

LinkedIn: [Kelvin Kimotho](#)

Scavenger Hunt



Easy

Web Exploitation

picoCTF 2021

AUTHOR: MADSTACKS

Description

There is some interesting information hidden around this site <http://mercury.picoctf.net:39698/>. Can you find it?

Hints

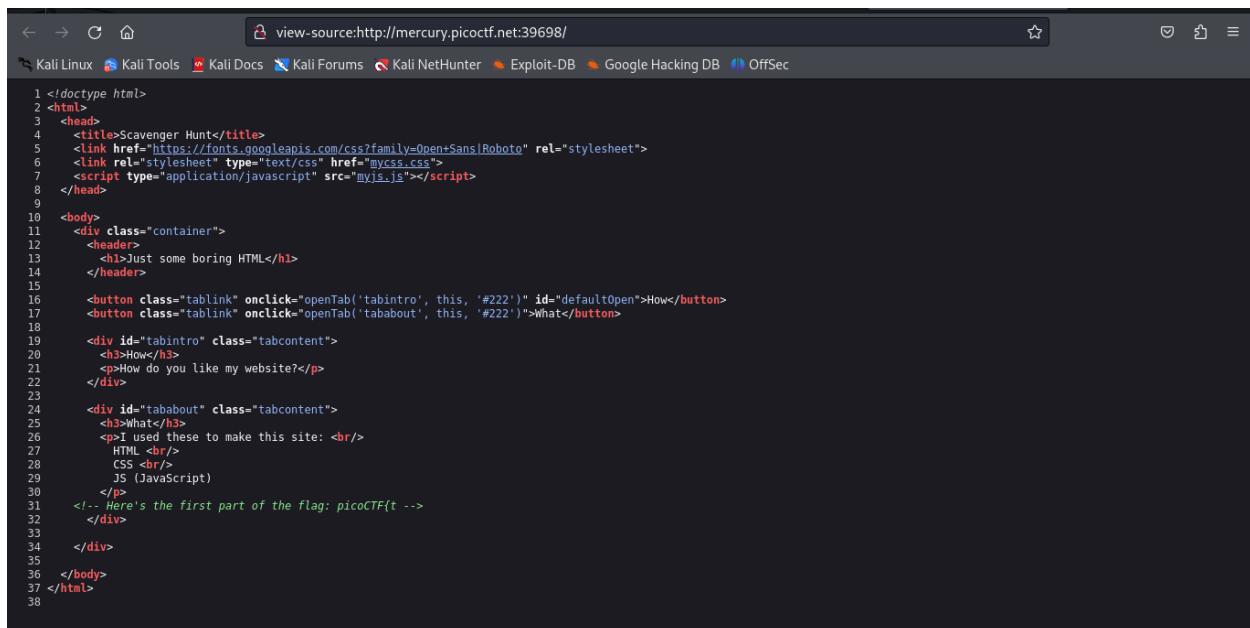
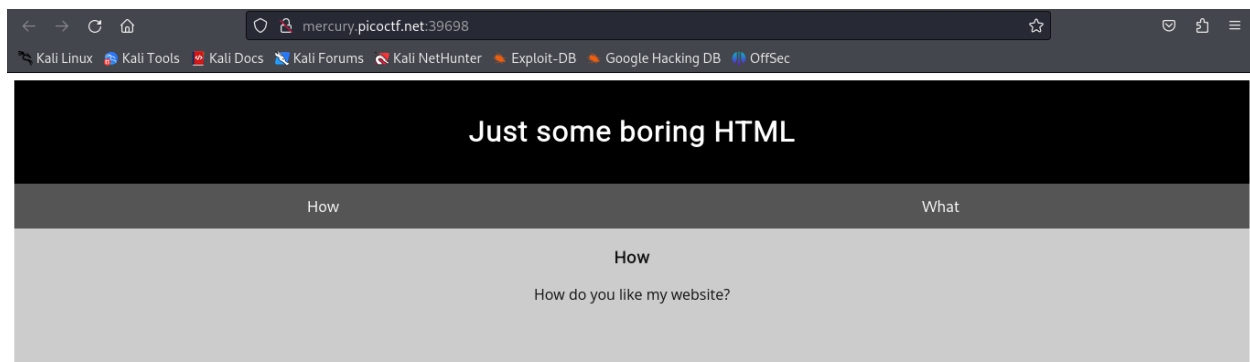
1

You should have enough hints to find the files, don't run a brute forcer.

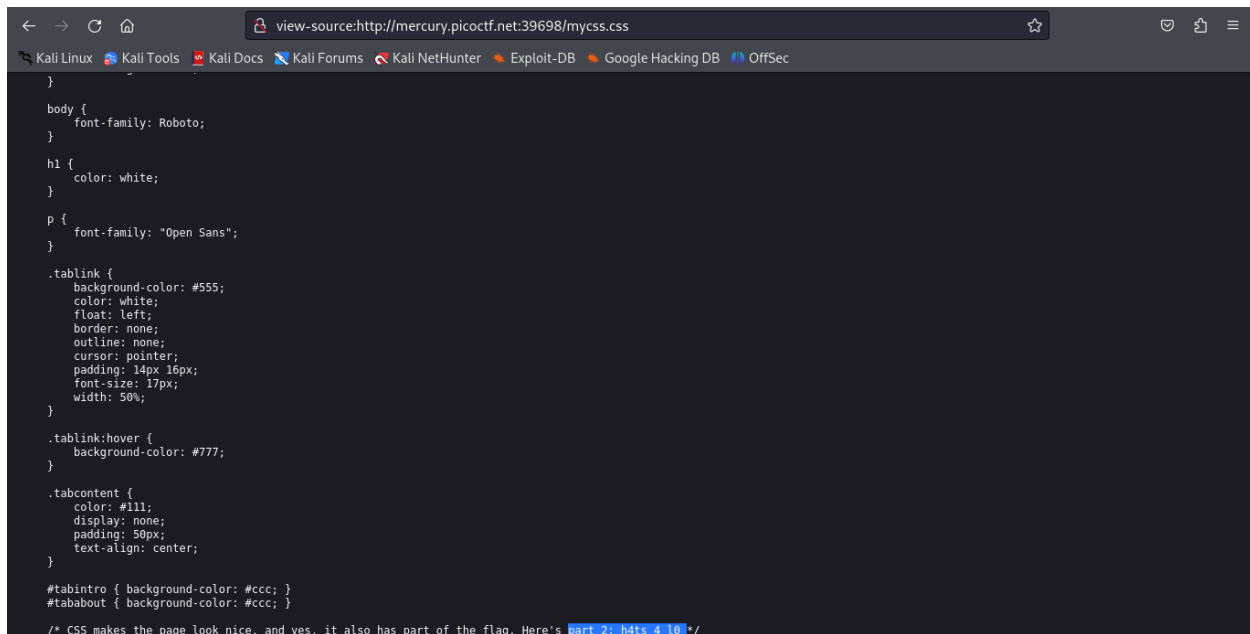
Solution

From the description, I went ahead investigating the site, all the aspects of a website i.e. Examining the **source code**, **robots.txt** contents etc.

The first step was examining the html code where i discovered a segment of the flag **picoCTF{t**



I went ahead examining CSS code used to style html components in a web page. I also discovered a fragment **h4ts_4_10.**”



```
view-source:http://mercury.picocftf.net:39698/mycss.css

body {
  font-family: Roboto;
}

h1 {
  color: white;
}

p {
  font-family: "Open Sans";
}

.tablink {
  background-color: #555;
  color: white;
  float: left;
  border: none;
  outline: none;
  cursor: pointer;
  padding: 14px 16px;
  font-size: 17px;
  width: 50%;
}

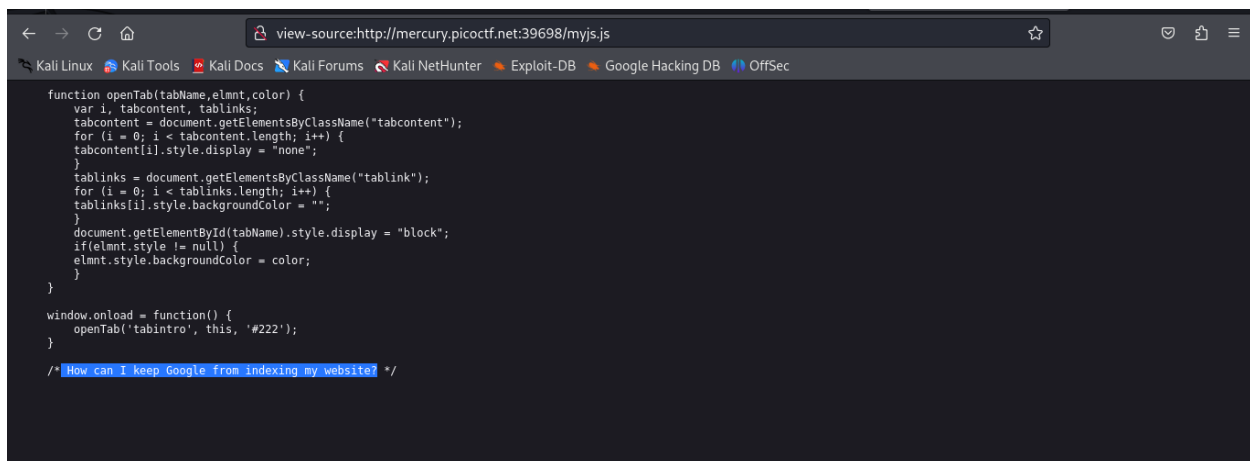
.tablink:hover {
  background-color: #777;
}

.tabcontent {
  color: #111;
  display: none;
  padding: 50px;
  text-align: center;
}

#tabintro { background-color: #ccc; }
#tababout { background-color: #ccc; }

/* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts 4 l0 */
```

Examining the JavaScript source code only revealed a hint ” **How can I keep Google from indexing my website?**”. JavaScript adds functionality making the pages dynamic.



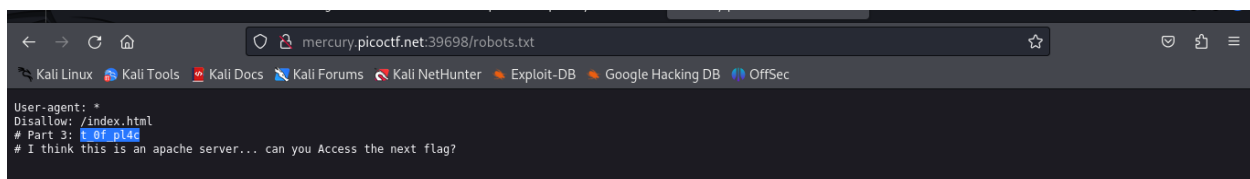
```
view-source:http://mercury.picocftf.net:39698/myjs.js

function openTab(tabName,elmnt,color) {
  var i, tabcontent, tablinks;
  tabcontent = document.getElementsByClassName("tabcontent");
  for (i = 0; i < tabcontent.length; i++) {
    tabcontent[i].style.display = "none";
  }
  tablinks = document.getElementsByClassName("tablink");
  for (i = 0; i < tablinks.length; i++) {
    tablinks[i].style.backgroundColor = "";
  }
  document.getElementById(tabName).style.display = "block";
  if(elmnt.style != null) {
    elmnt.style.backgroundColor = color;
  }
}

window.onload = function() {
  openTab('tabintro', this, '#222');
}

/* How can I keep Google from indexing my website? */
```

From the previous hint , ” **How can I keep Google from indexing my website?**”, I went ahead and examined the **robots.txt** file which gave me the third segment of the flag ” **t_Of_pl4c**” together with another hint ” **I think this is an apache server... can you Access the next flag?**”.

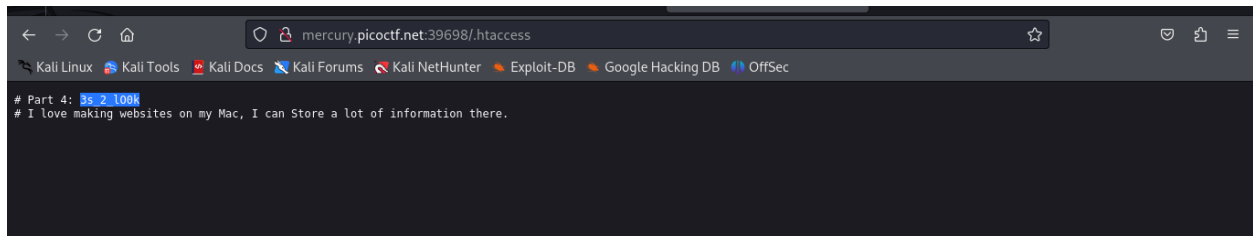


```
mercury.picocftf.net:39698/robots.txt

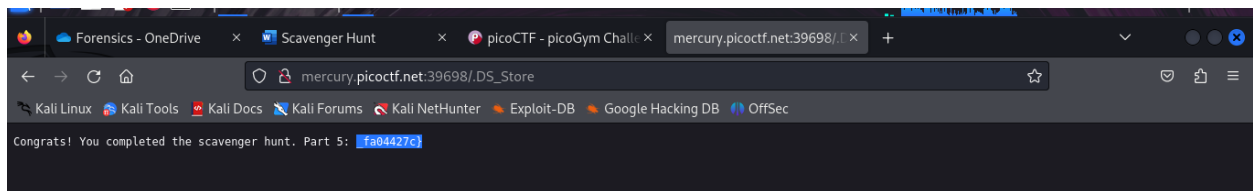
User-agent: *
Disallow: /index.html
# Part 3: t_Of_pl4c
# I think this is an apache server... can you Access the next flag?
```

htaccess file is a powerful website file that **controls the high-level configuration of your website**. On servers that run Apache (a web server software), the **.htaccess** file allows you to

make changes to your website's configuration without having to edit server configuration files. After some googling i learnt about this file . I went ahead and accessed its contents where i retrieved another flag segment "3s_2_100k" together with a hint "I love making websites on my Mac, I can Store a lot of information there."



From the hint, I tried googling where I learnt about (Desktop Services Store) a system file created by the macOS operating system. The purpose of .DS_Store file is storing custom attributes of a folder, such as the position of icons, background color, etc. I went ahead and tried accessing the .DS_Store file in browser and that's how I retrieve the last part of the Flag "_fa04427c"}".



I merged the flag segments and the final flag was picoCTF{th4ts_4_10t_of_pl4c3s_2_100k_fa04427c}.