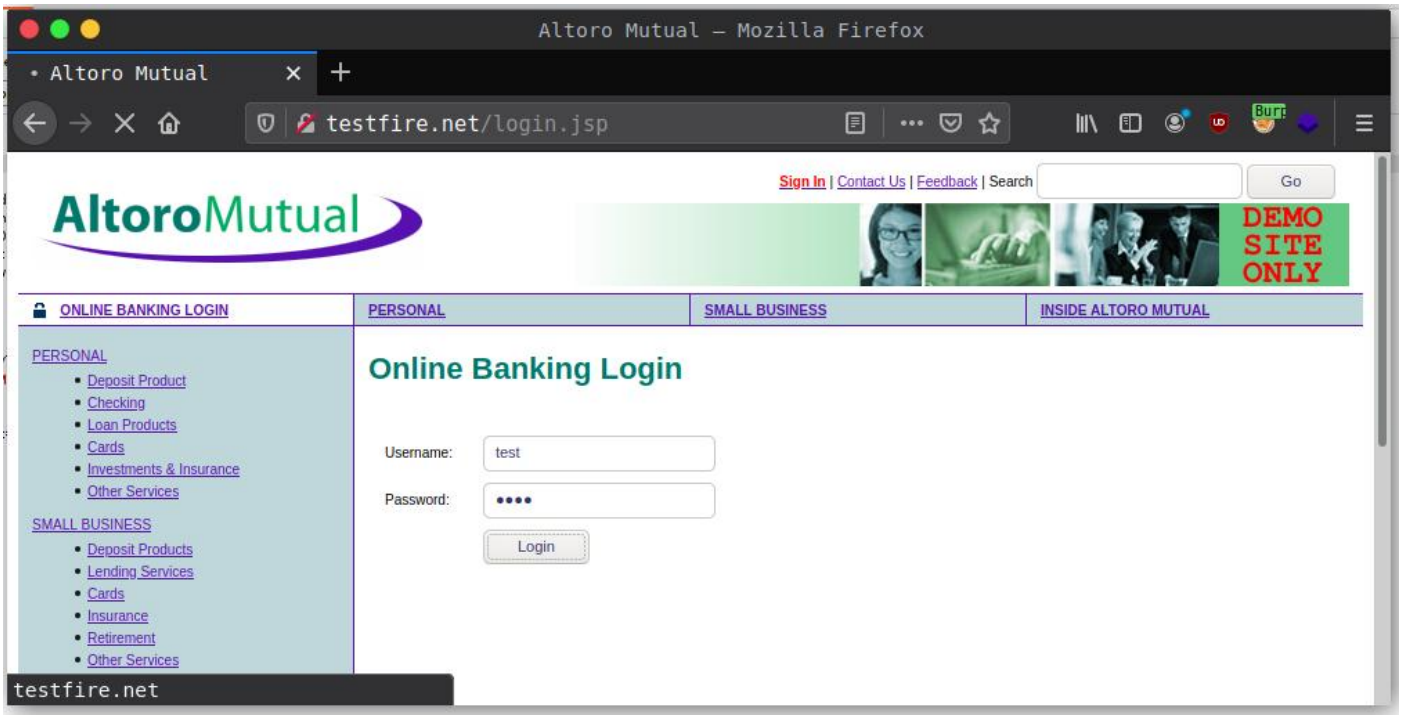
DATE : 23-10-2021

TOPIC :
a. Online password cracking.
b. Offline password cracking.

ONLINE PASSWORD CRACKING

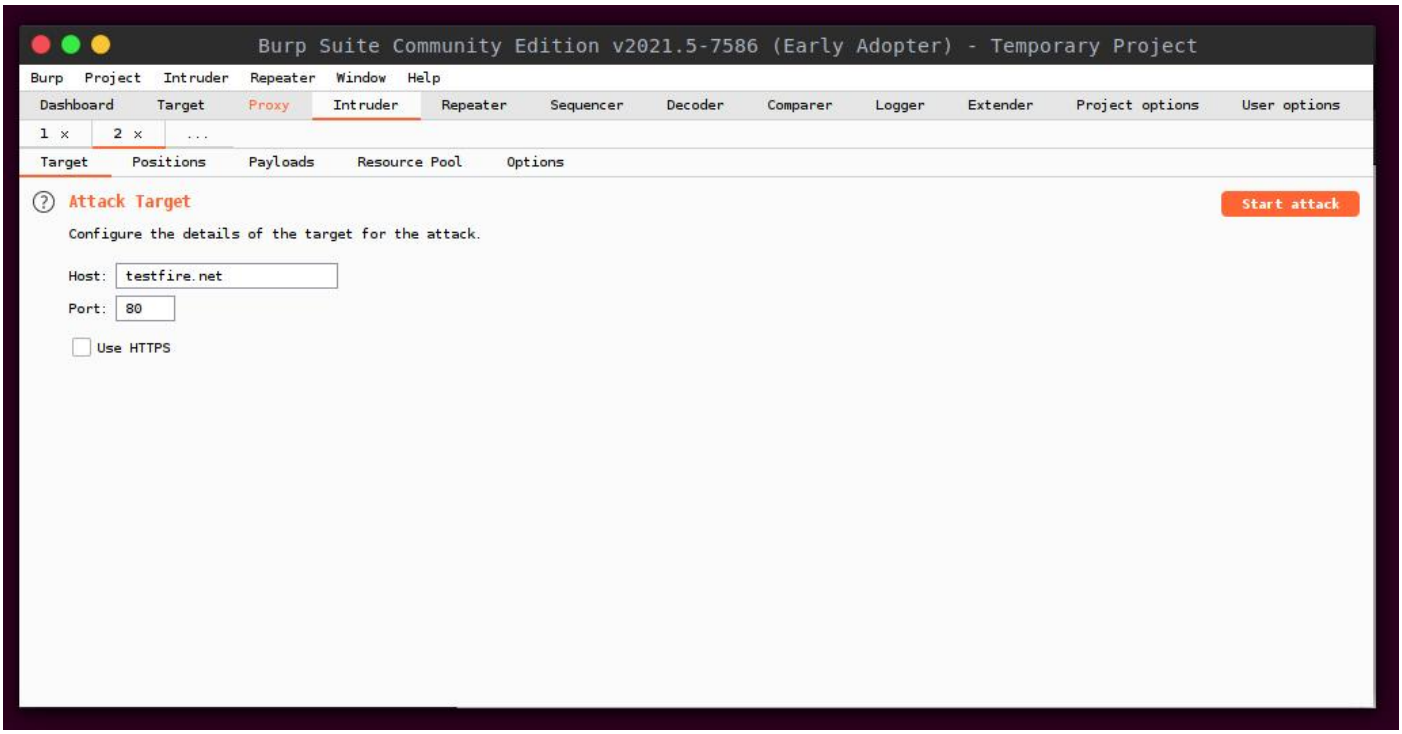
Configure firefox with burpsuite in attacker machine, here the extension foxyproxy is used.

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

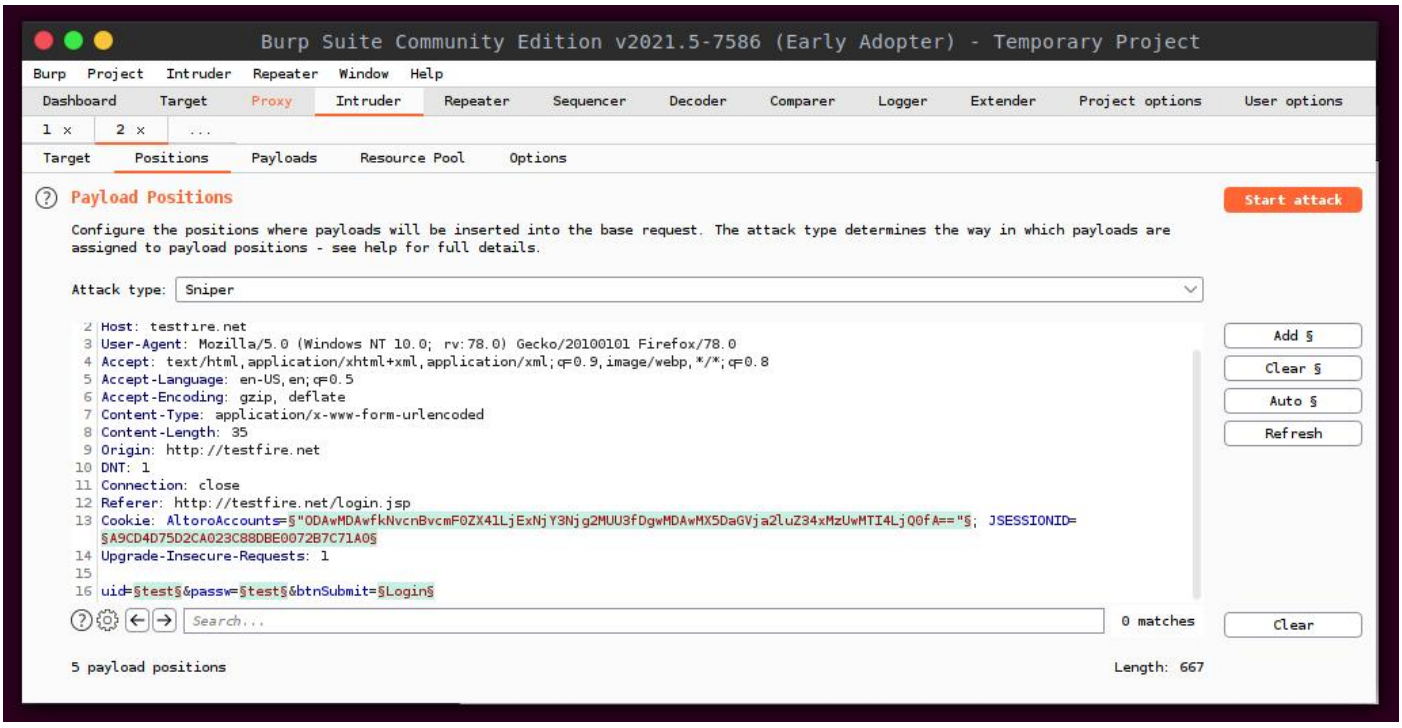


2. Intercept the request in burpsuite.

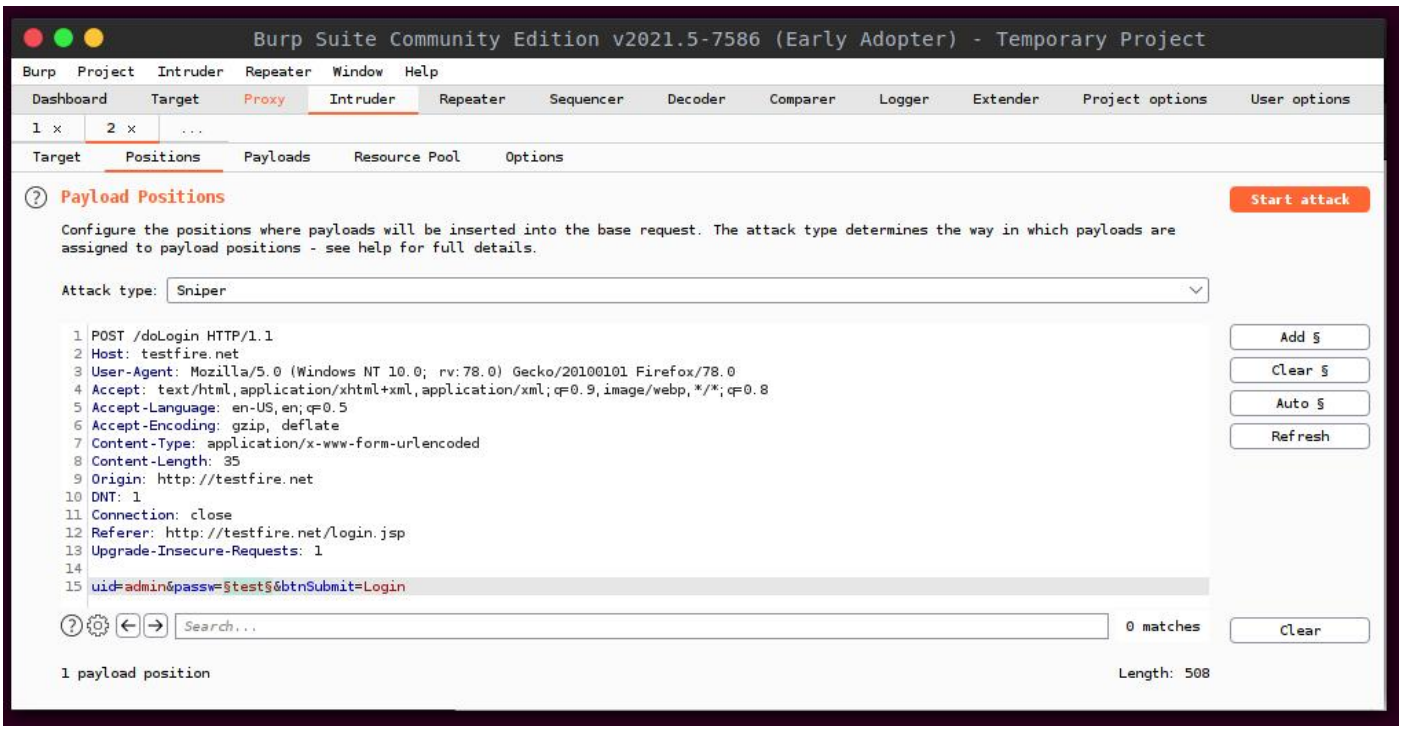
3. Right click on proxy tab, and click send to intruder.



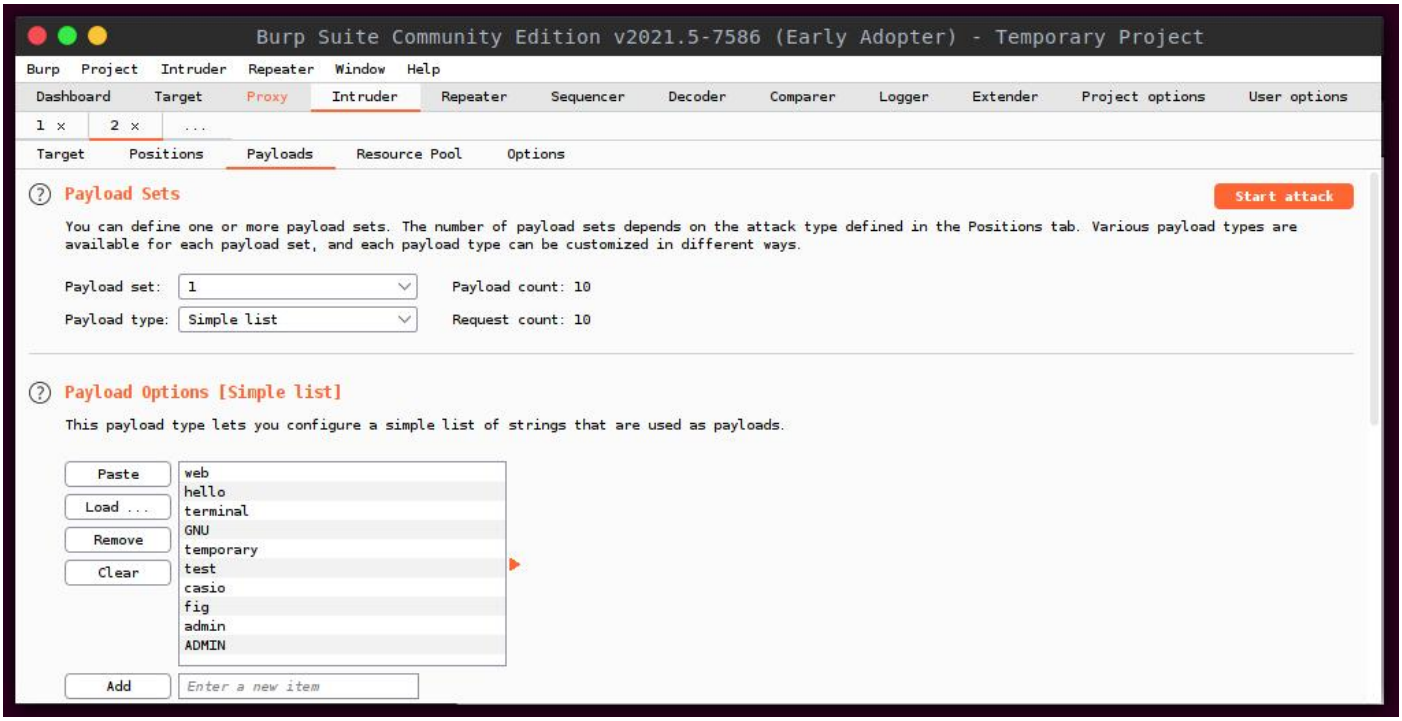
4. In intruder tab, go to positions tab and clear the cookie and click clear.



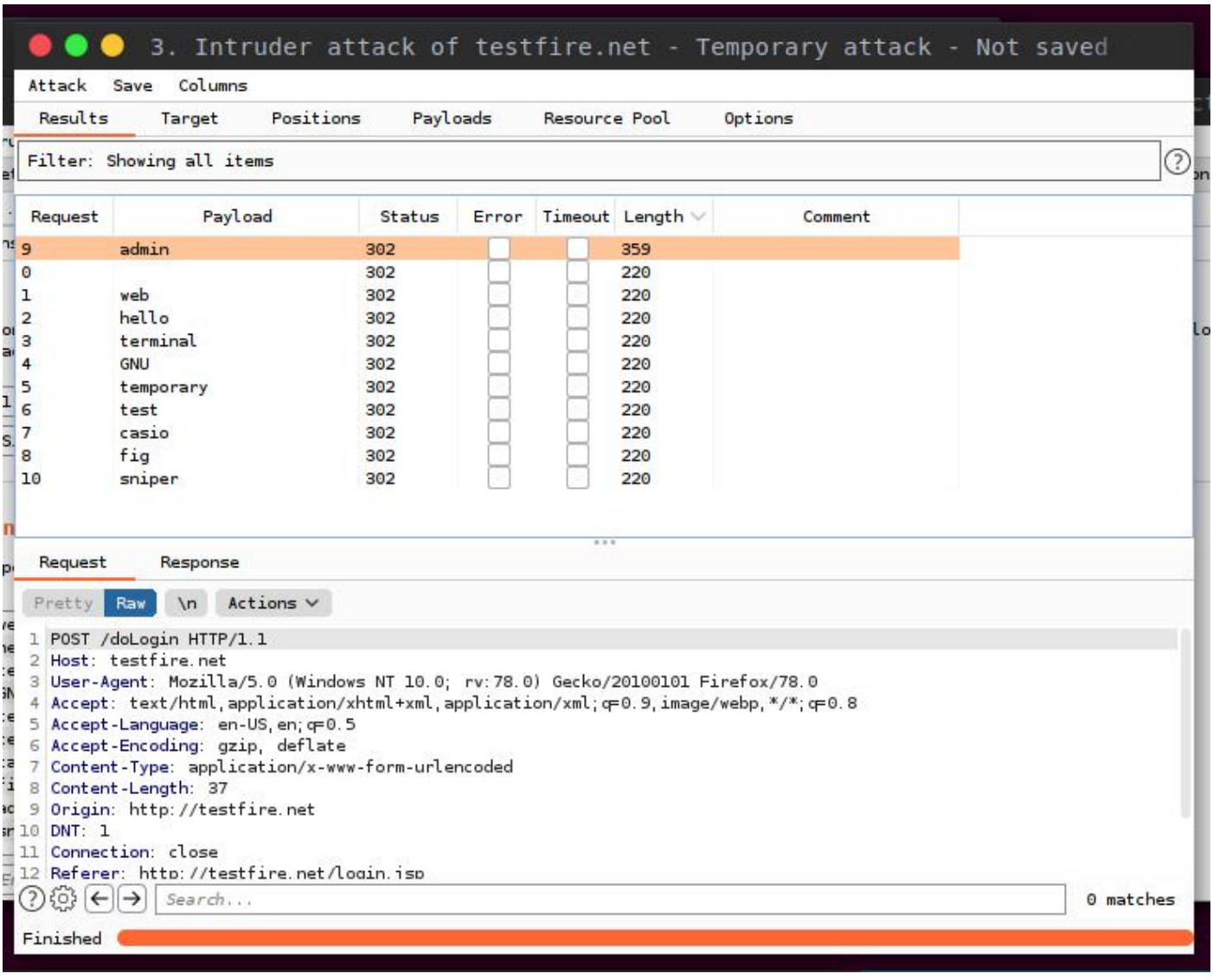
5. Assuming we know the username, click clear and change username value to “admin”. Highlight password value and click add.



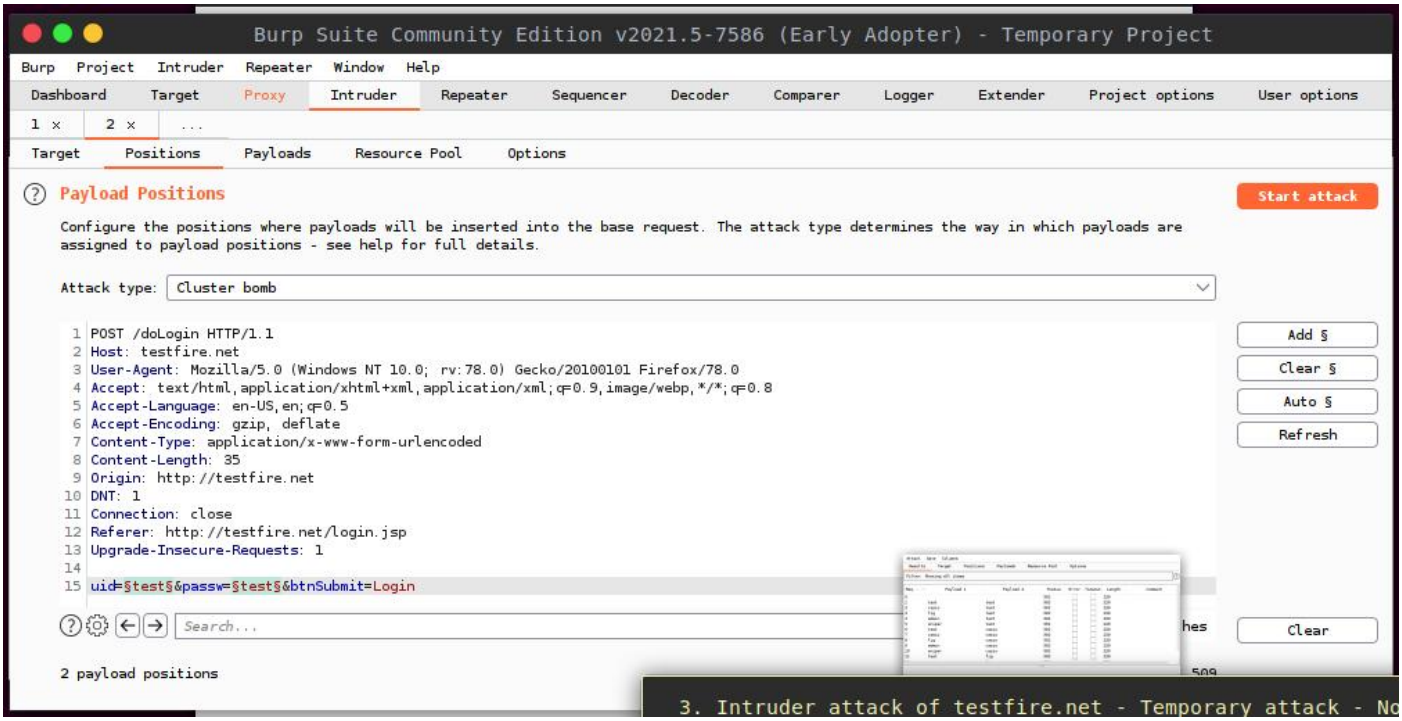
6. Now in payloads tab, click on load and choose the wordlist file.



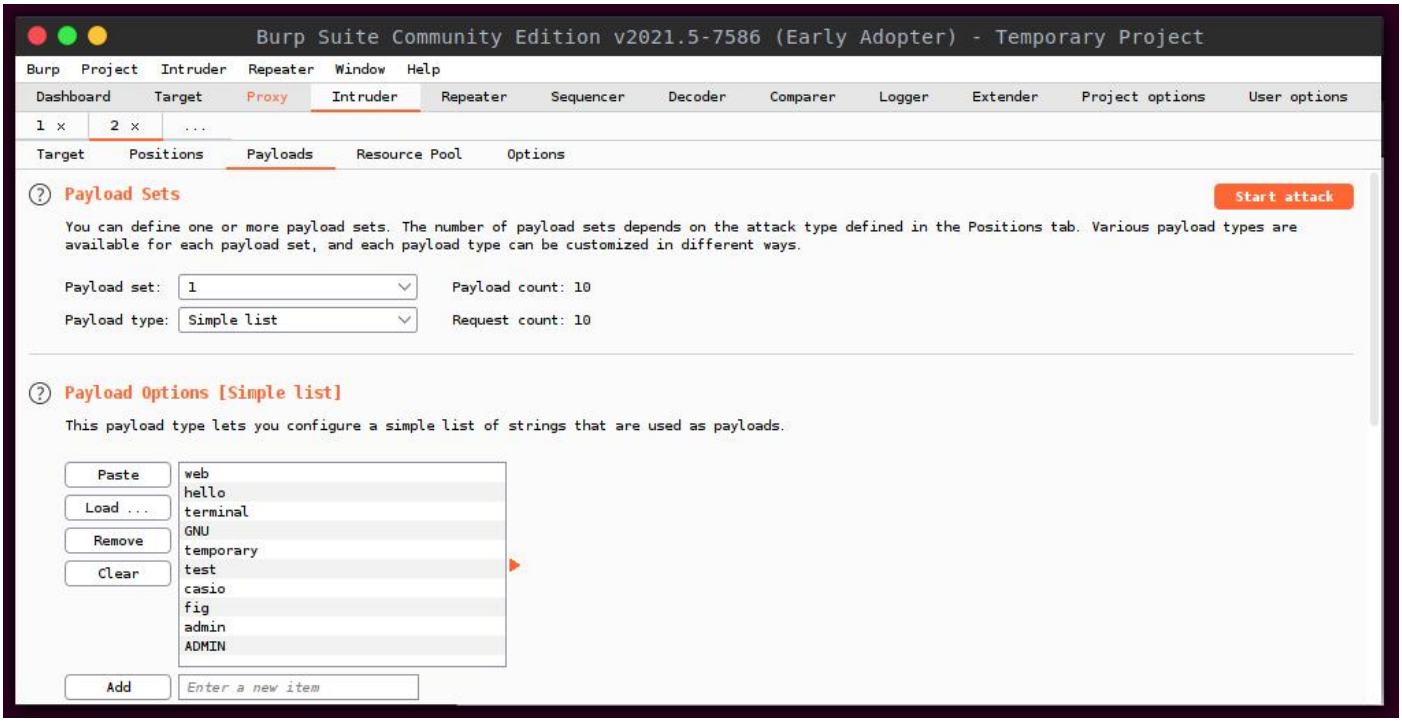
7. Start attack and find the option having highest value. This gives the correct credentials.



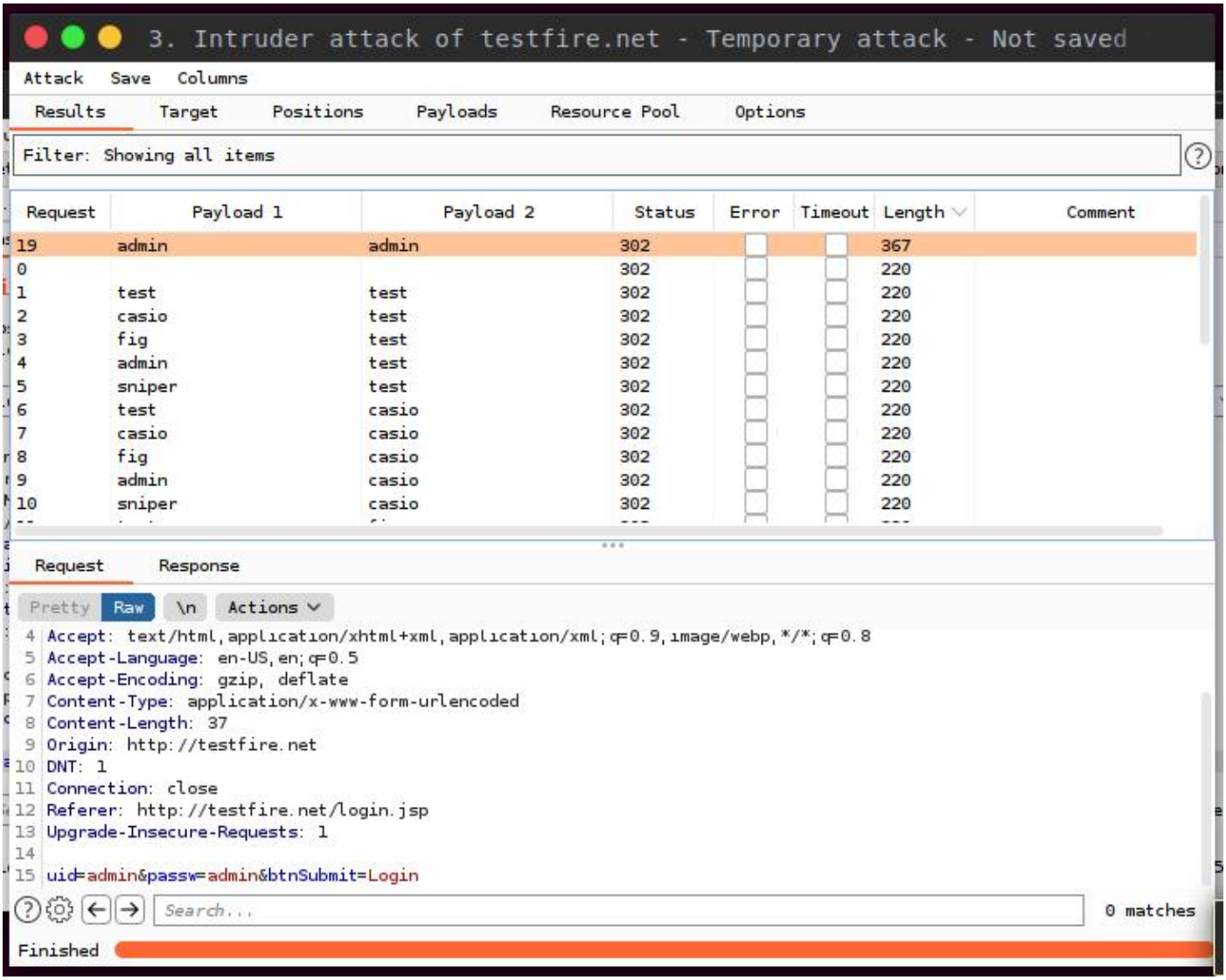
8. Assuming we don't know both username and password, in positions tab, highlight both username value and password value. Change attack type to cluster bomb.



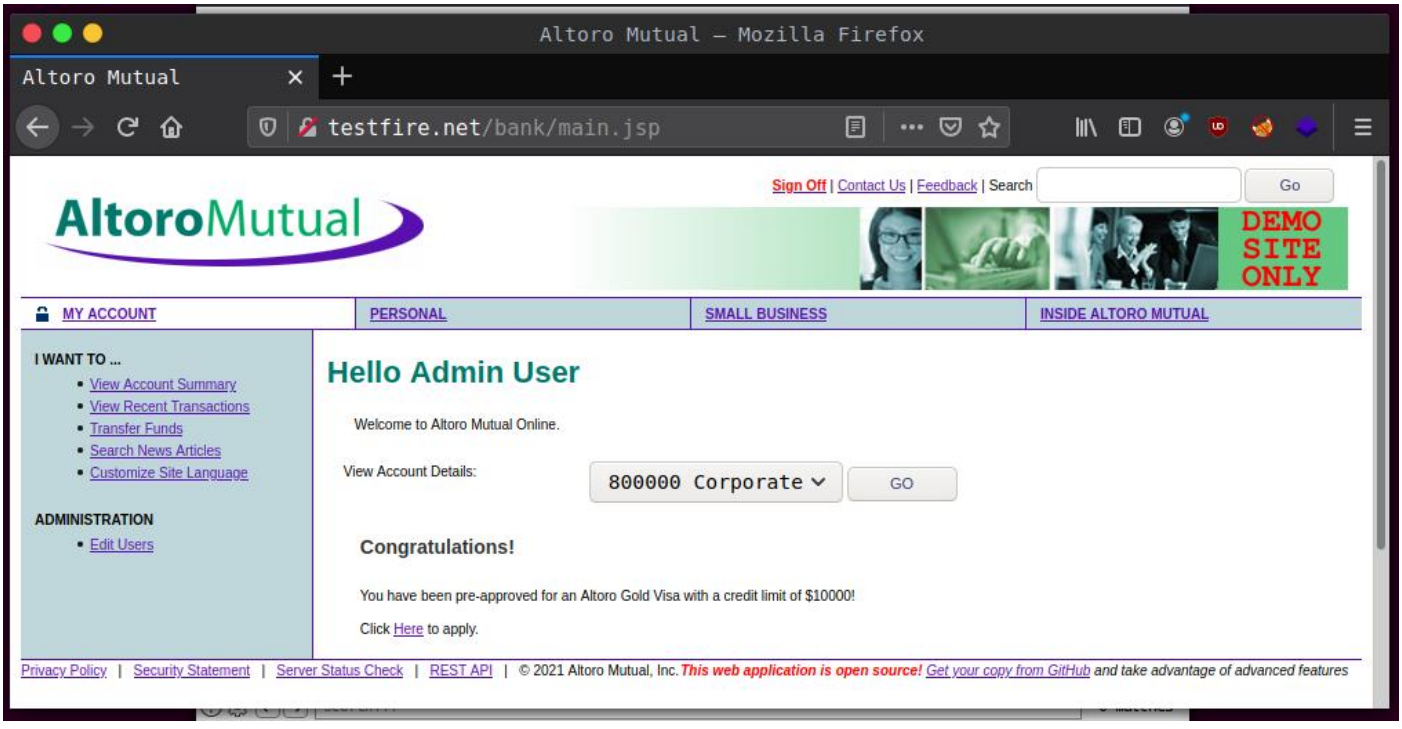
9. In payloads tab, configure both payload set and load wordlists file.



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



11. Log in using correct credentials.



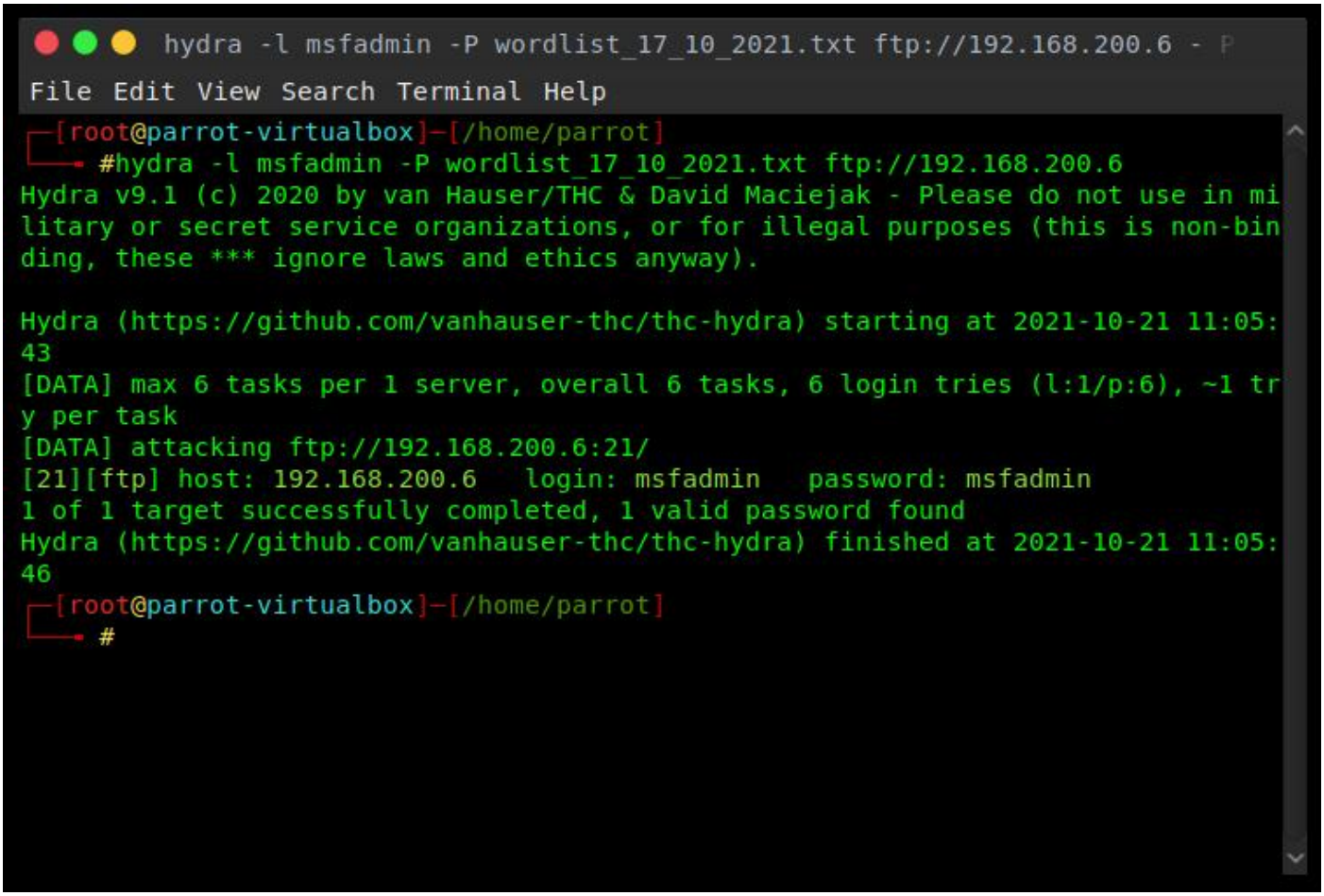
OFFLINE PASSWORD CRACKING

1. Start metasploitable machine (Victim) and parrot machine (Attacker).

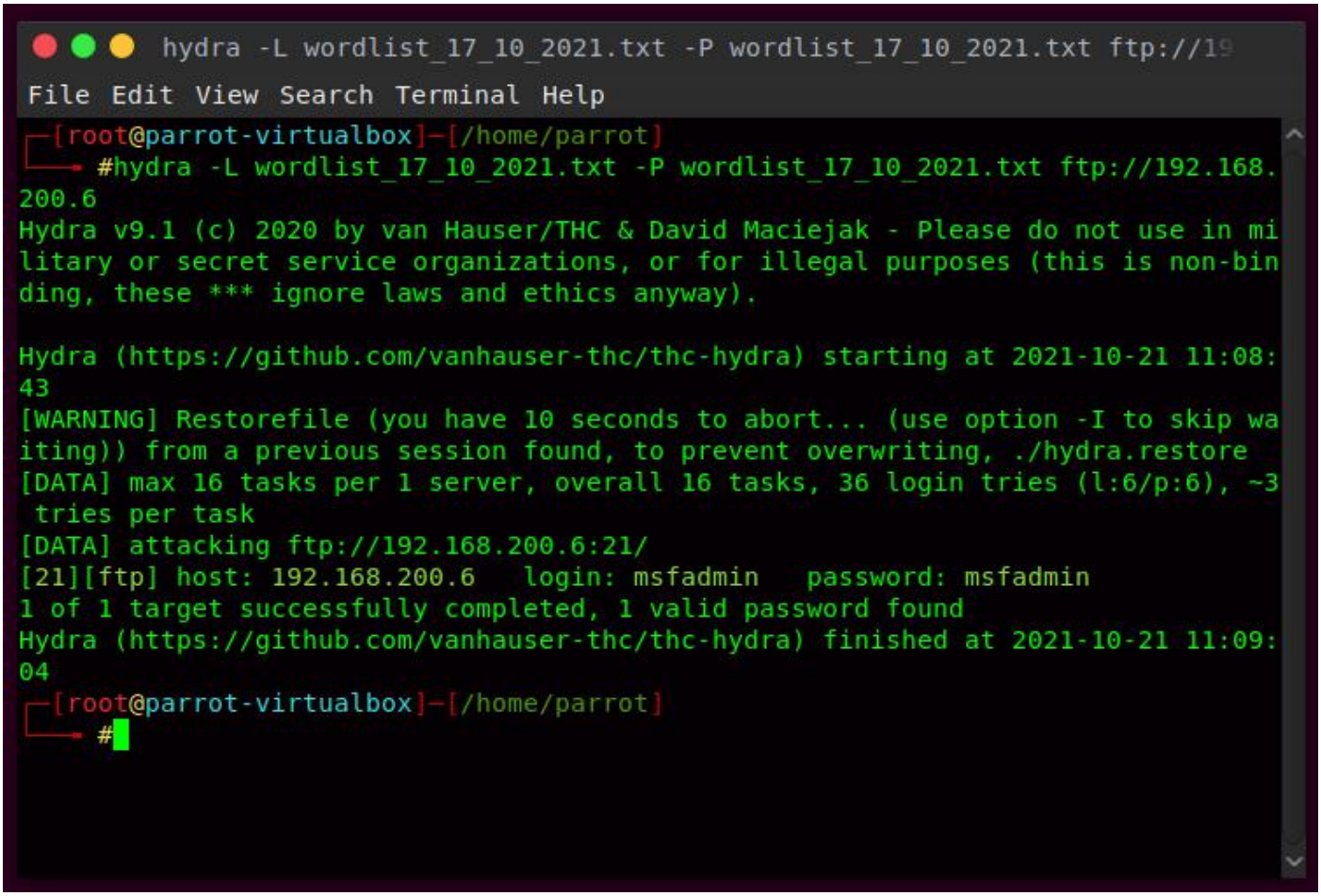
2. In attacker terminal, use create a username and password wordlists or use an existing one.

3. Case 1, suppose we know the username “msfadmin” and not the password.

4. Use hydra tool to crack the password.



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



6. We get the credentials.