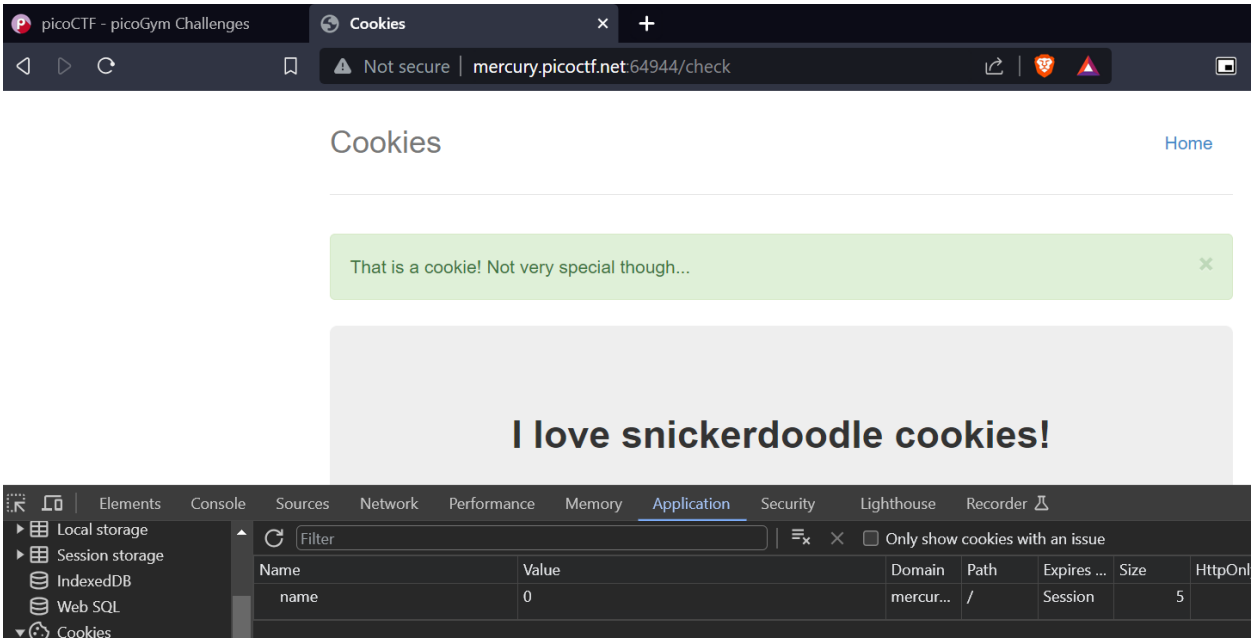
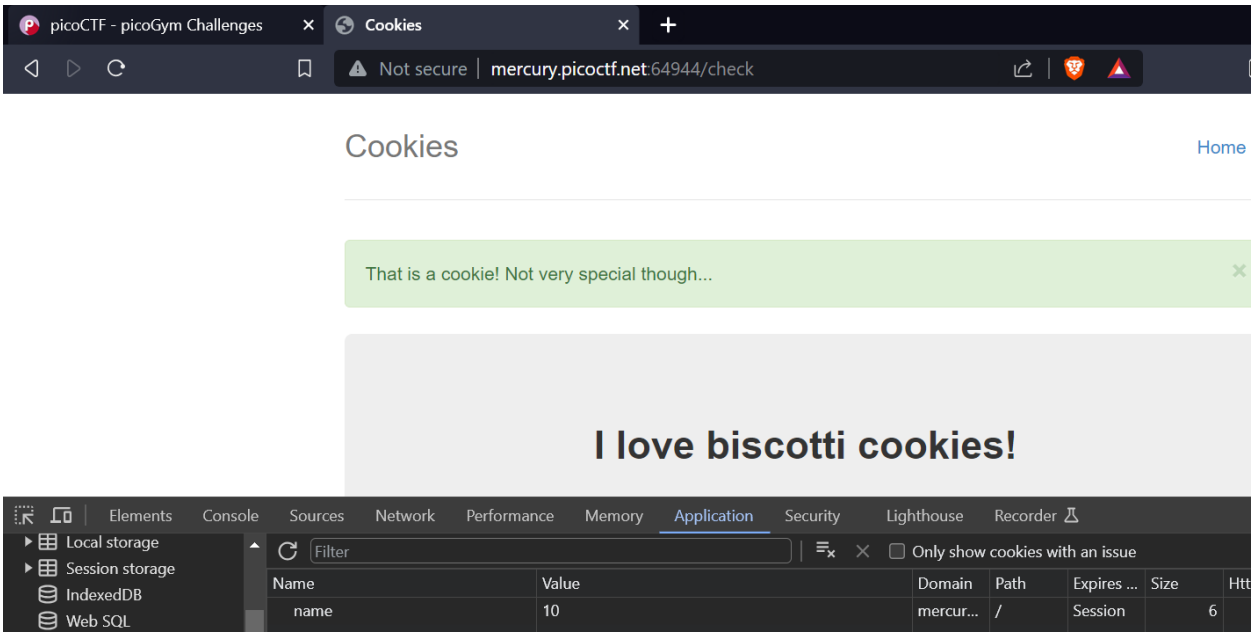
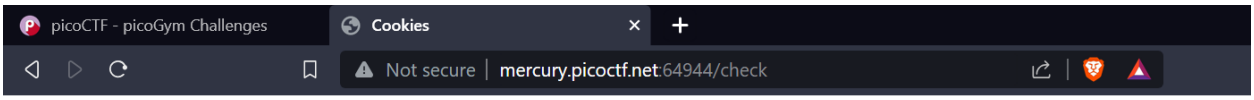
Pamela Mena – 00211564

Homework 3

Cookies

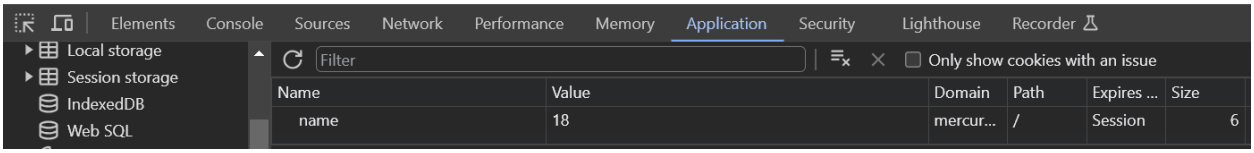




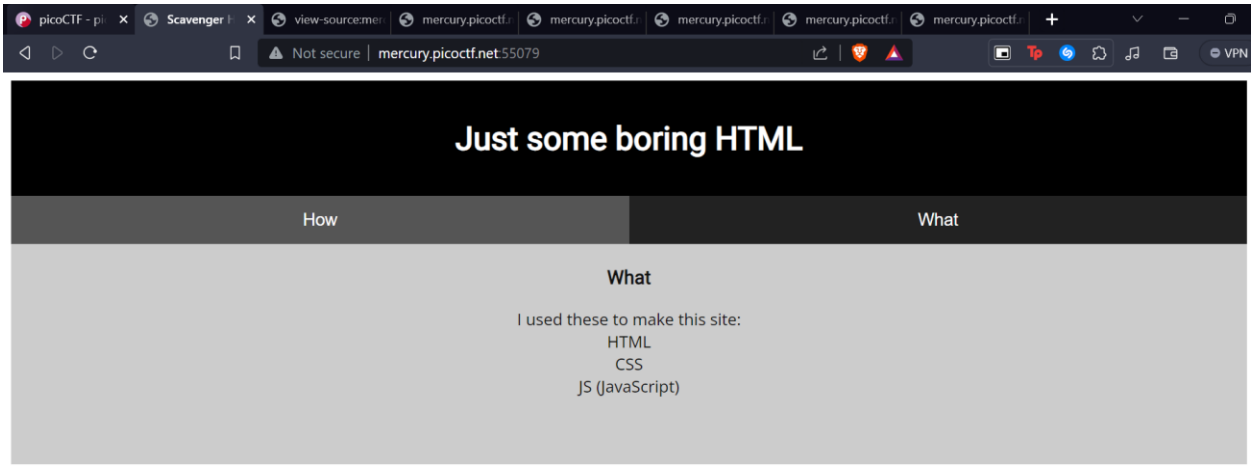


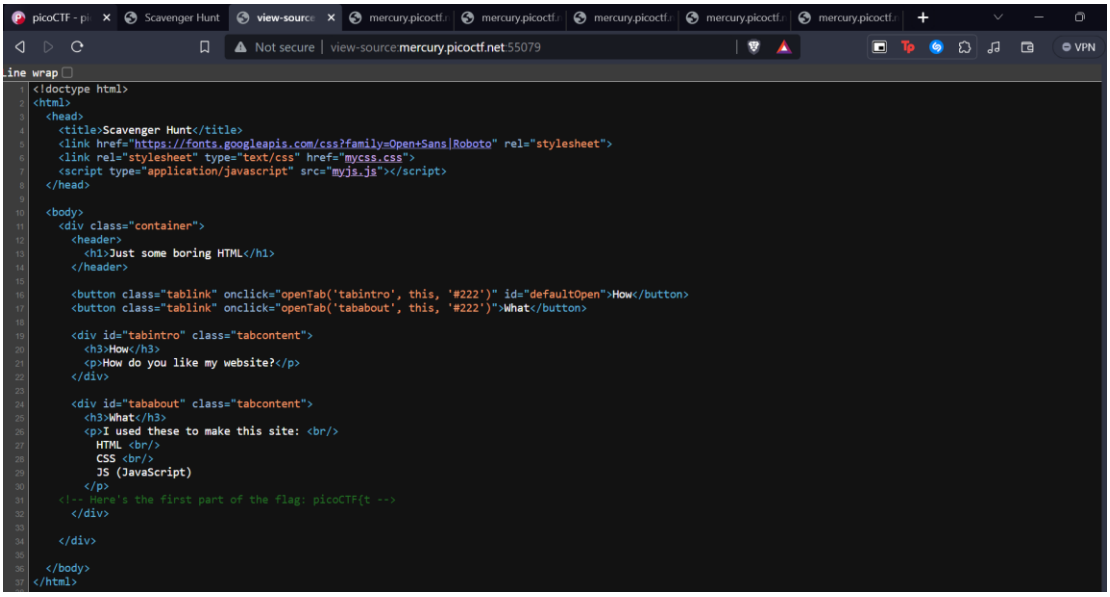
Flag:

`picoCTF{3v3ry1_l0v3s_c00k135_cc9110ba}`



Scavenger Hunt




picoCTF - pi
Scavenger Hunt
view-source
mercury.picoctf.r
mercury.picoctf.r
mercury.picoctf.r
mercury.picoctf.r
mercury.picoctf.r
Not secure | view-source:mercury.picoctf.net:55079
VPN
ine wrap
<!doctype html>
<html>
<head>
<title>Scavenger Hunt</title>
<link href="https://fonts.googleapis.com/css?family=Open+Sans|Roboto" rel="stylesheet">
<link rel="stylesheet" type="text/css" href="mycss.css">
<script type="application/javascript" src="myjs.js"></script>
</head>
<body>

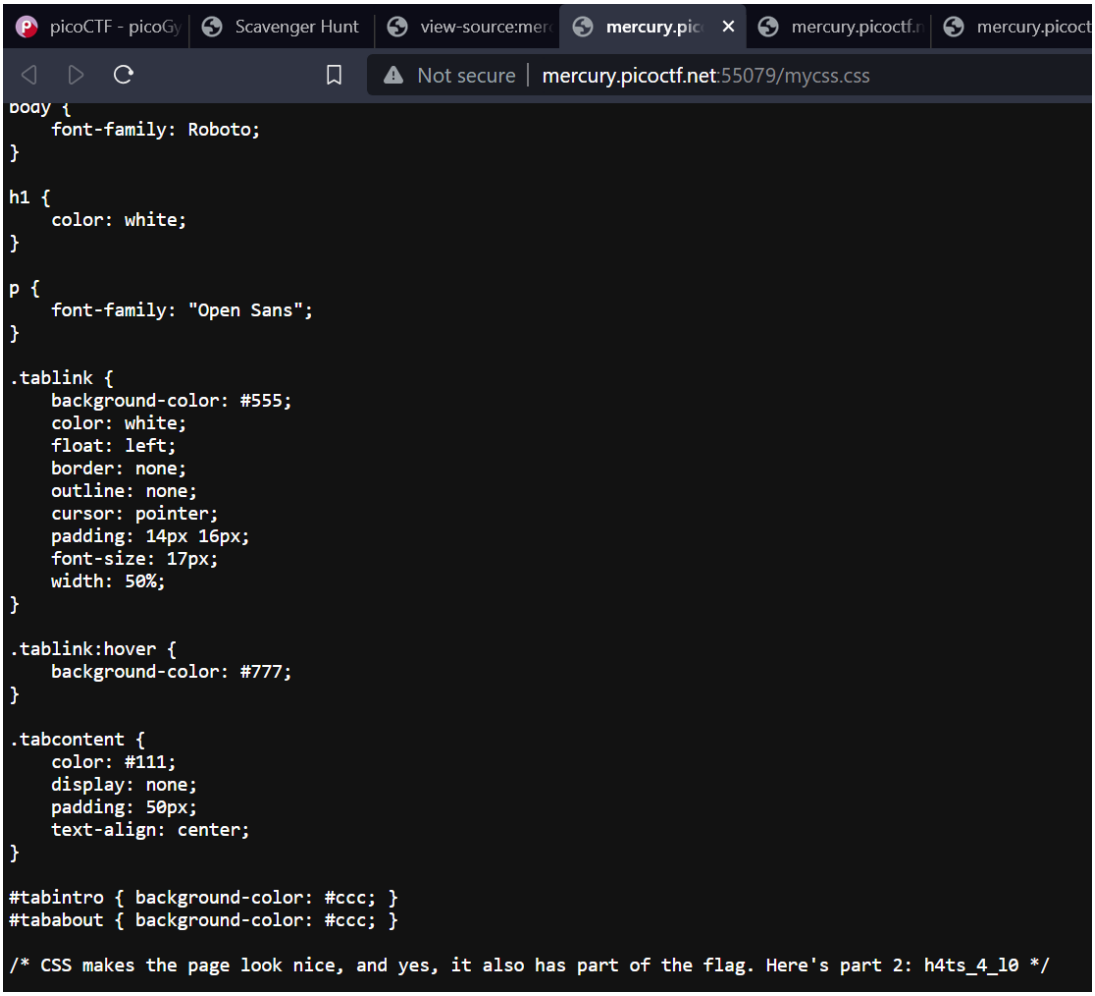
<header>
<h1>Just some boring HTML</h1>
</header>
<button class="tablink" onclick="openTab('tabintro', this, '#222')" id="defaultOpen">How</button>
<button class="tablink" onclick="openTab('tababout', this, '#222')">What</button>

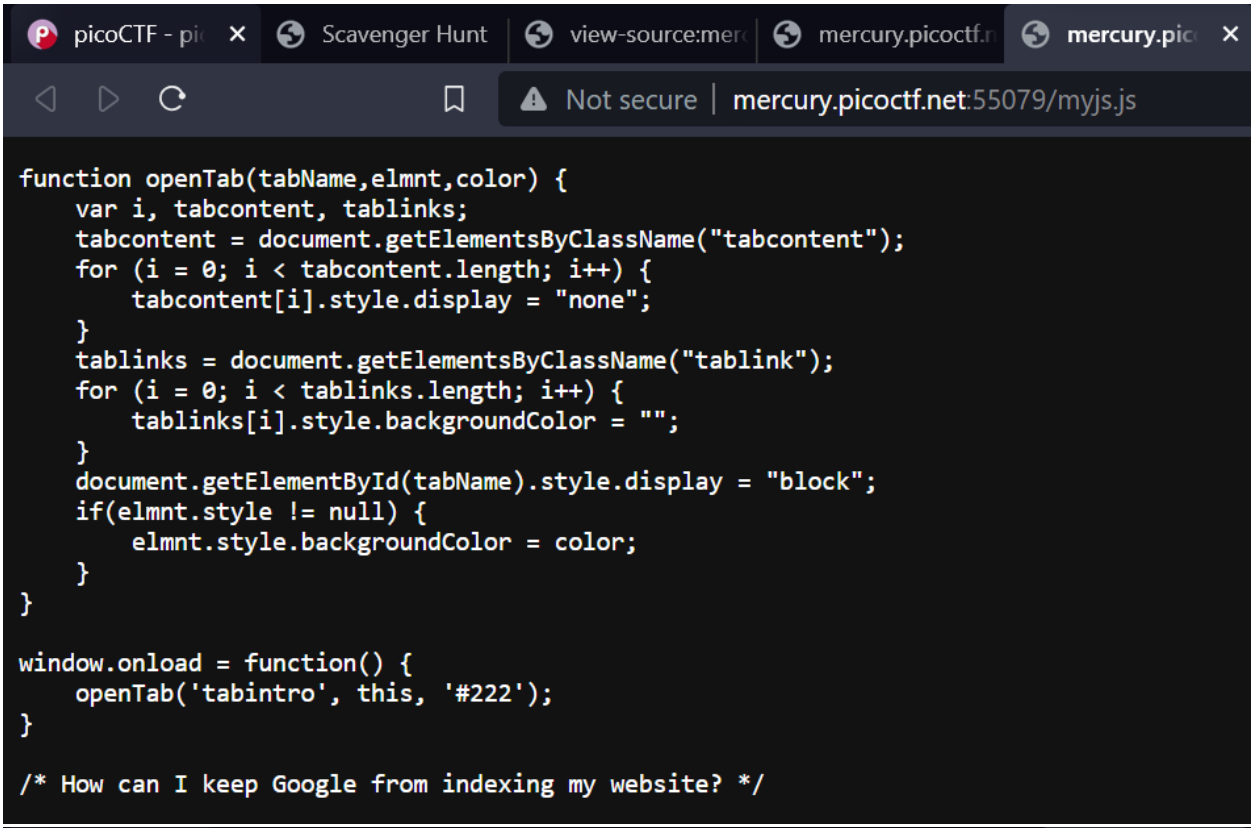
<h3>How</h3>
How do you like my website?

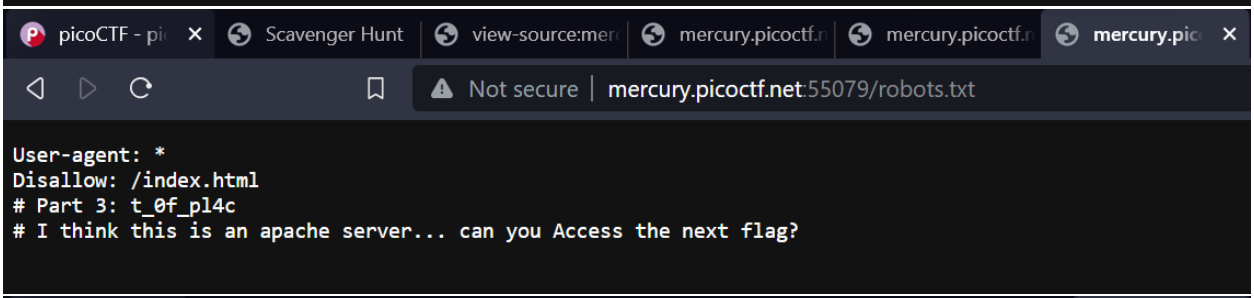
<h3>What</h3>
I used these to make this site:
HTML
CSS
JS (JavaScript)

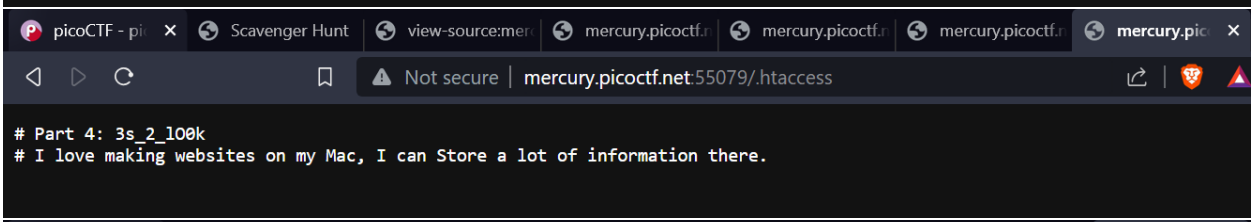
<!-- Here's the first part of the flag: picoCTF{t -->

</body>
</html>


picoCTF - picoGy
Scavenger Hunt
view-source:mer
mercury.pic
mercury.picoctf.n
mercury.picoct
Not secure
mercury.picoctf.net:55079/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 */


picoCTF - pi
Scavenger Hunt
view-source:mer
mercury.picoctf.n
mercury.pic
Not secure | mercury.picoctf.net:55079/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? */


picoCTF - pi
Scavenger Hunt
view-source:mer
mercury.picoctf.n
mercury.picoctf.n
mercury.pic
Not secure | mercury.picoctf.net:55079/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?


picoCTF - pi
Scavenger Hunt
view-source:mer
mercury.picoctf.n
mercury.picoctf.n
mercury.picoctf.n
mercury.pic
Not secure | mercury.picoctf.net:55079/.htaccess
Part 4: 3s_2_l00k
I love making websites on my Mac, I can Store a lot of information there.


picoCTF - pi
Scavenger Hunt
view-source:mer
mercury.picoctf.n
mercury.picoctf.n
mercury.picoctf.n
mercury.picoctf.n
mercury.pic
Not secure | mercury.picoctf.net:55079/.DS_Store
Congrats! You completed the scavenger hunt. Part 5: _74cceb07}

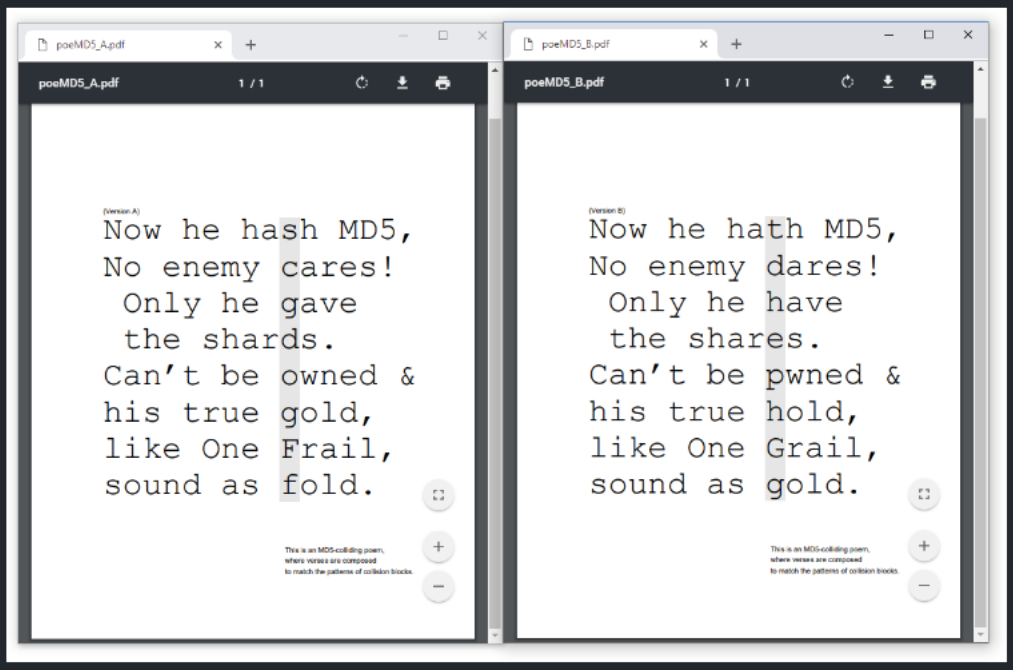
Inspect HTML

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>On Histiaeus</title>
  </head>
  <body>
    <h1>On Histiaeus</h1>
    <p>However, according to Herodotus, Histiaeus was unhappy having to stay in
       Susa, and made plans to return to his position as King of Miletus by
       instigating a revolt in Ionia. In 499 BC, he shaved the head of his
       most trusted slave, tattooed a message on his head, and then waited for
       his hair to grow back. The slave was then sent to Aristagoras, who was
       instructed to shave the slave's head again and read the message, which
       told him to revolt against the Persians.</p>
    <br>
    <p> Source: Wikipedia on Histiaeus </p>
    <!--picoCTF{1n5p3t0r_0f_h7ml_1fd8425b}-->
  </body>
</html>

```

It's my Birthday

https://github.com/corkami/collisions#pdf

Examples: poeMD5 A ↔ poeMD5 B



A true cryptographic artistic creation :)

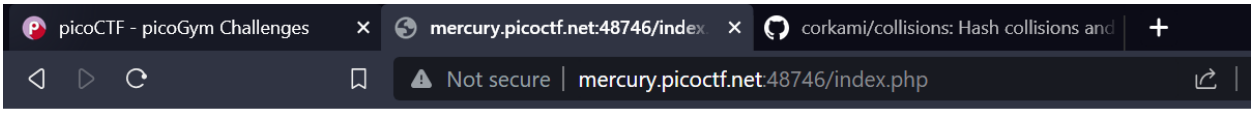
It is my Birthday

See if you are invited to my party!

Choose File poeMD5_A.pdf

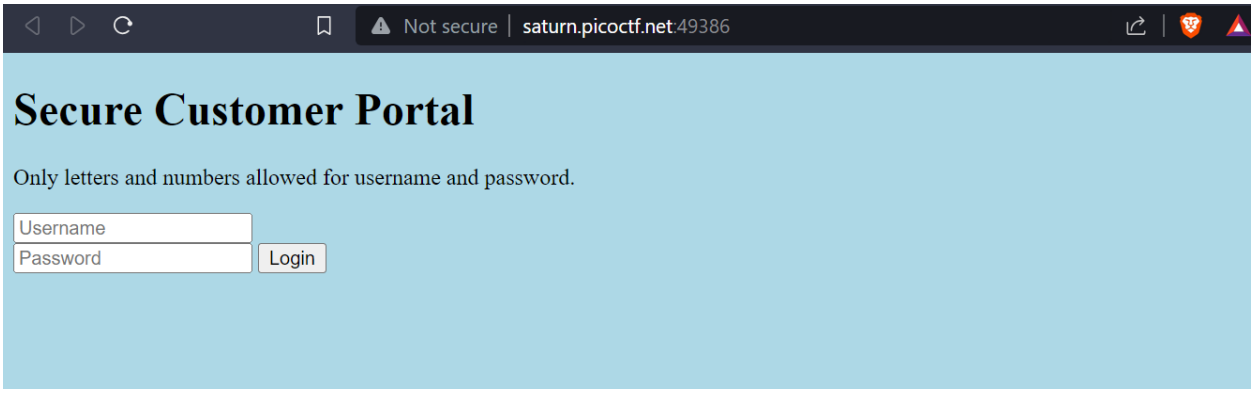
Choose File poeMD5_B.pdf

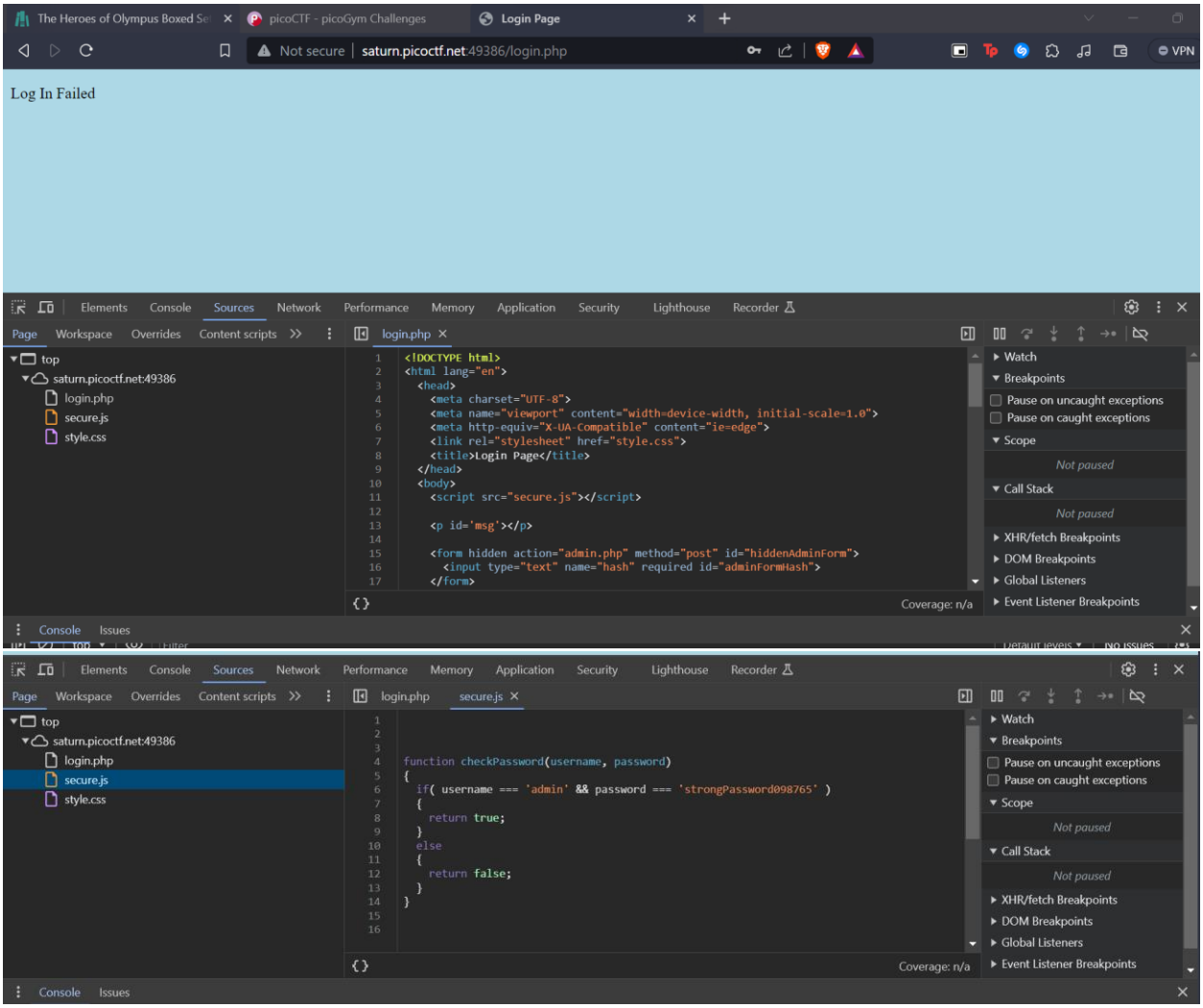
Upload



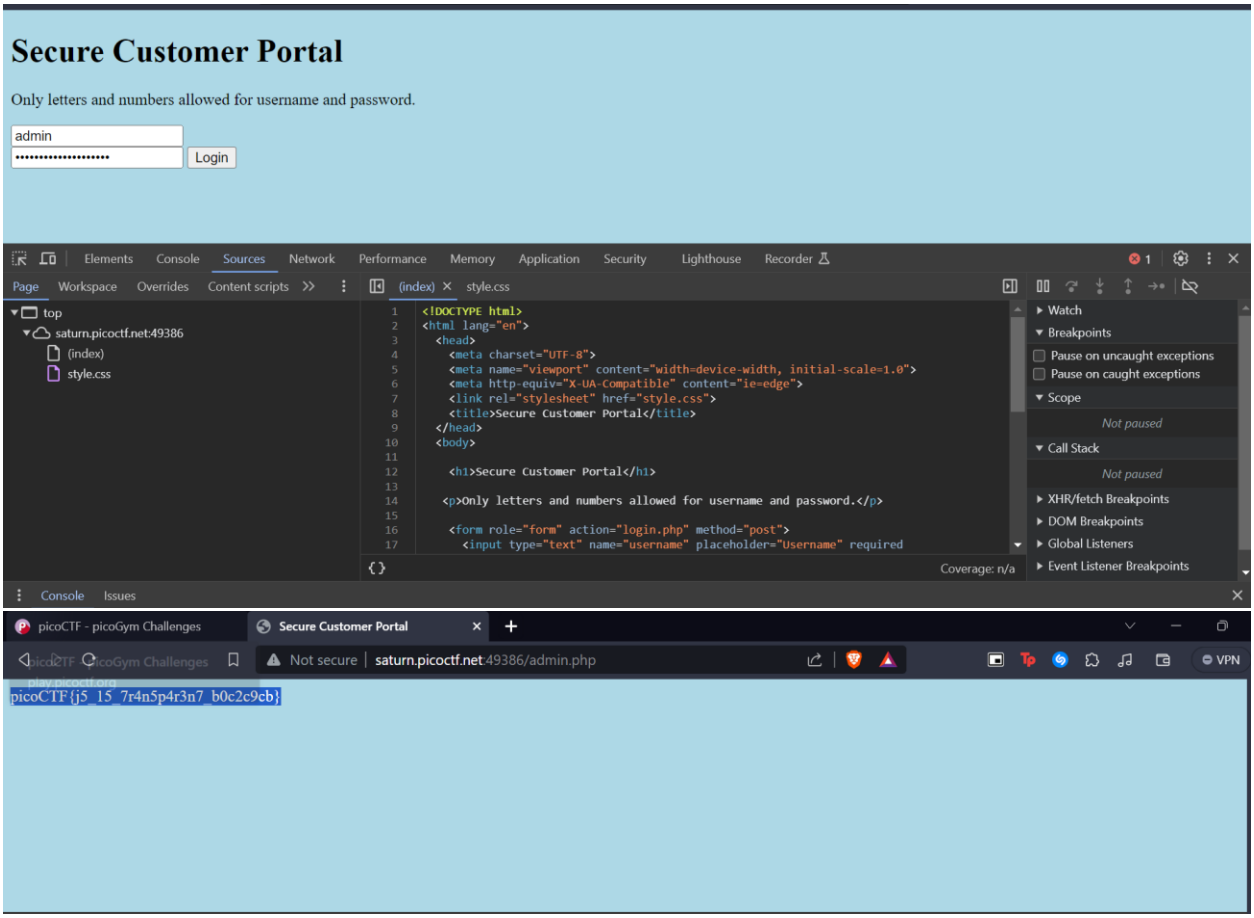

```php
<?php

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_aebcbf39}

?>
```

Local Authority

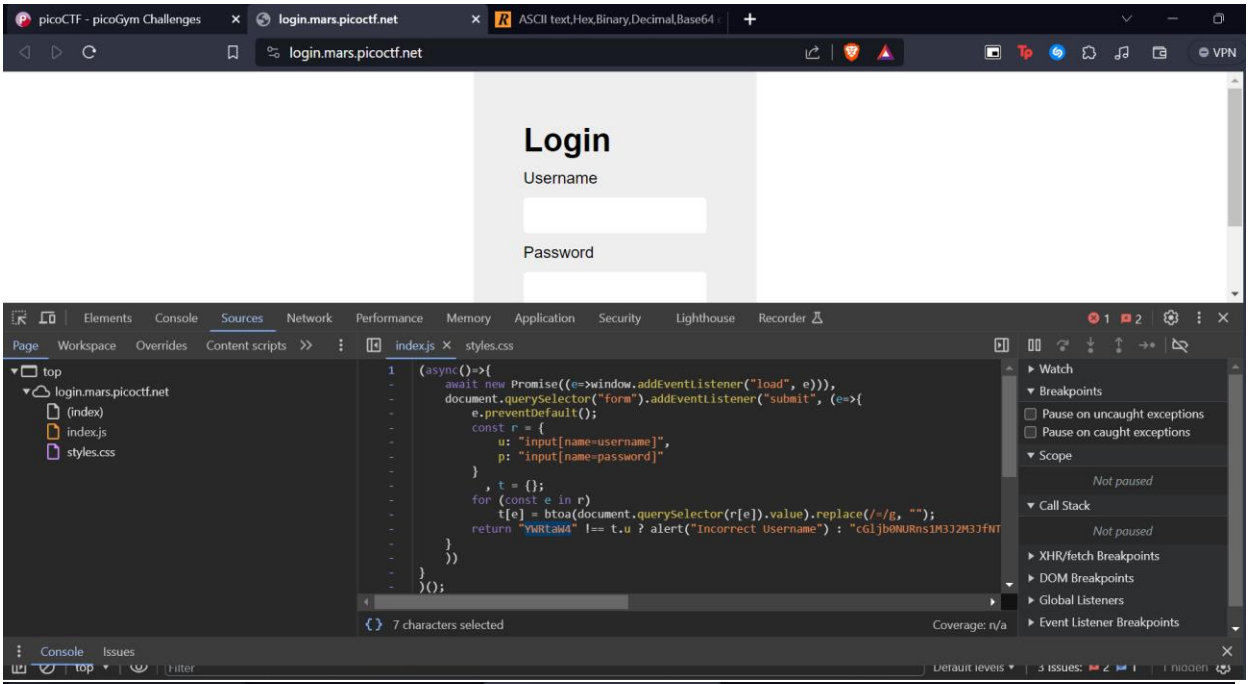


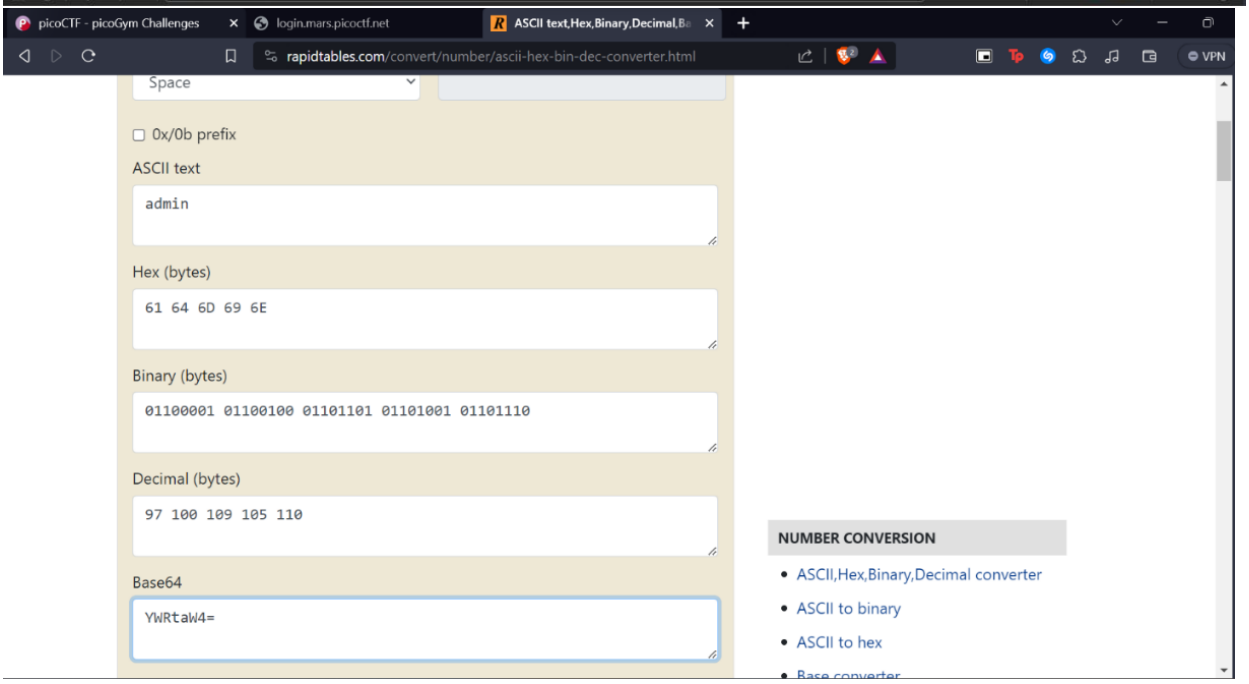

The Heroes of Olympus Boxed Se
picoCTF - picoGym Challenges
Login Page
Not secure | saturn.picoctf.net:49386/login.php
VPN
Log In Failed
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder
Page Workspace Overrides Content scripts
top
saturn.picoctf.net:49386
login.php
secure.js
style.css
login.php
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="stylesheet" href="style.css">
<title>Login Page</title>
</head>
<body>
<script src="secure.js"></script>

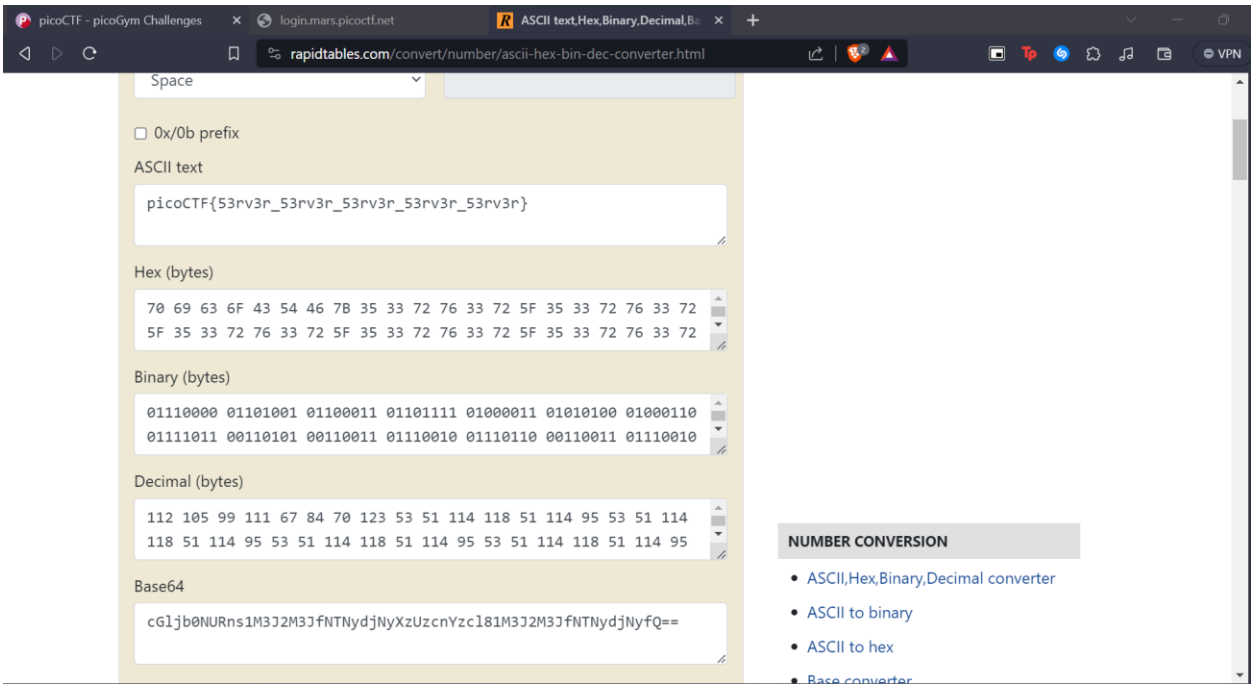
<form hidden action="admin.php" method="post" id="hiddenAdminForm">
<input type="text" name="hash" required id="adminFormHash">
</form>
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
Coverage: n/a
Console Issues
Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder
Page Workspace Overrides Content scripts
login.php
secure.js
top
saturn.picoctf.net:49386
login.php
secure.js
style.css
function checkPassword(username, password)
{
if(username === 'admin' && password === 'strongPassword098765')
{
return true;
}
else
{
return false;
}
}
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
Coverage: n/a
Console Issues


Secure Customer Portal
Only letters and numbers allowed for username and password.
admin
Login
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Page
Workspace
Overrides
Content scripts
(index)
style.css
top
saturn.picoctf.net:49386
(index)
style.css
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<link rel="stylesheet" href="style.css">
<title>Secure Customer Portal</title>
</head>
<body>
<h1>Secure Customer Portal</h1>
Only letters and numbers allowed for username and password.
<form role="form" action="login.php" method="post">
<input type="text" name="username" placeholder="Username" required
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
Coverage: n/a
Console
Issues
picoCTF - picoGym Challenges
Secure Customer Portal
Not secure
saturn.picoctf.net:49386/admin.php
VPN
picoCTF{j5_15_7r4n5p4r3n7_b0c2c9cb}

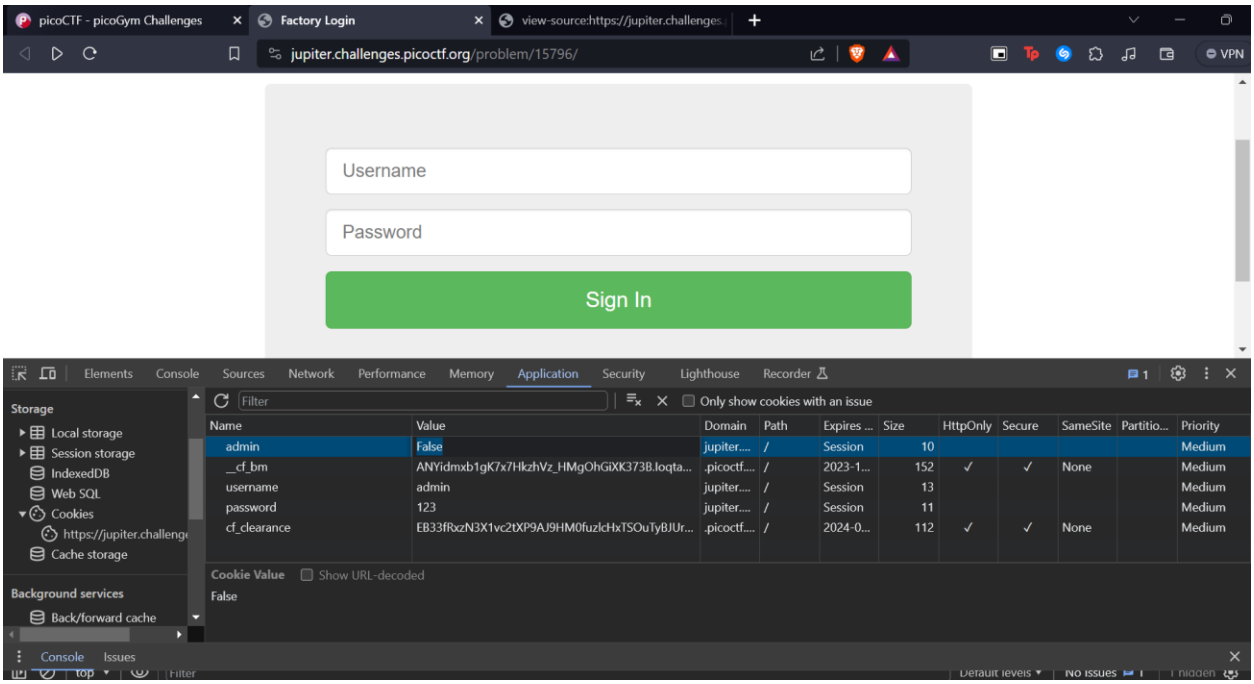
Login

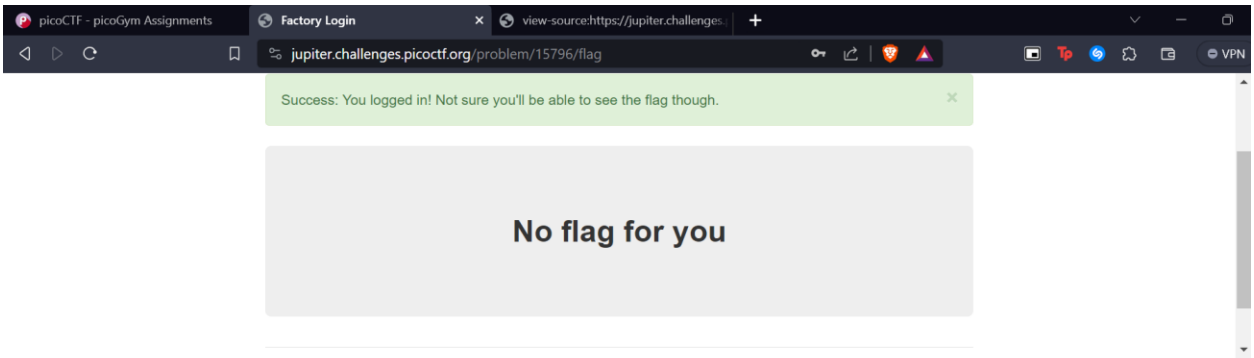

picoCTF - picoGym Challenges
login.mars.picoctf.net
ASCII text,Hex,Binary,Decimal,Base64
login.mars.picoctf.net
VPN
Login
Username
Password
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Page
Workspace
Overrides
Content scripts
index.js
styles.css
top
login.mars.picoctf.net
(index)
index.js
styles.css
(async()=>{
await new Promise((e=>window.addEventListener("load", e))),
document.querySelector("form").addEventListener("submit", (e=>{
e.preventDefault();
const r = {
u: "input[name=username]",
p: "input[name=password]"
}
, t = {};
for (const e in r)
t[e] = btoa(document.querySelector(r[e]).value).replace(/=/g, "");
return "YWRtaW4" !== t.u ? alert("Incorrect Username") : "cGljb0NURns1M3J2M3JfNT
}
))
}
)();
7 characters selected
Coverage: n/a
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
Console
Issues

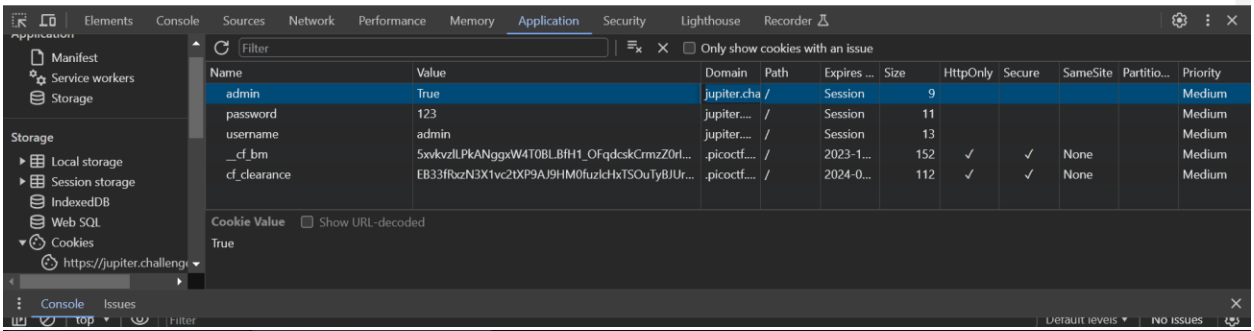

picoCTF - picoGym Challenges
login.mars.picoctf.net
ASCII text,Hex,Binary,Decimal,Ba
rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html
VPN
Space
0x/0b prefix
ASCII text
admin
Hex (bytes)
61 64 6D 69 6E
Binary (bytes)
01100001 01100100 01101101 01101001 01101110
Decimal (bytes)
97 100 109 105 110
Base64
YWRtaW4=
NUMBER CONVERSION
ASCII,Hex,Binary,Decimal converter
ASCII to binary
ASCII to hex

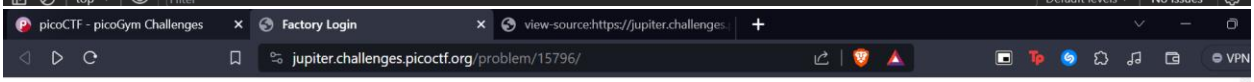

picoCTF - picoGym Challenges
login.mars.picoctf.net
ASCII text,Hex,Binary,Decimal,Be
rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html
VPN
Space
0x/0b prefix
ASCII text
picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}
Hex (bytes)
70 69 63 6F 43 54 46 7B 35 33 72 76 33 72 5F 35 33 72 76 33 72
5F 35 33 72 76 33 72 5F 35 33 72 76 33 72 5F 35 33 72 76 33 72
Binary (bytes)
01110000 01101001 01100011 01101111 01000011 01010100 01000110
01111011 00110101 00110011 01110010 01110110 00110011 01110010
Decimal (bytes)
112 105 99 111 67 84 70 123 53 51 114 118 51 114 95 53 51 114
118 51 114 95 53 51 114 118 51 114 95 53 51 114 118 51 114 95
Base64
cGljb0NURns1M3J2M3JfNTNydjNyXzUzcnYzcl81M3J2M3JfNTNydjNyfQ==
NUMBER CONVERSION
ASCII,Hex,Binary,Decimal converter
ASCII to binary
ASCII to hex
Base converter

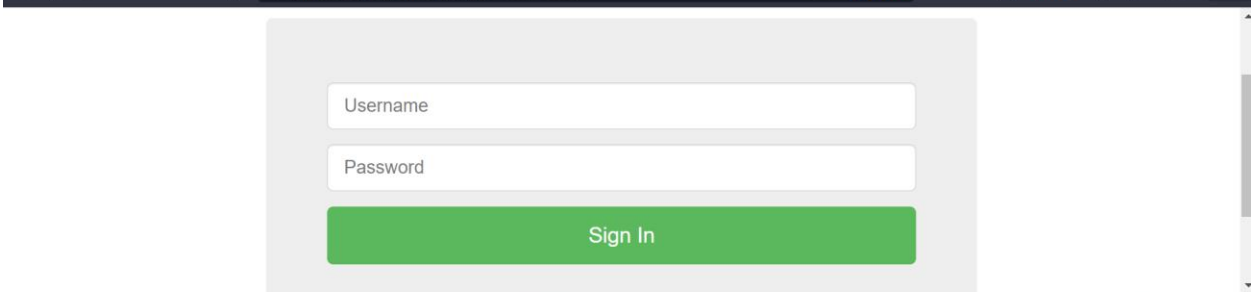
Logon

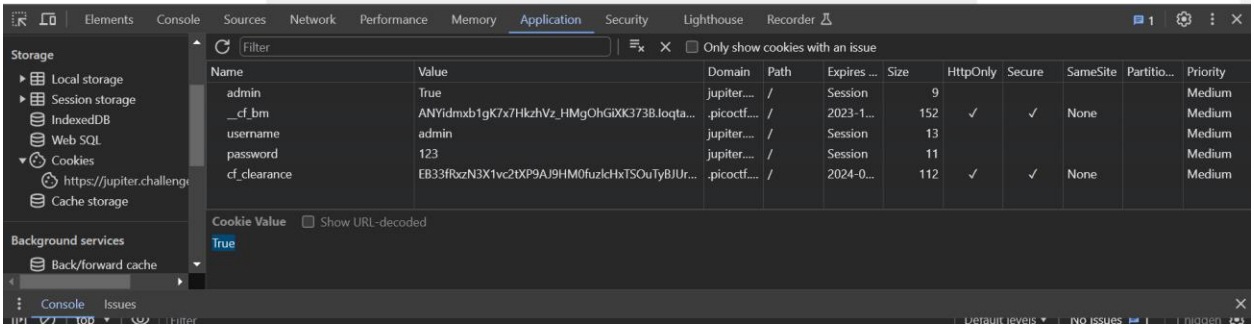

picoCTF - picoGym Challenges
Factory Login
view-source:https://jupiter.challenges.
jupiter.challenges.picoctf.org/problem/15796/
VPN
Username
Password
Sign In
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Storage
Local storage
Session storage
IndexedDB
Web SQL
Cookies
https://jupiter.challenge
Cache storage
Background services
Back/forward cache
Filter
Only show cookies with an issue
Name
Value
Domain
Path
Expires ...
Size
HttpOnly
Secure
SameSite
Partitio...
Priority
admin
False
jupiter....
/
Session
10
Medium
__cf_bm
ANYidmxb1gK7x7HkzhVz_HMgOhGiXK373B.loqta...
.picoctf....
/
2023-1...
152
✓
✓
None
Medium
username
admin
jupiter....
/
Session
13
Medium
password
123
jupiter....
/
Session
11
Medium
cf_clearance
EB33fRxzN3X1vc2tXP9AJ9HM0fuzlcHxTSOuTyBJUr...
.picoctf....
/
2024-0...
112
✓
✓
None
Medium
Cookie Value
Show URL-decoded
False
Console
Issues


picoCTF - picoGym Assignments
Factory Login
view-source:https://jupiter.challenges.
jupiter.challenges.picoctf.org/problem/15796/flag
VPN
Success: You logged in! Not sure you'll be able to see the flag though.
No flag for you

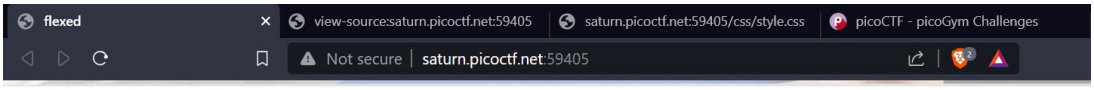

Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Manifest
Service workers
Storage
Storage
Local storage
Session storage
IndexedDB
Web SQL
Cookies
https://jupiter.challenge
Filter
Only show cookies with an issue
Name
Value
Domain
Path
Expires ...
Size
HttpOnly
Secure
SameSite
Partitio...
Priority
admin
True
jupiter.cha
/
Session
9
Medium
password
123
jupiter....
/
Session
11
Medium
username
admin
jupiter....
/
Session
13
Medium
__cf_bm
5xvkvzlLPkANggxW4T0BL_BfH1_OFqdcskCrmzZ0rI...
.picoctf....
/
2023-1...
152
✓
✓
None
Medium
cf_clearance
EB33fRxzN3X1vc2tXP9AJ9HM0fuzlcHxTSOuTyBJUr...
.picoctf....
/
2024-0...
112
✓
✓
None
Medium
Cookie Value
Show URL-decoded
True
Console
Issues

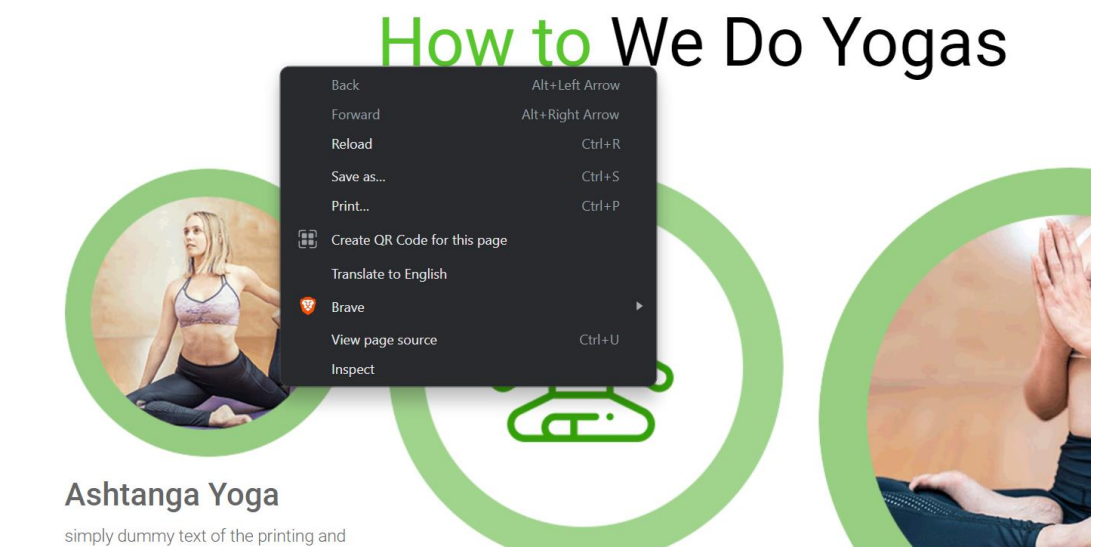

picoCTF - picoGym Challenges
Factory Login
view-source:https://jupiter.challenges.
jupiter.challenges.picoctf.org/problem/15796/
VPN

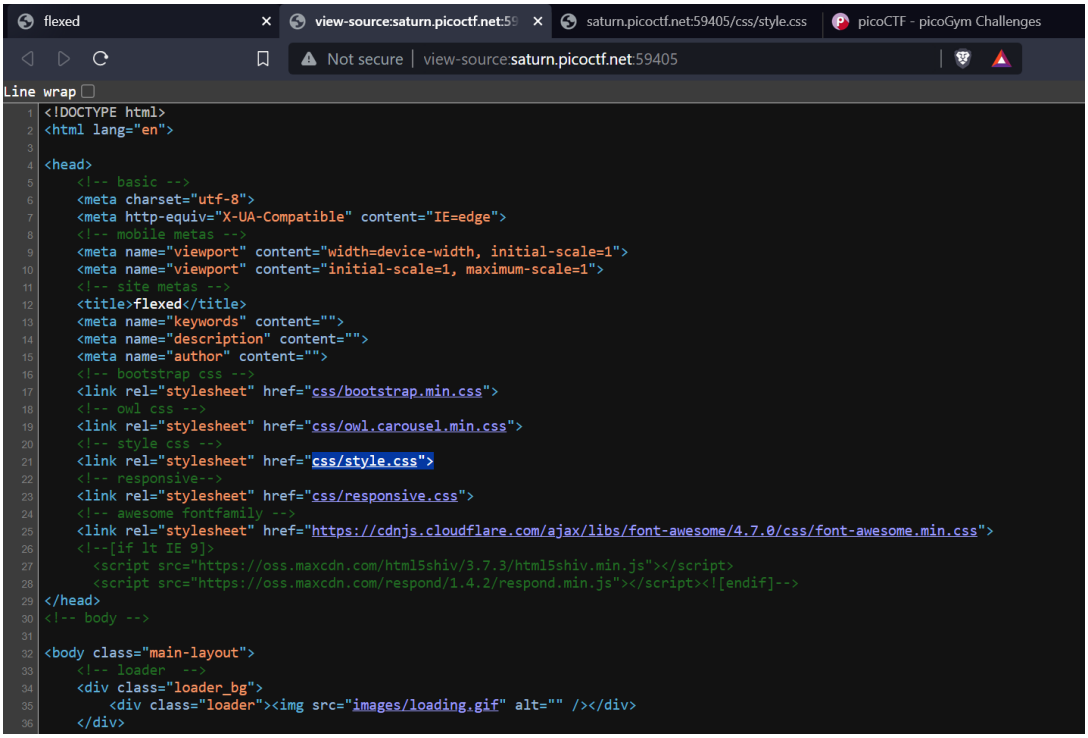

Username
Password
Sign In

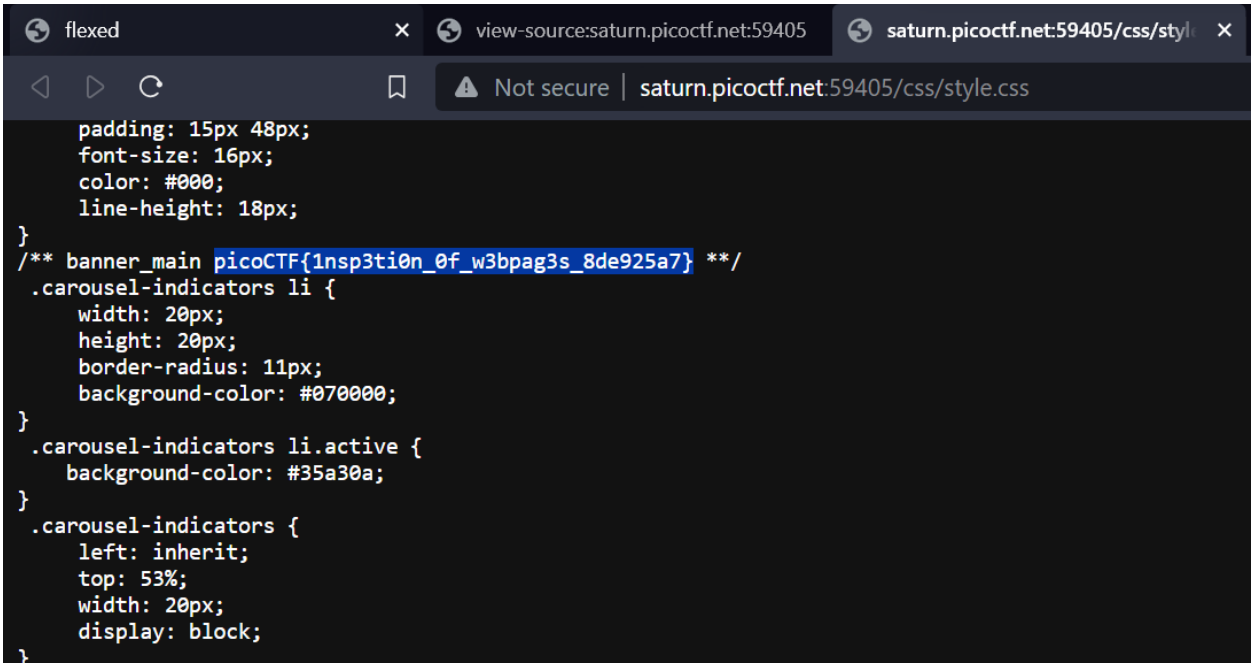

Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Storage
Local storage
Session storage
IndexedDB
Web SQL
Cookies
https://jupiter.challenge
Cache storage
Background services
Back/forward cache
Filter
Only show cookies with an issue
Name
Value
Domain
Path
Expires ...
Size
HttpOnly
Secure
SameSite
Partitio...
Priority
admin
True
jupiter....
/
Session
9
Medium
__cf_bm
ANYidmxb1gK7x7HkzhVz_HMgOhGiXK373B.loqta...
.picoctf....
/
2023-1...
152
✓
✓
None
Medium
username
admin
jupiter....
/
Session
13
Medium
password
123
jupiter....
/
Session
11
Medium
cf_clearance
EB33fRxzN3X1vc2tXP9AJ9HM0fuzlcHxTSOuTyBJUr...
.picoctf....
/
2024-0...
112
✓
✓
None
Medium
Cookie Value
Show URL-decoded
True
Console
Issues

Search Source

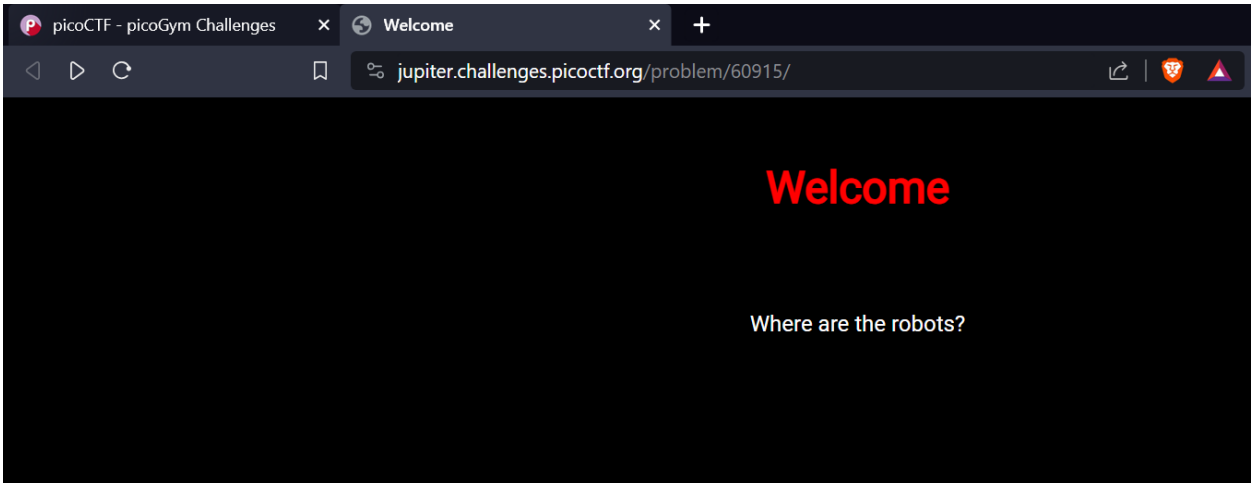


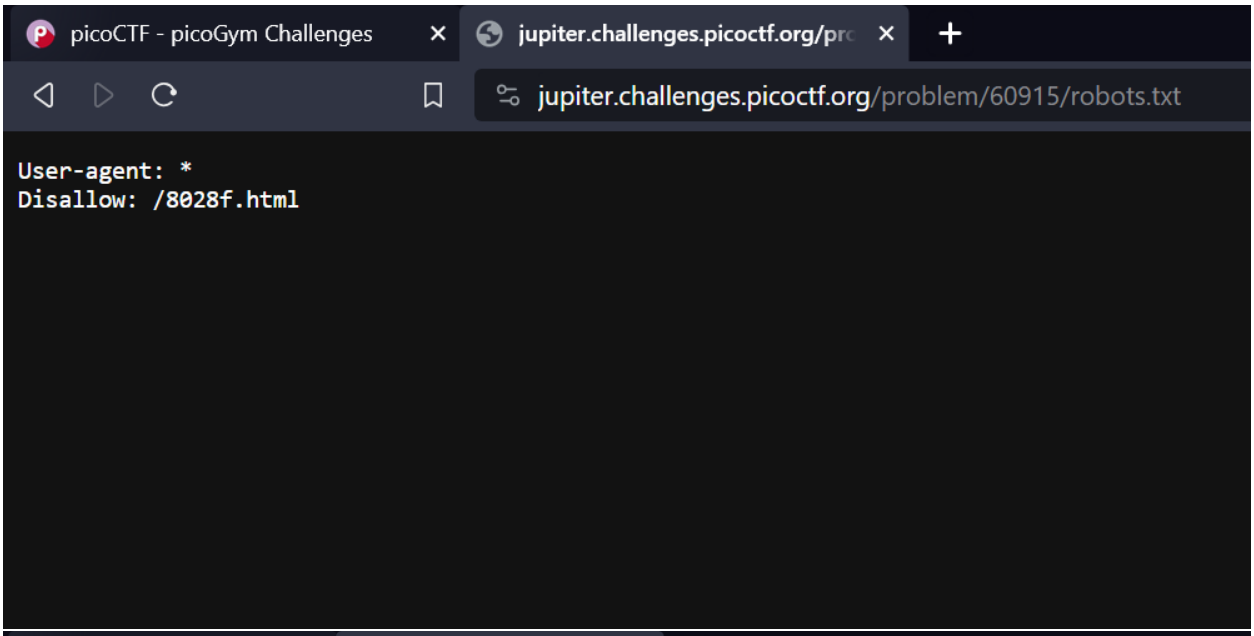


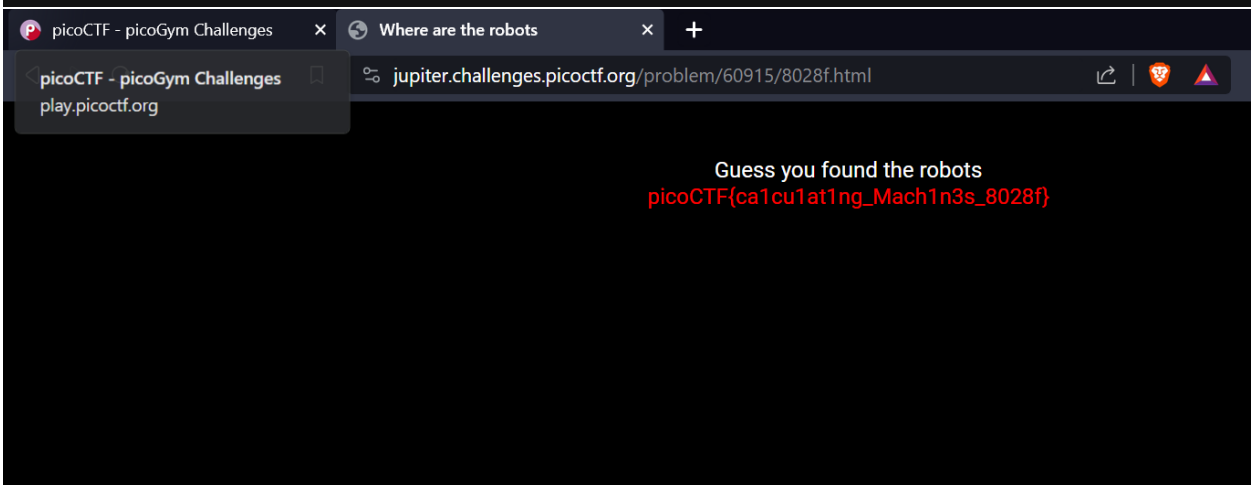




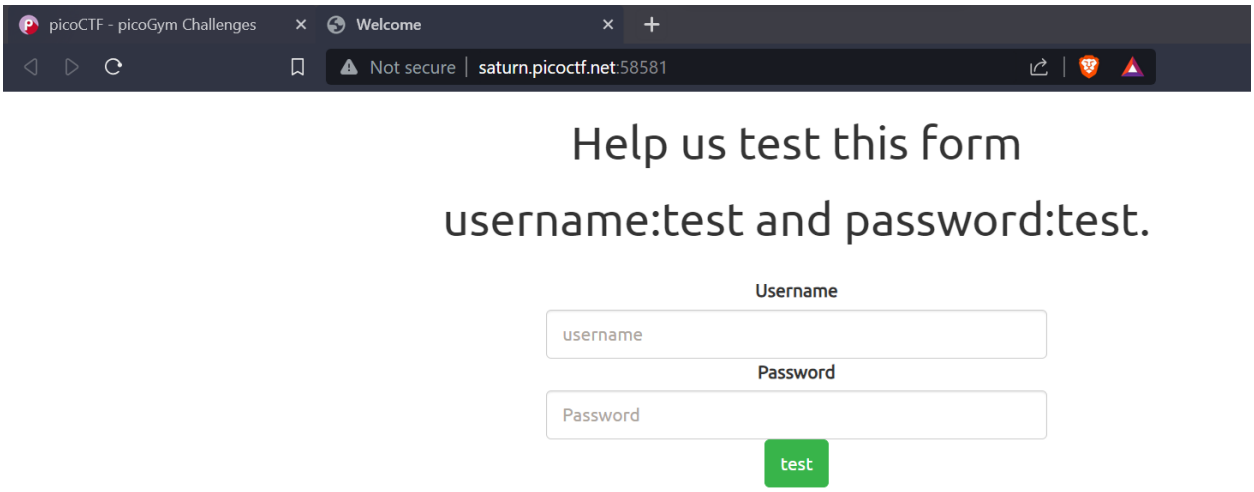
Where are the robots

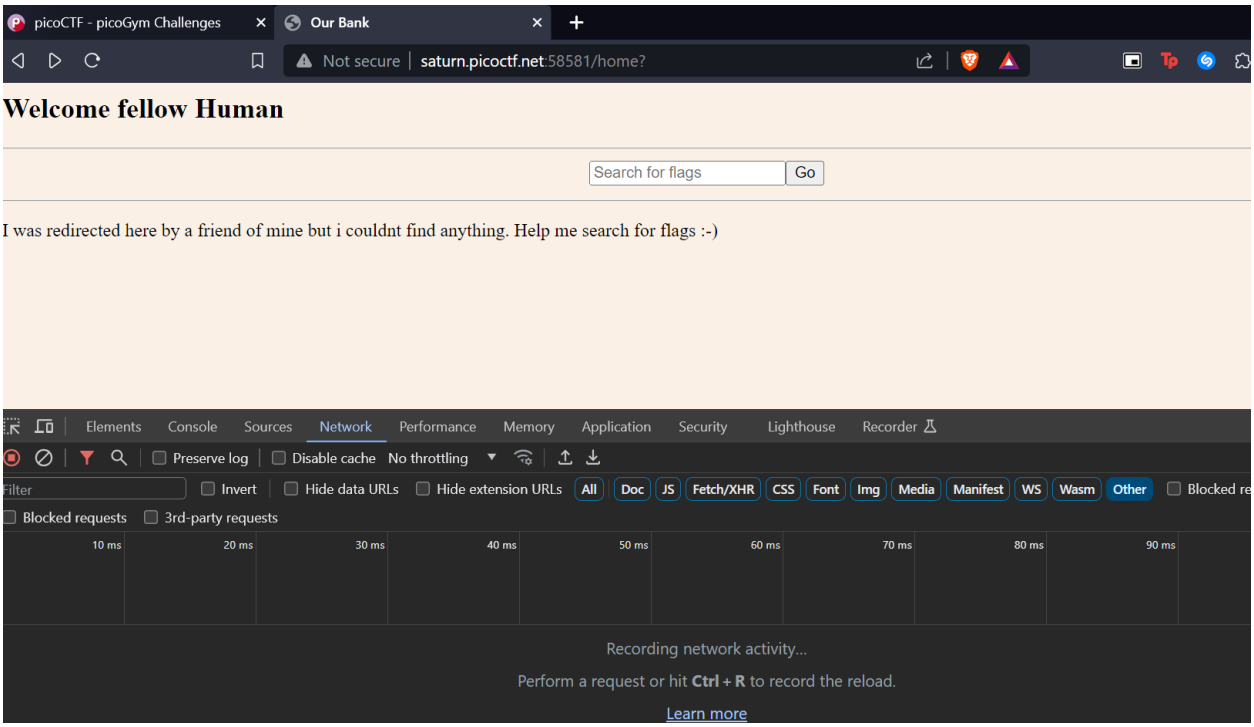


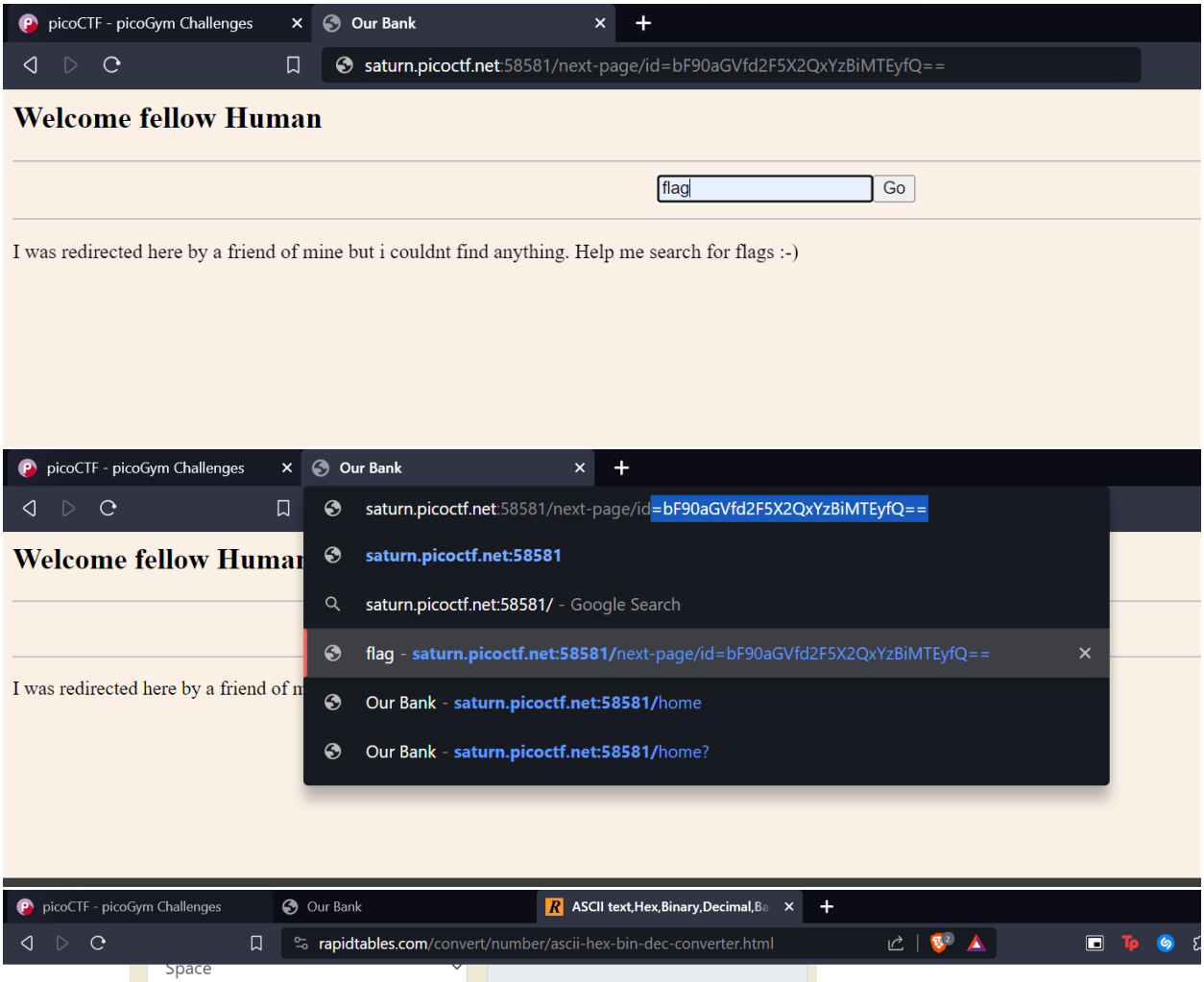

picoCTF - picoGym Challenges
jupiter.challenges.picoctf.org/pro
jupiter.challenges.picoctf.org/problem/60915/robots.txt
User-agent: *
Disallow: /8028f.html

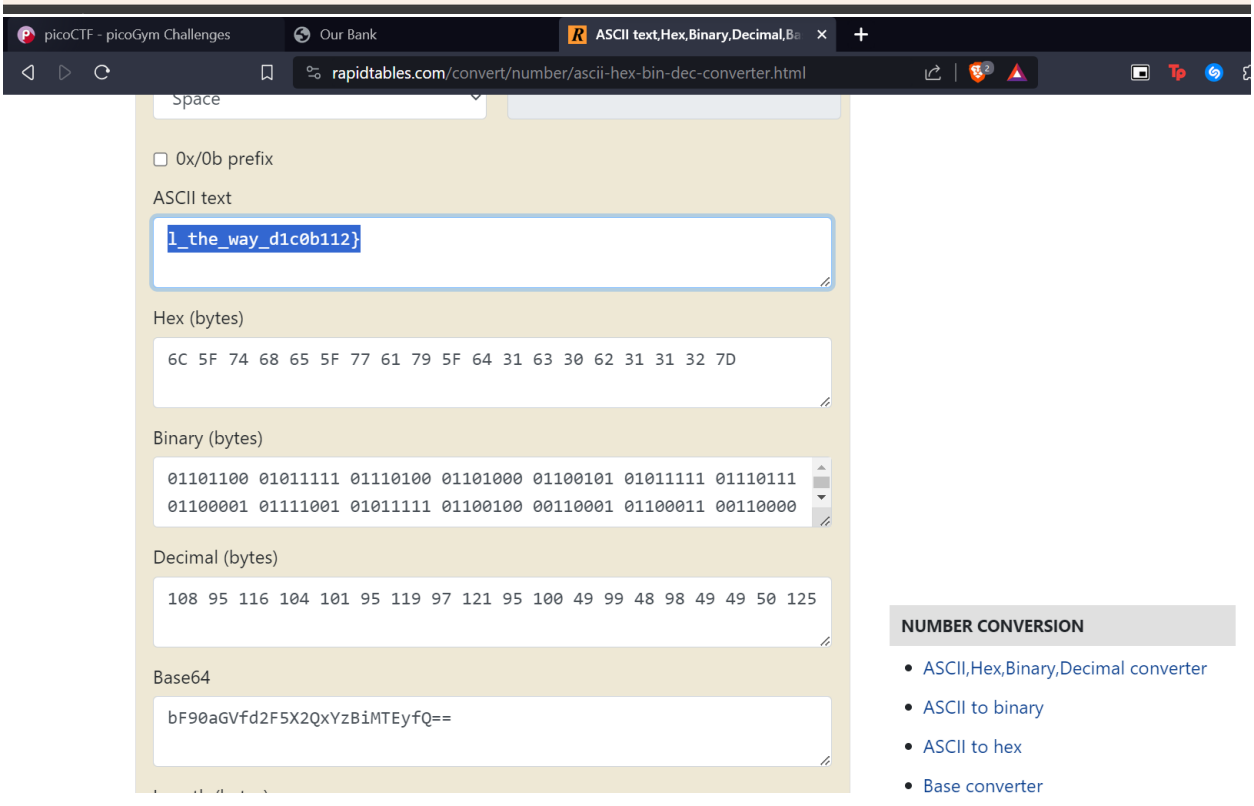

picoCTF - picoGym Challenges
Where are the robots
picoCTF - picoGym Challenges
play.picoctf.org
jupiter.challenges.picoctf.org/problem/60915/8028f.html
Guess you found the robots
picoCTF{ca1cu1at1ng_Mach1n3s_8028f}

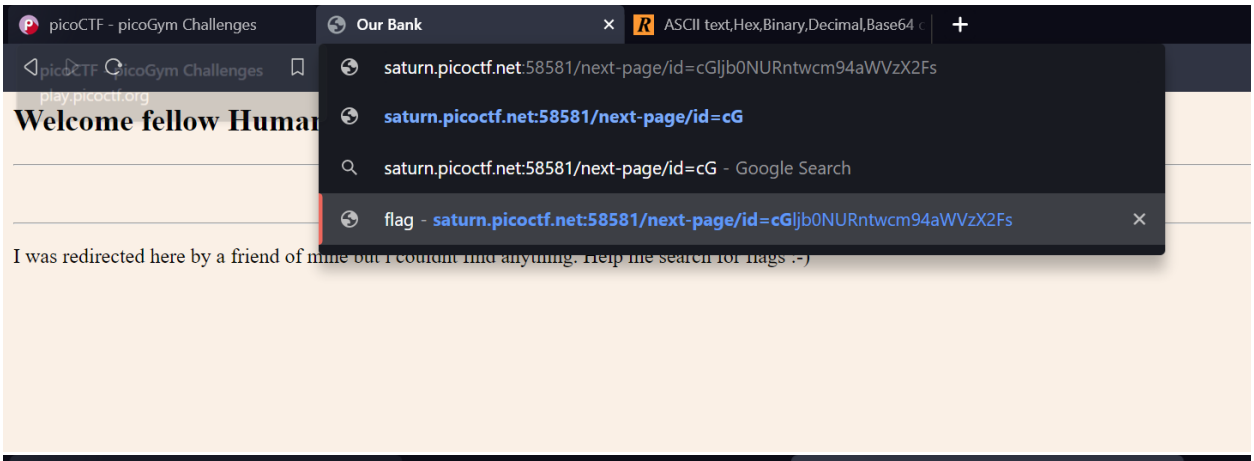
Find Me

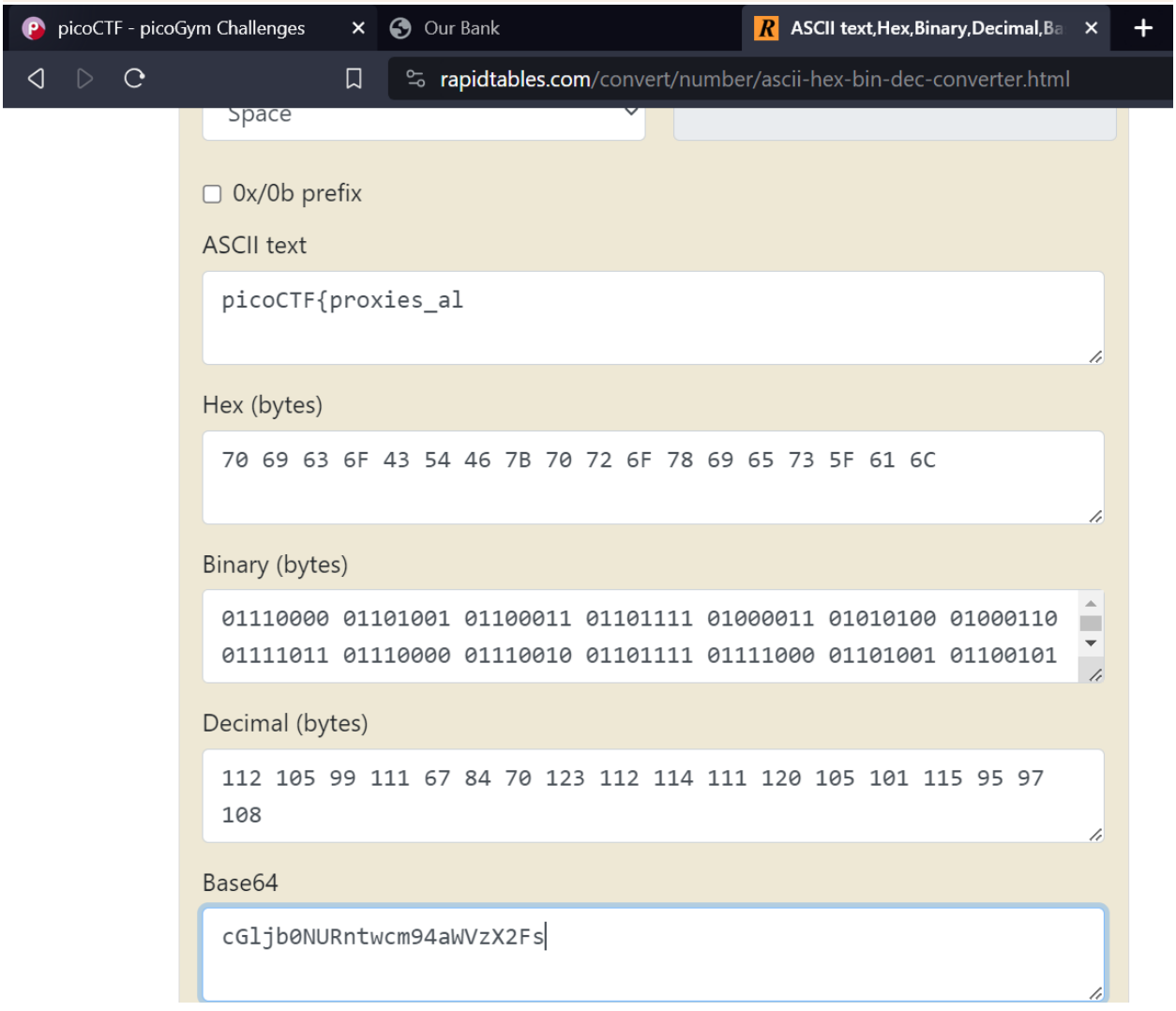

picoCTF - picoGym Challenges
Welcome
Not secure | saturn.picoctf.net:58581
Help us test this form
username:test and password:test.
Username
username
Password
Password
test


picoCTF - picoGym Challenges
Our Bank
Not secure | saturn.picoctf.net:58581/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
Lighthouse
Recorder
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
All
Doc
JS
Fetch/XHR
CSS
Font
Img
Media
Manifest
WS
Wasm
Other
Blocked requests
3rd-party requests
10 ms
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
80 ms
90 ms
Recording network activity...
Perform a request or hit Ctrl + R to record the reload.
Learn more


picoCTF - picoGym Challenges
Our Bank
saturn.picoctf.net:58581/next-page/id=bF90aGVfd2F5X2QxYzBiMTEyfQ==
Welcome fellow Human
flag
Go
I was redirected here by a friend of mine but i couldnt find anything. Help me search for flags :-)
saturn.picoctf.net:58581/next-page/id=bF90aGVfd2F5X2QxYzBiMTEyfQ==
saturn.picoctf.net:58581
saturn.picoctf.net:58581/ - Google Search
flag - saturn.picoctf.net:58581/next-page/id=bF90aGVfd2F5X2QxYzBiMTEyfQ==
Our Bank - saturn.picoctf.net:58581/home
Our Bank - saturn.picoctf.net:58581/home?


picoCTF - picoGym Challenges
Our Bank
ASCII text,Hex,Binary,Decimal,Ba
rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html
Space
0x/0b prefix
ASCII text
l_the_way_d1c0b112}
Hex (bytes)
6C 5F 74 68 65 5F 77 61 79 5F 64 31 63 30 62 31 31 32 7D
Binary (bytes)
01101100 01011111 01110100 01101000 01100101 01011111 01110111
01100001 01111001 01011111 01100100 00110001 01100011 00110000
Decimal (bytes)
108 95 116 104 101 95 119 97 121 95 100 49 99 48 98 49 49 50 125
Base64
bF90aGVfd2F5X2QxYzBiMTEyfQ==
NUMBER CONVERSION
ASCII,Hex,Binary,Decimal converter
ASCII to binary
ASCII to hex
Base converter


picoCTF - picoGym Challenges
Our Bank
ASCII text,Hex,Binary,Decimal,Base64
saturn.picoctf.net:58581/next-page/id=cGljb0NURntwcm94aWVzX2Fs
saturn.picoctf.net:58581/next-page/id=cG
saturn.picoctf.net:58581/next-page/id=cG - Google Search
flag - saturn.picoctf.net:58581/next-page/id=cGljb0NURntwcm94aWVzX2Fs
Welcome fellow Human
I was redirected here by a friend of mine but I couldn't find anything. Help me search for flags :-)


picoCTF - picoGym Challenges
Our Bank
ASCII text,Hex,Binary,Decimal,Ba
rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html
Space
0x/0b prefix
ASCII text
picoCTF{proxies_al
Hex (bytes)
70 69 63 6F 43 54 46 7B 70 72 6F 78 69 65 73 5F 61 6C
Binary (bytes)
01110000 01101001 01100011 01101111 01000011 01010100 01000110
01111011 01110000 01110010 01101111 01111000 01101001 01100101
Decimal (bytes)
112 105 99 111 67 84 70 123 112 114 111 120 105 101 115 95 97
108
Base64
cGljb0NURntwcm94aWVzX2Fs