Grab the PicoCTF Flags

De Silva K.R.K.D

Abstract

The PicoCTF platform is a well-known platform in the field of cybersecurity education and skill development which offers a variety of tasks aimed to evaluate and improve participants' abilities. It is very important to help to beginners. By reading this report, one can get an overview of how the flags were found in web exploitation. Each challenge includes a set of challenges and issues that require analytical thinking and technical expertise. In this report, I have put screenshots for each step and describe how to find flags within steps. The report conclusion includes a description of my viewpoints as well.

Table of contents

ABSTRACT……...……...2

INTRODUCTION TO THE TOPIC……...……...5

Methodology……6

CTF Challenges And Solutions……...……..7

1) Insp3c0r……...……...……7
Description……..……..7
Hints……...……..7
Walkthrough……..……7

2) Scavenger Hunt……...9
Description……..9
Hints……..9
Walkthrough……..9

3) Some Assembly Required 1……..……12
Description……12
Walkthrough……12

4) Where are the robots……..……...13
Description……..13
Hints……..13
Walkthrough……13

5) Logon……....15
Description……..15
Hint……..15
Walkthrough……..15

6) dont-use-client-side……..18
Description……..18
Hints……..18
Walkthrough……..18

7) It is my Birthday……...20
Description……20
Hints……..20
Walkthrough……..21

8) Includes…….23
Description……..*23*
Hints……..,… *23*
Walkthrough……..,,*23*

9) Search source…….25
Description……..*25*
Hints……..*25*
Walkthrough……*25*

10) Findme……..27
Description……..*27*
Walkthrough……*27*

11) Inspect HTML……..29
Description……..*29*
Hints……..*29*
Walkthrough……*29*

12) Local Authority…….31
Description……..*31*
Hints……..*31*
Walkthrough……*31*

Conclusion……..…….33
References……33

Introduction to the topic

The world of cybersecurity has become more complex and challenging in the era of modern technology. The methods that are used by bad actors change along with advances in technology. As a consequence, the area of cybersecurity is continually growing, placing an important priority on practical skill development and practical expertise. In this context, Capture The Flag(CTF) challenges have become popular as a dynamic platform for developing cybersecurity knowledge, with PicoCTF standing out as a top space for the purpose.

“Grab the PicoCTF flags” launches a thorough investigation of the PicoCTF challenge universe. These issues cover a wide range of cybersecurity disciplines, including cryptography, forensics, and binary exploitation. The trick to these problems is the find “flags”, which are symbolic examples of smart problem-solving and code-breaking. A flag shows a participant’s success over particular challenges and the highest point of their technical expertise, creativity, and strategic thinking. In a CTF or capture-theflag competition, competitors must utilize a variety of methods to overcome challenges or solve problems in order to earn a flag[1]. When PicoCTF initially started, it was a unique game-based CTF tournament that employed offensive methods to instruct middle and high school students about cybersecurity[1].

In addition to the technical aspects, PicoCTF challenges build a comprehensive skill set important in the cybersecurity industry. Critical thinking, and analytical skills. Participants are encouraged to bridge the gaps throughout computer science, linguistics, and other fields as a result of the problems’ constant overcoming of specific discipline boundaries. The range and variety of difficulties provided by PicoCTF will be examined. So as to help both beginners and seasoned professionals, we will explain the methods used for solving these problems. Since 2011, PicoCTF has worked to gradually lower the challenges to enrollment in cybersecurity education, becoming one of the most reliable, excellent, and free sources of information security training for students and teachers worldwide[2].

Learners of all ability levels may access cybersecurity content, think, creatively, solve problems, and have fun while learning cybersecurity principles with PicoCTF’s more thorough and integrated learning framework, new platform, and all year access to picoGYM[2]. “Grab the PicoCTF flags” is an invitation to participate in the exciting realm of cybersecurity difficulties, where competitors try to capture the symbolic flags that stand for success over challenging digital riddles. We will explore the instructional, important, and technological aspects of PicoCTF issues as we go along, illuminating their crucial importance in the ongoing effort to strengthen digital barriers in a constantly changing digital environment.

Methodology

The “Grab the PicoCTF flags” concept focuses on using a methodical process to address problems in the PicoCTF competition. To understand the goals and context of the challenges, participants must first carefully read the descriptions of each one. Choosing the right techniques requires understanding the challenge type, such as forensics, web exploitation, reverse engineering, or others. The initial step is to examine any offered data or materials for any secret data or hints. The next step is for participants to perform research and educate themselves on pertinent terms, tools, and techniques, especially if the challenge is related to an unfamiliar field.

Developing unusual methods that depart from the standard frequently calls for creative thinking, problem-solving abilities can be improved over time by trying out new techniques, keeping track of results, and picking up lessons from mistakes. Successful flag grabbing finally shows competitors’ prowess in cybersecurity and technical problem-solving. This process of taking on multiple difficulties encourages constant learning and a deeper comprehension of many cybersecurity disciplines.

CTF Challenges And Solutions

1) Inp3ct0r

Description

Kishor Balan tipped us off that the following code may need inspection:

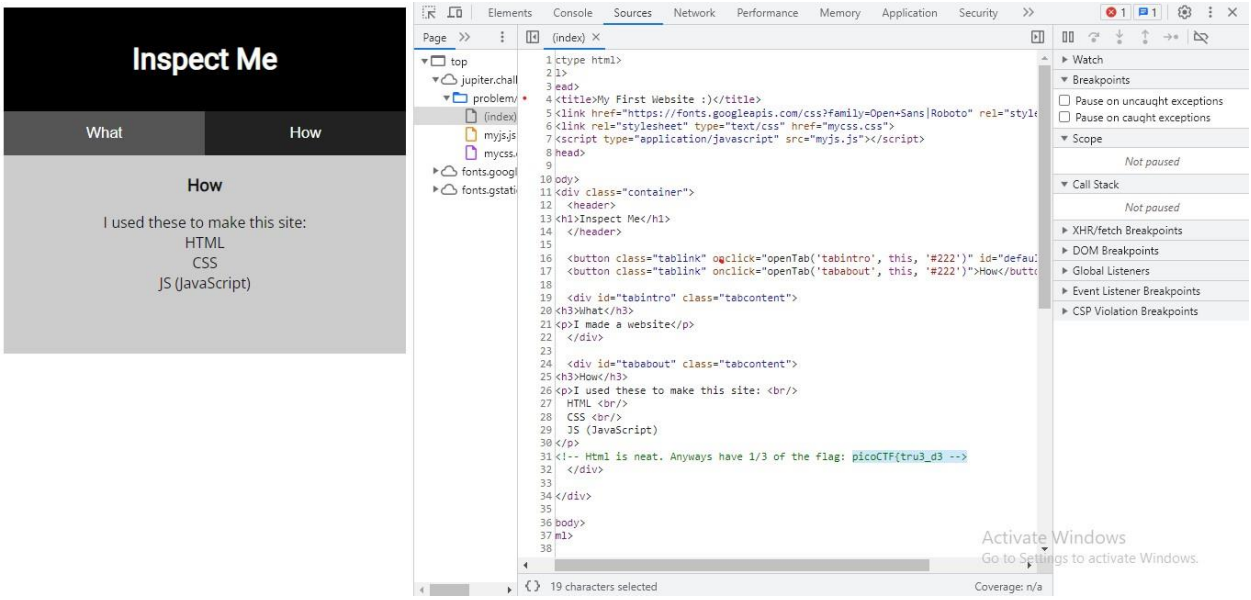
`https://jupiter.challenges.picoctf.org/problem/9670/` (link)[3]

Hints

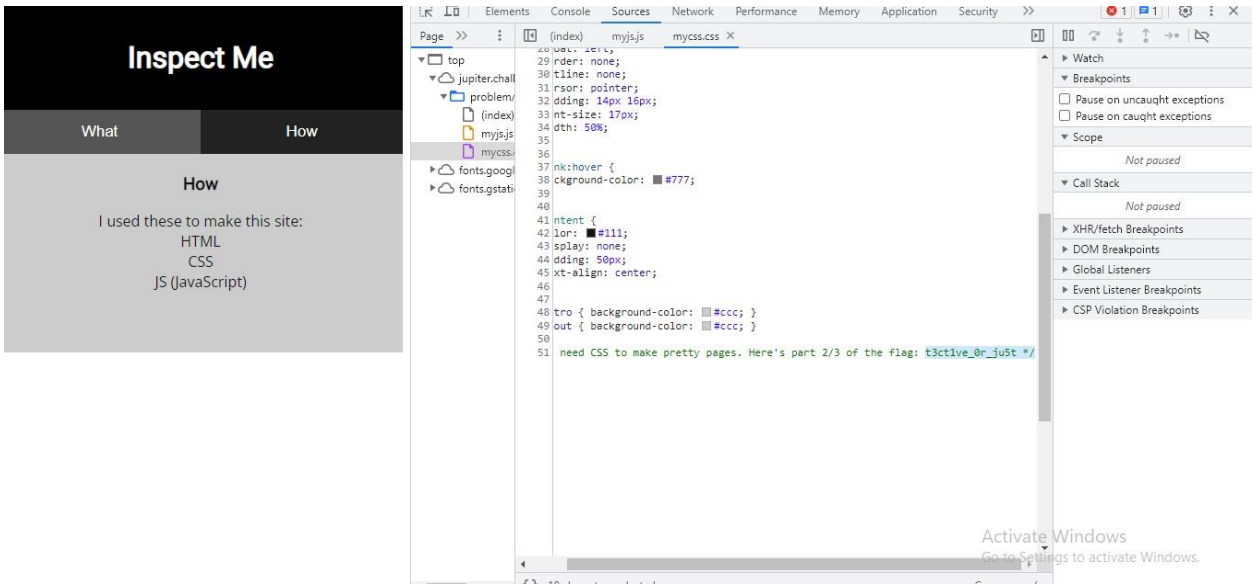
- How do you inspect web code on a browser?[3]
- There's 3 parts[3]

Walkthrough

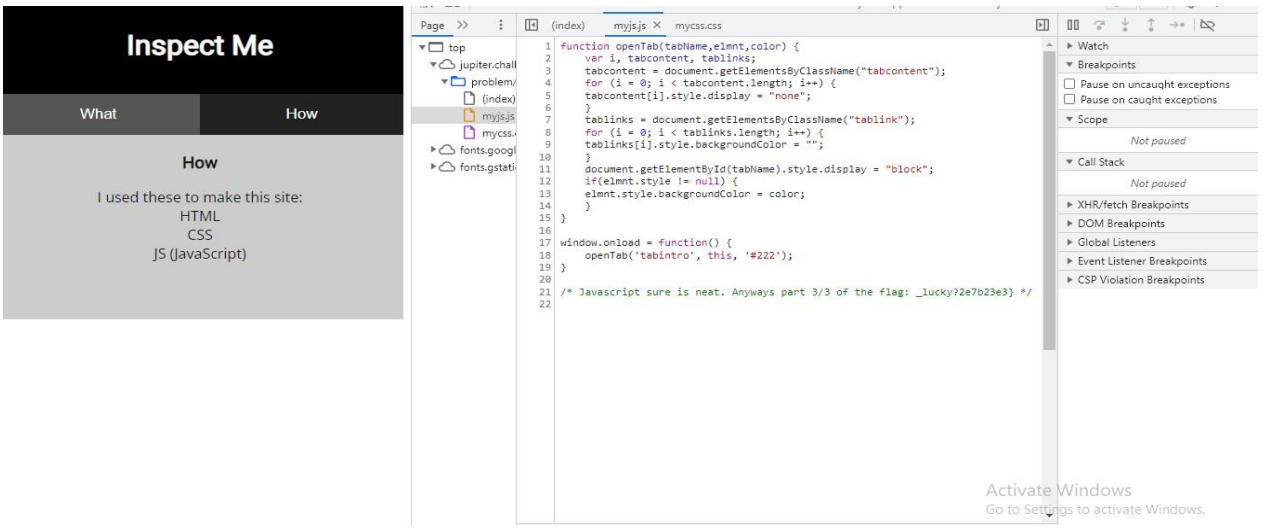
- First go to the website that says. "The following code may need inspection", After reading this, I inspected that webpage. We can see developer tools and go the "Sources". It has some contents like index, myjs.js, and my css.css. Initially go to the index and can we see the first part of the flag.



- Now go to the mycss.css part and we can see the send part of the flag.



- Finally go to the myjs.js part and find the third part of the flag.



As we can see green color sentences in these images, concatenate the parts of the flag in proper order.

2) Scavenger Hunt

Description

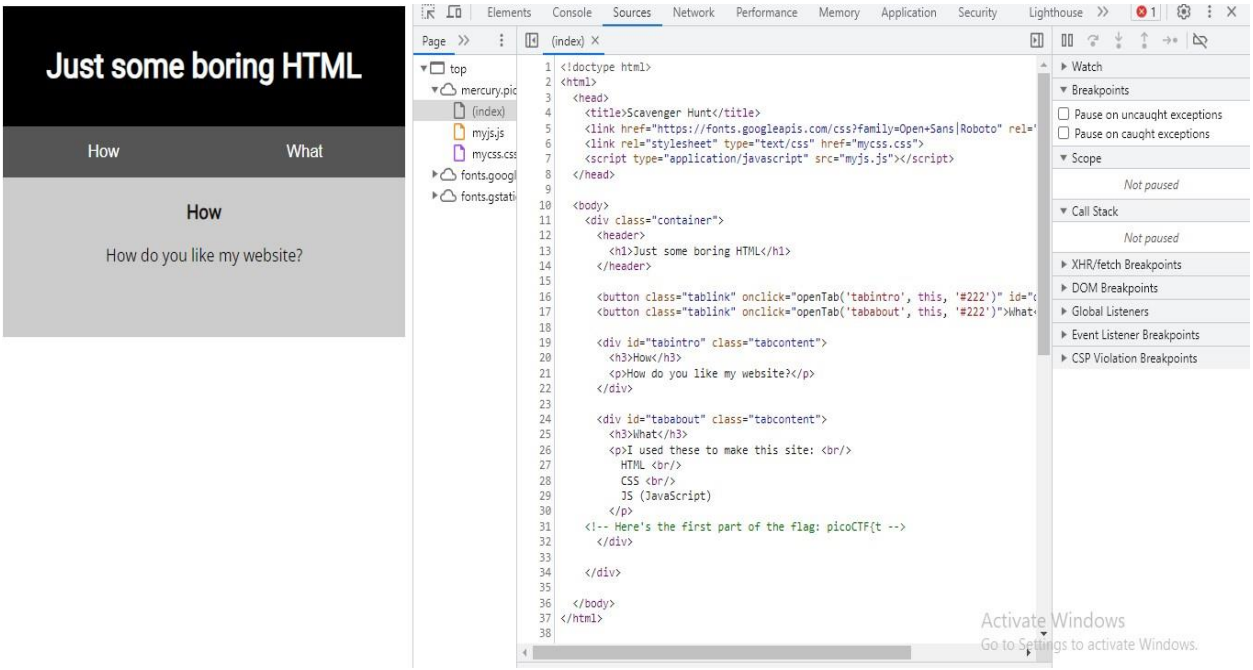
There is some interesting information hidden around this site http://mercury.picoctf.net:39698/. Can you find it?[4]

Hints

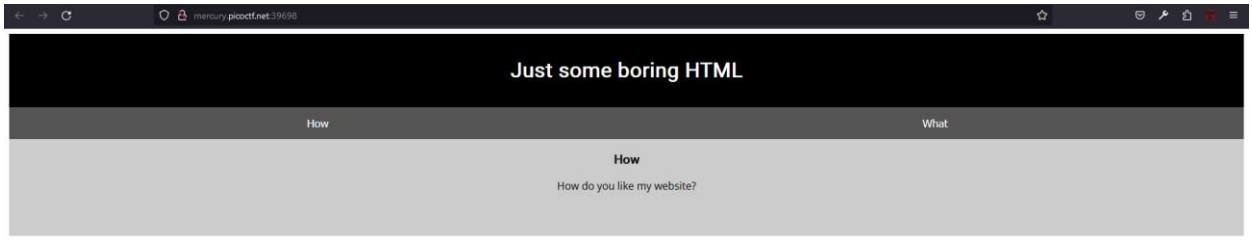
You should have enough hints to find the files, don't run a brute forcer.[4]

Walkthrough

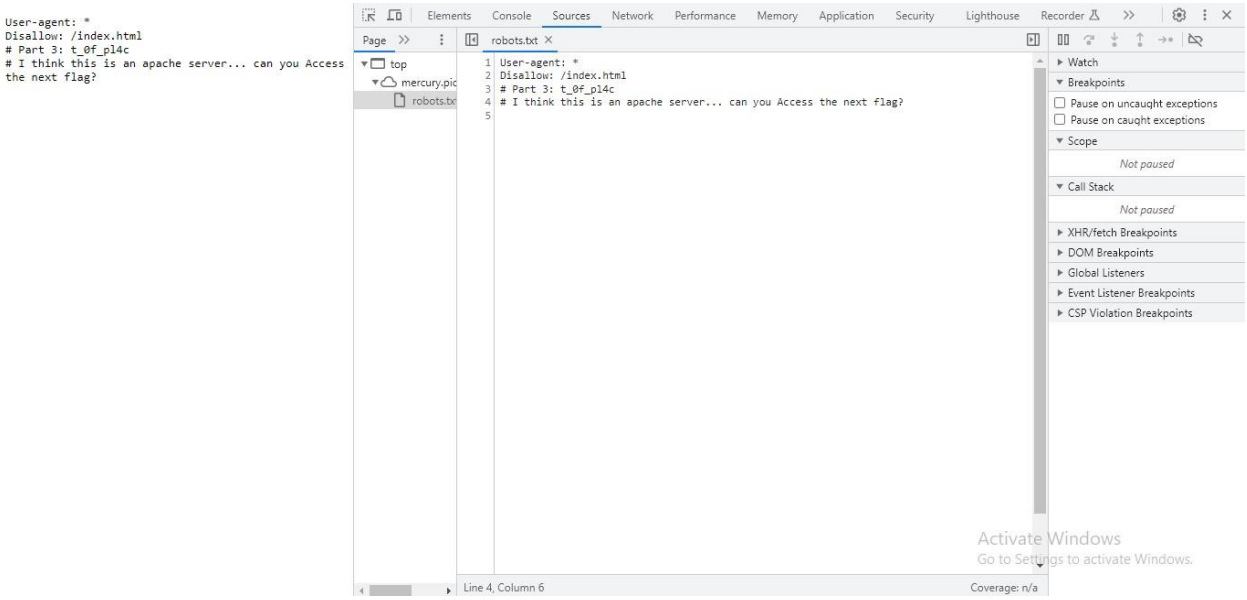
- Browsers the web page they mentioned. Inspect that webpage. Go to the “Sources” and go inside the “index” and find the first part of the flag.



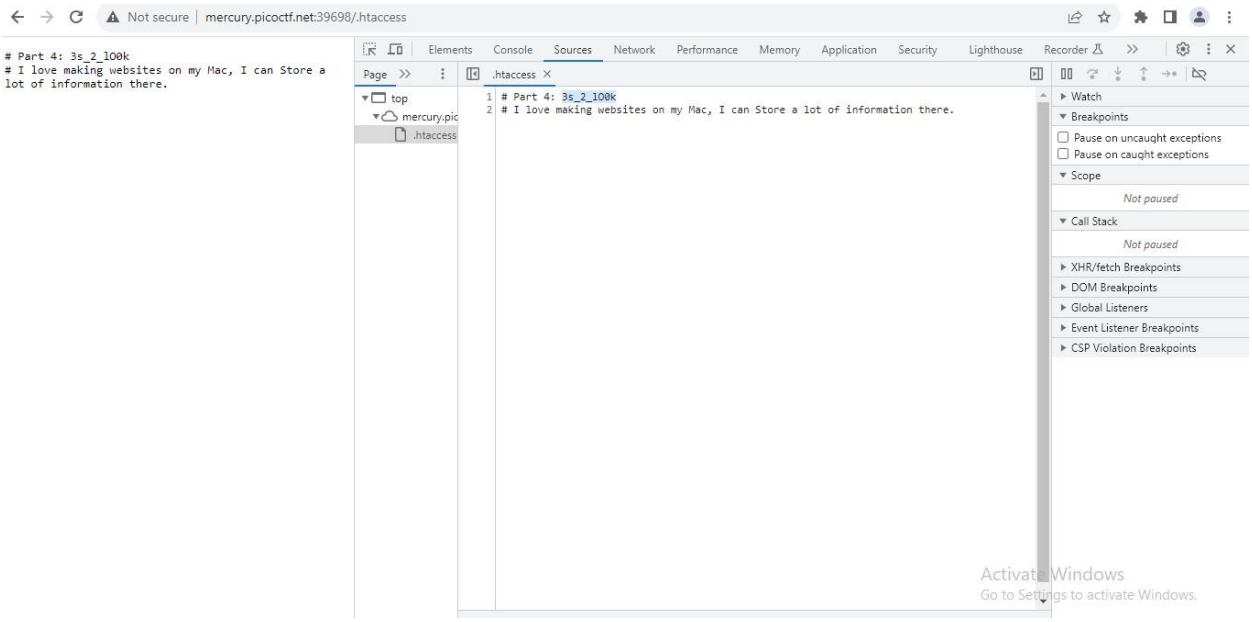
- Then go to “Style editor” and we can see the second part of the flag.



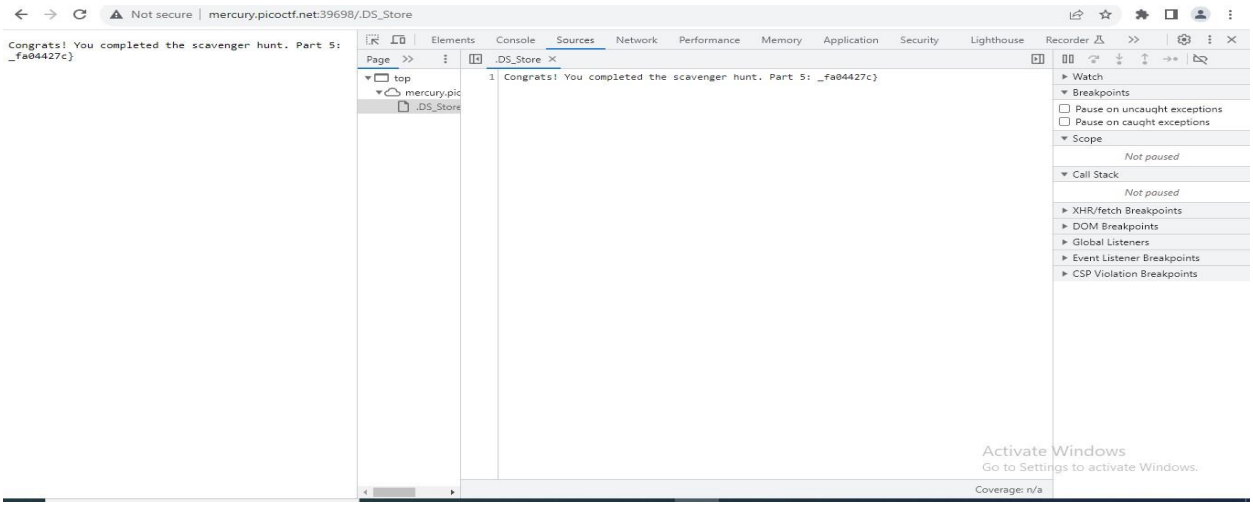
- Then go to the myjs.js and find some hints. Now apply this behind the link on the webpage. “robots.txt”. Then find the third part of the flag and another hint for the next part of the flag.



- The previous part they show us “I think this is an apache server… can you access the next flag?” After reading this I browser to the “/.htaccess” page and found the fourth part of the flag and hint of the next part.



- That hint says, they store a lot of information on my Mac. So I changed the link to “/.DS_Store” and found the final part of the flag.



As we can see green color sentences in these images, concatenate the parts of the flag in proper order.

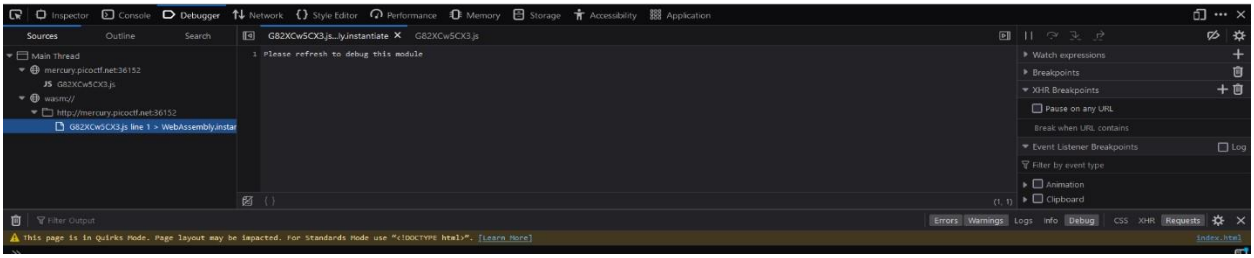
3) Some Assembly Required 1

Description

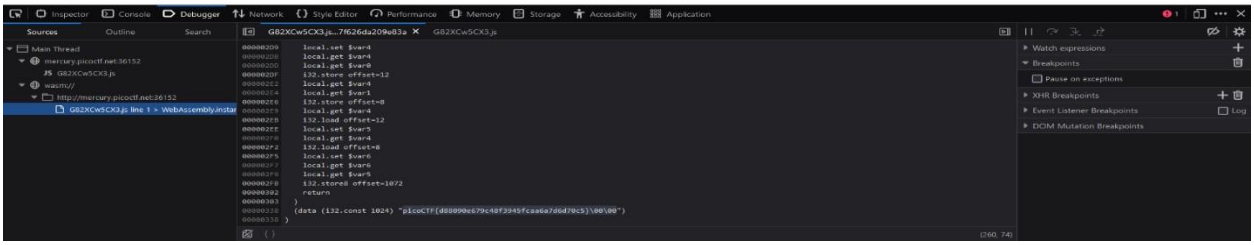
http://mercury.picoctf.net:36152/index.html

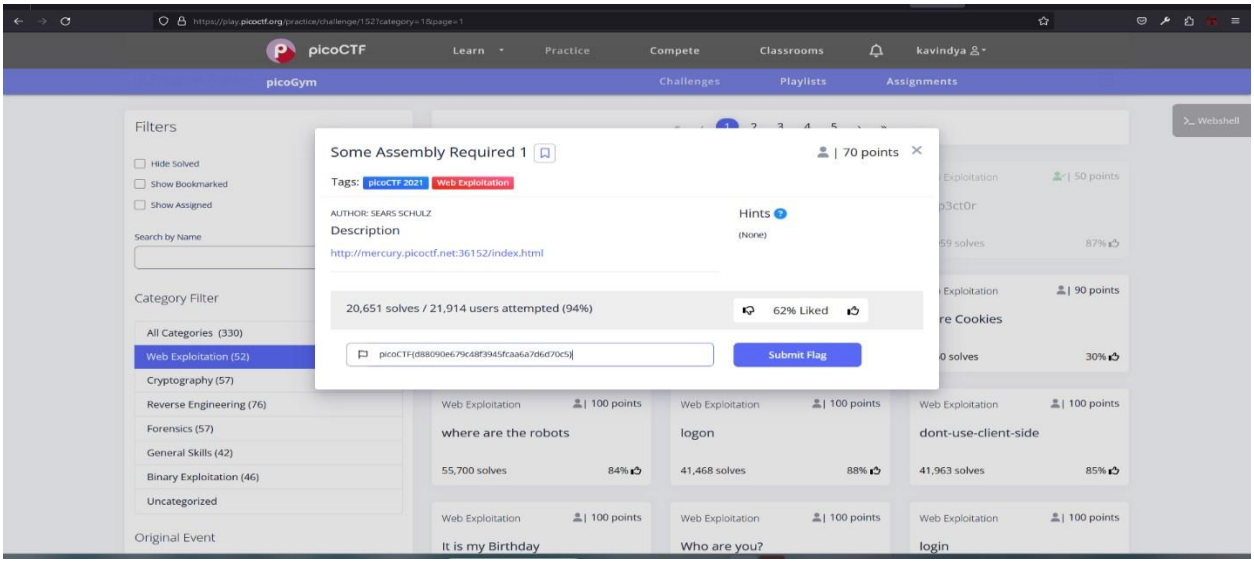
Walkthrough

- They did not give us any hints. So I decided to inspect that webpage and went to Debugger to find the flag or hint. So I saw a hint" Please refresh to doing this module".



- When refresh the page and find the flag.





- This challenge gives us the full flag when we complete some steps.

4) Where are the robots.

Description

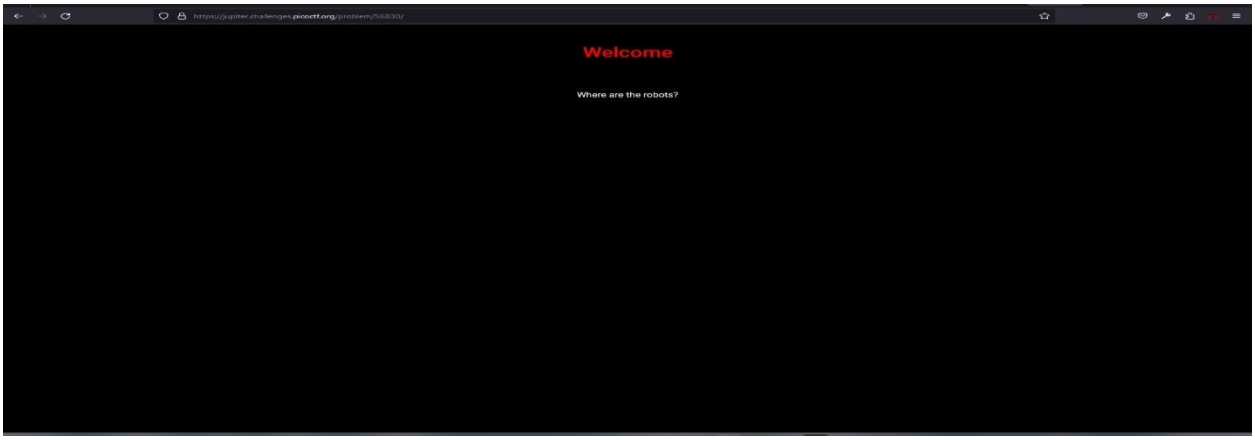
Can you find the robots? `https://jupiter.challenges.picoctf.org/problem/56830/` ([link])[5]

Hints

What part of the website could tell you where the creator doesn't want you to look?[5]

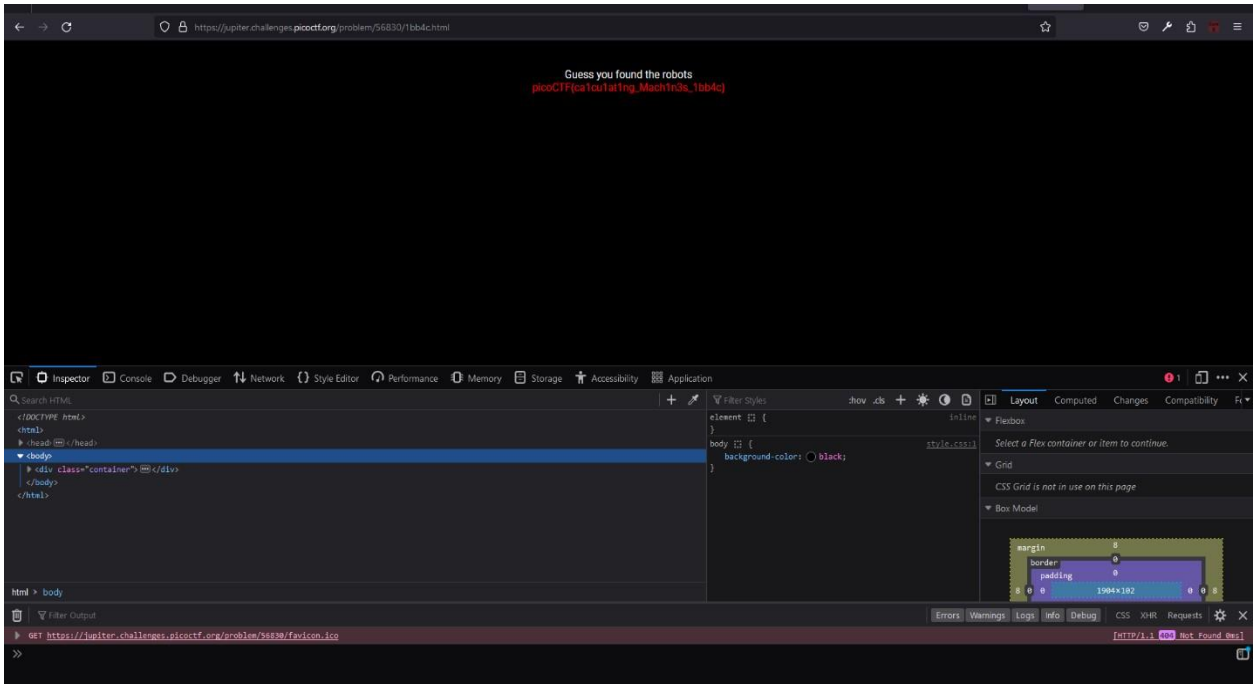
Walkthrough

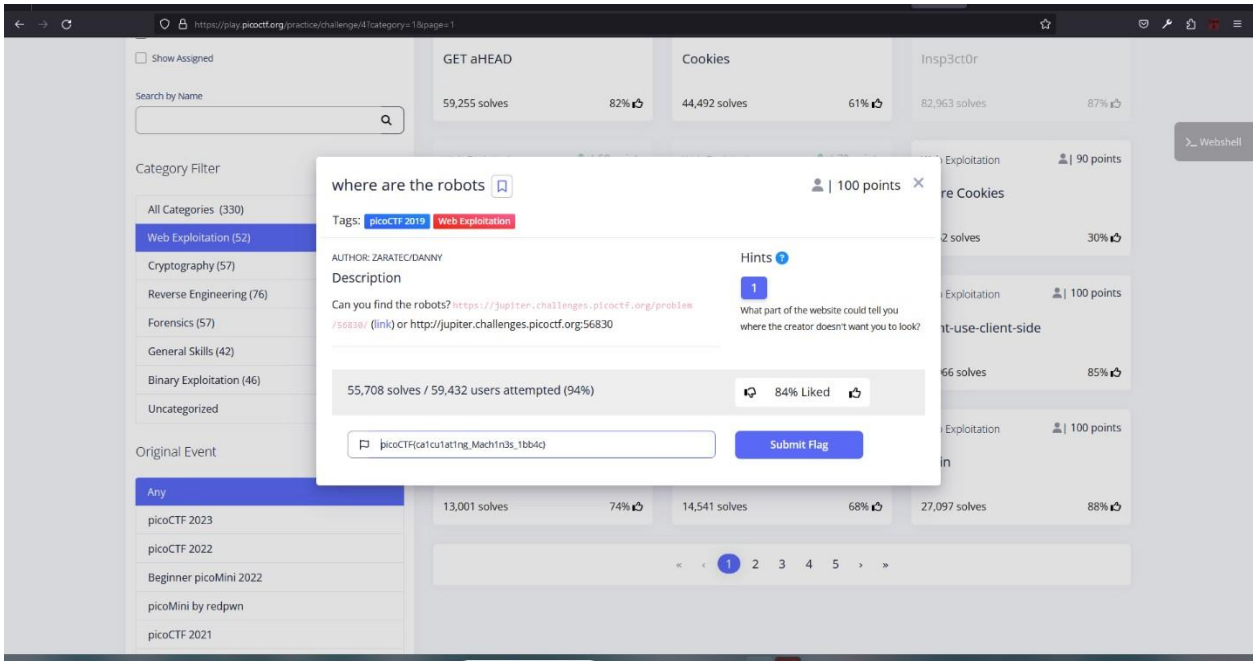
- This challenge they ask “Can you find the robots?”. Firstly go to this link and try to find any hint. Again they ask about robots. So I thought that flag was put on the “robots.txt” page.



- Then go to that robot.txt page and can find one part of some webpage link.

- Using that part of the link we can find the flag.





When we find the link we can complete this challenge using this link.

5) Logon

Description

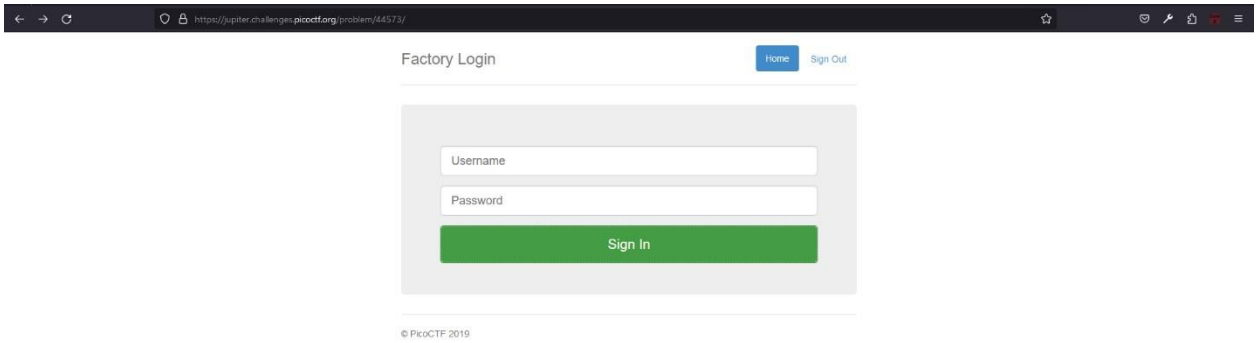
The factory is hiding things from all of its users. Can you login as Joe and find what they've been looking at? `https://jupiter.challenges.picoctf.org/problem/44573/` (link)[6]

Hints

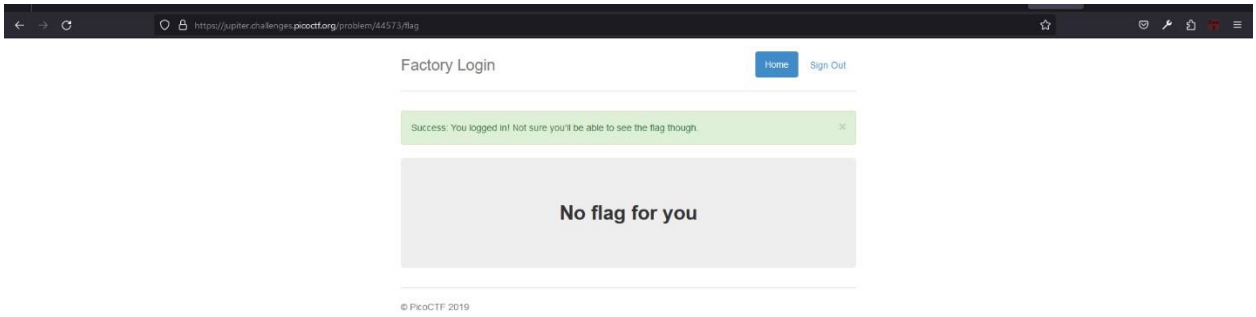
Hmm it doesn't seem to check anyone's password, except for Joe's?[6]

Walkthrough

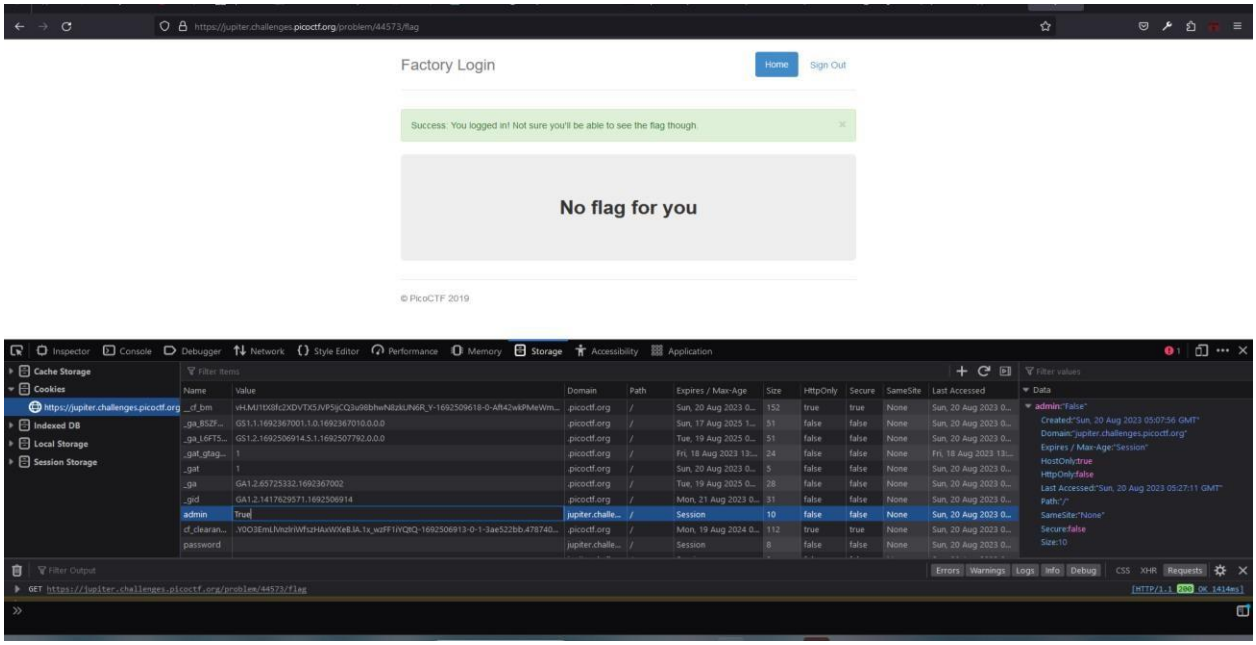
- Firstly click the link that they give. Then we can see a login page. But we cannot log into this site without knowing the username and password. So we need to find a hint or something to log.



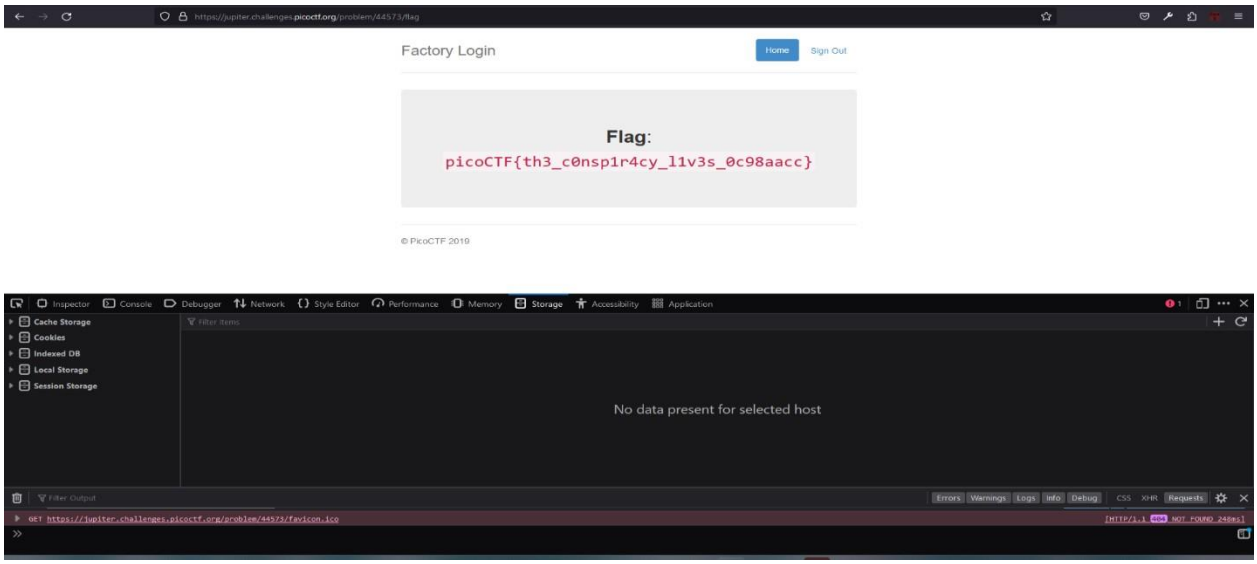
- I desided try to log with random username and password. Then I got some message on the screen.



- But I have not seen the flag yet. Then I open inspect and go to the “Storage”. Scroll down it and see name with “admin” and value is “false”. I changed that value to “True”.



- Then reload the page and got the flag.



- Analyze the contents and we can see the flag.

6) dont-use-client-side

Description

Can you break into this super secure portal?

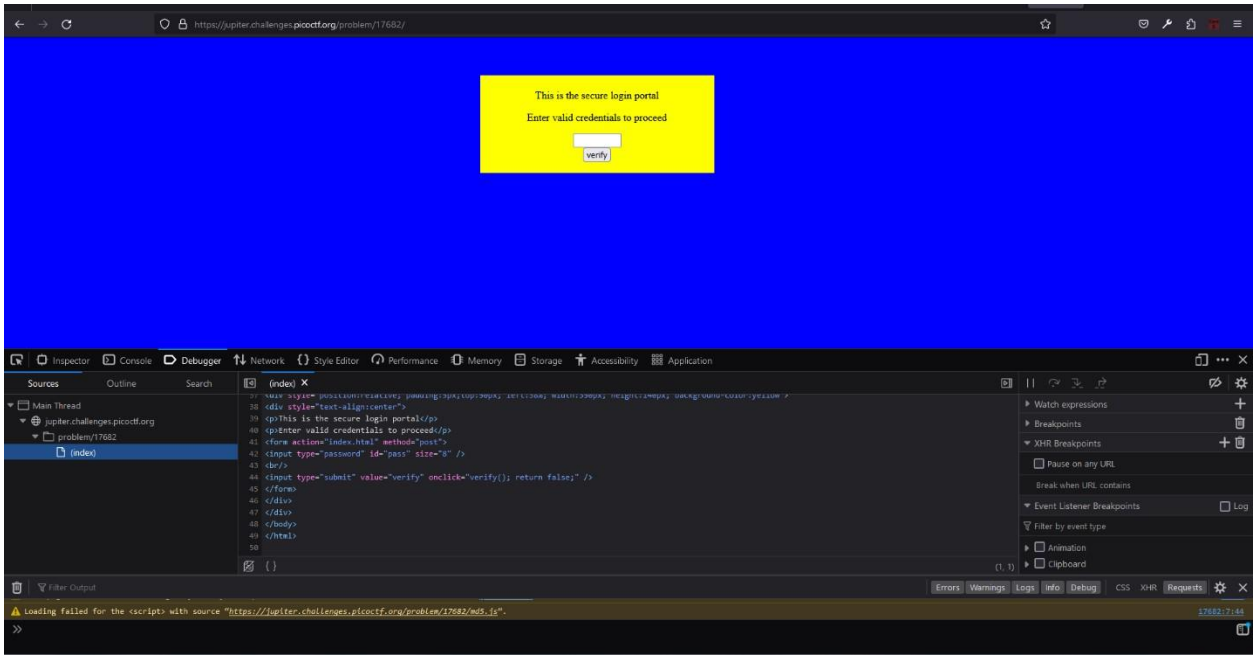
`https://jupiter.challenges.picoctf.org/problem/17682/` (link)[7]

Hint

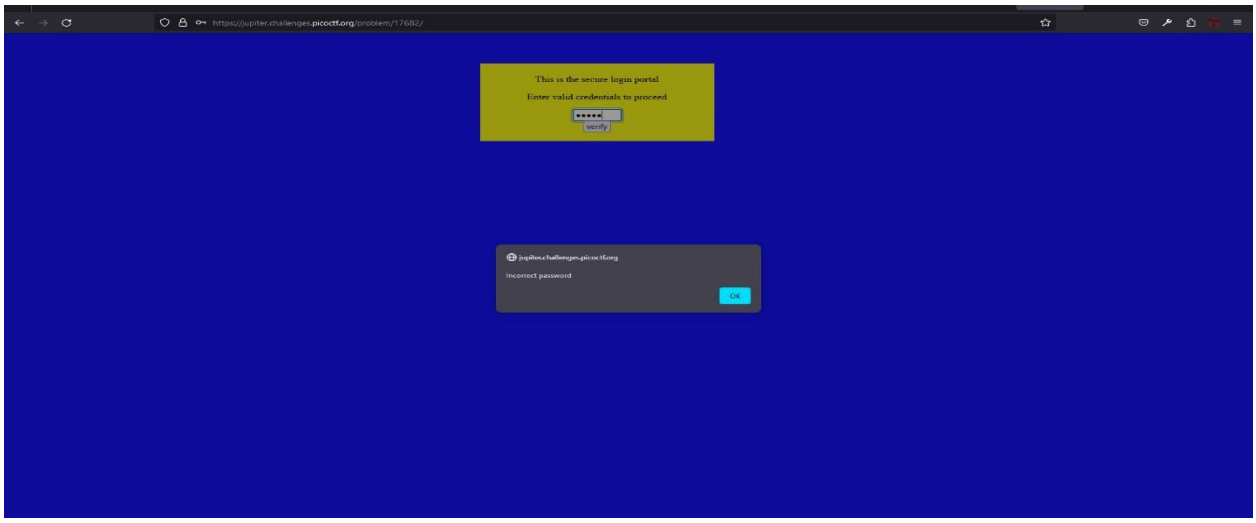
Never trust the client[7]

Walkthrough

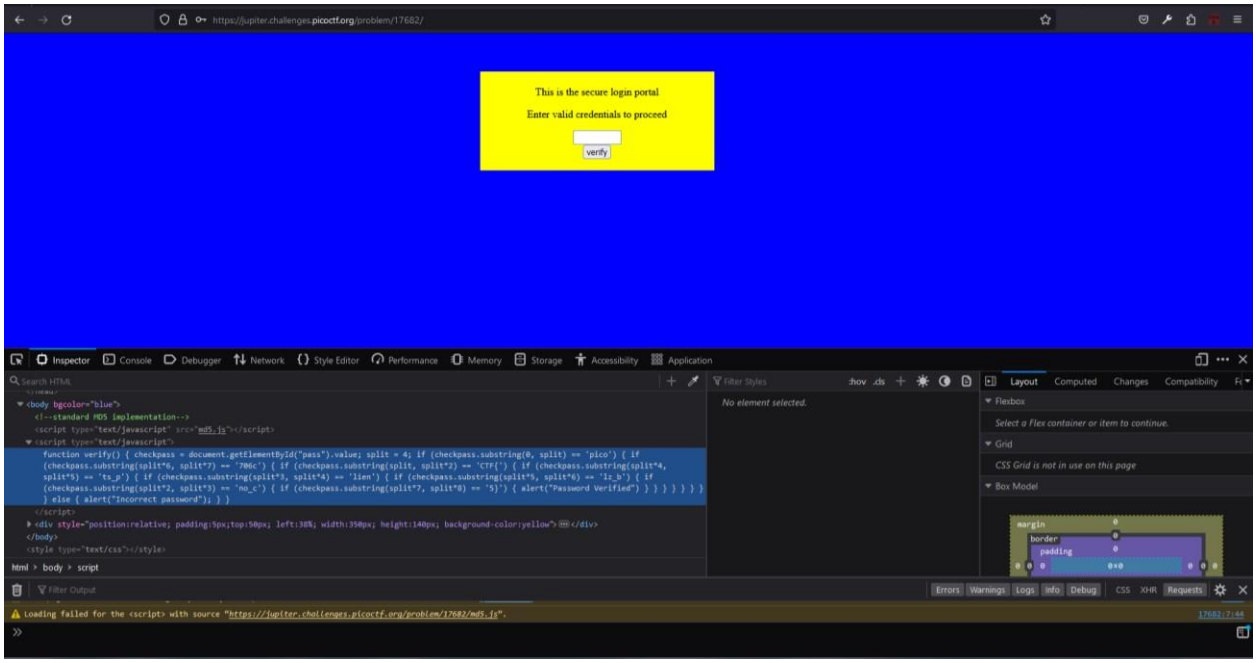
- Initially, visit the website. Then see login portal. And I try to credentials into inspect.

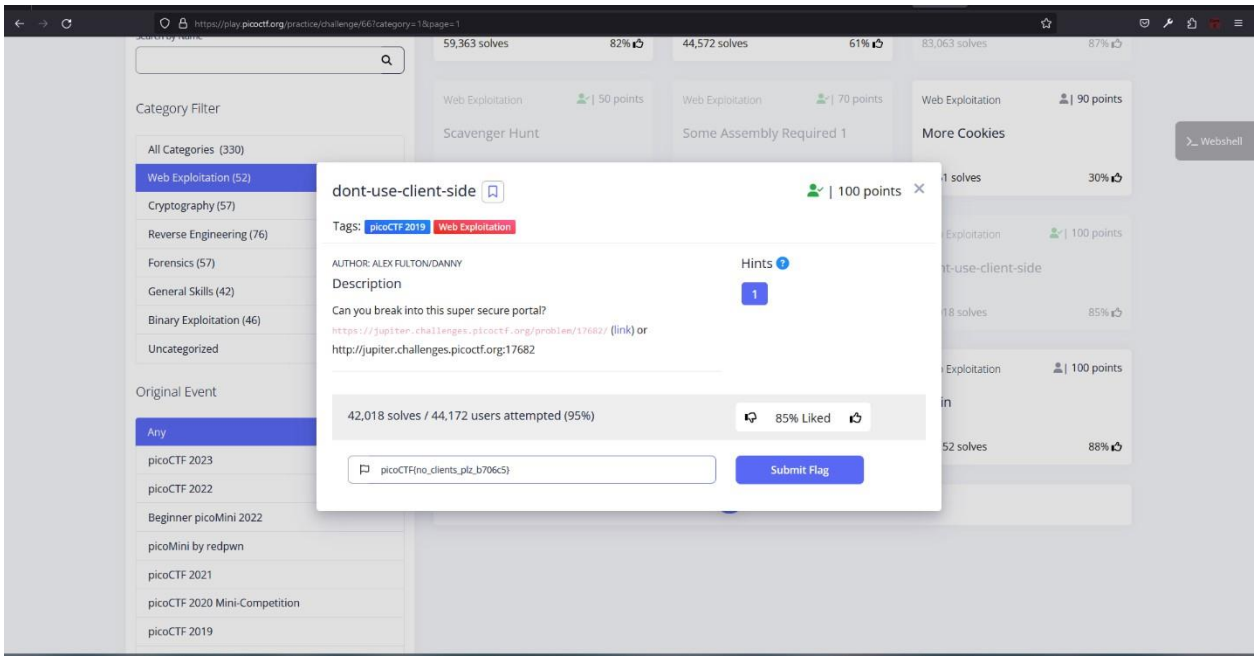


- I try to verify using random credential. Then I got an alert.



- And try to find something about flag using inspect again. Then I saw JavaScript code in the inspect. In that JavaScript code I got the flag. But it was not the full flag. After analyzing it I made the full flag.





This challenge gives us hint, but our input is stored in the checkpass variable, and each segment method in this case sets us to 4 characters starting with the method's first parameter. Accordingly, we put together the credentials and the flag.

7) It is my birthday

Description

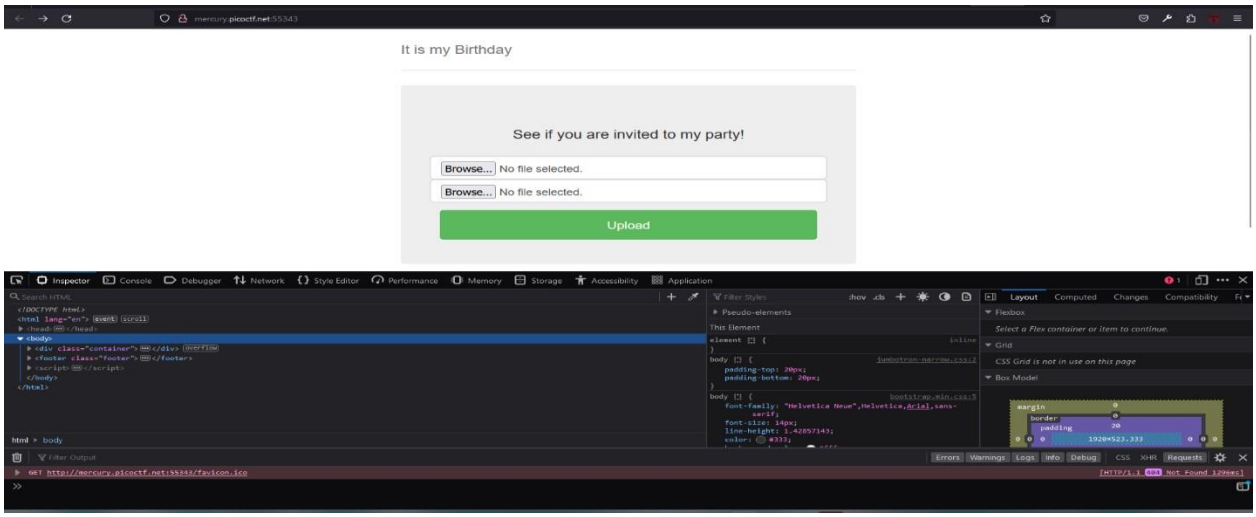
I sent out 2 invitations to all of my friends for my birthday! I'll know if they get stolen because the two invites look similar, and they even have the same md5 hash, but they are slightly different! You wouldn't believe how long it took me to find a collision. Anyway, see if you're invited by submitting 2 PDFs to my website. http://mercury.picoctf.net:55343/ [8]

Hints

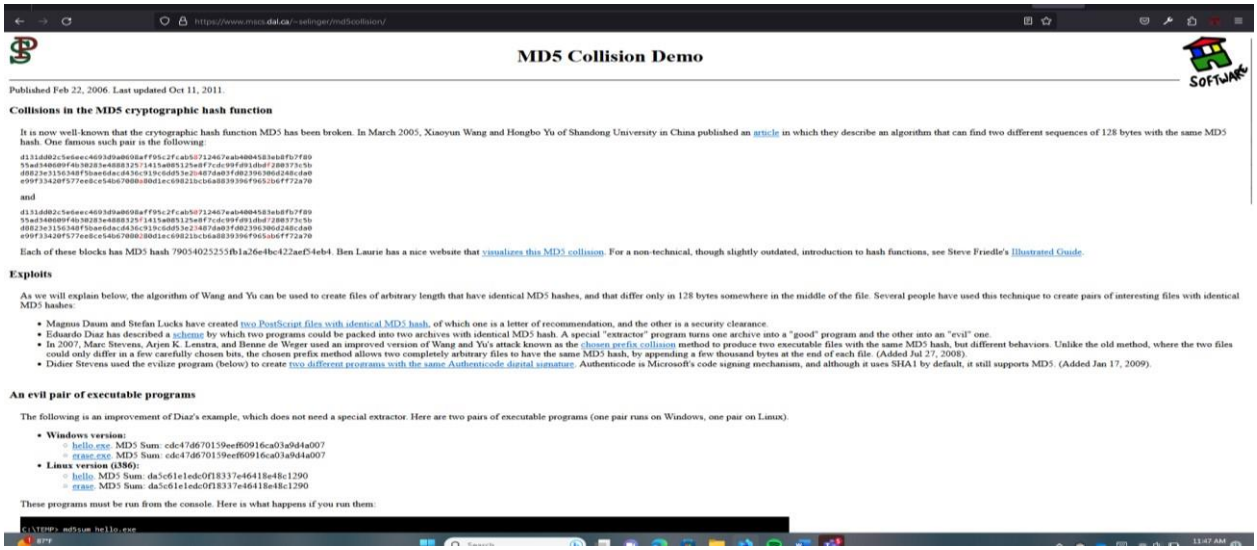
- Look at the category of this problem.[8]
- How may a PHP site check the rules in the description?[8]

Walkthrough

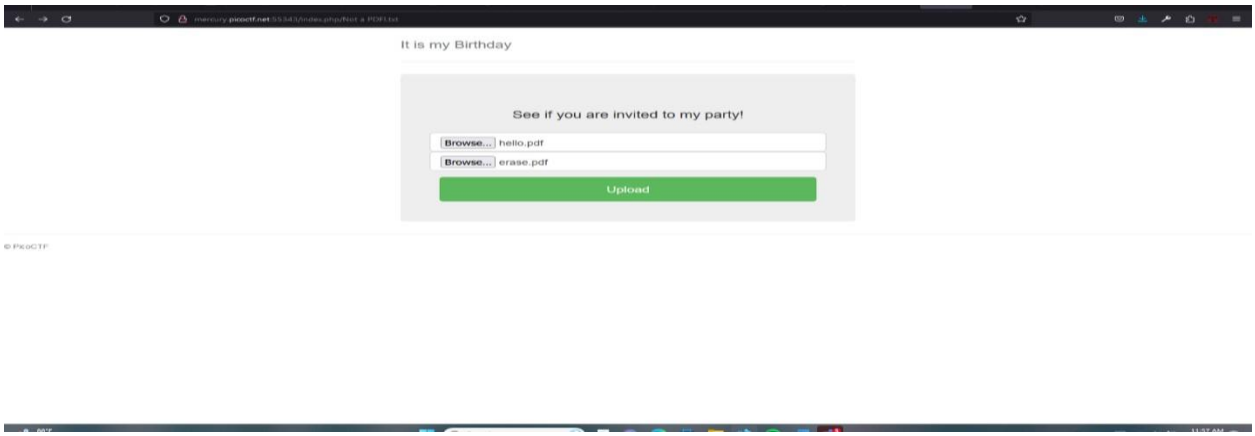
- Go to the website and see that there are two files to upload . But still, I have not those files.



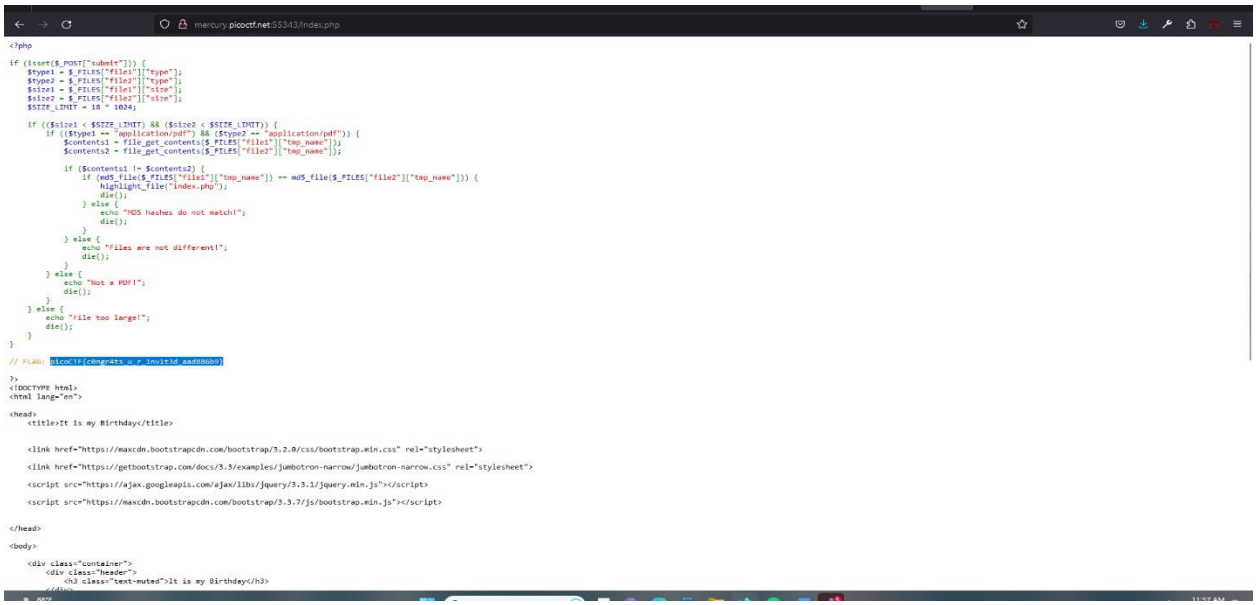
- After the reading description, I go this website https://www.mscs.dal.ca/~selinger/md5collision/ Now I see Those two files. I downloaded them.



- I try to upload them but they are not pdf files. After I changed their file extensions and uploaded them.



- After I upload files I came another page. It called “index.php”. And I got the flag.



This challenge has to upload two pdf. Complete those steps and finally we can find the flag for win this challenge.

8) Includes

Description

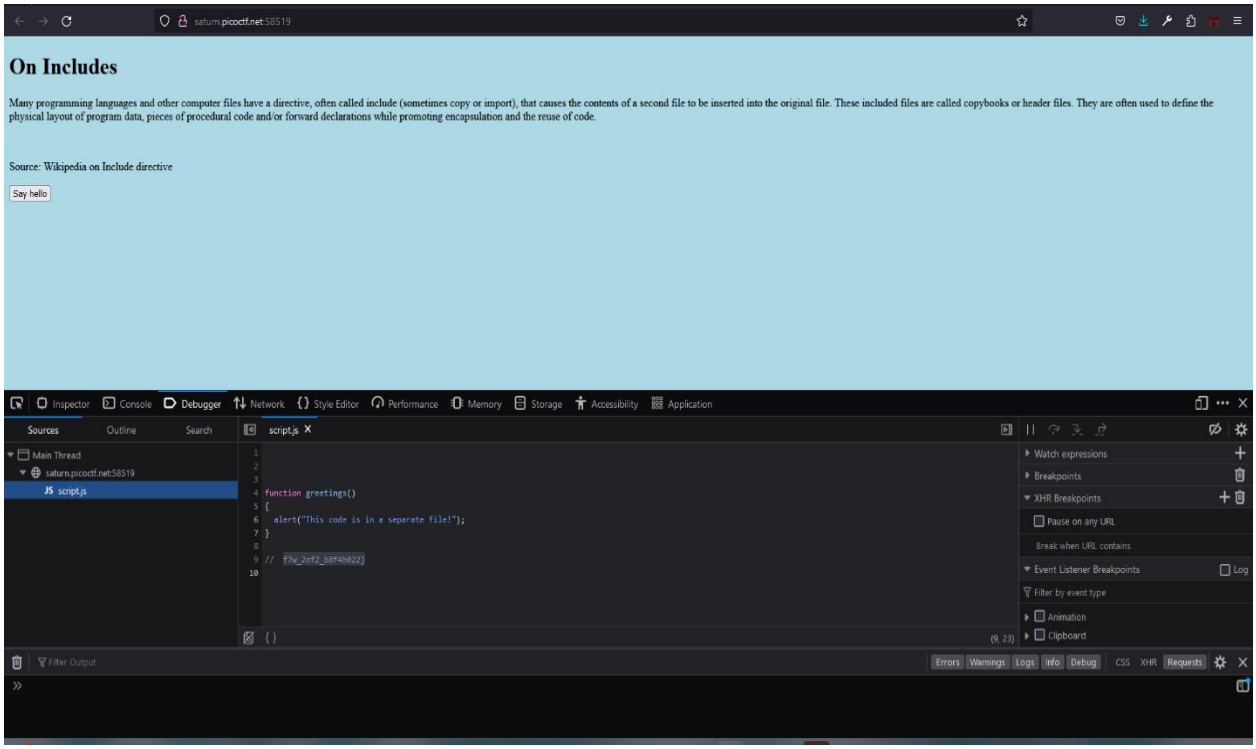
Can you get the flag? Go to this website and see what you can discover. [9]

Hints

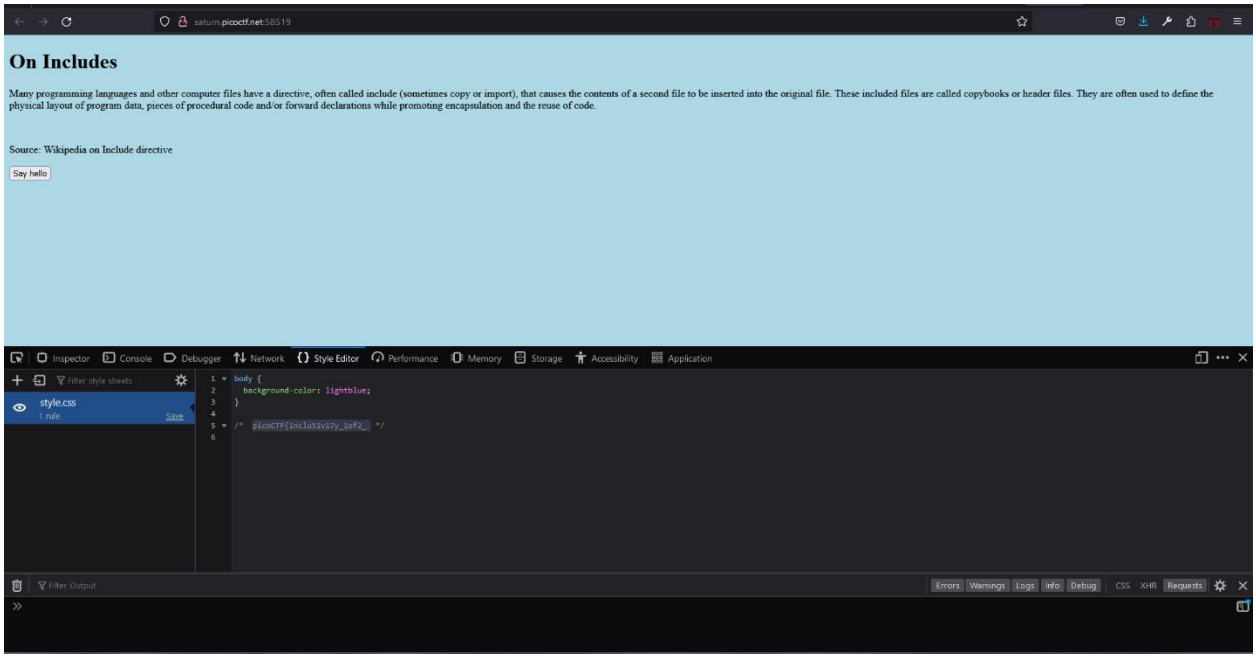
Is there more code than what the inspector initially shows?[9]

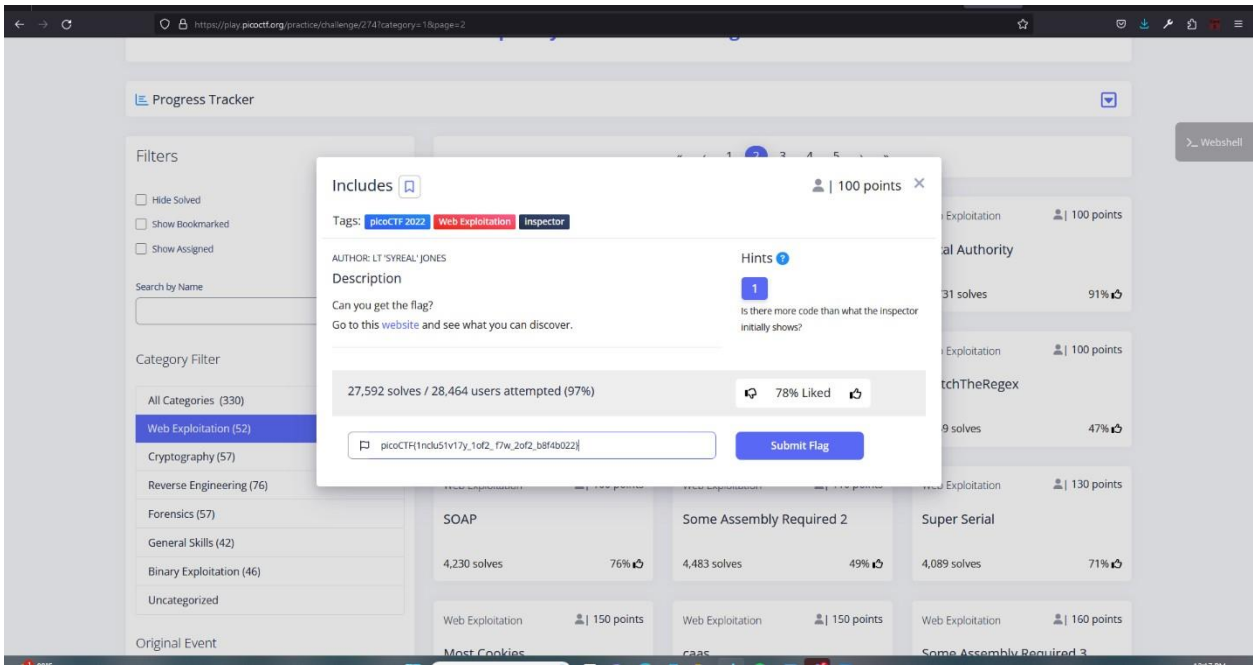
Walkthrough

- Initially, go the webpage. We can see a description and a button. Open the inspect and go to the debugger, It has a JavaScript code called script.js. In that code, we can see a part of the flag.



- Now go to the “Style Editor” and find the first part of the flag.





There are two pieces of the flag we need to find. They are included in JavaScript file and CSS files.

9) Search Source

Description

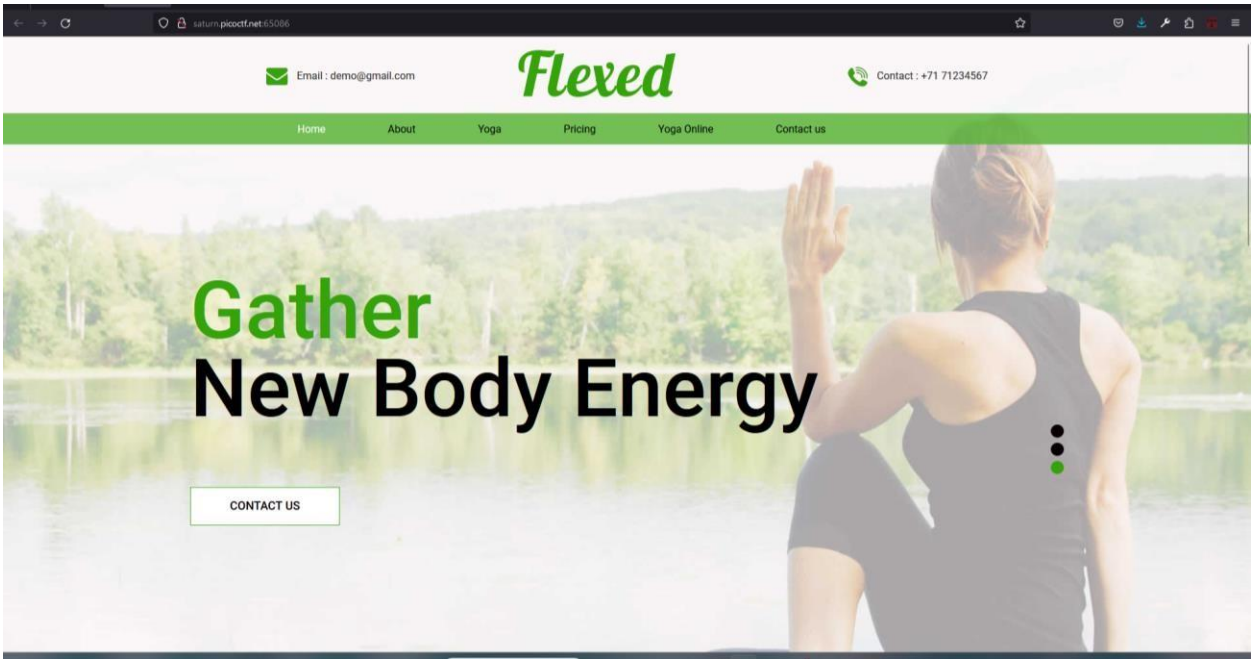
The developer of this website mistakenly left an important artifact in the website source, can you find it? The website is here [10]

Hints

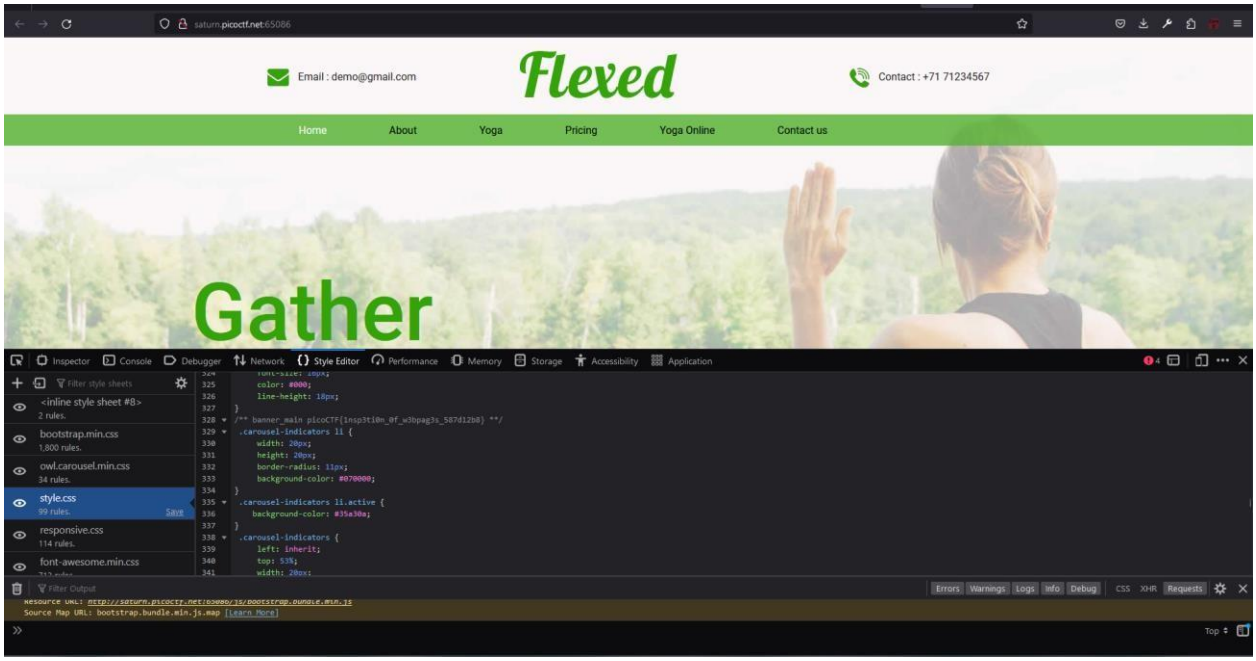
How could you mirror the website on your local machine so you could use more powerful tools for searching? [10]

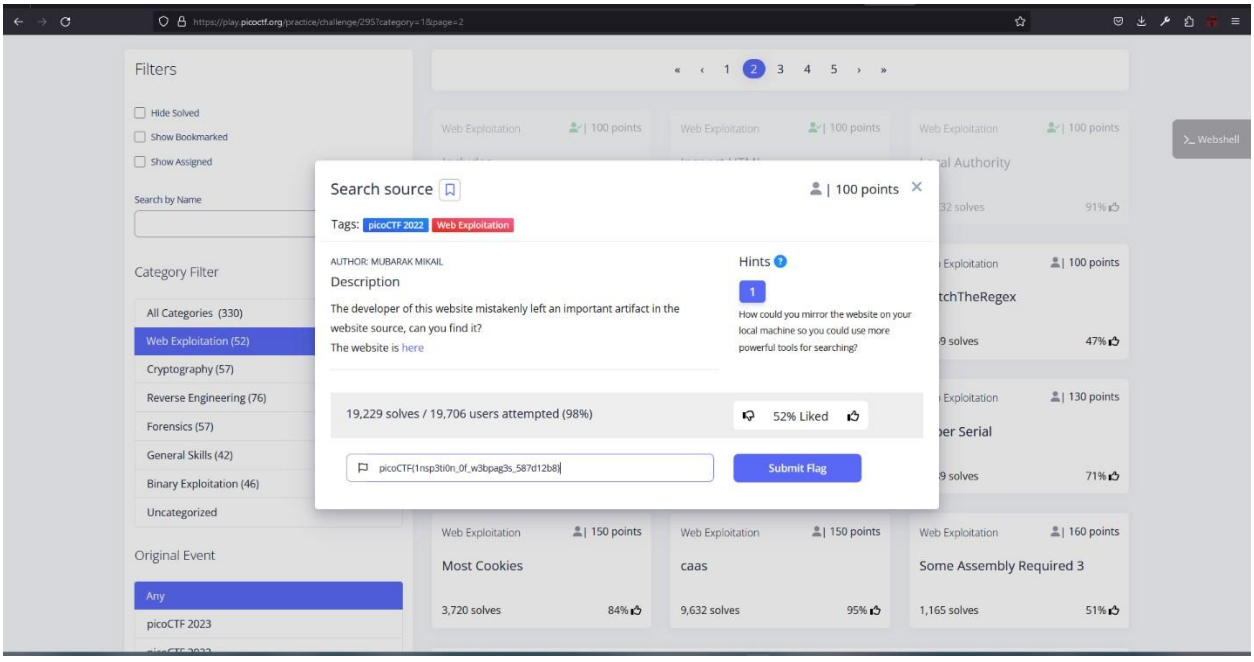
Walkthrough

- Go to the website as they mentioned.



- Now open inspect and go style editor. Choose style.css and find the flag.





The flag is hidden in the style editor. But it has more files. So choose the correct file and find the flag.

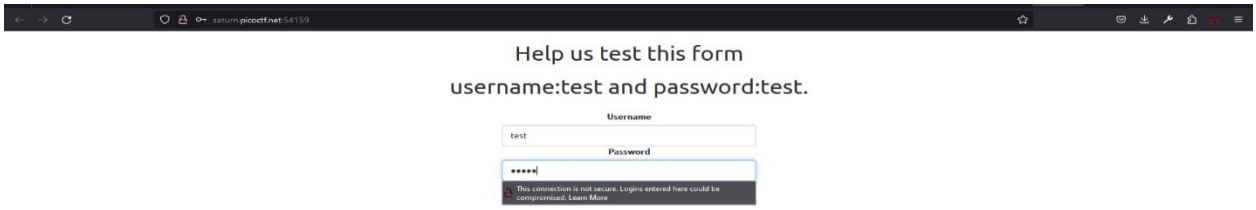
10) Findme

Description

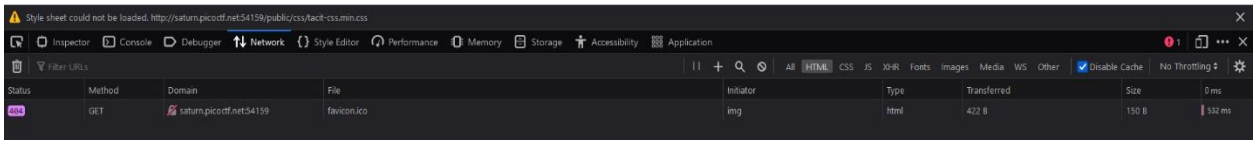
Help us test the form by submiting the username as `test` and password as `test`!
Additional details will be available after launching your challenge instance. [11]

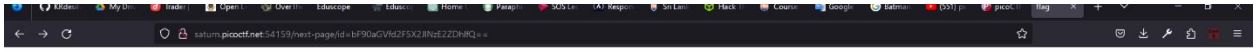
Walkthrough

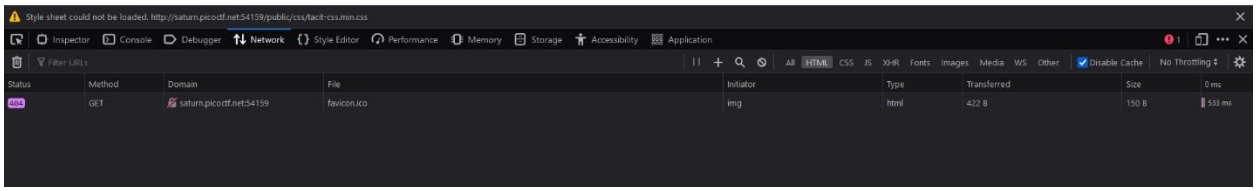
- When we go to the webpage, it ask us username and password. As the description says we can use username: test and password: test!



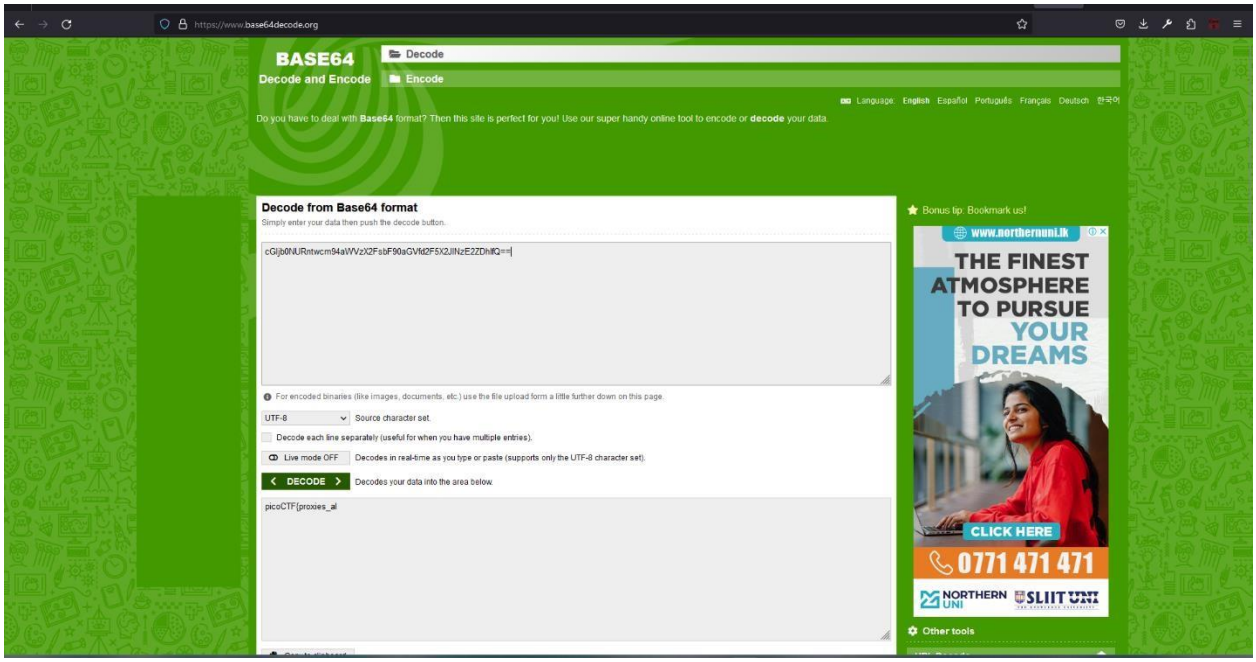
- Now we are in another page but, still we cannot see the flag. Then go back one page. Now we can see a part of the flag. Again go back one page we can see another part of the flag.

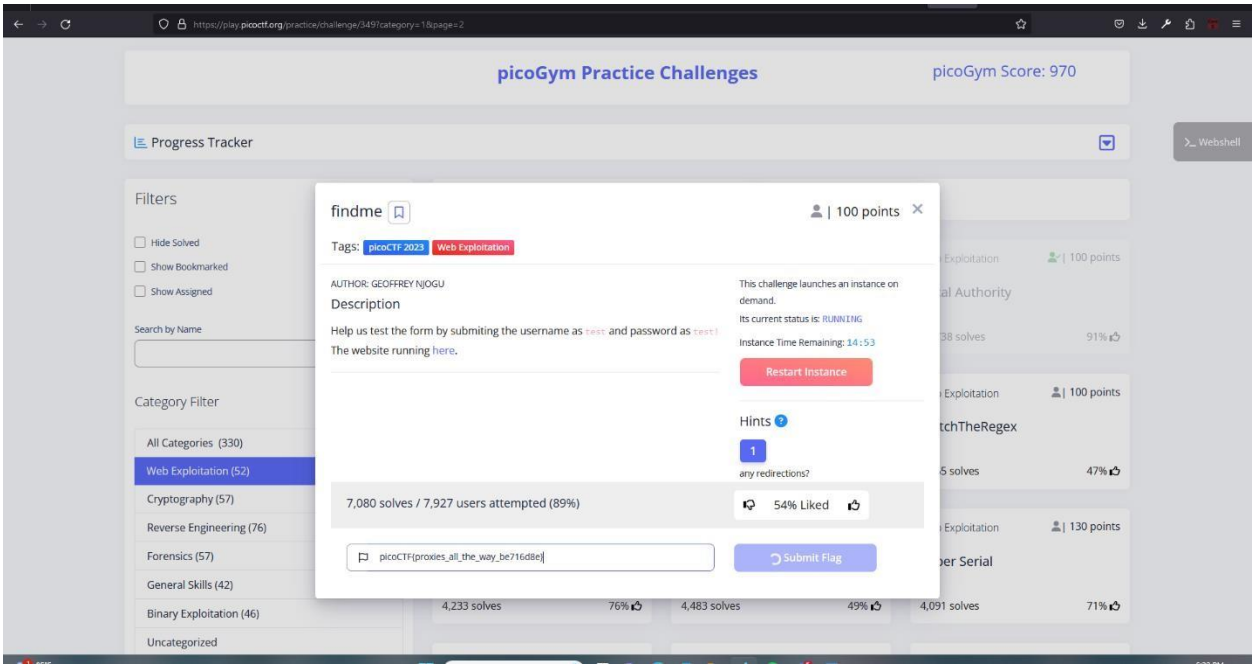






- If we found the flag, we need to decode it. Go to the website called “base 64 decode” and decode it.





This challenge has a time reminder. This flag is encoded flag. So we should decode and find the correct flag.

11) Inspect HTML

Description

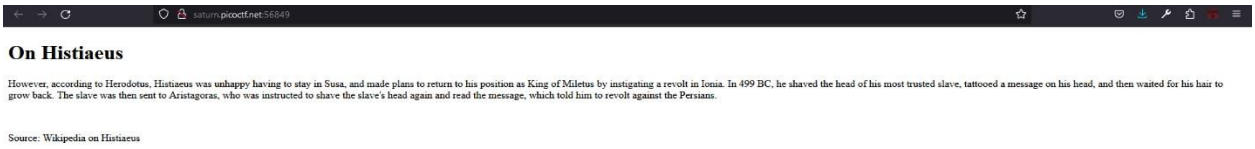
Can you get the flag? Go to this website and see what you can discover. [12]

Hint

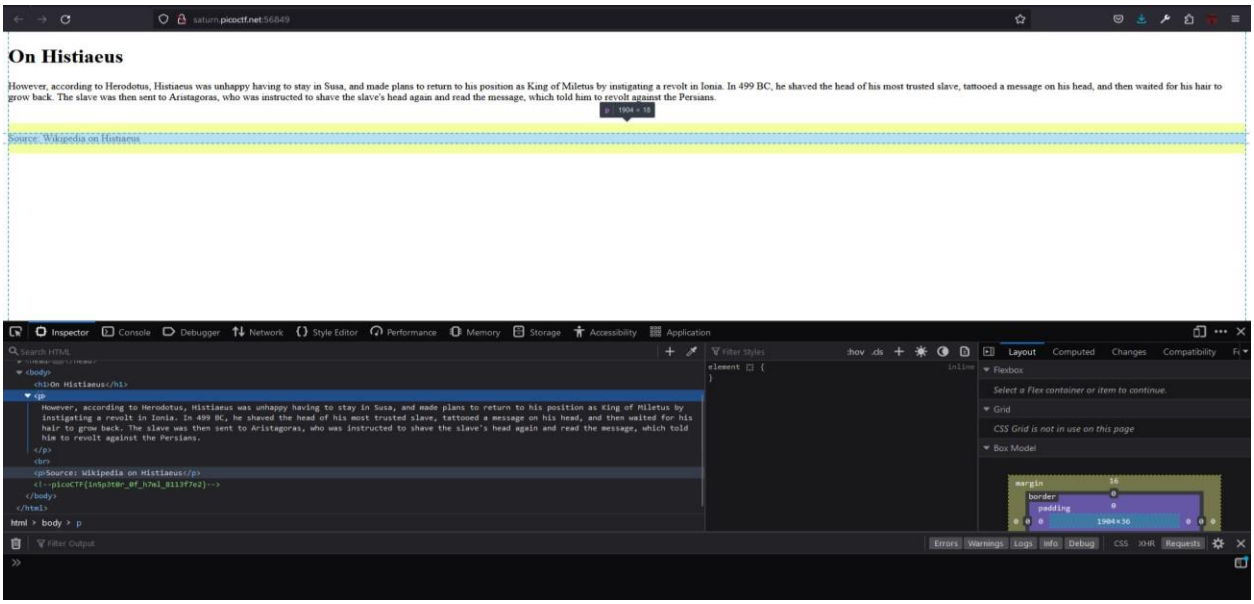
What is the web inspector in web browsers? [12]

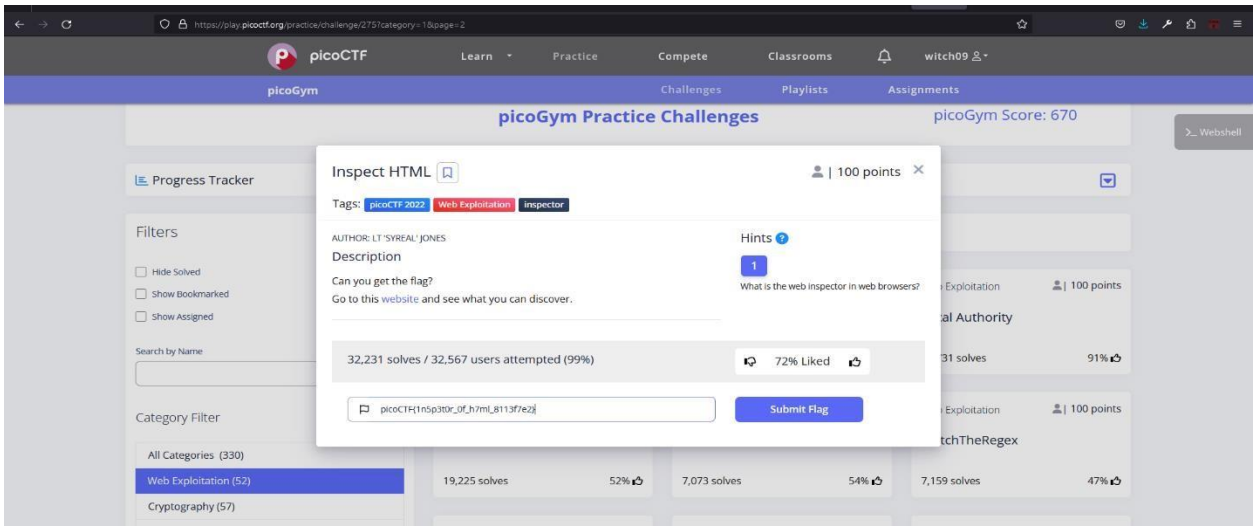
Walkthrough

- Go to the website using link. The we can see a topic and a paragraph.



- Open inspect and go to “inspector”. Now we can see the flag.





This flag is hidden in inspector. Look at that code and we can easily find the flag.

12)Local Authority

Description

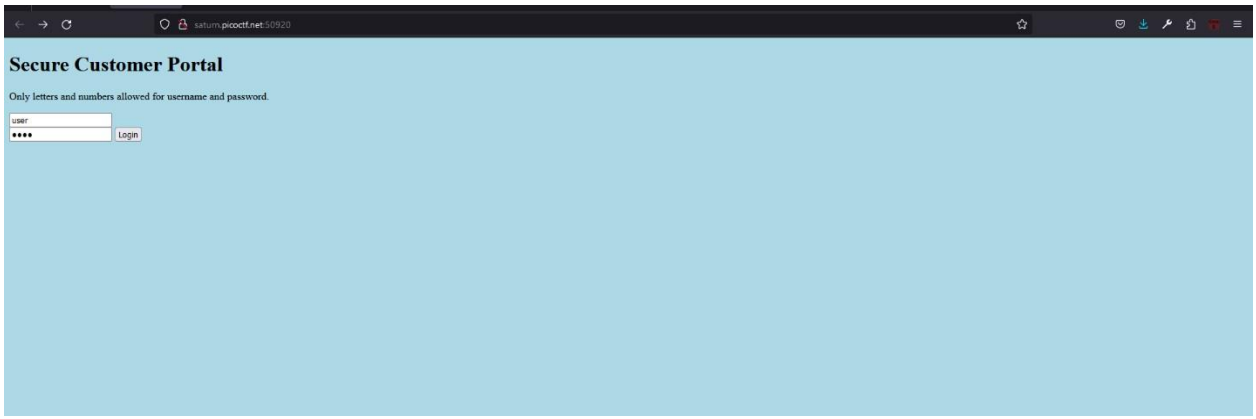
Can you get the flag? Go to this website and see what you can discover. [13]

Hints

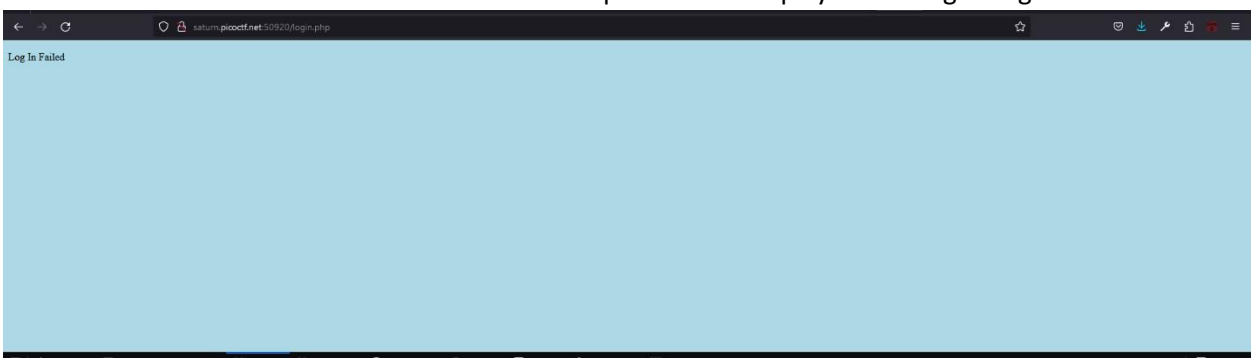
How is the password checked on this website? [13]

Walkthrough

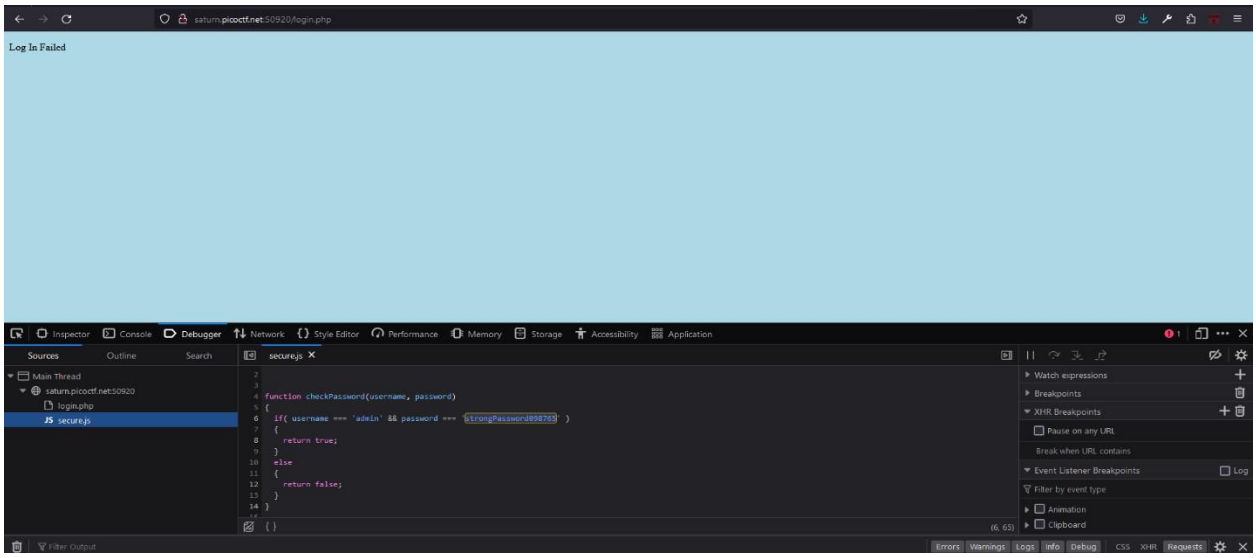
- Go to the website. It has a portal. But we do not know username and password. So I tried to fill it in with random username and password.



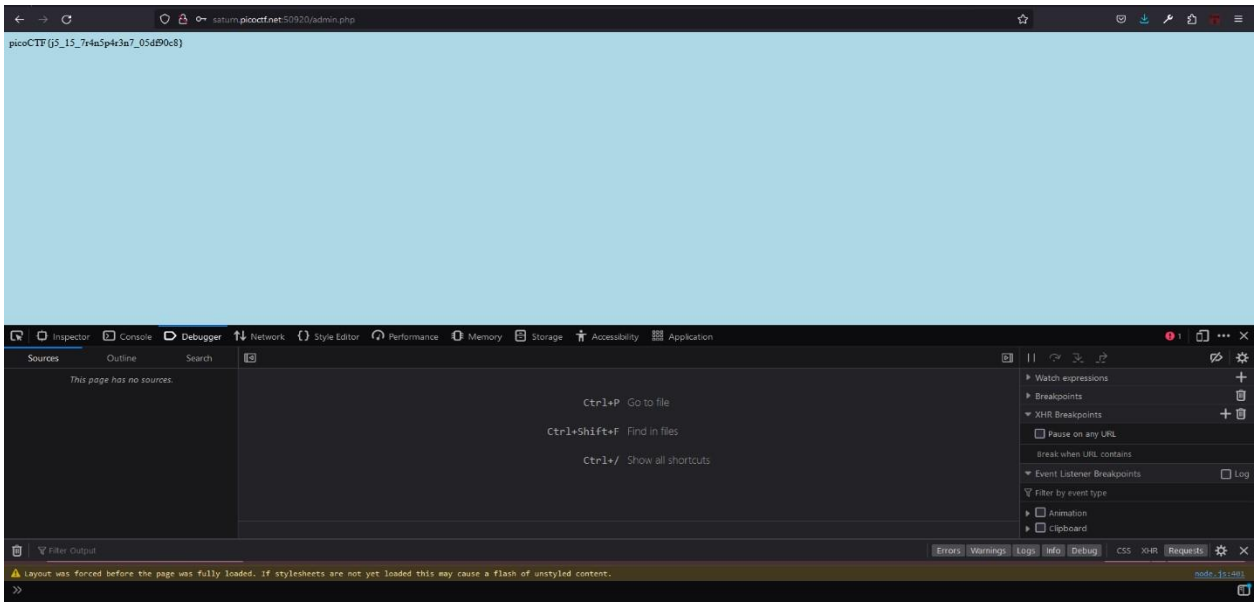
- When it filled with random username and password it displays a message “Login failed”



- Open inspect and go to “Debugger”, Now we can see “secure.js” file. When open it they give the correct username and password.



- Using that username and password we can access the flag.



For this challenge we need to find the correct username and password initially. Then they give us the flag.

Conclusion

The multifaceted word of PicoCTF challenges has been informed by “Grab the PicoCTF flags.” These difficulties extend outside technical competence, encouraging universal and critical thinking abilities. Participants go on a journey of continual learning as they capture flags, demonstrating the durability required in the dynamic cybersecurity environment. PicoCTF challenges represent the commitment to protecting digital spaces by proactive knowledge, not just victories. In addition to serving as a training ground for cybersecurity experts, PicoCTF is a symbol of the flexibility and group intelligence required to protect our digital environment. This illustrates a defense morality that emphasizes proactive learning. The influence of participants’ skills spread over the larger cybersecurity area as they advance. A journey where each flag seized expresses the booming commitment to preserving our digital future. “Grab the PicoCTF fags” demonstrates the way to strengthen cyber competency in the digital age when dangers are constantly evolving.

References

[1] pico-Boo!: How to avoid scaring students away in a CTF competition. “Introduction”, Available: https://picoctf.org/pdfs/FINAL_CISSE_paper.pdf

[2] picoCTF: How gamified cybersecurity piques curiosity in STEM “Kyle Thornton”, Available: https://blogs.cisco.com/csr/picoctf-how-gamified-cybersecurity-piques-curiosity-in-stem

[3] picoCTF - Web exploitation : Insp3c0r

[4] picoCTF - Web exploitation: Scavenger Hunt

[5] picoCTF - Web exploitation: Where are the robots

[6] picoCTF - Web exploitation: logon

[7] picoCTF - Web exploitation: don’t-use-client-side

[8] picoCTF - Web exploitation: It is my Birthday

[9] picoCTF - Web exploitation: Includes

[10] picoCTF - Web exploitation: Search Source

[11] picoCTF - Web exploitation: Findme

[12] picoCTF - Web exploitation: Inspect HTML

[13] picoCTF - Web exploitation: Local Authority