

# Scavenger Hunt

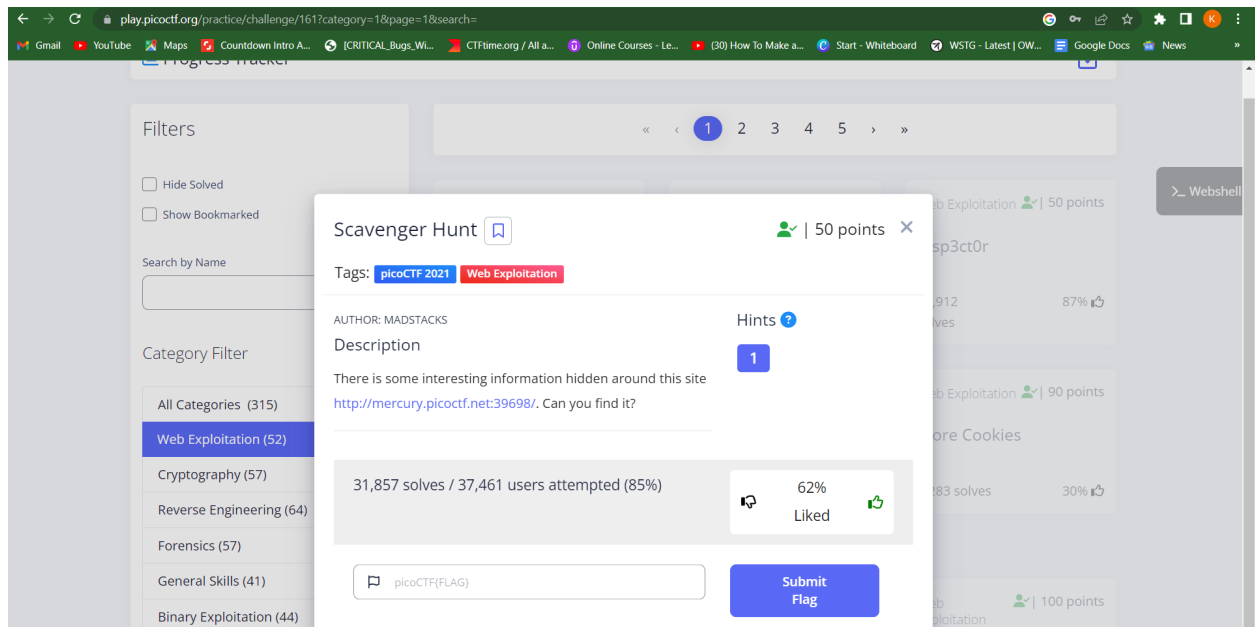
Link to Solve the Lab:-

<https://play.picoctf.org/practice/challenge/161?category=1&page=1&search=>

Hello Everyone,

So Today we are Solving the Lab in the 'Cryptography' Category

All the things we are doing are in the Kali Linux.

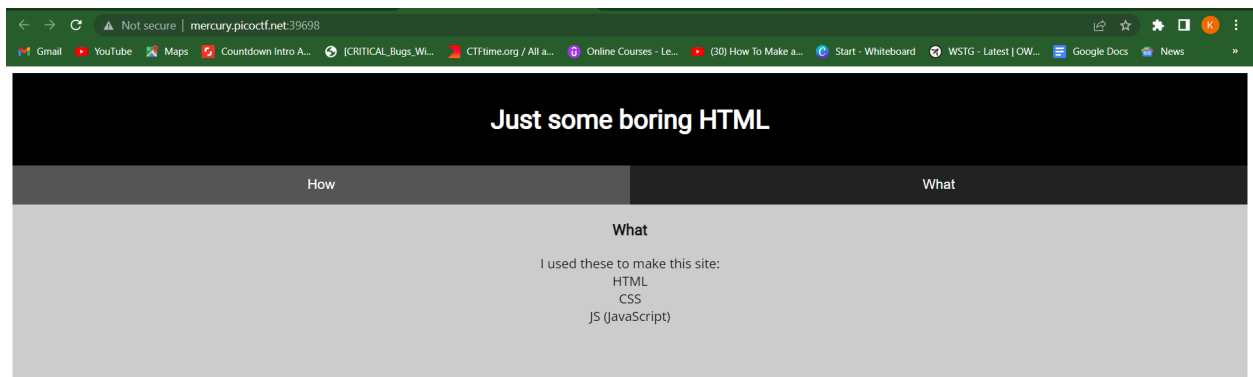


As you can see from the Description, we have to find the Website's hidden information.

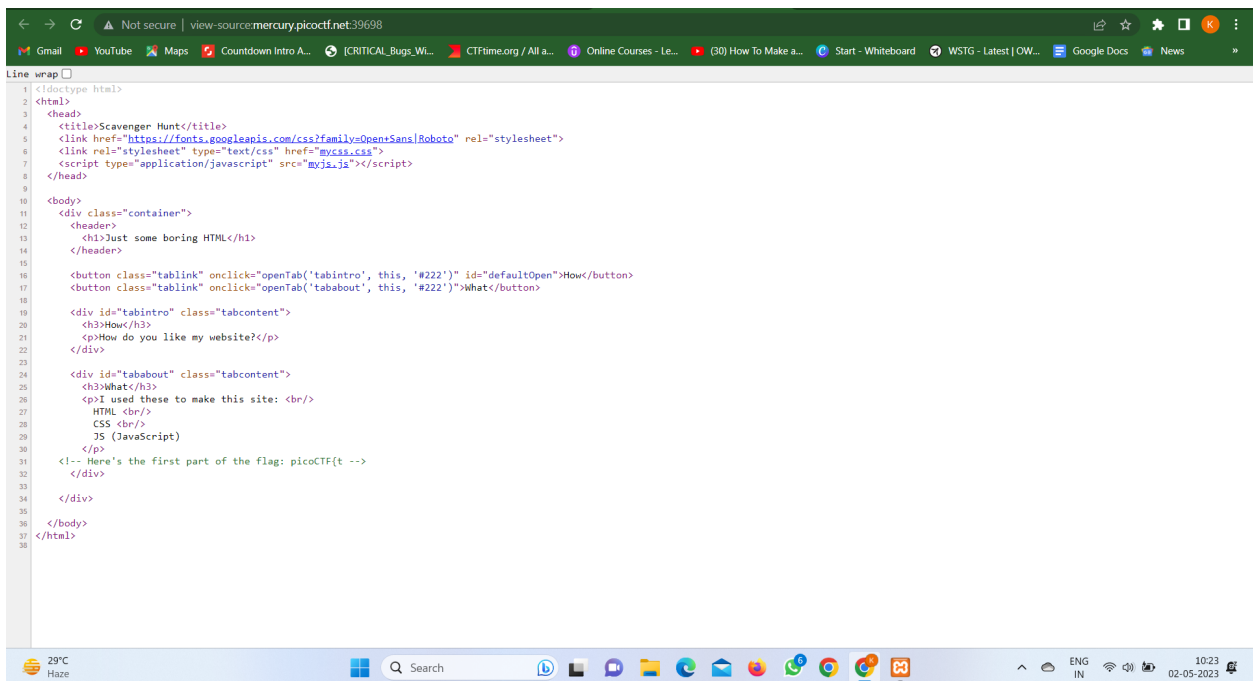
What can we, therefore, infer from this?

We have to find the flag that is hidden on the website.

The home page of our target website is shown in the screenshot below, as you can see.

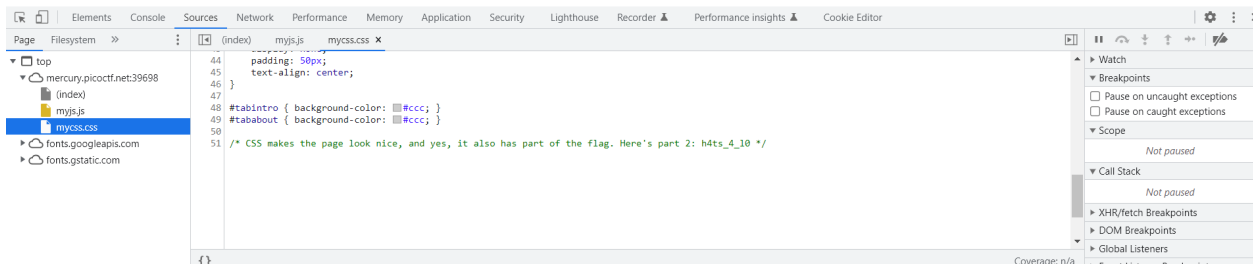
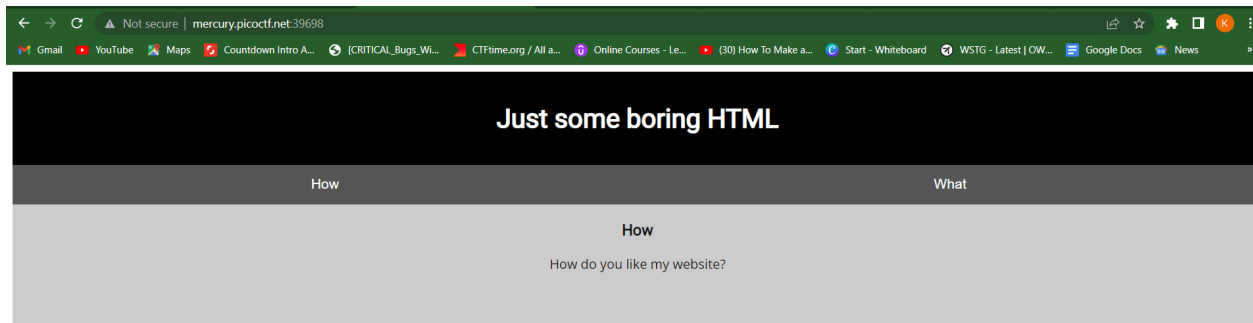


Let's begin with the source code.



As you can see, the first part of the flag, "picoCTF{t" is in the comment.

So let's examine additional Source files, such as the javascript and CSS files.



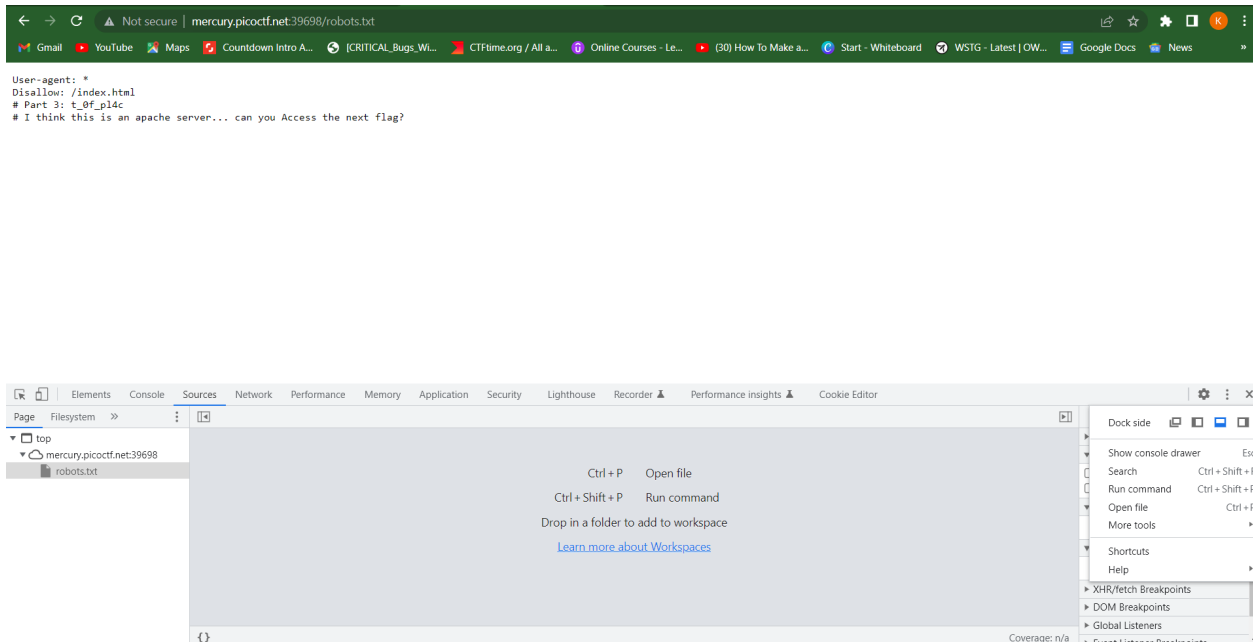
The mycss.css file, which you can see in the screenshot above, contains the second portion of the flag, which is "h4ts\_4\_10".

Let's look at this myjs.js file to see what information it contains and I got Hint, "How can I keep Google from indexing my website?"

What then does it explain?

As far as we are aware, Search Engine Crawls website automatically finds the content that has been searched for, so they check a file called "robots.txt" that contains information like what to permit. or what should we forbid?

Let's say the admin page is required, but the Google crawler does not need to visit it, so it is forbidden. Thus, the "robots.txt" file contains information of this type.

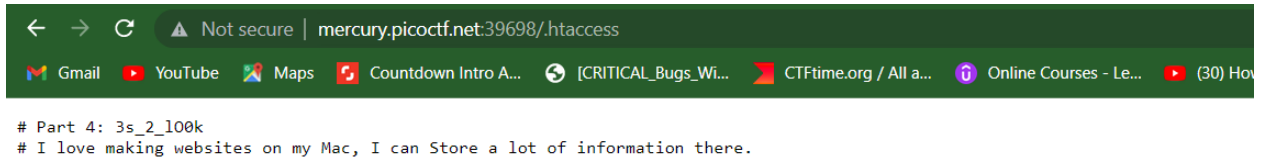


As you can see, part three of the flag was discovered. The Hint "I think this is an Apache server... can you access the next flag" is also present.

.htaccess is a configuration file used by Apache web servers to control various aspects of the server's behavior. The file contains a set of directives that define rules for handling requests to the server, such as redirecting URLs, setting custom error pages, password protecting directories, and enabling or disabling certain features of the server.

The .htaccess file is placed in the root directory of a website and affects all files and directories within that directory, as well as any subdirectories unless a subdirectory has its own .htaccess file with different rules.

So let's look at the web.

A screenshot of a web browser window. The address bar shows 'mercury.picoctf.net:39698/.htaccess' with a 'Not secure' warning. The browser's tab bar includes 'Gmail', 'YouTube', 'Maps', 'Countdown Intro A...', '[CRITICAL\_Bugs\_Wi...', 'CTFtime.org / All a...', 'Online Courses - Le...', and '(30) How'. The main content area displays two lines of text: '# Part 4: 3s\_2\_100k' and '# I love making websites on my Mac, I can Store a lot of information there.'

```
# Part 4: 3s_2_100k
# I love making websites on my Mac, I can Store a lot of information there.
```

Consequently, we discovered the next flag's hint as well as its fourth part.

So it is saying “I love making websites on my Mac, I can Store a lot of information there.”

Let's look for that file name now.

.DS\_Store is a hidden file created by the macOS operating system that stores custom attributes of a folder, such as the position of icons and other display settings. The file is automatically created by the Finder application when a folder is opened and modified, and it is usually not visible to the user unless they have enabled the option to show hidden files.

Let's look into it



Finally, we located the flag.

Add all the components together, submit it, and the lab is finished.

FLag :- picoCTF{th4ts\_4\_l0t\_of\_pl4c3s\_2\_l00k\_7a46d25d}