Flag 1 Solution:

Objective: Log in as admin to the website

Skills: Performing a brute force attack

Solution: Carry out a brute force attack to find the password. The login is the basic one, i.e. "admin".

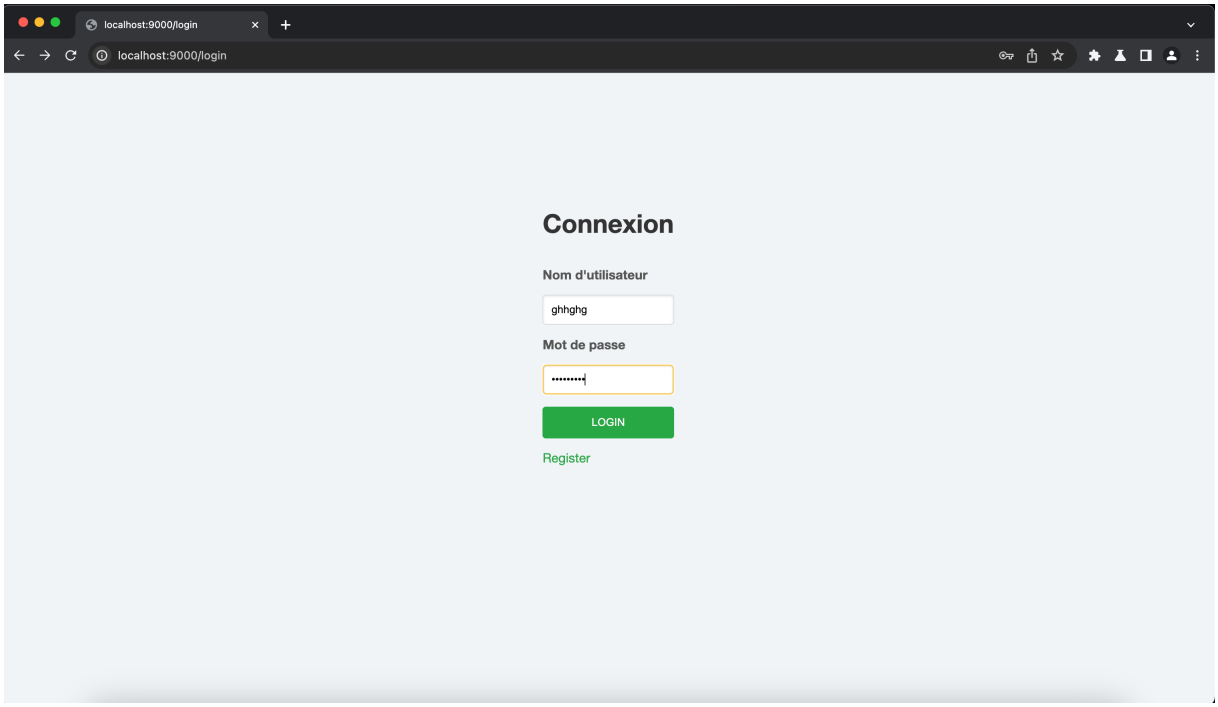
Suggested solution (other possibilities):

To carry out the Brute Force attack, we will use the "Burp" software, but other methods are possible using other tools (Hydra, John the Ripper, etc.).

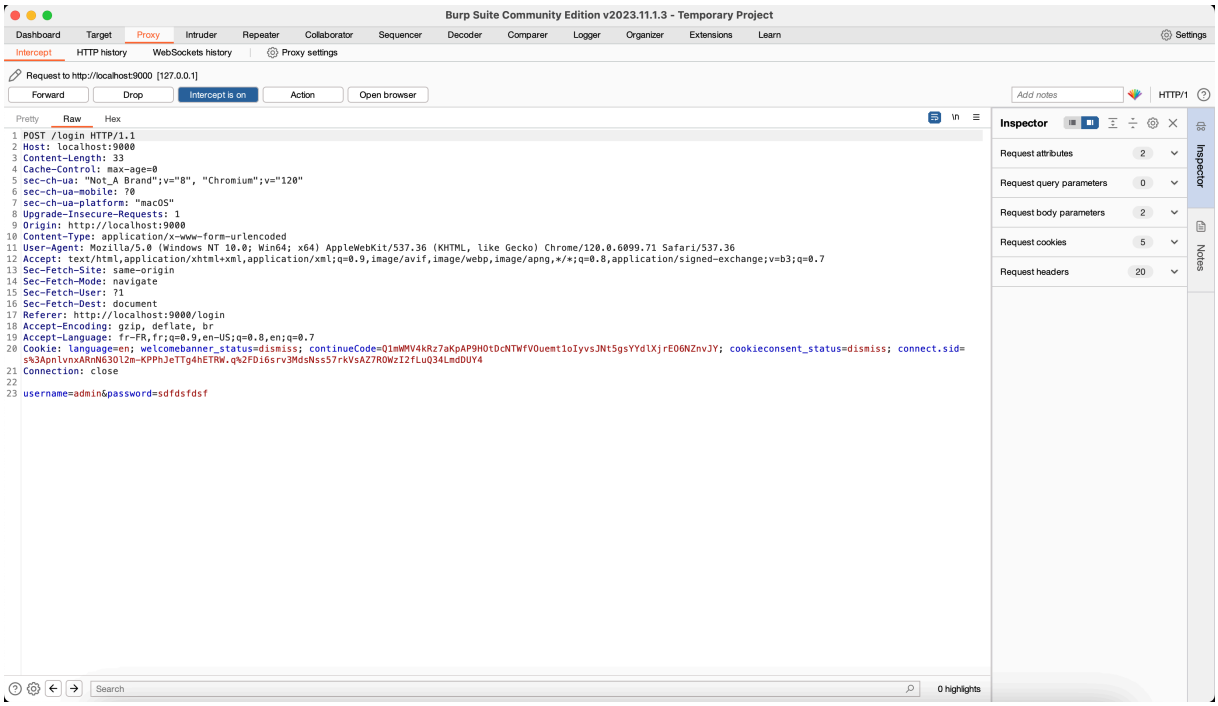
1/ Open Burp and go to the "Proxy" tab.
Click on "Open browser" and go to the website (here http://localhost:9000/).
Fa
2/ Then go to the login page on the website.

3/ Return to Burp to activate the "Intercept is on" option.

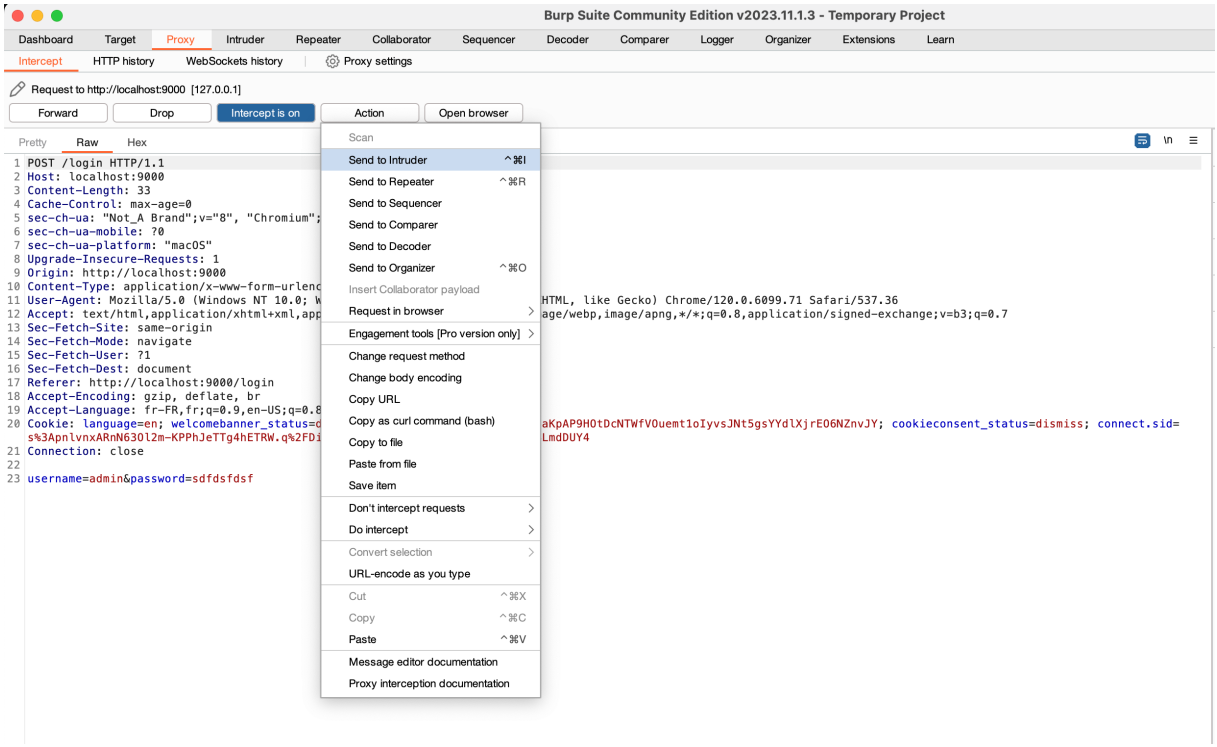
4/ Enter the login "admin" and any password. Then send the request by clicking on "login".



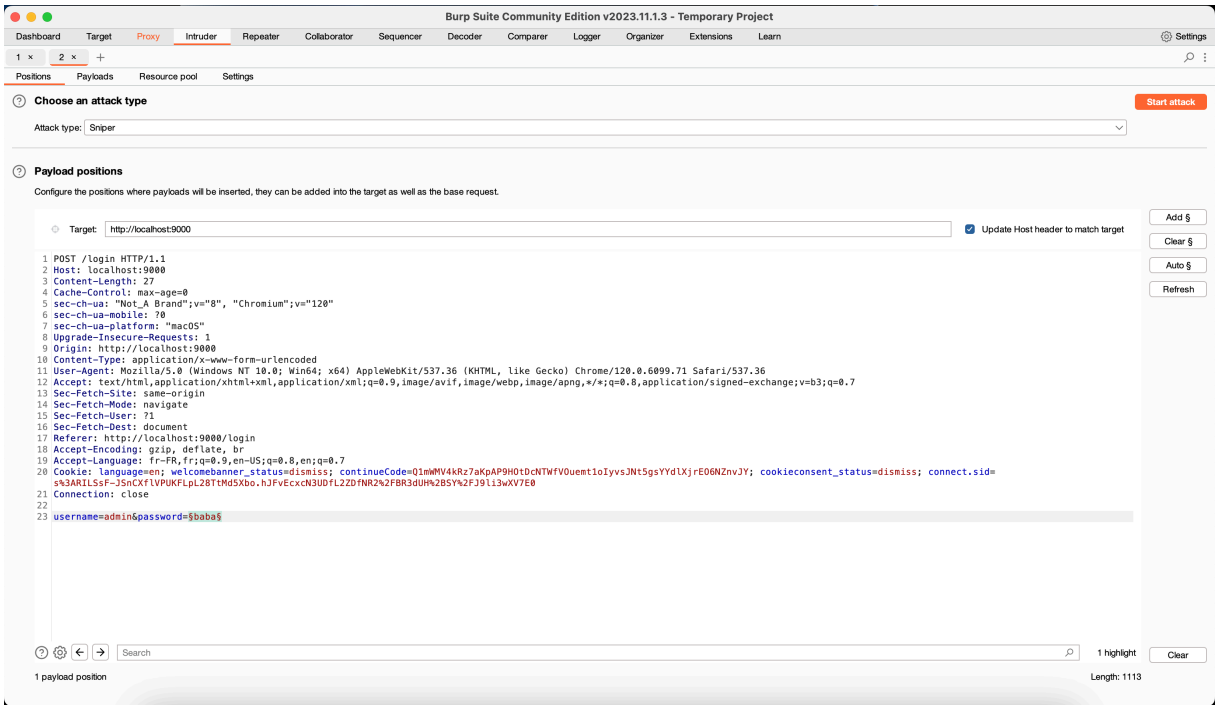
5/ When we return to Burp, we have intercepted the request with the login and password entered:



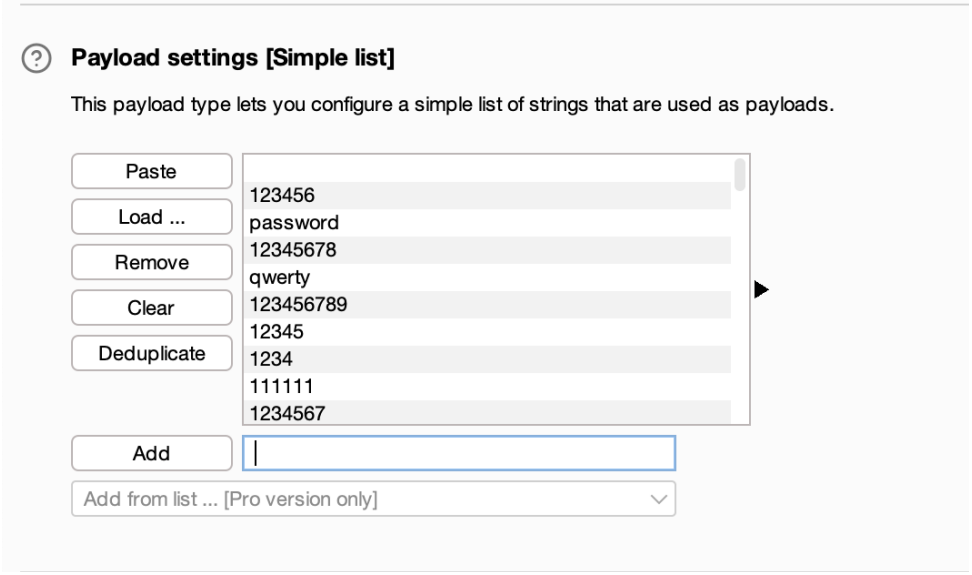
6/ Then click on "Send to Intruder":



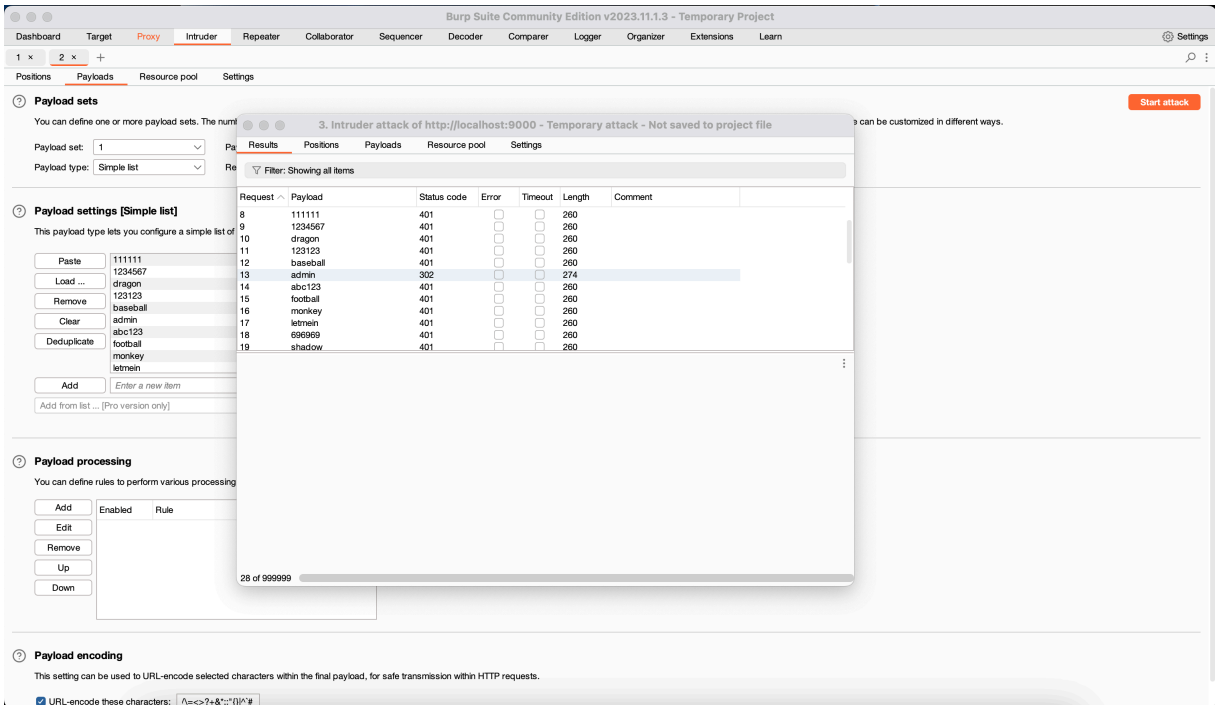
7/ Then go to the "Intruder" tab. Once on this tab, select the field you want to test and click on 'Add'.



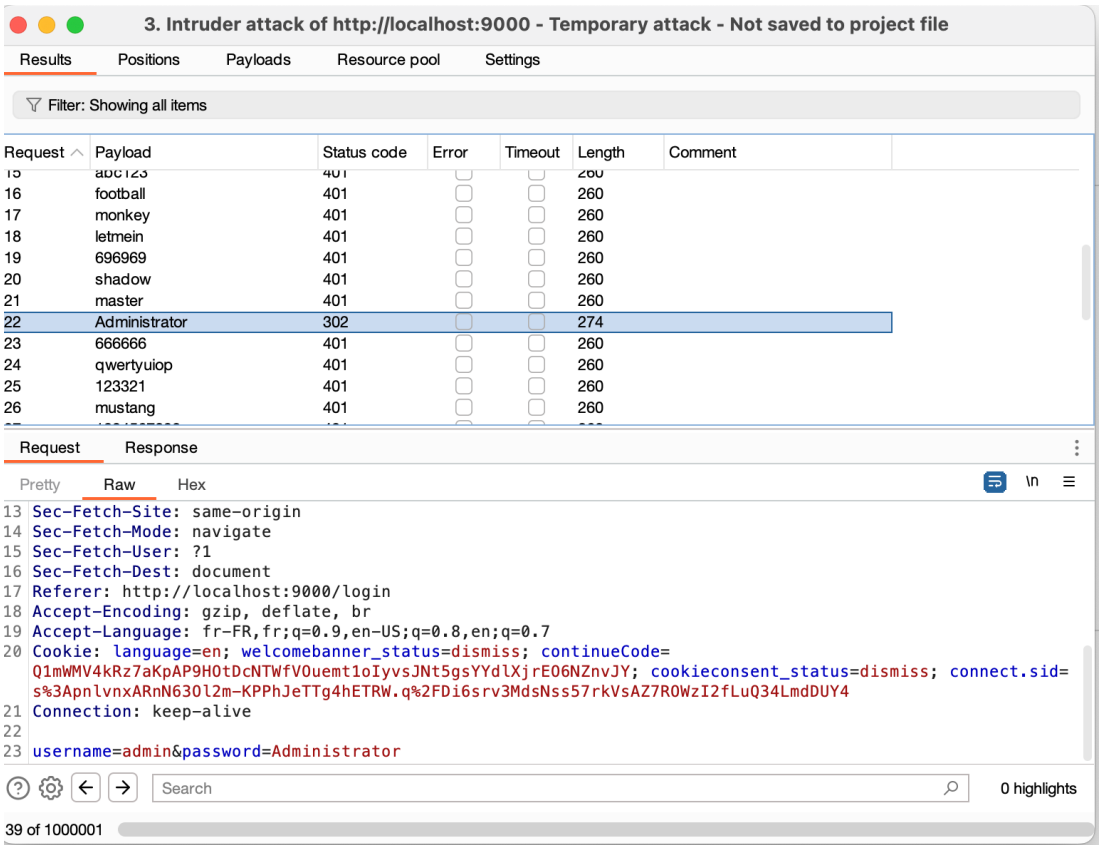
8/ Once this has been done, you need to go to "Payloads" and "Load..." a known password file (as supplied in the solution).



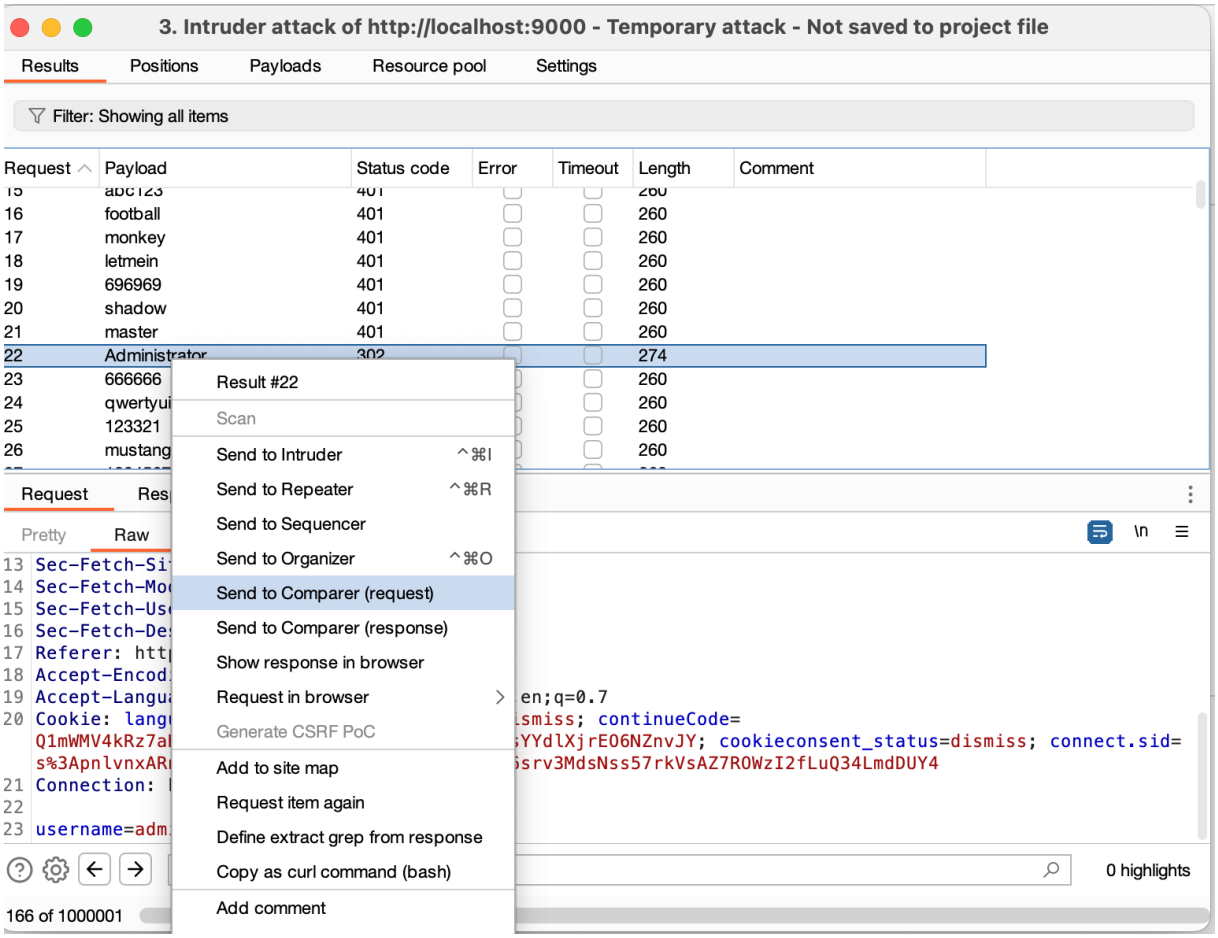
9/ You can then launch the Brute Force attack by clicking on "Start attack".

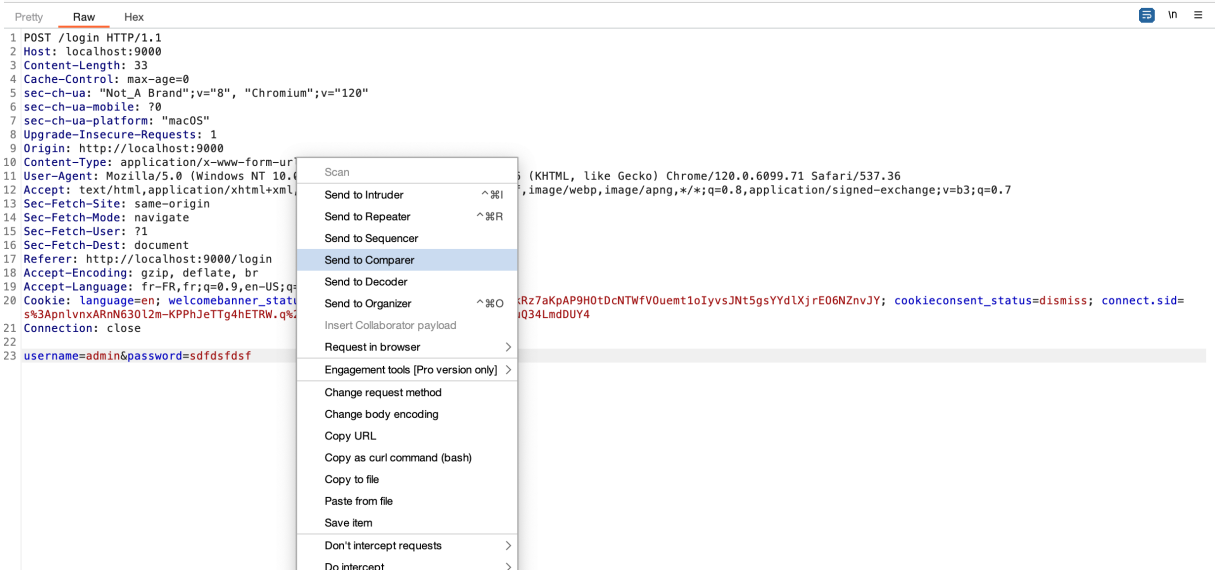


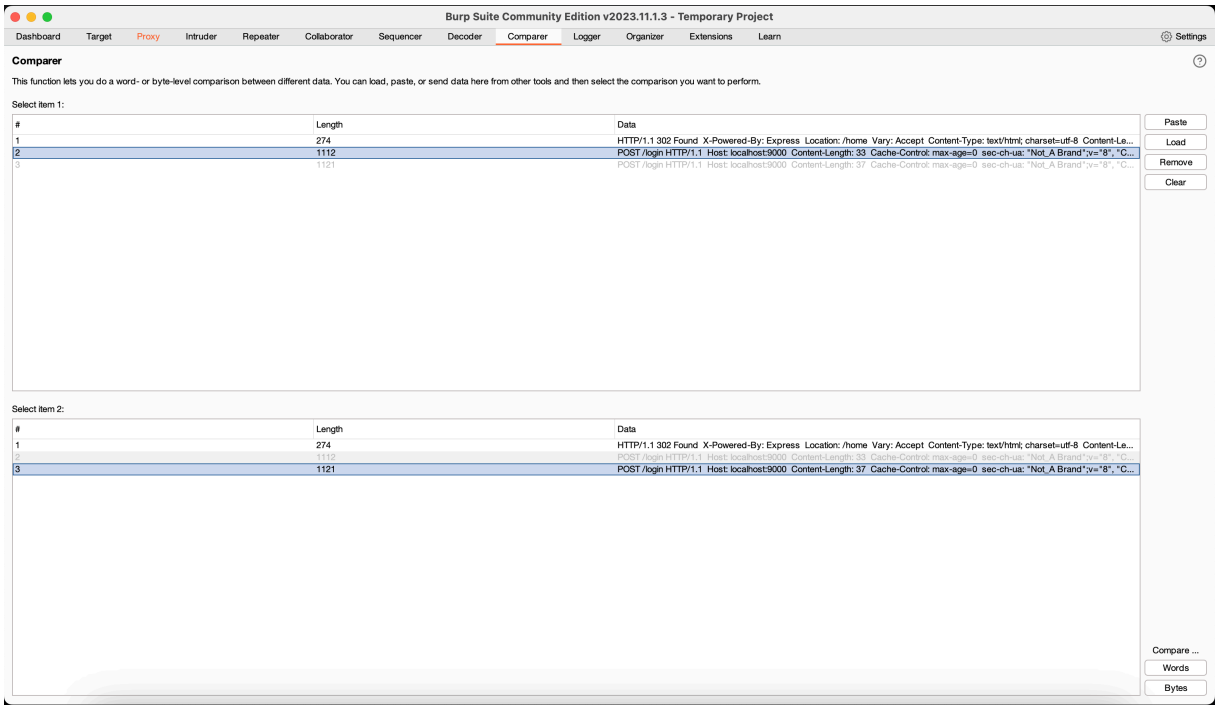
10/ The brute force attack is launched and tests all the passwords in the file as it goes along, as can be seen.
During the attack, you may notice that one of the status codes differs. This indicates that the tested password has worked in connection with the login tested.



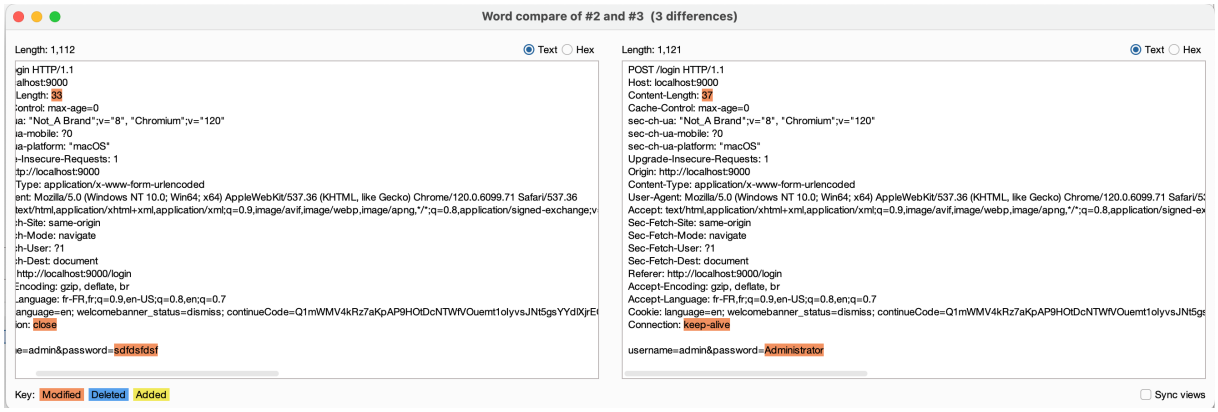
11/ You can then "Send to Comparer" using the password you obtained and the one you initially tested from the website.







12/ When we compare the answers obtained with the "Compare" function, we see that the connection is maintained with the "Administrator" password, whereas it is closed with the wrong password.



13/ Then, when you test the "administrator" password from the website, you manage to connect as admin and a message appears saying that you've found Flag_1!