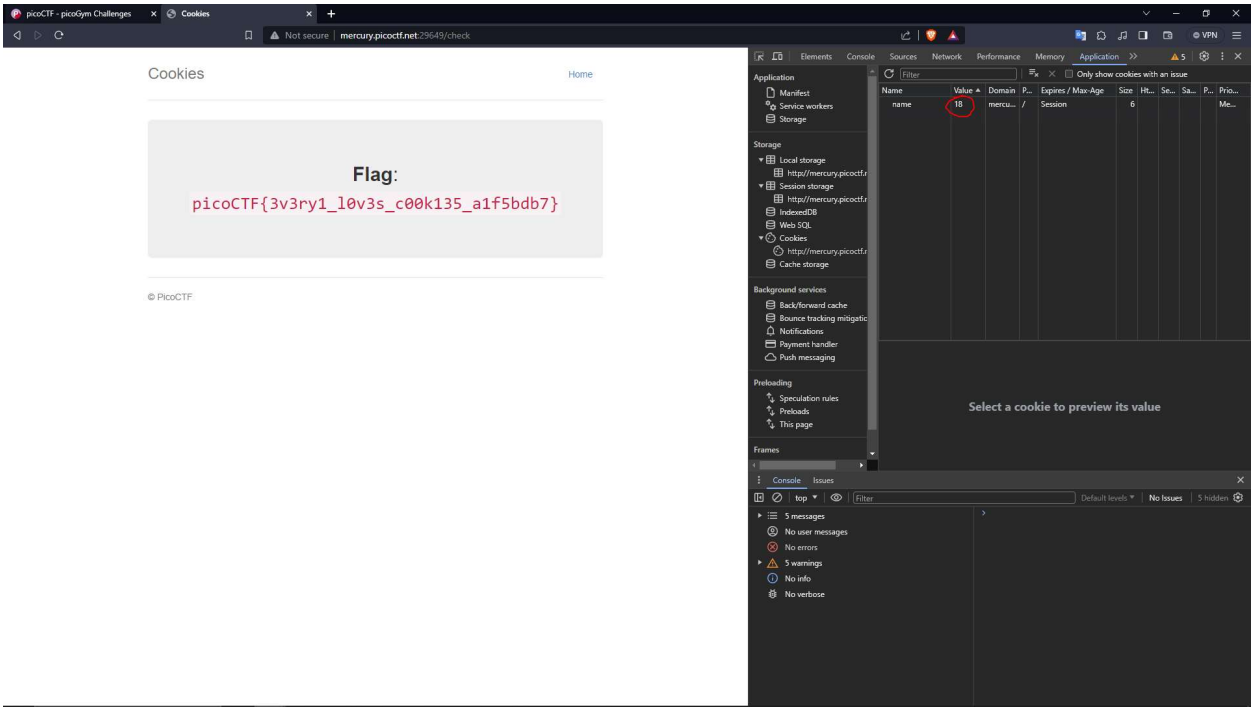
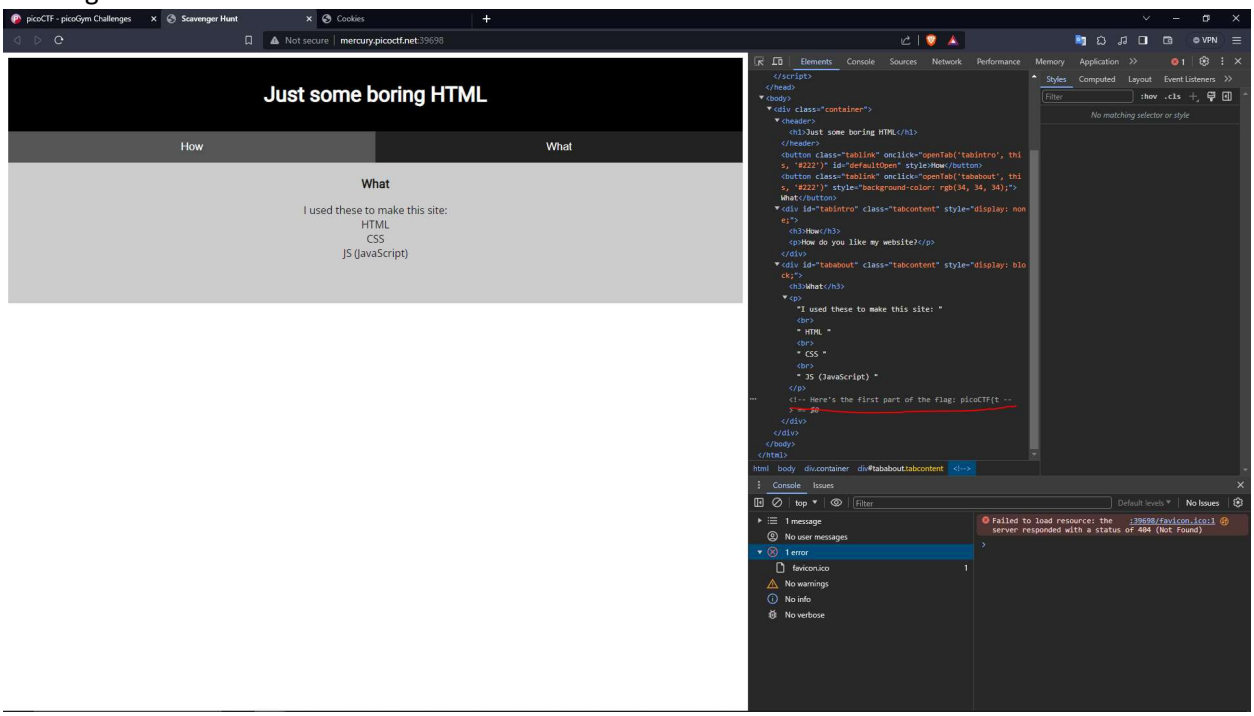
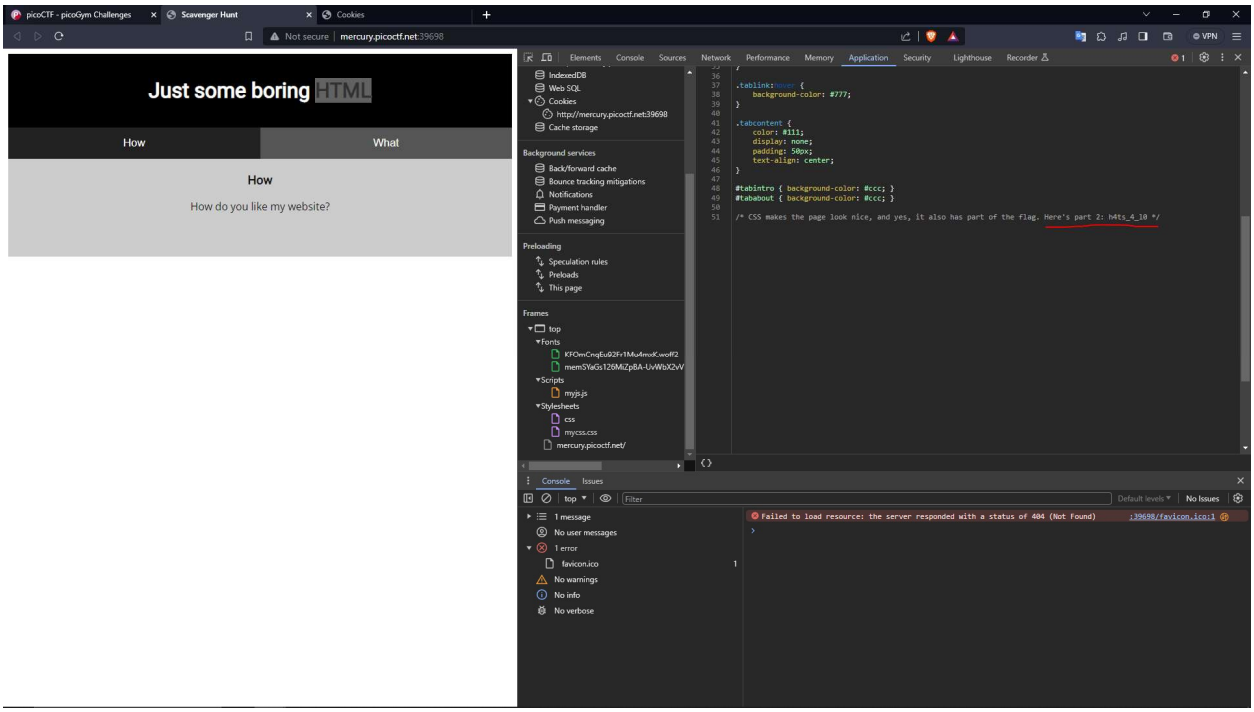
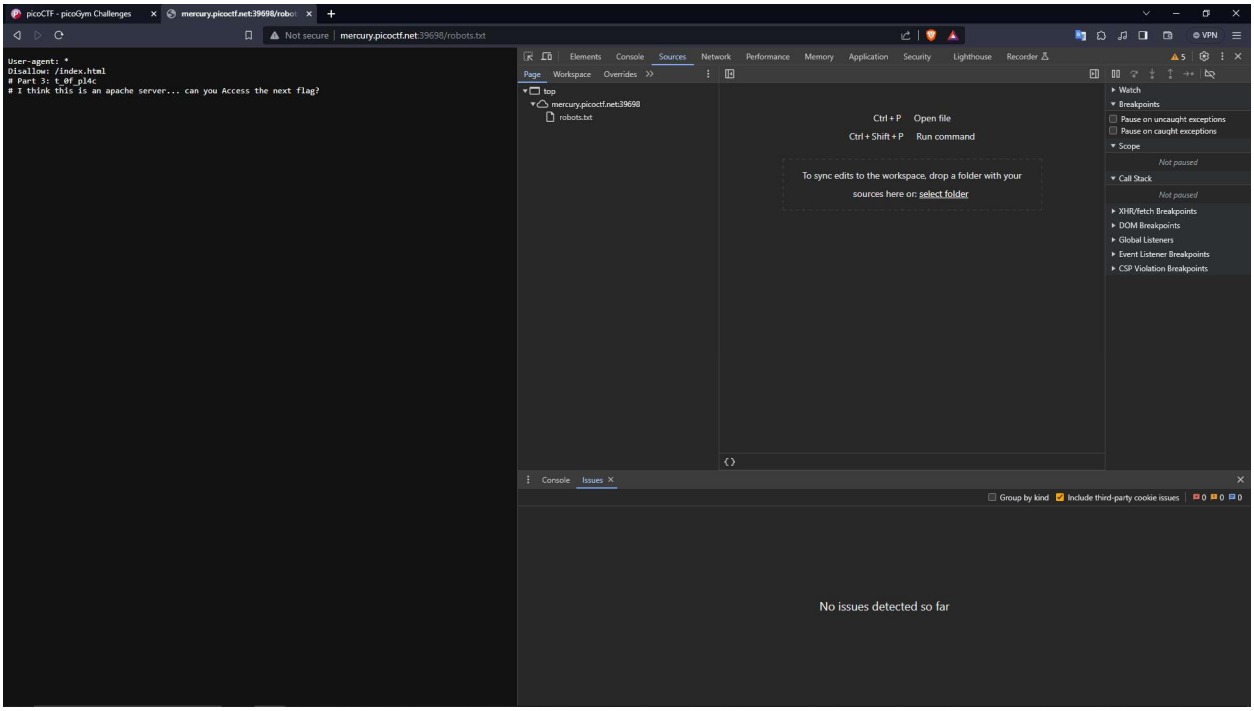
Cookies

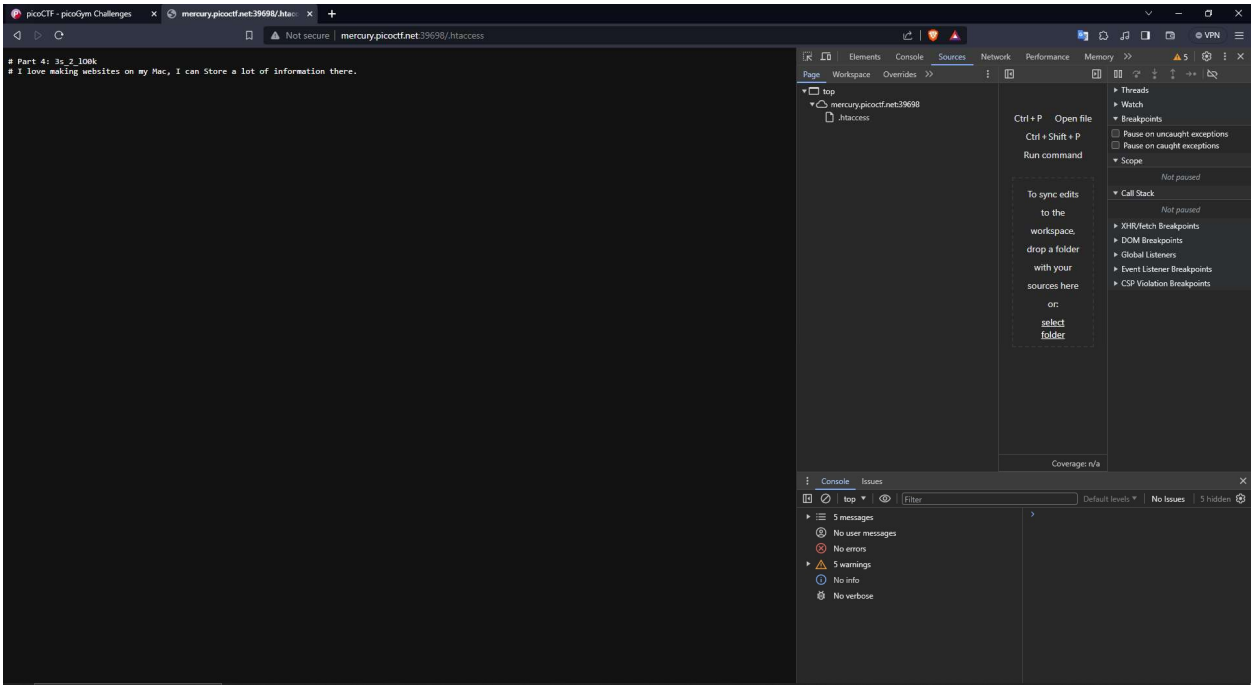


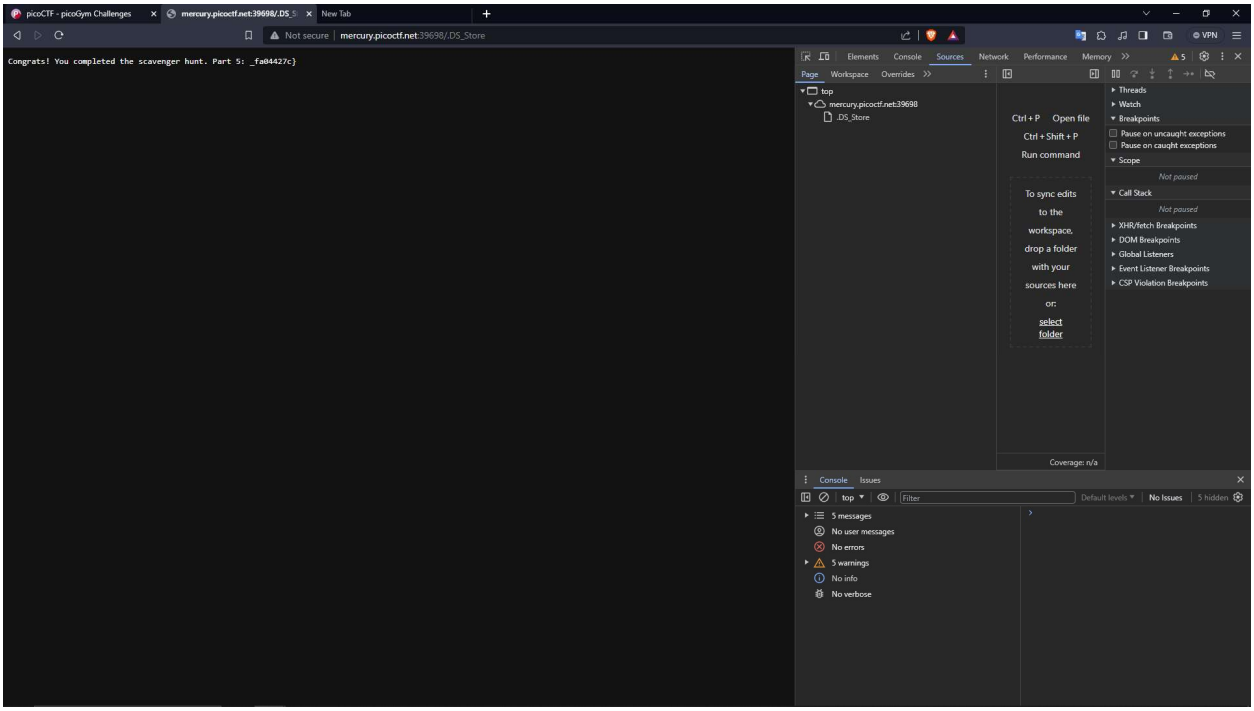
Scavenger hunt



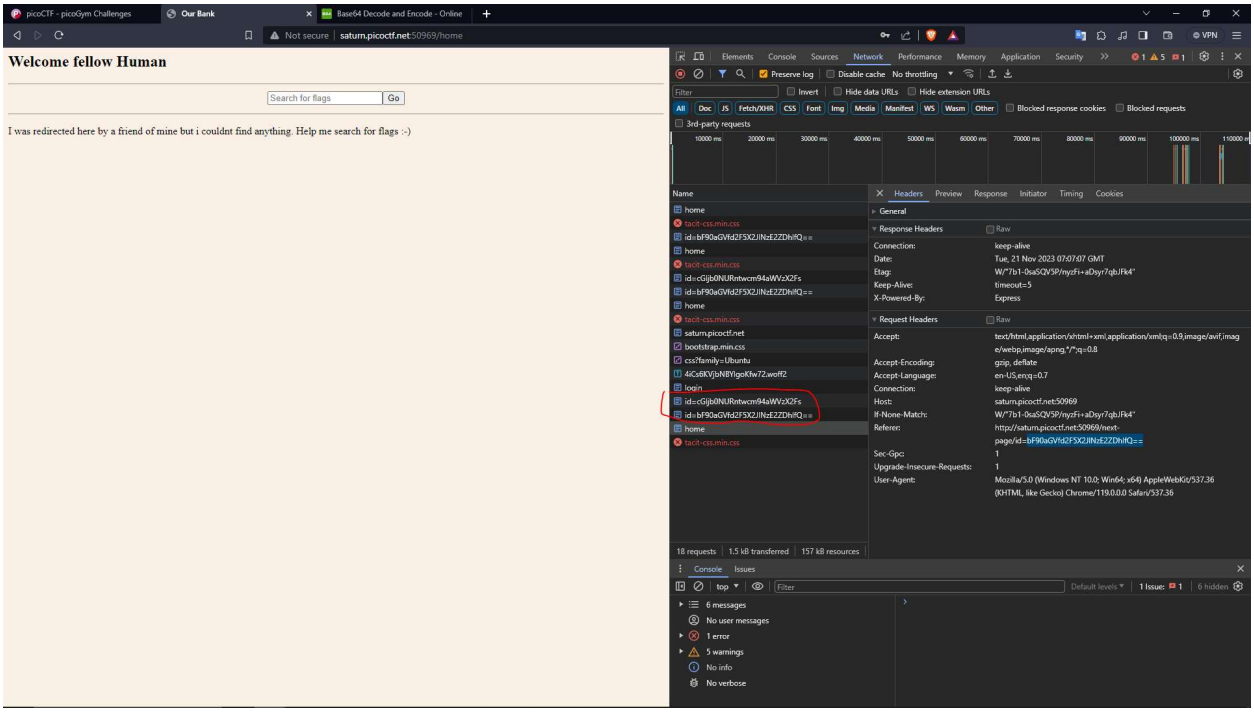

picoCTF - picoGym Challenges
Scavenger Hunt
Cookies
Not secure
mercury.picoctf.net:39698
Just some boring HTML
How
What
How
How do you like my website?
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
IndexedDB
Web SQL
Cookies
http://mercury.picoctf.net:39698
Cache storage
Background services
Back/forward cache
Bounce tracking mitigations
Notifications
Payment handler
Push messaging
Preloading
Speculation rules
Preloads
This page
Frames
top
Fonts
Scripts
myjs.js
Stylesheets
css
mycss.css
mercury.picoctf.net/
.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 */
Console
Issues
top
Filter
Default levels
No Issues
1 message
No user messages
1 error
favicon.ico
No warnings
No info
No verbose
Failed to load resource: the server responded with a status of 404 (Not Found)
:39698/favicon.ico:1

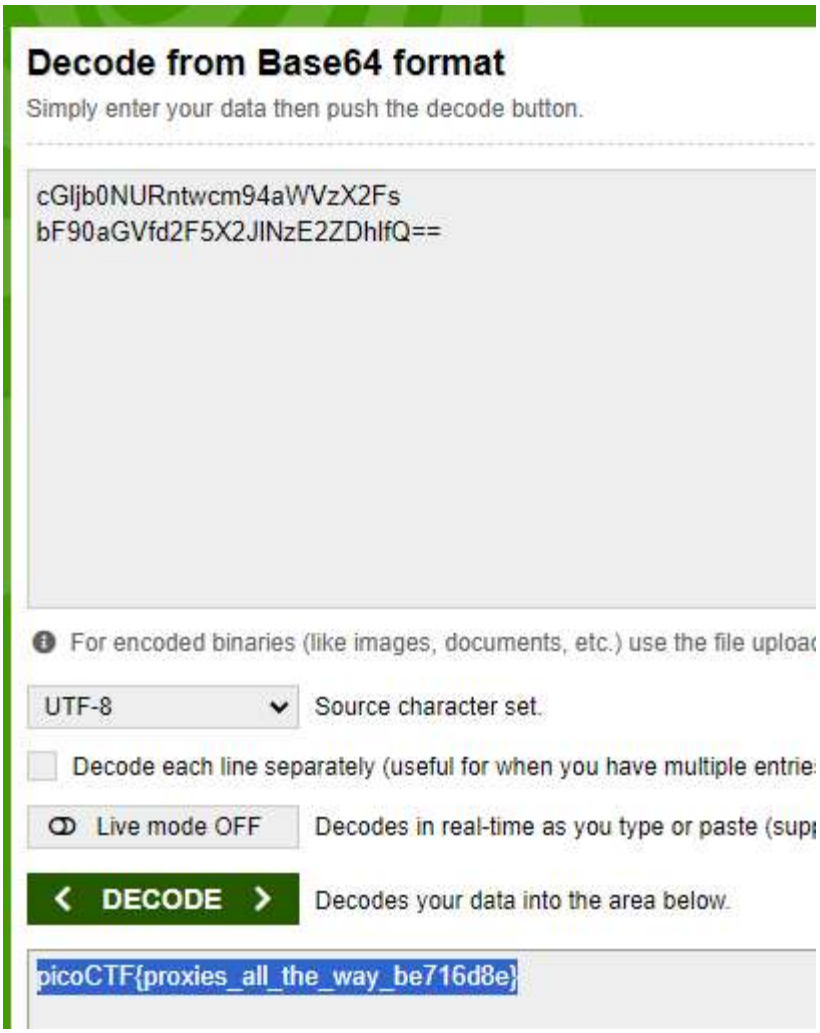

picoCTF - picoGym Challenges
mercury.picoctf.net:39698/robots.txt
Not secure
mercury.picoctf.net:39698/robots.txt
User-agent: *
Disallow: /index.html
Part 3: t_0f_pl4c
I think this is an apache server... can you Access the next flag?
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Page
Workspace
Overrides
top
mercury.picoctf.net:39698
robots.txt
Ctrl + P Open file
Ctrl + Shift + P Run command
To sync edits to the workspace, drop a folder with your sources here or: select folder
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
Console
Issues
Group by kind
Include third-party cookie issues
No issues detected so far


Part 4: 3s_2_l00k
I love making websites on my Mac, I can Store a lot of information there.

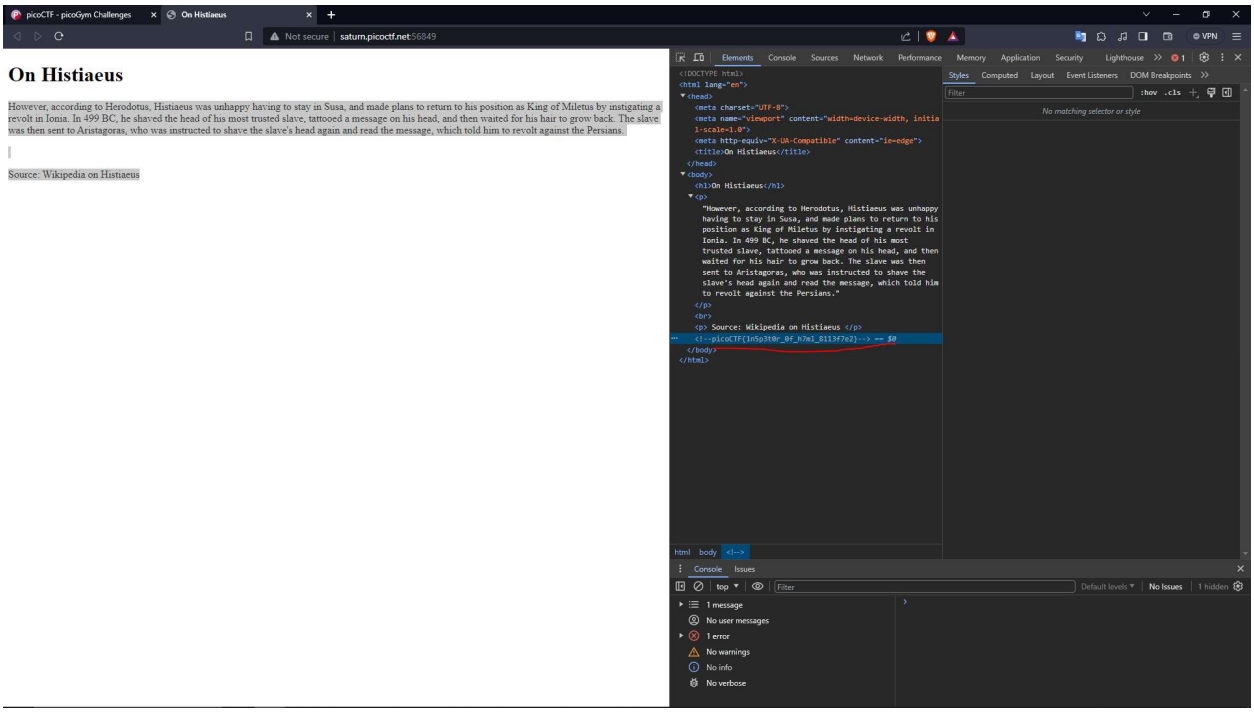

Congrats! You completed the scavenger hunt. Part 5: _fa04427c}

Findme

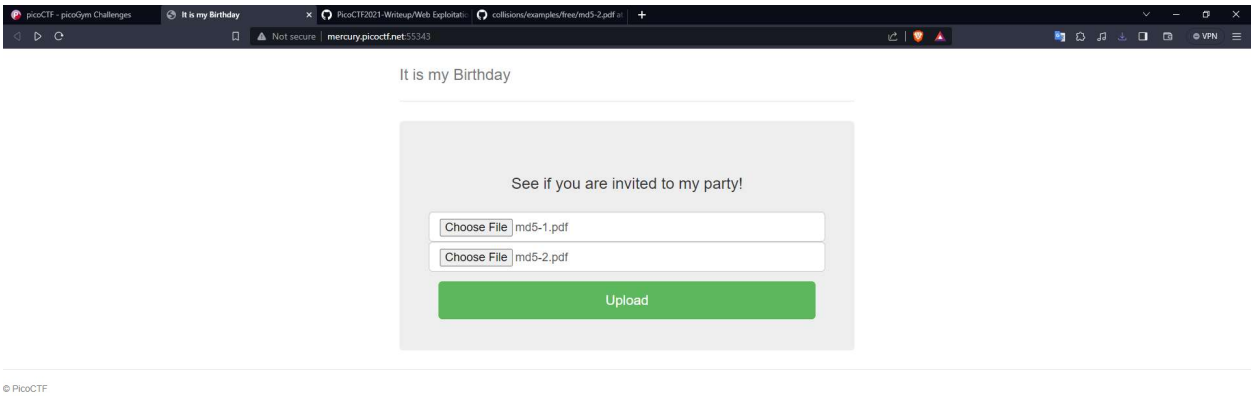

picoCTF - picoGym Challenges
Our Bank
Base64 Decode and Encode - Online
Not secure
saturn.picoctf.net:50969/home
Welcome fellow Human
Search for flags
Go
I was redirected here by a friend of mine but i couldnt find anything. Help me search for flags :-)
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Preserve log
Disable cache
No throttling
Hide data URLs
Hide extension URLs
Blocked response cookies
Blocked requests
3rd-party requests
Name
home
tacit-css.min.css
id=bF90aGVfd2F5X2JlNzE2ZDhlfQ==
id=cGljb0NURntwcm94aWVzX2Fs
saturn.picoctf.net
bootstrap.min.css
css?family=Ubuntu
4iCs6KVjbNBYlgoKfw72.woff2
login
Headers
Preview
Response
Initiator
Timing
Cookies
General
Response Headers
Request Headers
Connection: keep-alive
Date: Tue, 21 Nov 2023 07:07:07 GMT
Etag: W/"7b1-0saSQV5P/nyzFi+aDsyr7qbJFk4"
Keep-Alive: timeout=5
X-Powered-By: Express
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.7
Connection: keep-alive
Host: saturn.picoctf.net:50969
If-None-Match: W/"7b1-0saSQV5P/nyzFi+aDsyr7qbJFk4"
Referer: http://saturn.picoctf.net:50969/next-page/id=bF90aGVfd2F5X2JlNzE2ZDhlfQ==
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
18 requests
1.5 kB transferred
157 kB resources
Console
Issues
6 messages
No user messages
1 error
5 warnings
No info
No verbose

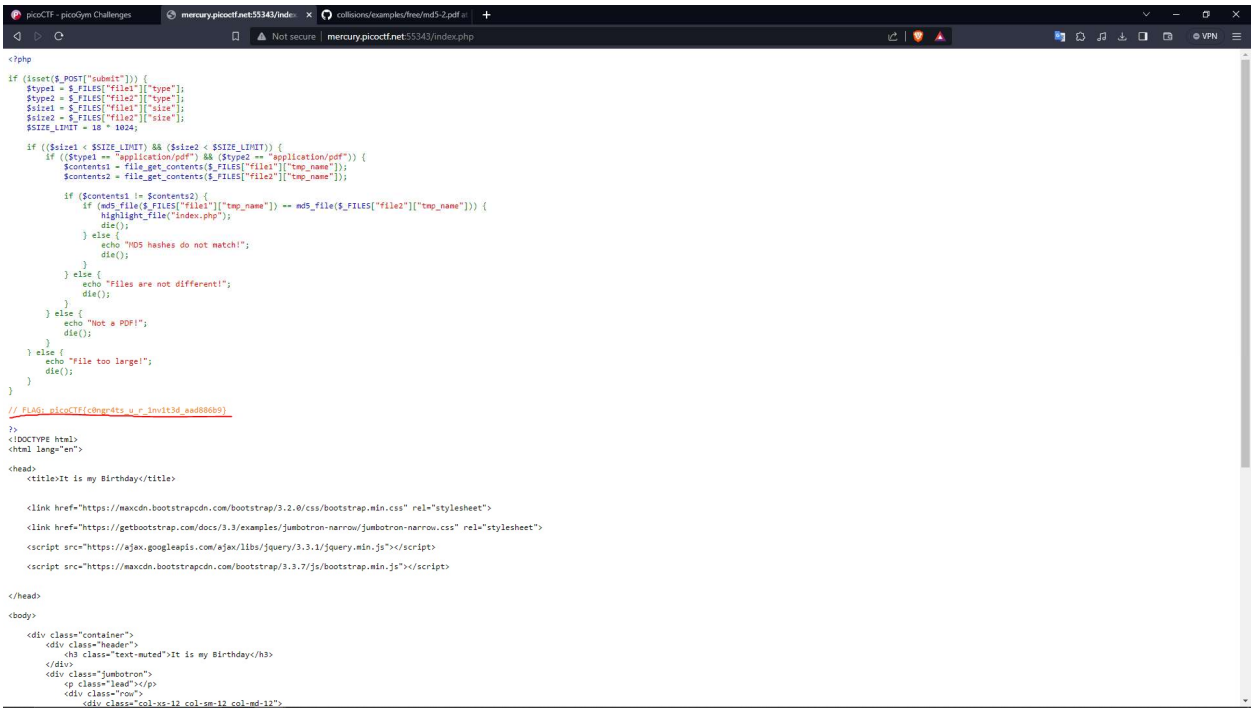


Inspect HTML



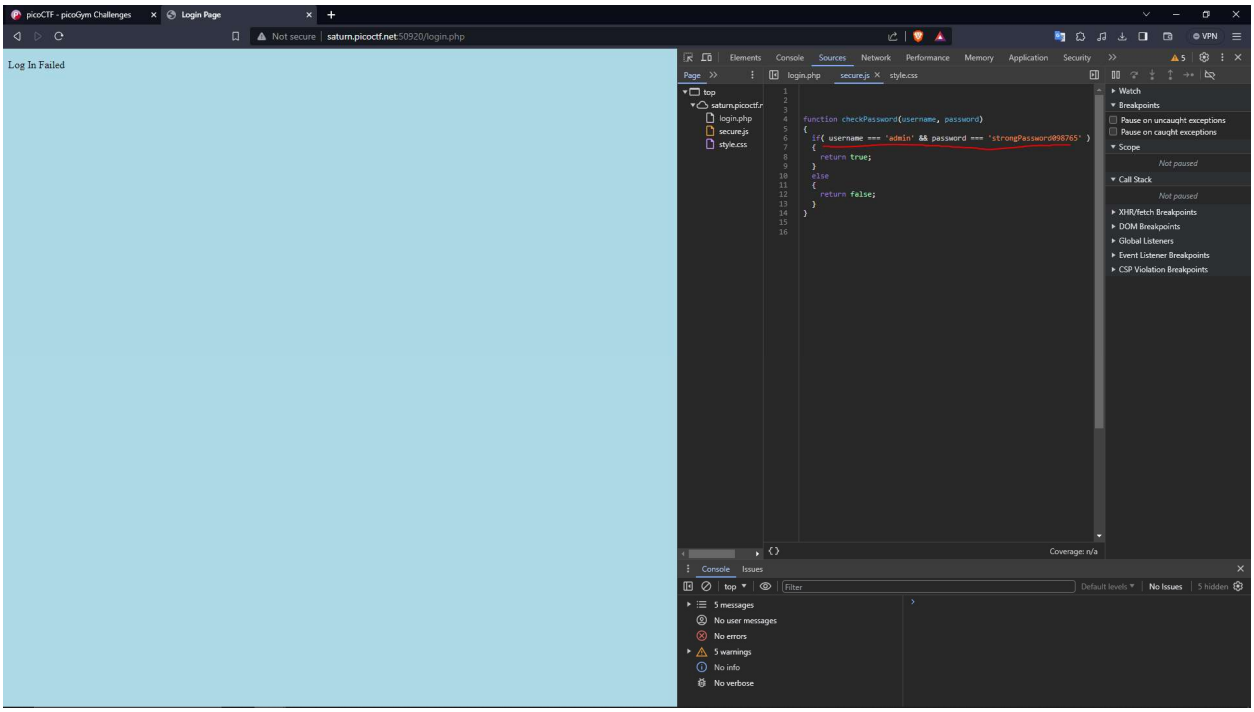
It is my birthday

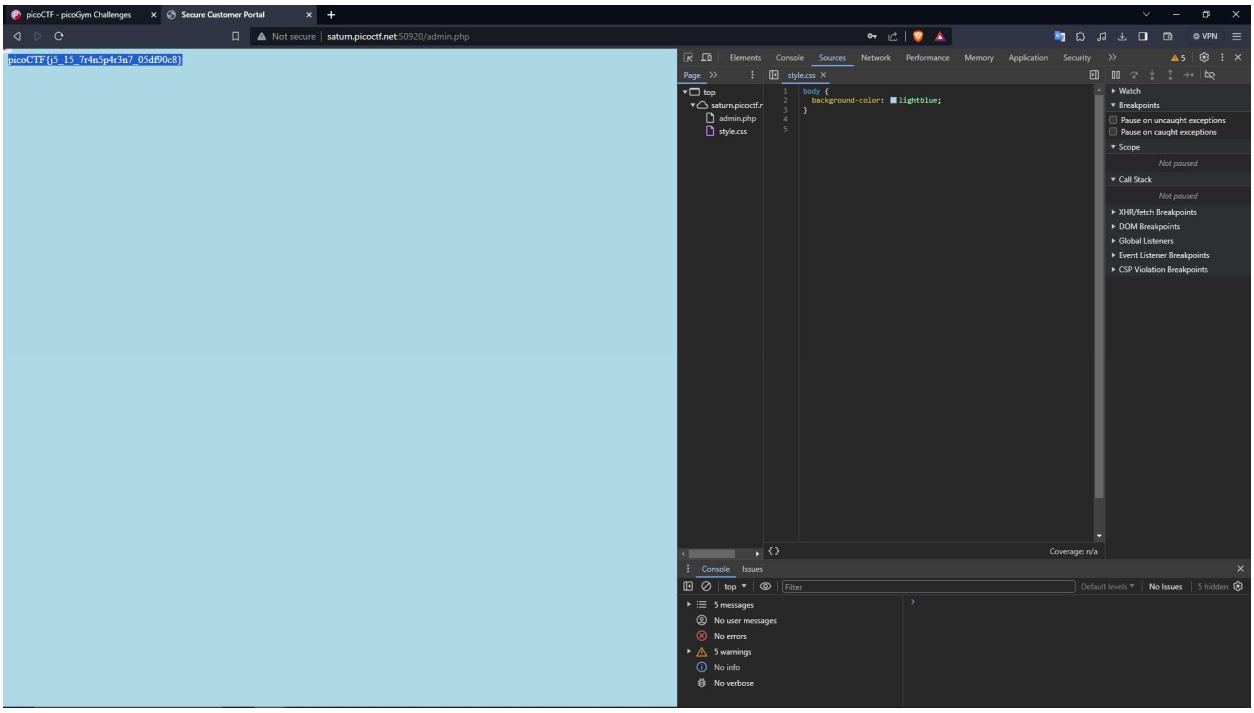




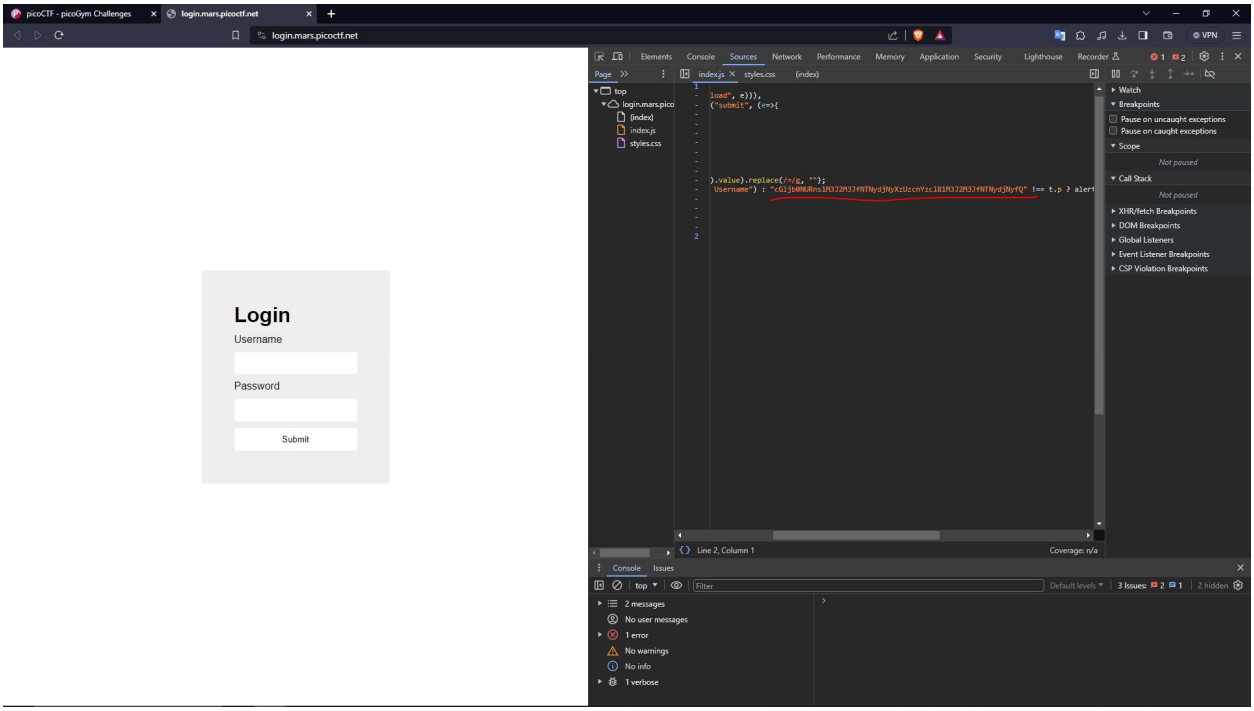

```php
<?php

if (isset($_POST["submit"])) {
    $type1 = $_FILES["file1"]["type"];
    $type2 = $_FILES["file2"]["type"];
    $size1 = $_FILES["file1"]["size"];
    $size2 = $_FILES["file2"]["size"];
    $SIZE_LIMIT = 18 * 1024;

    if (($size1 < $SIZE_LIMIT) && ($size2 < $SIZE_LIMIT)) {
        if (($type1 == "application/pdf") && ($type2 == "application/pdf")) {
            $contents1 = file_get_contents($_FILES["file1"]["tmp_name"]);
            $contents2 = file_get_contents($_FILES["file2"]["tmp_name"]);

            if ($contents1 != $contents2) {
                if (md5_file($_FILES["file1"]["tmp_name"]) == md5_file($_FILES["file2"]["tmp_name"])) {
                    highlight_file("index.php");
                    die();
                } else {
                    echo "MD5 hashes do not match!";
                    die();
                }
            } else {
                echo "Files are not different!";
                die();
            }
        } else {
            echo "Not a PDF!";
            die();
        }
    } else {
        echo "File too large!";
        die();
    }
}

// FLAG: picoCTF{c0ngr4ts_u_r_1nv1t3d_aad886b9}

?>
<!DOCTYPE html>
<html lang="en">

<head>
    <title>It is my Birthday</title>


    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">

    <link href="https://getbootstrap.com/docs/3.3/examples/jumbotron-narrow/jumbotron-narrow.css" rel="stylesheet">

    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>

    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>


</head>

<body>

    <div class="container">
        <div class="header">
            <h3 class="text-muted">It is my Birthday</h3>
        </div>
        <div class="jumbotron">
            <p class="lead"></p>
            <div class="row">
                <div class="col-xs-12 col-sm-12 col-md-12">
```

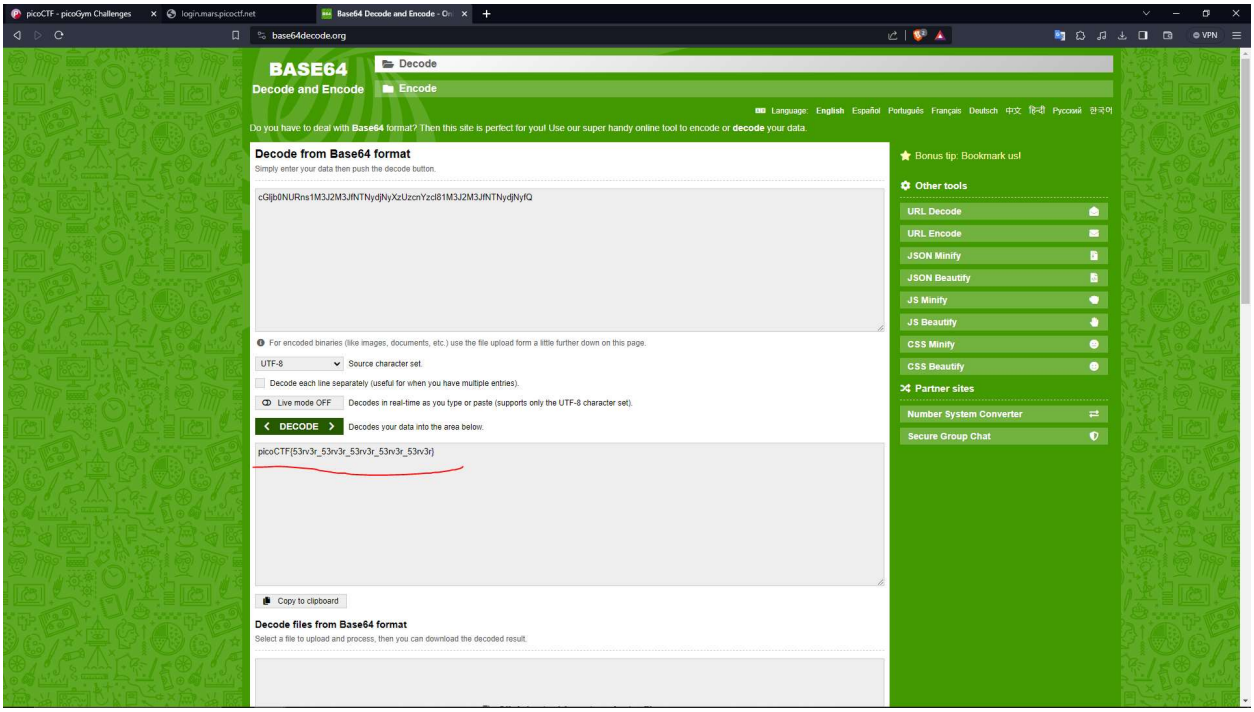
Local Authority



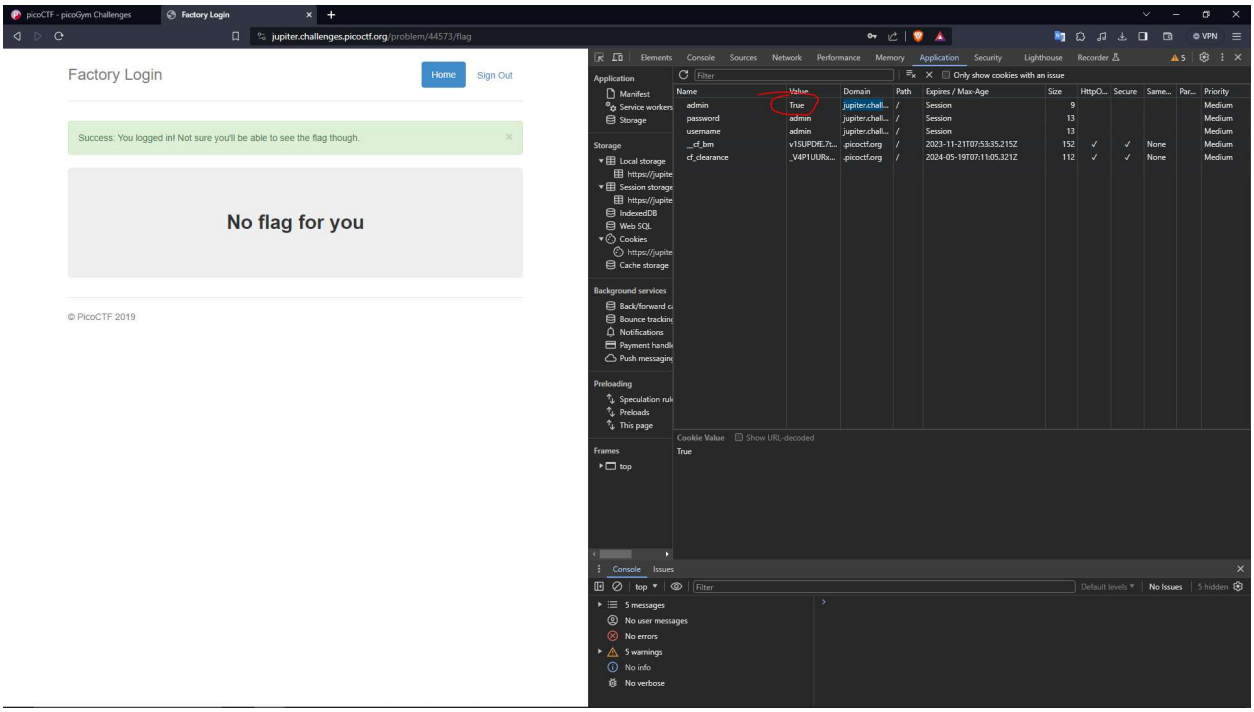

picoCTF - picoGym Challenges
Secure Customer Portal
Not secure | saturn.picoctf.net:50920/admin.php
picoCTF{j5_7r4n5p4r3n7_05df90c8}
Elements
Console
Sources
Network
Performance
Memory
Application
Security
style.css
body {
background-color: lightblue;
}
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
Coverage: n/a
Console
Issues
5 messages
No user messages
No errors
5 warnings
No info
No verbose

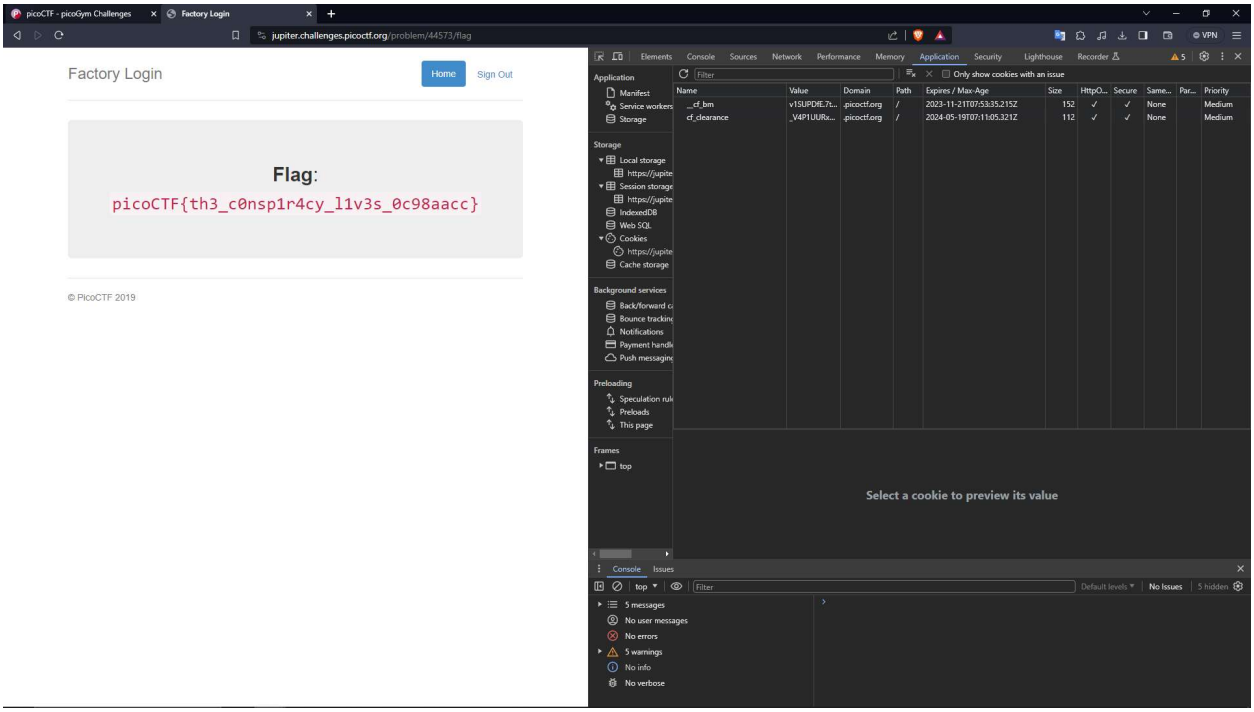
Login


picoCTF - picoGym Challenges
login.mars.picoctf.net
Login
Username
Password
Submit
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
index.js
styles.css
(index)
load", e))),
("submit", (e=>{
).value).replace(/^/g, "");
Username") : "c6ljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzc181M3J2M3JfNTNydjNyfQ" !== t.p) alert
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
Line 2, Column 1
Coverage: n/a
Console
Issues
2 messages
No user messages
1 error
No warnings
No info
1 verbose

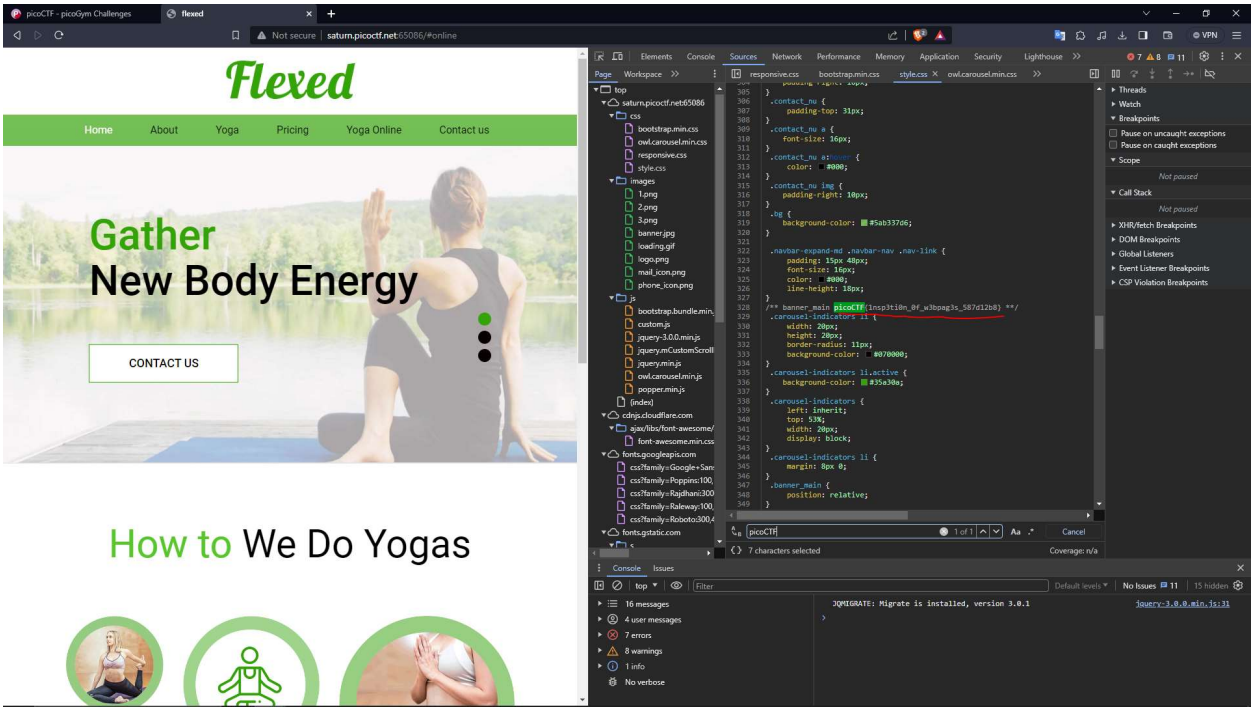


Factory Login

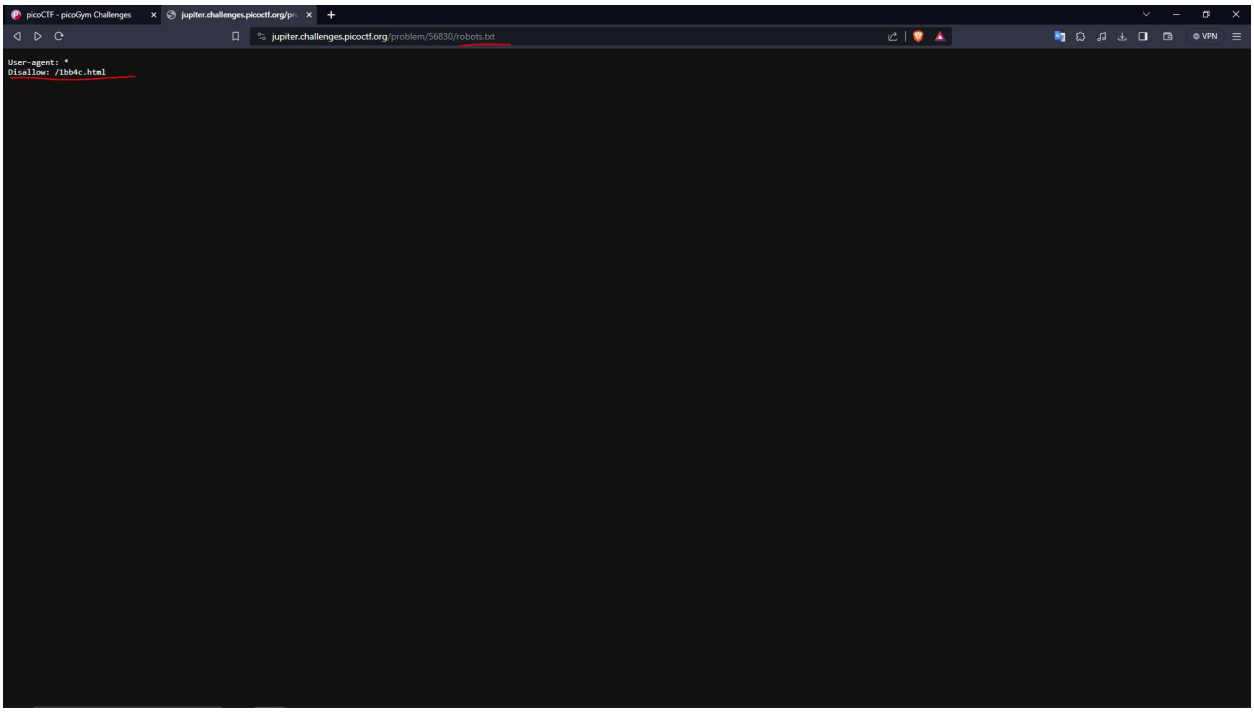


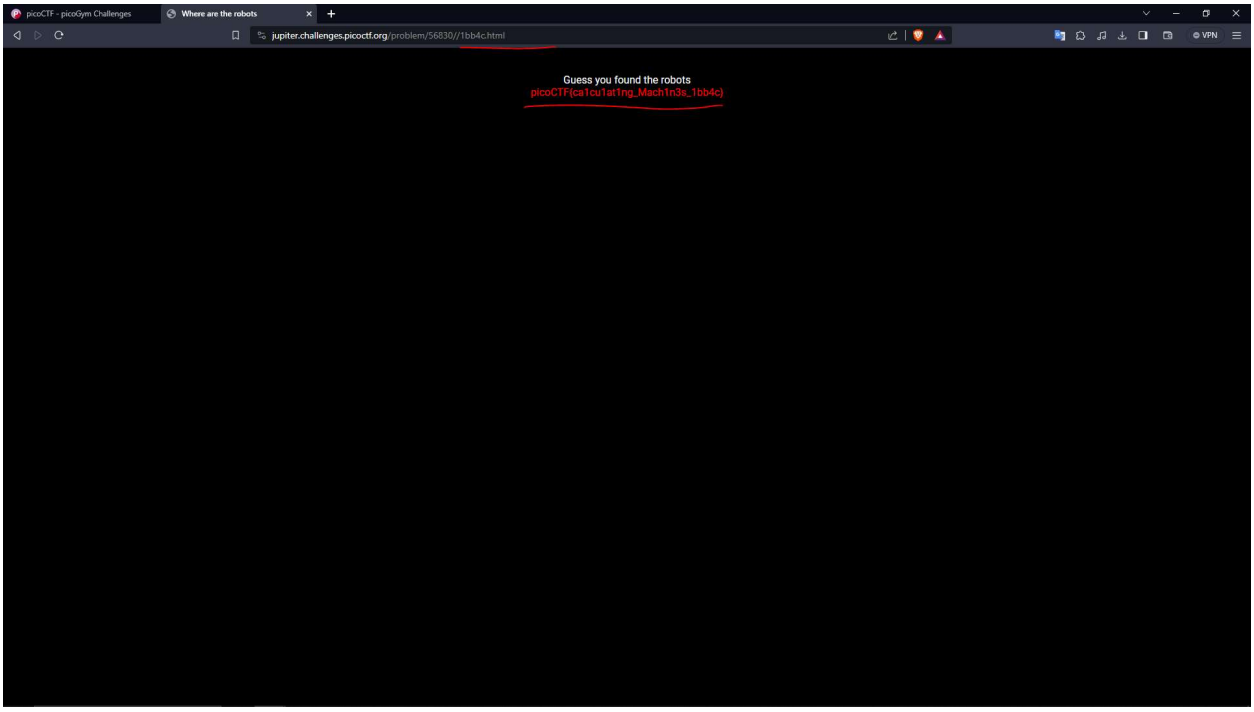


Search Source



Where are the robots


picoCTF - picoGym Challenges
jupiter.challenges.picoctf.org/pr
jupiter.challenges.picoctf.org/problem/56830/robots.txt
VPN
User-agent: *
Disallow: /1bb4c.html


picoCTF - picoGym Challenges
Where are the robots
jupiter.challenges.picoctf.org/problem/56830//1bb4c.html
VPN
Guess you found the robots
picoCTF{ca1cu1at1ng_Mach1n3s_1bb4c}