

Get A Head

Inspecting the webpage, we get

The method that was used for Red was "GET" and for Blue was "POST".

Checking out the webpage we get

```
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Content-type: text/html; charset=UTF-8
3
4
5 <!doctype html>
6 <html>
7 <head>
8   <title>
9     Blue
10   </title>
11   <link rel="stylesheet" type="text/css" href="//maxcdn.boot
12 </link>
13   <style>
14     body{
15       background-color:blue;
16     }
17   </style>
18 </head>
19 <body>
20   <div class="container">
21     <div class="row">
22       <div class="col-md-6">
23         <div class="panel panel-primary" style="margin-top:50px">
24           <div class="panel-heading">
25             <h3 class="panel-title" style="color:red">
26               Red
27             </h3>
28           </div>
29           <div class="panel-body">
30             <form action="index.php" method="GET">
31               <input type="submit" value="Choose Red"/>
32             </form>
33           </div>
34         </div>
35       </div>
36       <div class="col-md-6">
37         <div class="panel panel-primary" style="margin-top:50px">
38           <div class="panel-heading">
```

By using Burp Suite can intercept and change requests. Looking through the list, we see that the second request method is "HEAD" which seems quite familiar.

If we look back at the challenge title "Get aHead", the word Head stands out, probably referring to the HTTP Request method "HEAD".

```
Request
Pretty Raw Hex \n
1 POST /index.php HTTP/1.1
2 Host: mercury.picoctf.net:53554
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
4 Gecko/20100101 Firefox/78.0
5 Accept:
6 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 0
11 Origin: http://mercury.picoctf.net:53554
12 Connection: close
13 Referer: http://mercury.picoctf.net:53554/
14 Upgrade-Insecure-Requests: 1
```

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender	Project options	User options
Intercept	HTTP history	WebSockets history	Options								
Filter: Hiding CSS, image and general binary content											
# ^	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	
1	http://mercury.picoctf.net:53554	GET	/			200	1123	HTML		Red	
2	https://www.youtube.com	POST	/api/stats/qoe?fmt=136&afmt=251&cp...	✓		204	599	HTML			
3	http://mercury.picoctf.net:53554	GET	/			200	1123	HTML		Red	
4	http://mercury.picoctf.net:53554	GET	/index.php?			200	1123	HTML	php	Red	
5	http://mercury.picoctf.net:53554	POST	/index.php			200	1125	HTML	php	Blue	
6	http://mercury.picoctf.net:53554	POST	/index.php			200	1125	HTML	php	Blue	
7	http://mercury.picoctf.net:53554	GET	/			200	1123	HTML		Red	
8	http://mercury.picoctf.net:53554	GET	/								

Send Post request to Repeater and Change POST to HEAD

p Suite Community E... picoCTF - picoGym - Mo...

picoCTF - picoGym - Mozilla Firefox

Burp Suite Community Edition v2021.8.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project optio

1 x 2 x 3 x ...

Send Cancel < >

Request

Pretty Raw Hex \n

```

1 HEAD /index.php HTTP/1.1
2 Host: mercury.picoctf.net:53554
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/web
  p,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 0
9 Origin: http://mercury.picoctf.net:53554
10 Connection: close
11 Referer: http://mercury.picoctf.net:53554/
12 Upgrade-Insecure-Requests: 1
13
14

```

Response

Pretty Raw Hex Render \n

```

1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4l1ty_2e5ba39f}
3 Content-type: text/html; charset=UTF-8
4
5

```

GET aHEAD

| 20 points

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:53554/>

Hints

1 2

Maybe you have more than 2 choices

17,575 solves / 30,194 attempts (58%)

81% Liked

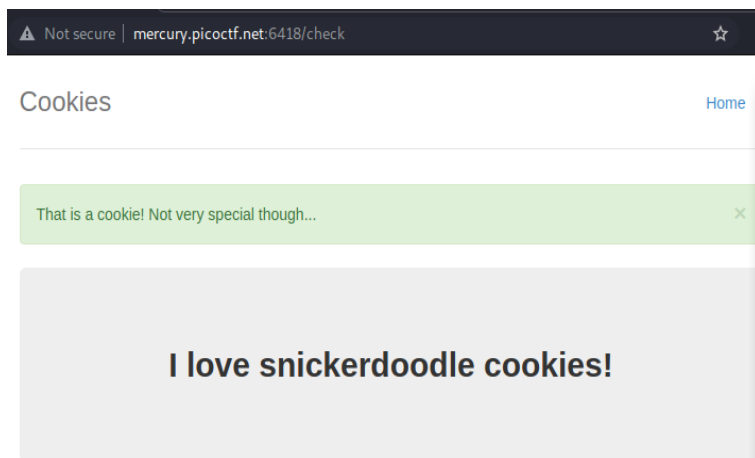
picoCTF{r3j3ct_th3_du4l1ty_2e5ba39f}

Submit Flag

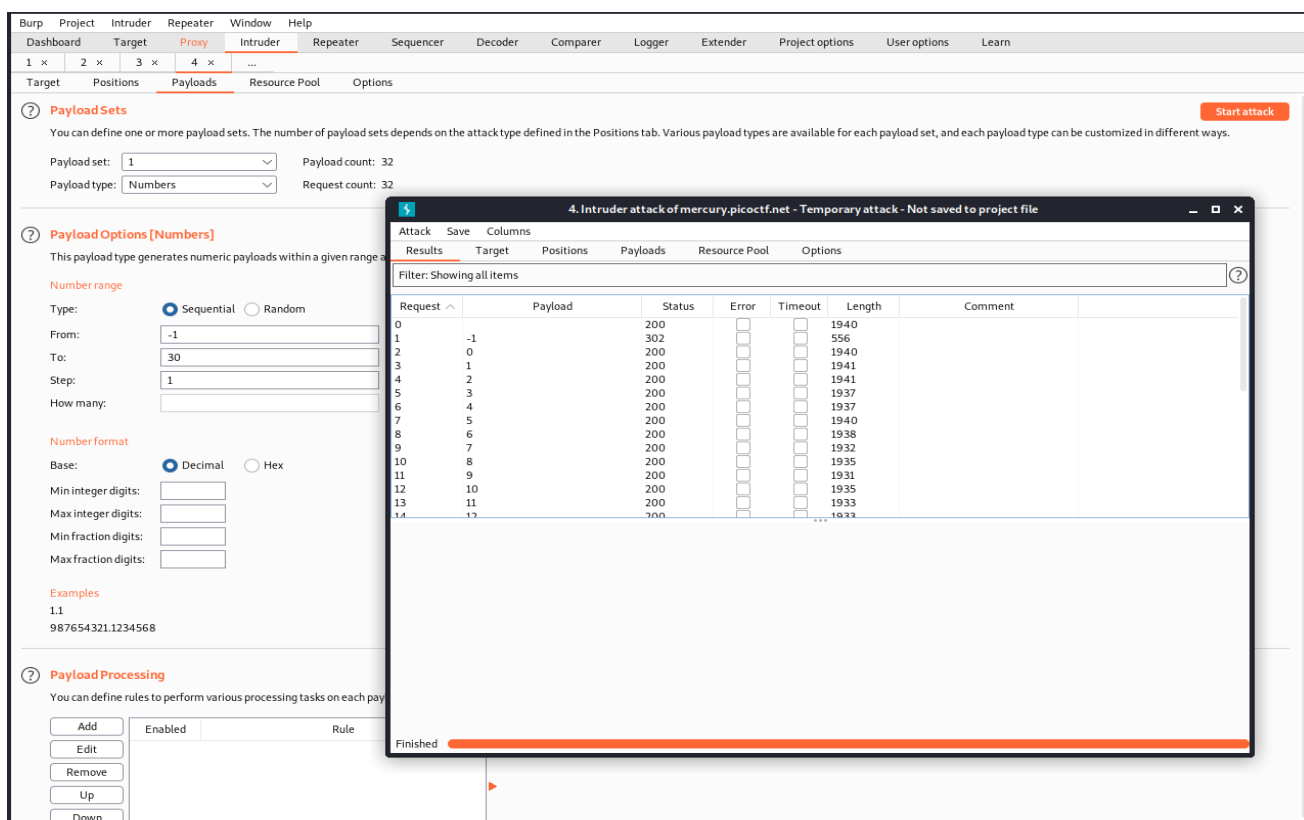
Cookies

Looking at the website provided, if we try to enter an input, it would prompt us that the input is invalid.

If we use the placeholder text snickerdoodle we see that it gives us a page where the text is set to I love snickerdoodle cookies.

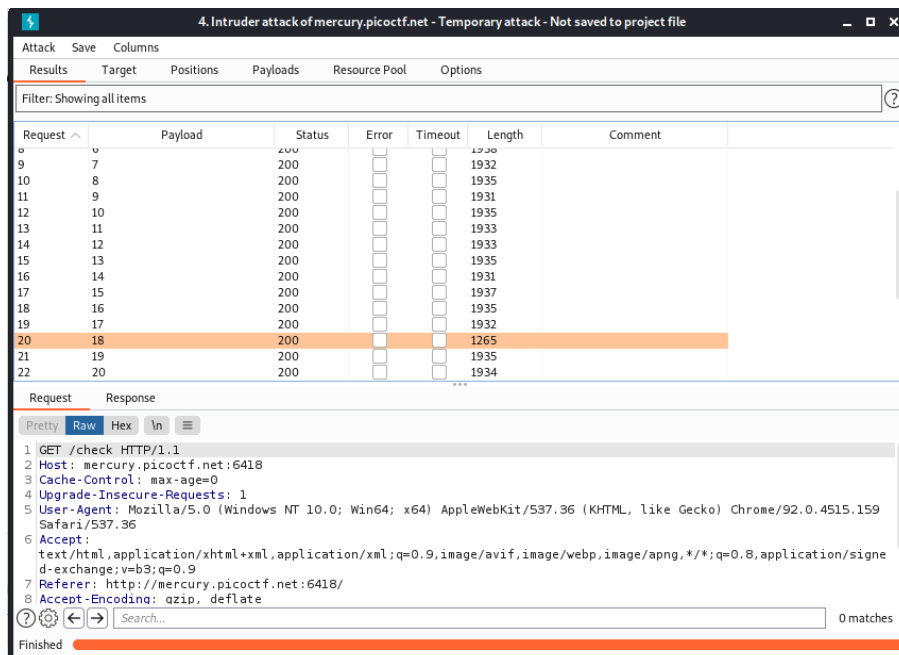


Looking at the cookie set after entering snickerdoodle we see that it has a value of 0. By testing around and changing the cookie value to 1, 2 etc. we see that it outputs a different name. My guess is that a certain cookie value will return us the flag.

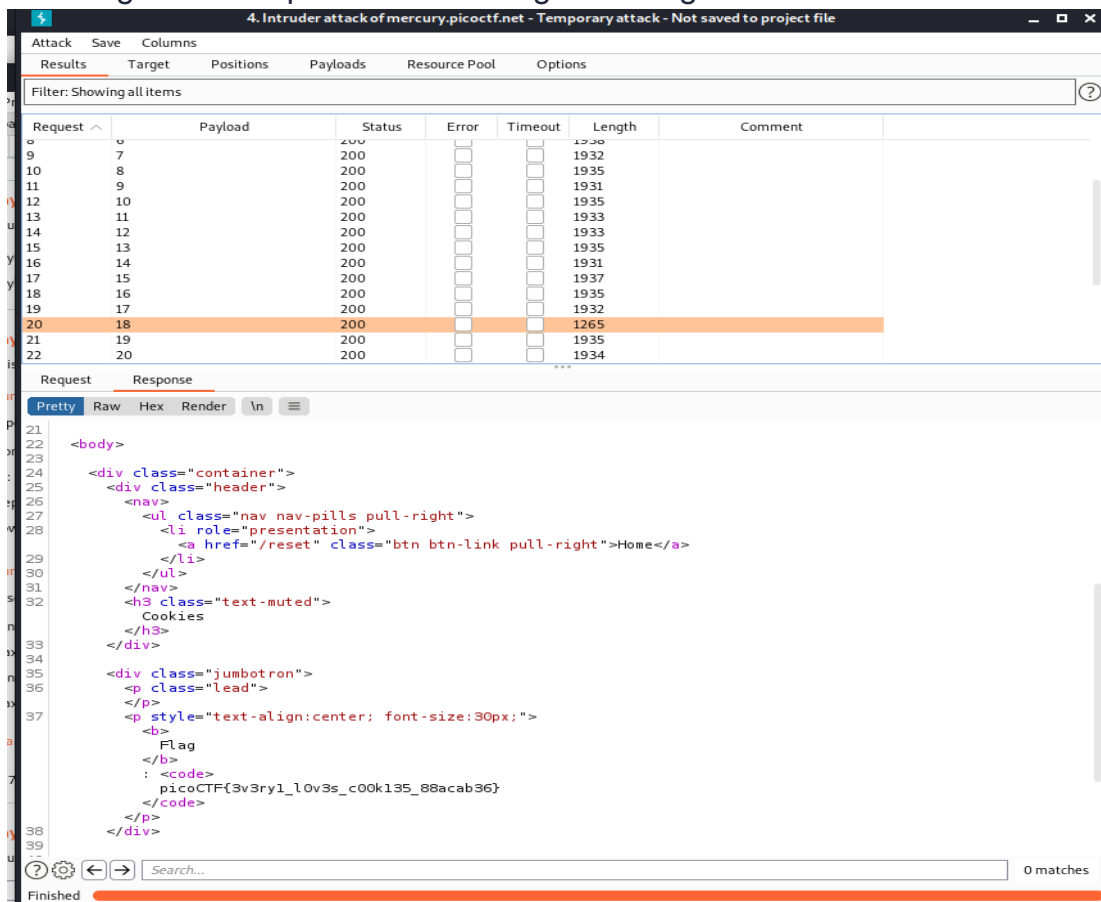


We use the payload form -1 to 30 to give different decimal values.

Checking unusual value at 20 (1265)



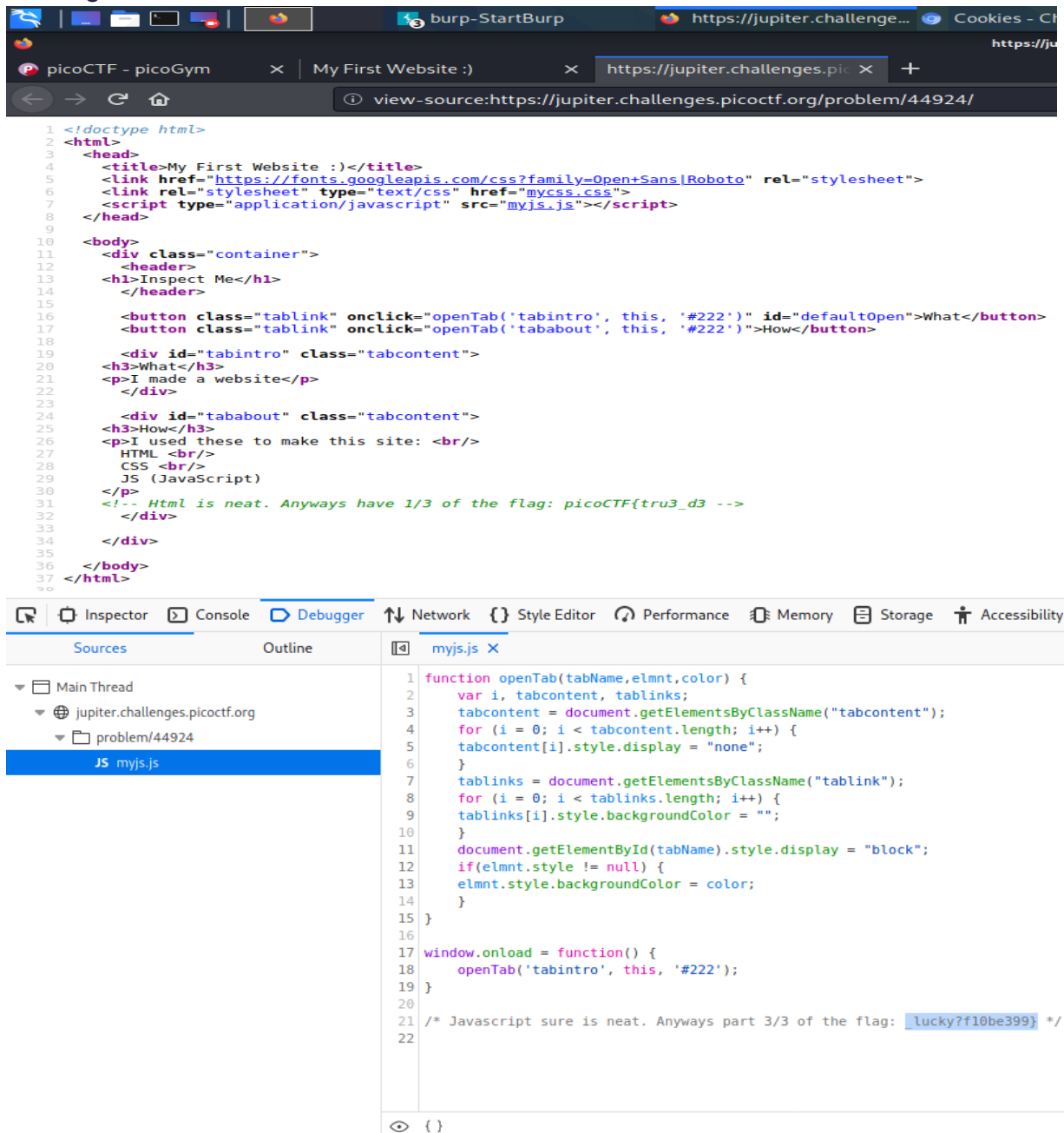
Scrolling down Request section we get the flag.

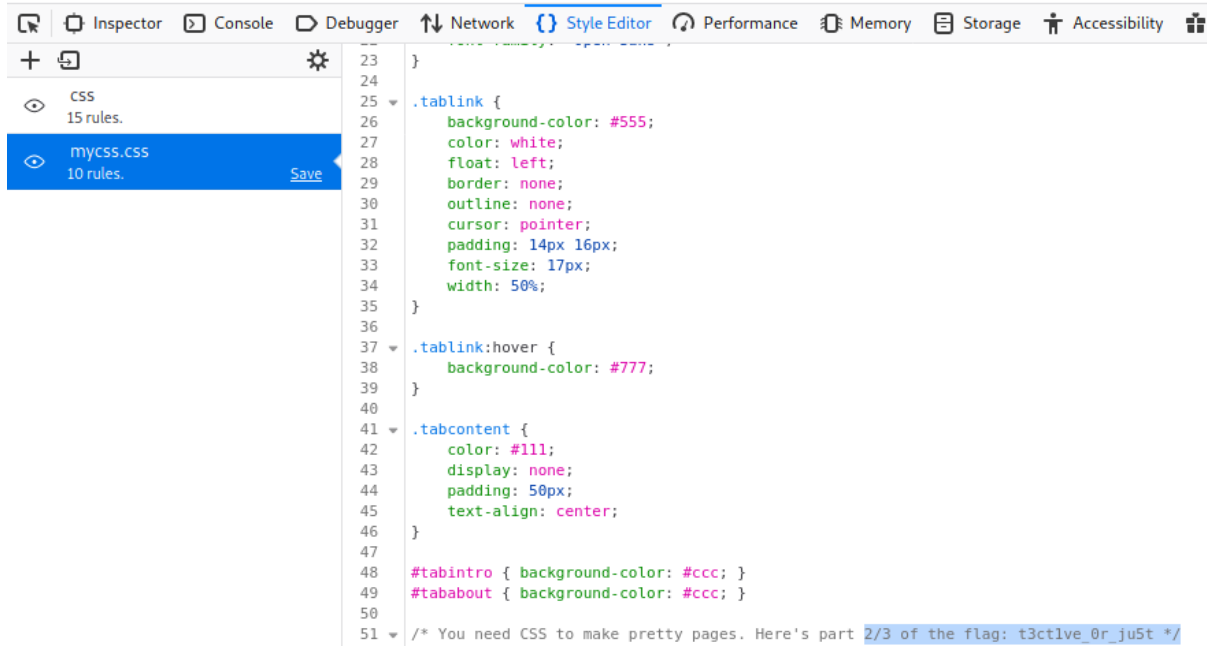


Insp3ct0r

The website has not much content. We are hinted by the problem statement to "inspect" the site. Using a browser's developer tools, we can see the source code of the site.

On Firefox, the Inspect Element option, which can be found by right clicking or Ctrl+Shift+C on Windows, Cmd+Shift+C on Linux/MacOS. We then go to the Source tab and view the index.html, mycss.css, and myjs.js files, each containing a part of the flag.

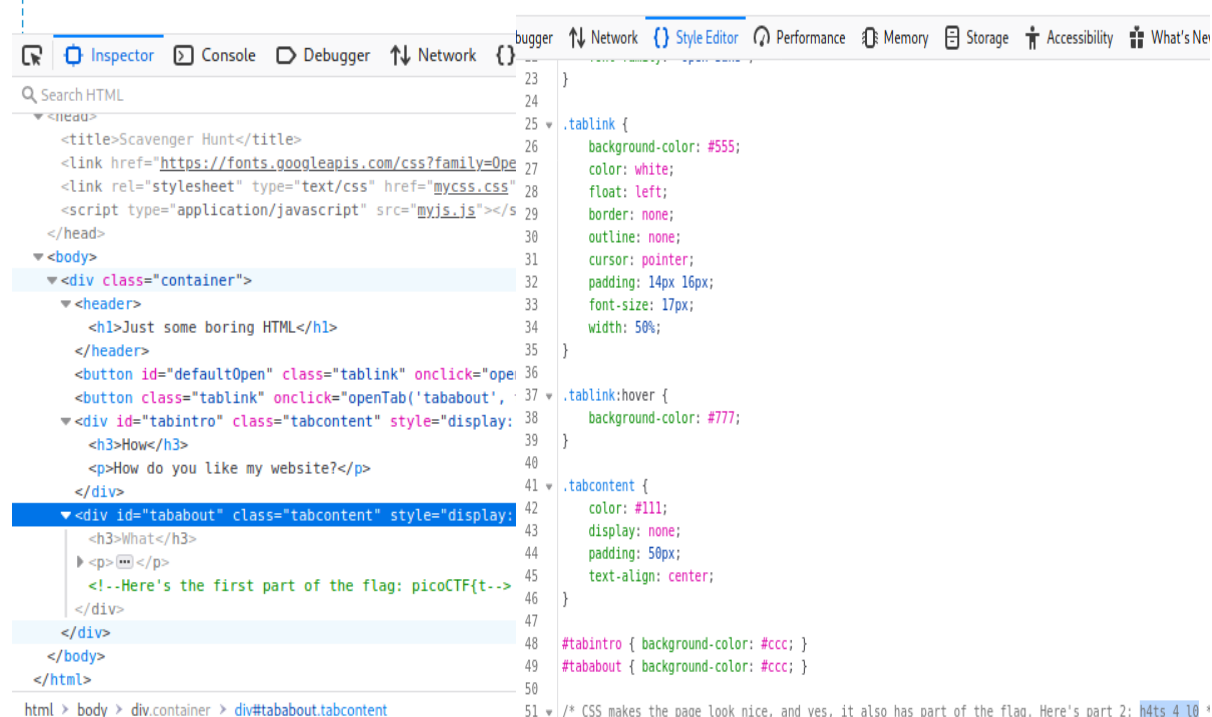




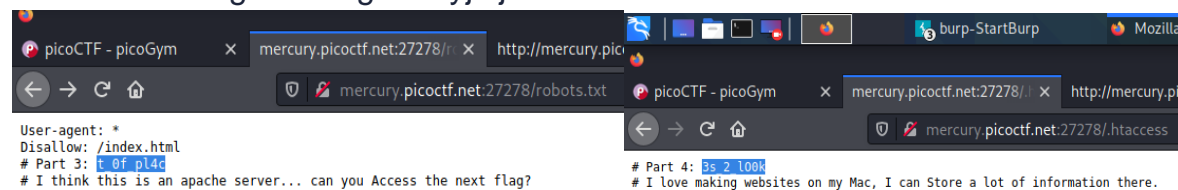
Scavenger Hunt

Clicking on the link brings us to Html page

Ctrl + Shift + I will show the source code of the page. It gives us the first part of the flag. Next, there are some files linked to it like the CSS and JS.

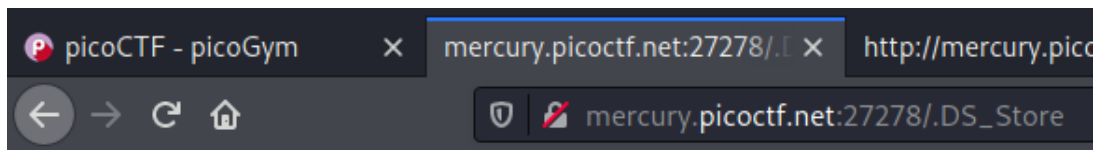


I searched up "index website on google" and it brought up things about web crawlers. This made me think it's possible a robots exclusion file (robots.txt) might have something. I changed myjs.js to robots.txt





The .htaccess file manages Apache server permissions. Replacing robots.txt with .htaccess got a half flag.

In Macs, a .DS_Store file stores the configurations for how the desktop looks (eg. icon location, etc.) Changing .htaccess with .DS_Store got another half of flag



Congrats! You completed the scavenger hunt. Part 5: _a69684fd}

Scavenger Hunt

 | 50 points 

Tags: Category: Web Exploitation

AUTHOR: MADSTACKS

Hints

Description

1

There is some interesting information hidden around this site
<http://mercury.picoctf.net:27278/>. Can you find it?

10,672 solves / 38,620 attempts (28%)

 59% Liked 

 picoCTF{th4ts_4_l0t_0f_pl4c3s_2_l00k_a69684fd}

Submit Flag