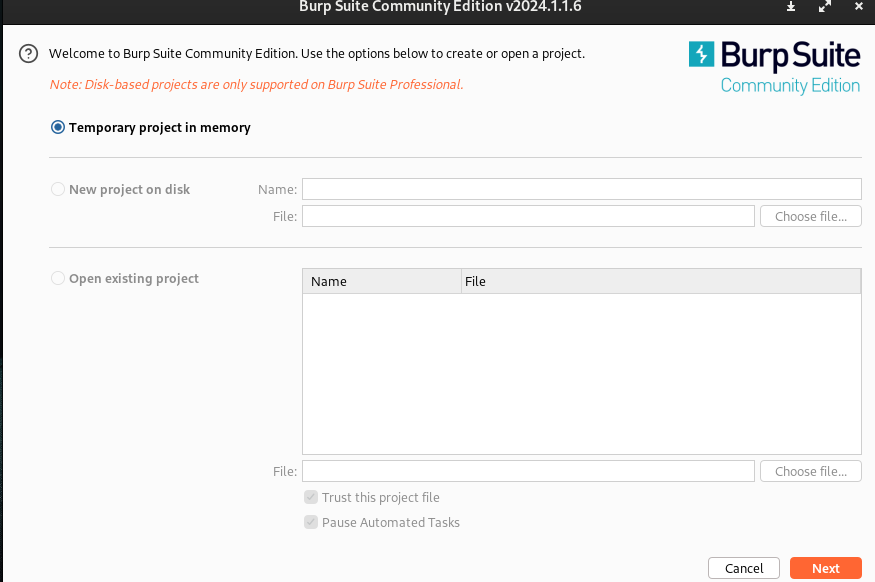
**LAB EXPERIMENT – 8**

**Bruteforce Attack: Using BurpSuite**

Brute force is a hacking technique to do various combinations with a trial-and-error approach to break systems. This technique could be automated using some programs.

1. **Burp suite**–This story’s essential tools to brute force. It doesn’t matter if you are using a community or professional version. It only needs your intentions to start and follow this technique until done.

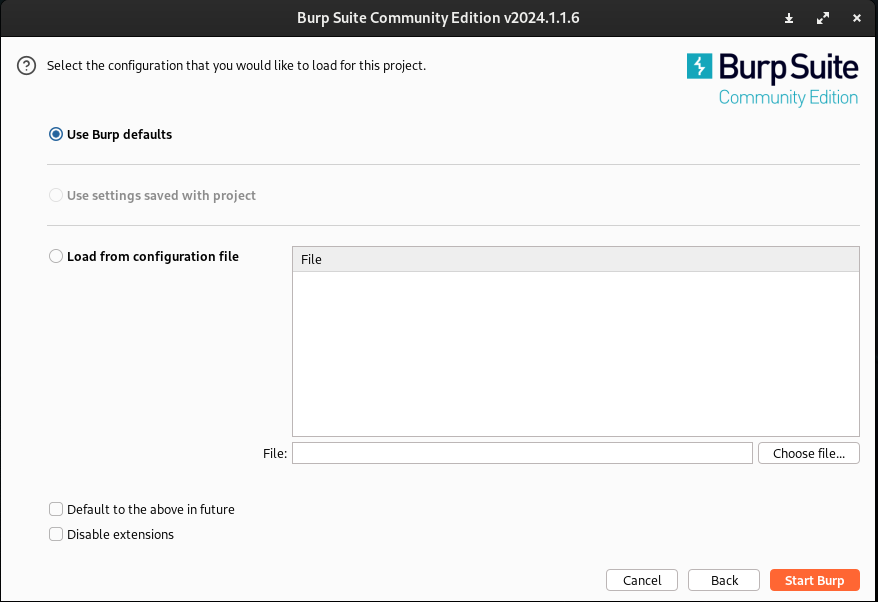
2. **Wordlists**— Lists of combinations for fulfilling the username and password. I would recommend the SecLists wordlist that you could access from their GitHub [here](https://github.com/danielmiessler/SecLists).

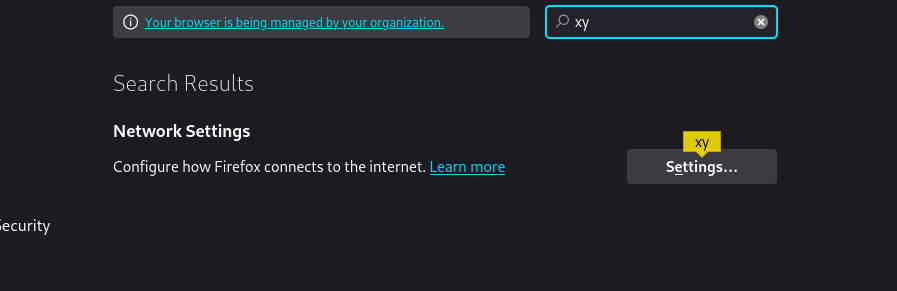
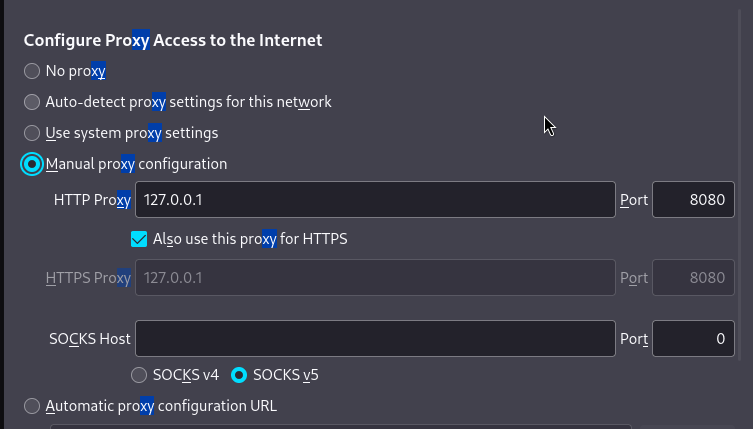


**The Technique**

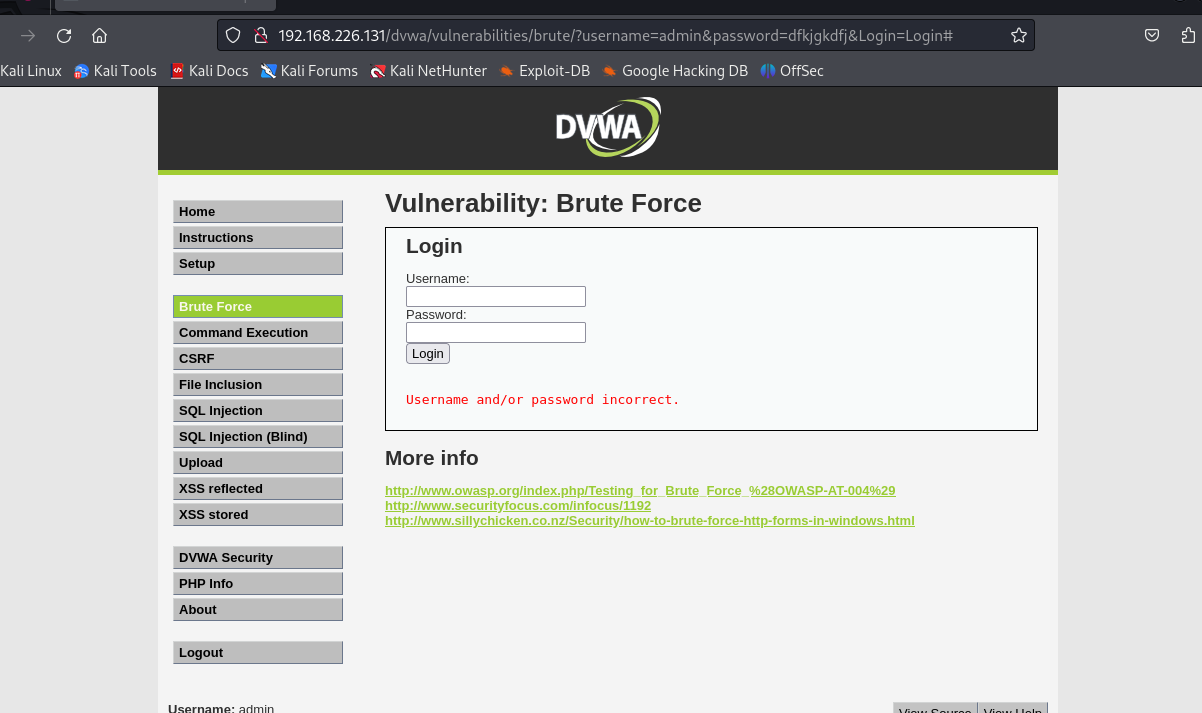
Let’s go to the technique of doing a brute force.

1. Open burp suite and start the browser (Target Tab > Open Browser).





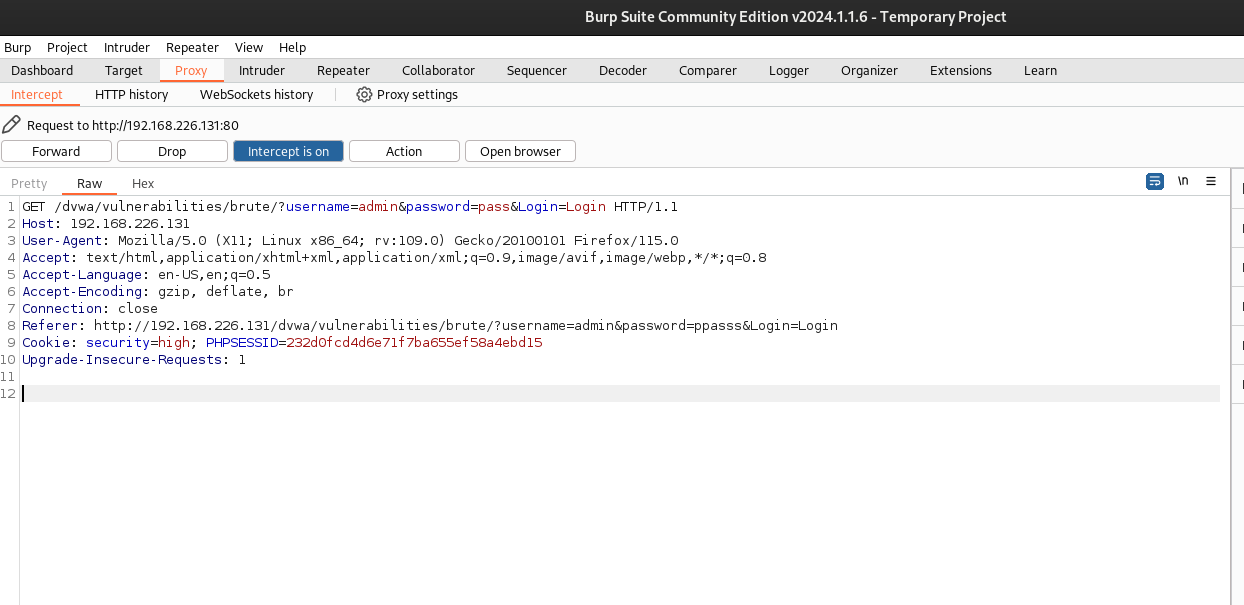
2. Access the target using the browser provided by the burp suite; if you observe, the burp suite will record your traffic in the browser. It means the browser is connected to the software.



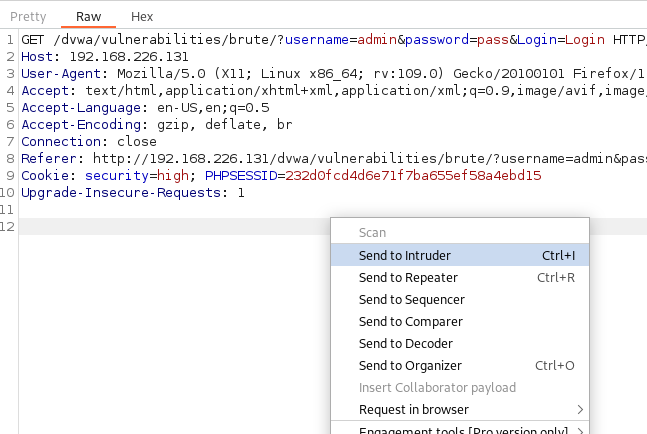
3. Login the dvwa account, username “admin” password “password” and go to the Brute Force section.

4. Fill in the username and password form but don’t press login, here I fill the username ‘user’ and password ‘1234’.

5. Go to the Proxy tab in your burp suite and click the “intercept is off” to activate it and become “intercept is on” like this.

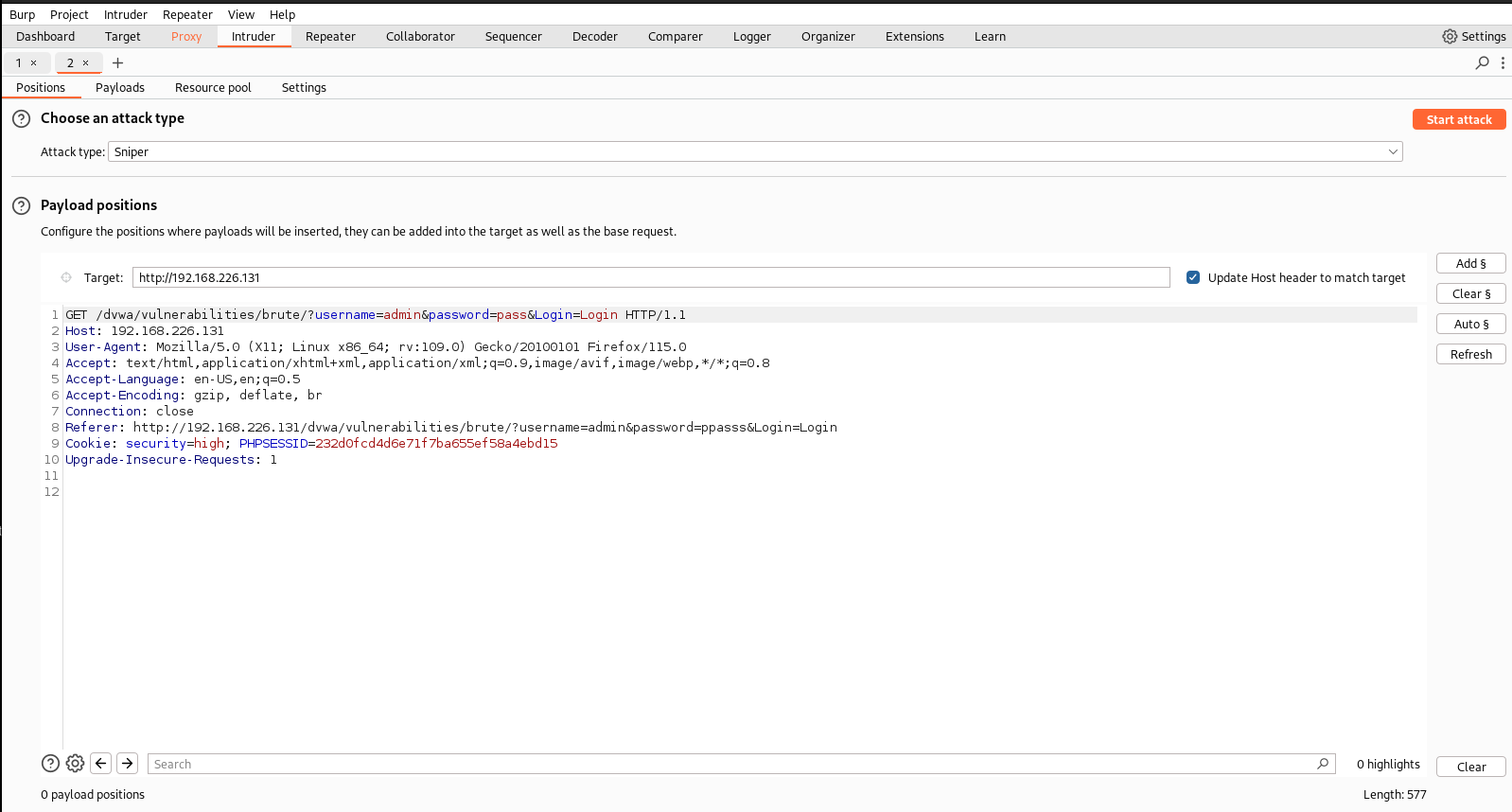


6. Back to the browser again, click login and look at the burp suite; the traffic will be recorded.



7. Right click on the burp suite, choose sent to intruder.

8. Go to the intruder tab, and before making changes to anything, click clear here to remove the “§” sign.



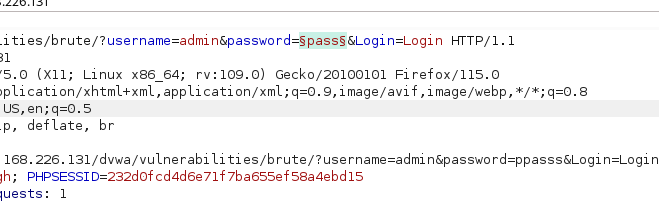
10. Next, hover on username and click add to add the “§” sign there.

Click Add to brute force on.

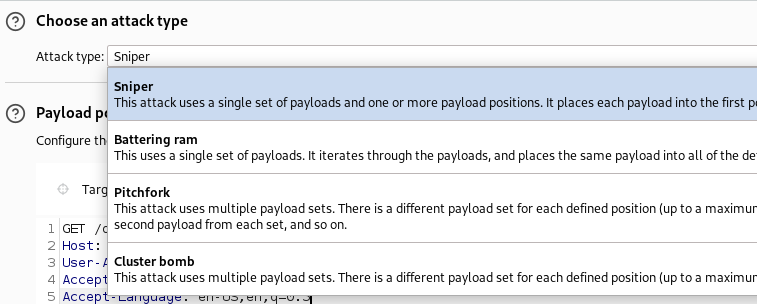


11. Do the same thing for the password like this. Do it sequentially; I will tell you why this is important later.

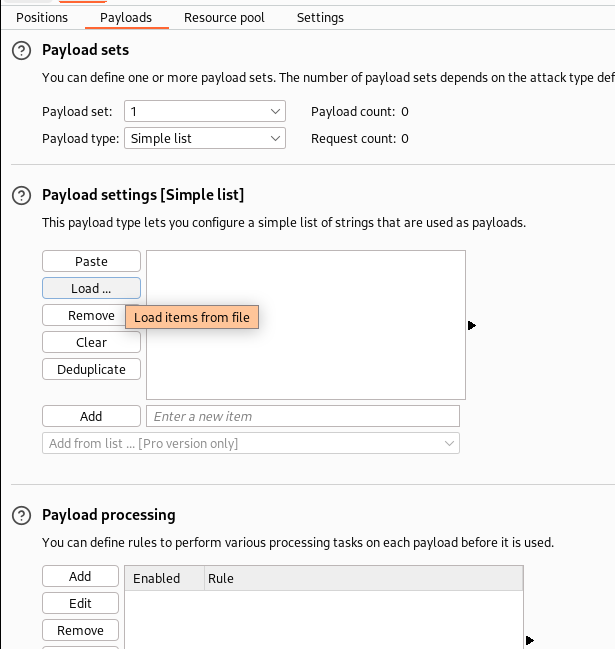
12. Because we are going to brute force in more than one parameter (password), choose the Cluster bomb in attack types.



12. Because we are going to brute force in more than one parameter (password), choose the Cluster bomb in attack types.

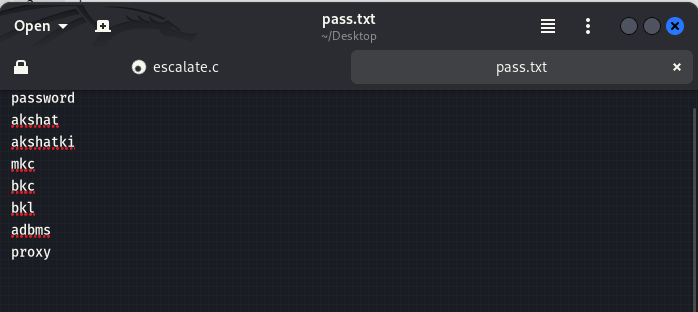


13. Next, go to the Payloads section, and look at the Payload set below; it will consist of two parameters, the first username and the second password. It is based on which position you add first.



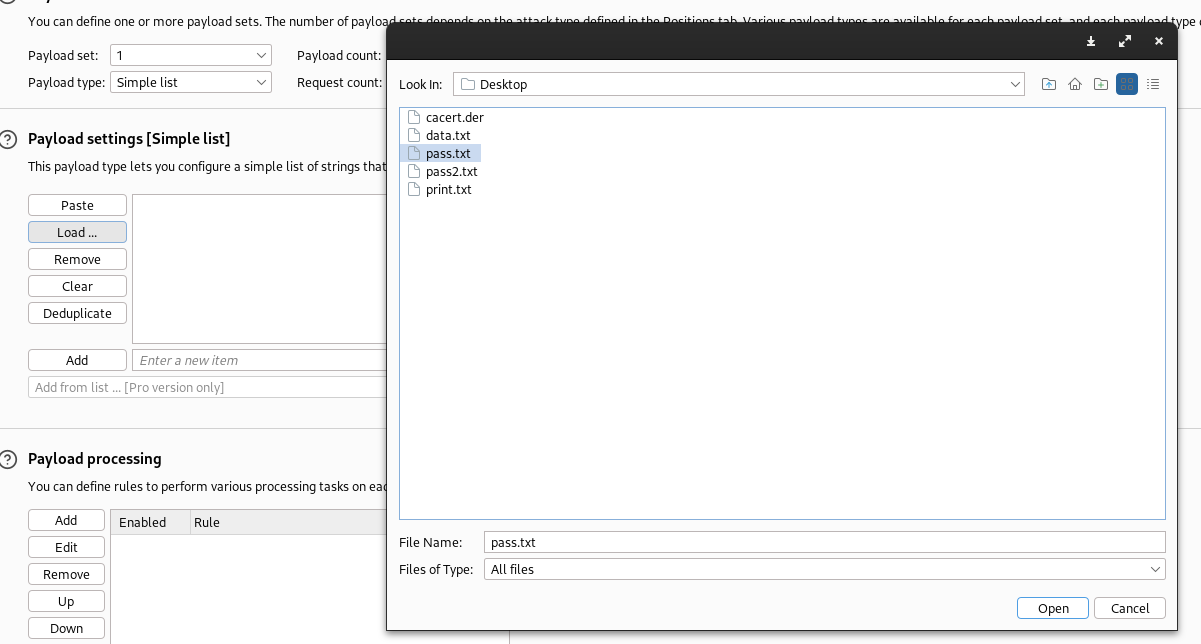
14. In the Payload set, you can enter the parameter manually or simply click load the file you download in my repo. As I said, the first parameter is the username, and the second is the password. The image below shows that I load the top-usernames into the first Payload.

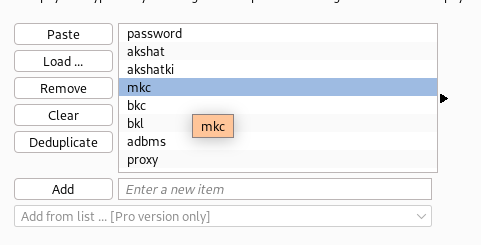
15. The output will be like this, and we can manually add it.



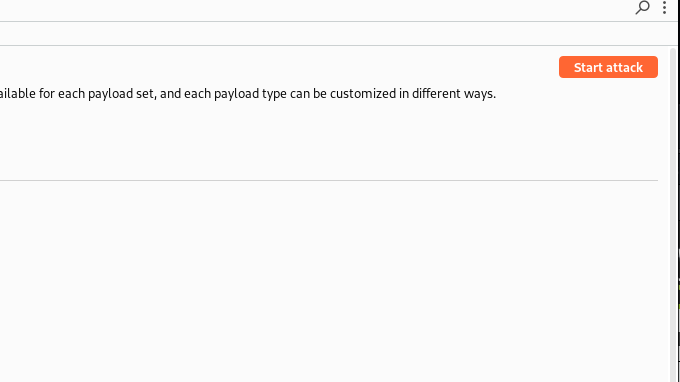
16. Next, we put the default password in the second parameter.

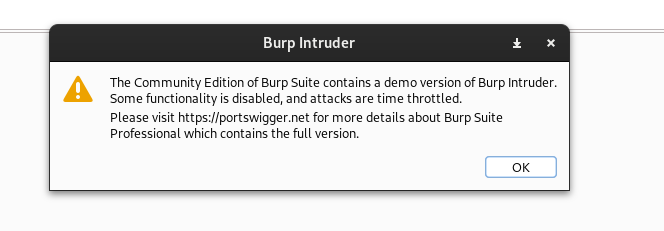
17. The bullet is already loaded into the weapon but before execution. See again; if you follow the steps correctly, it will show how many requests will be happened.



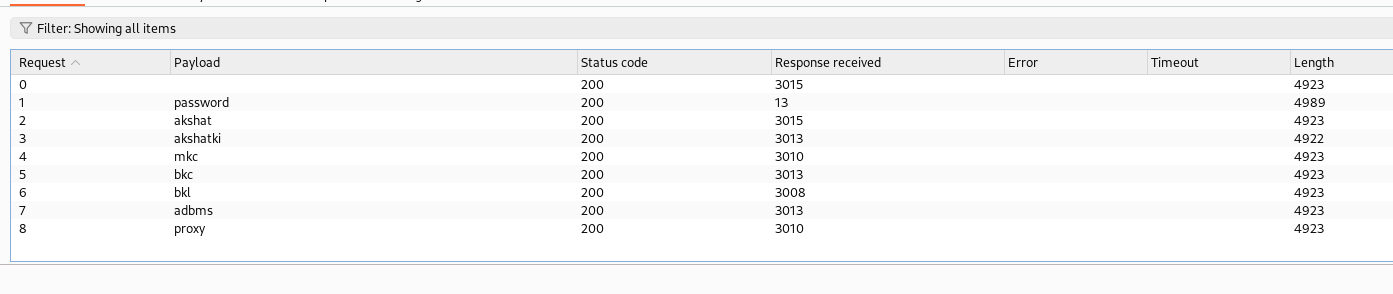


18. The brute force is starting, and it will take time.

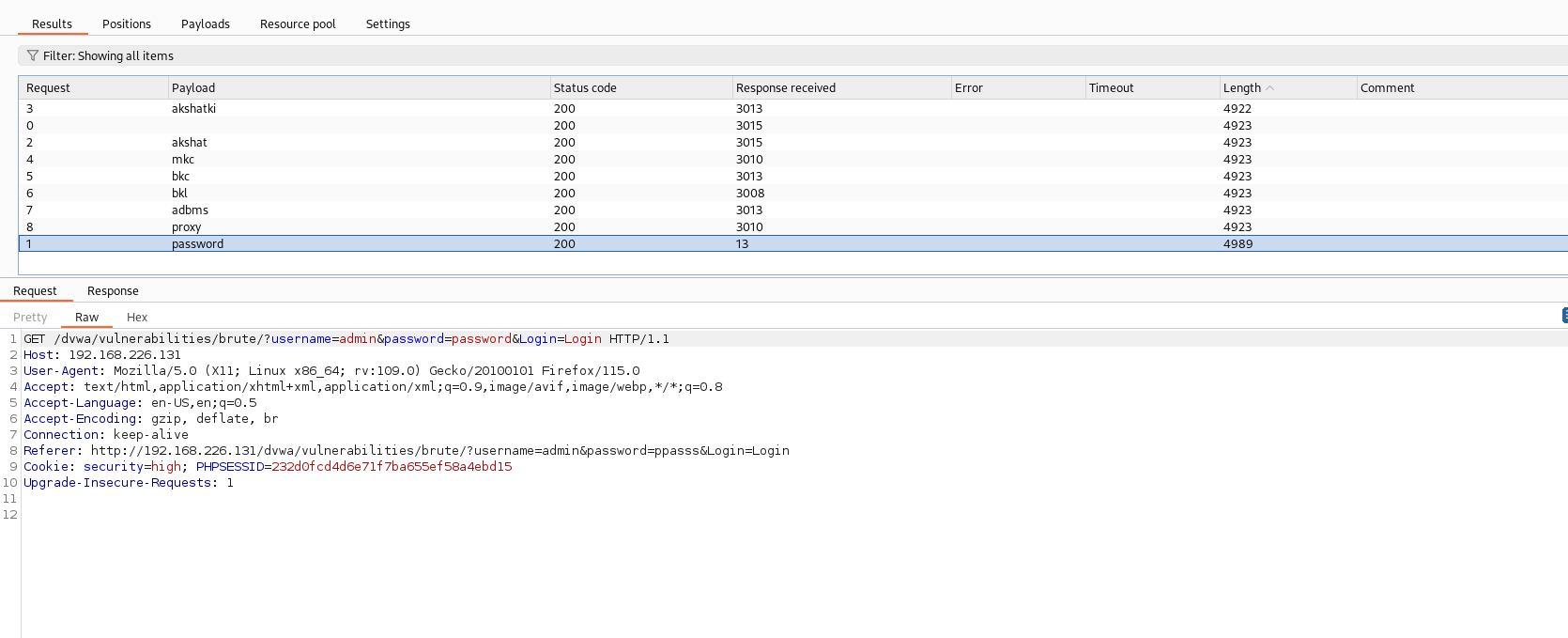


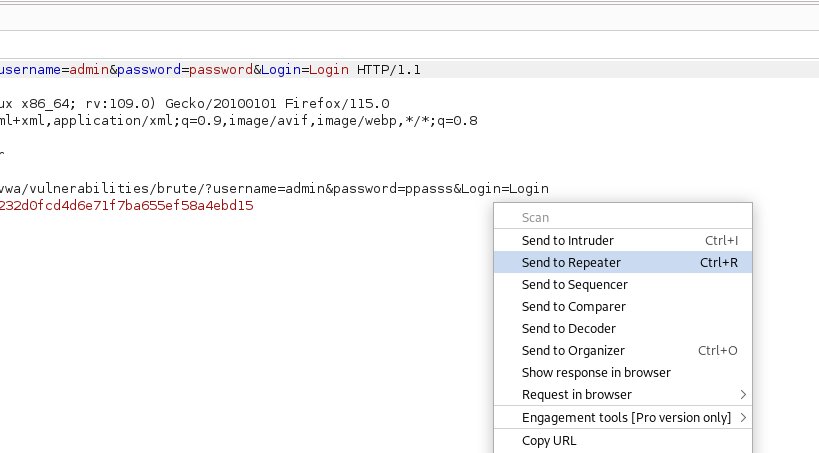


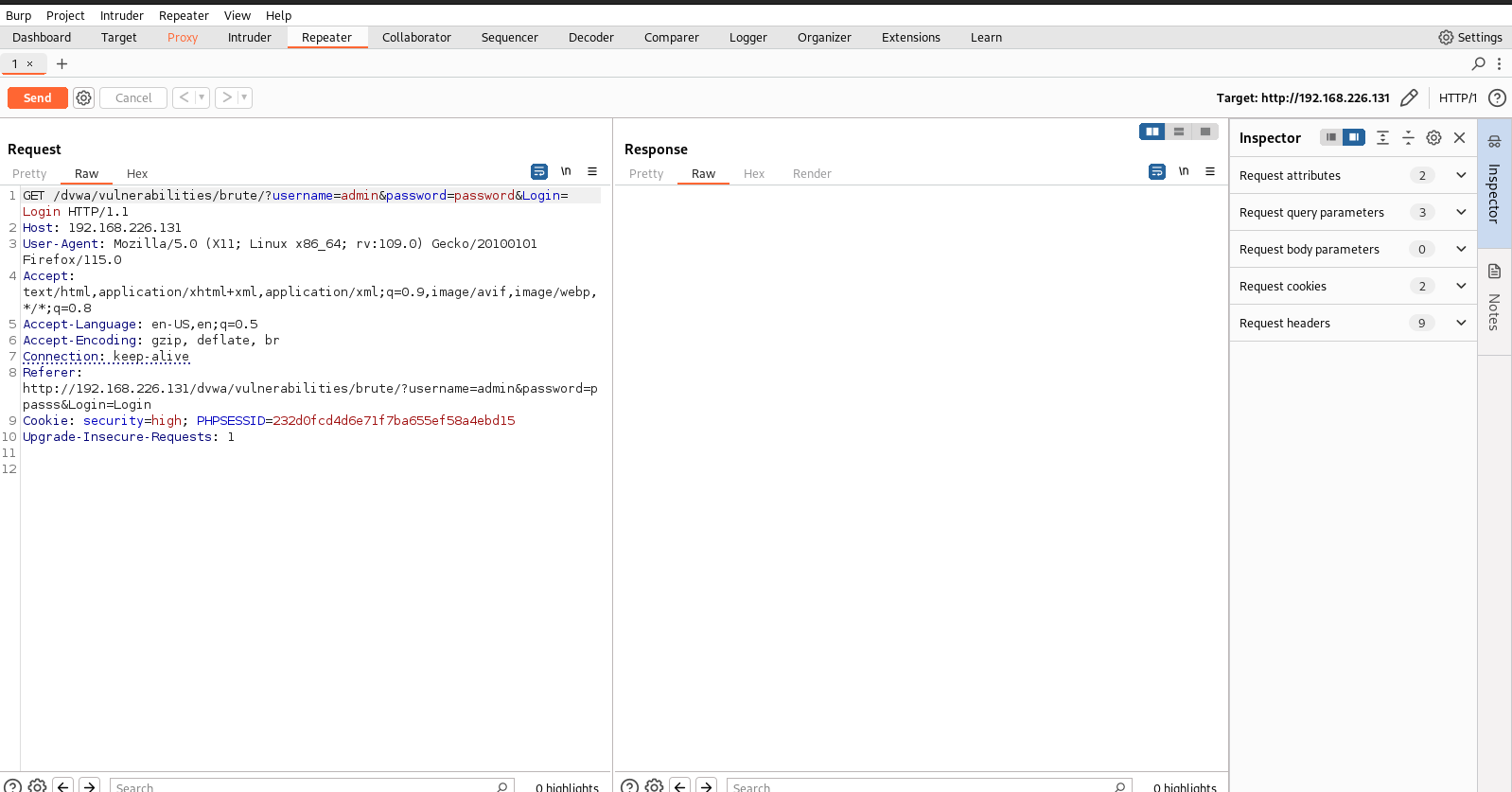
19. Look, everything is done below; the sign your brute force is a success or not is in the length section; if it shows a different length, it means the attack was a success.

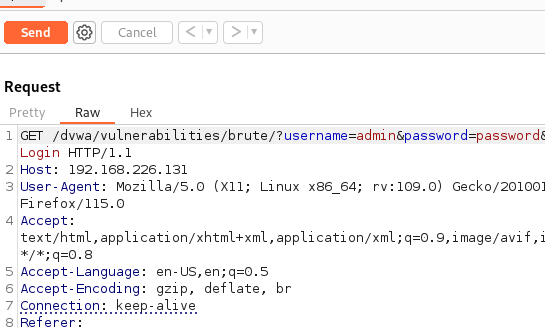


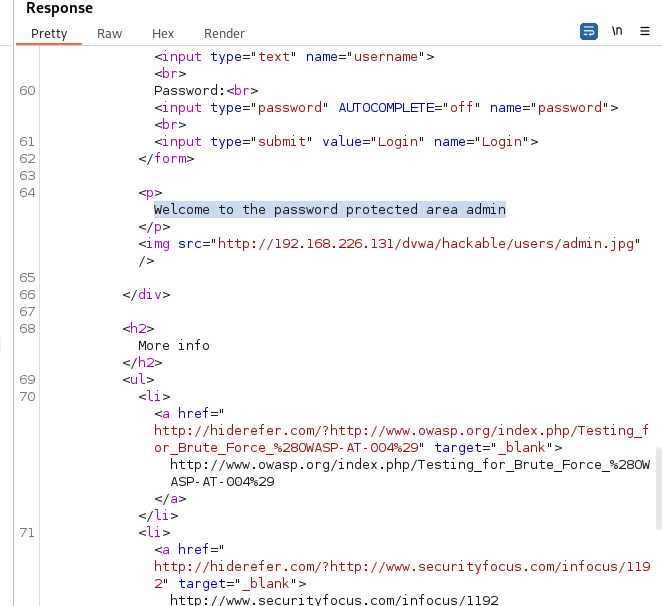
20. Because the length is different, look at the response or try login in using that account.

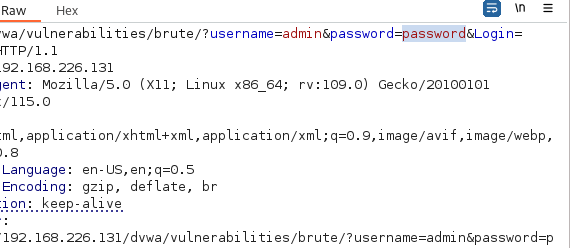


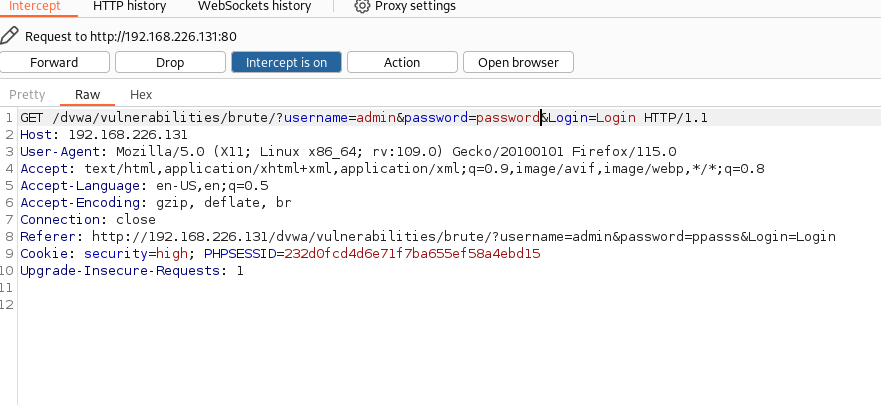


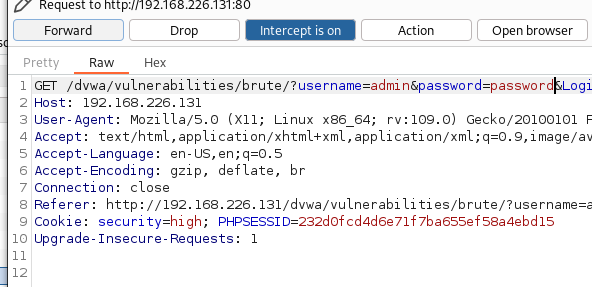


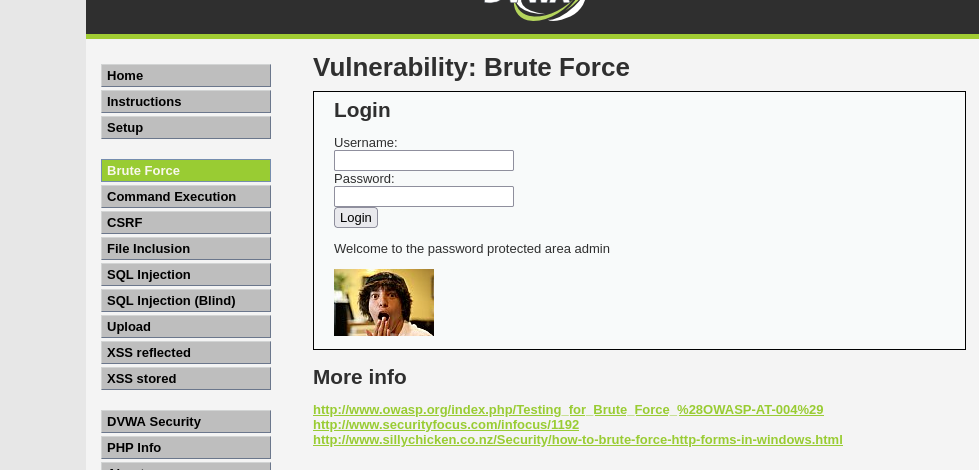












Congratulations, you are already making a brute-force attack.

*Congratulations, you are already making a brute-force attack.*