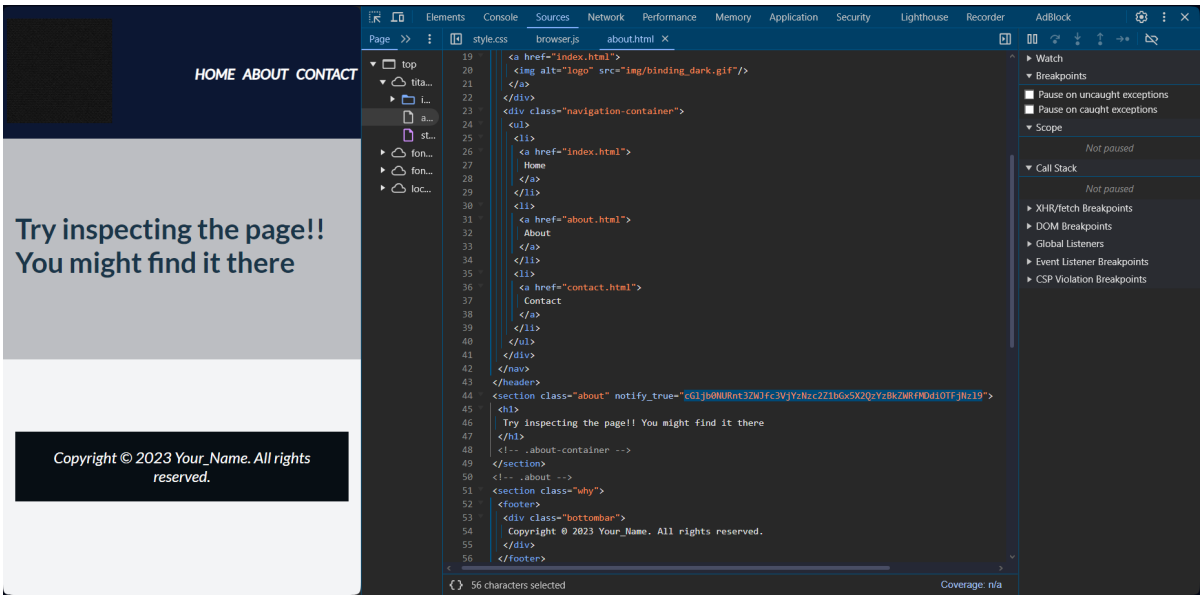
PICO CTF Write Up (All Easy Practices)

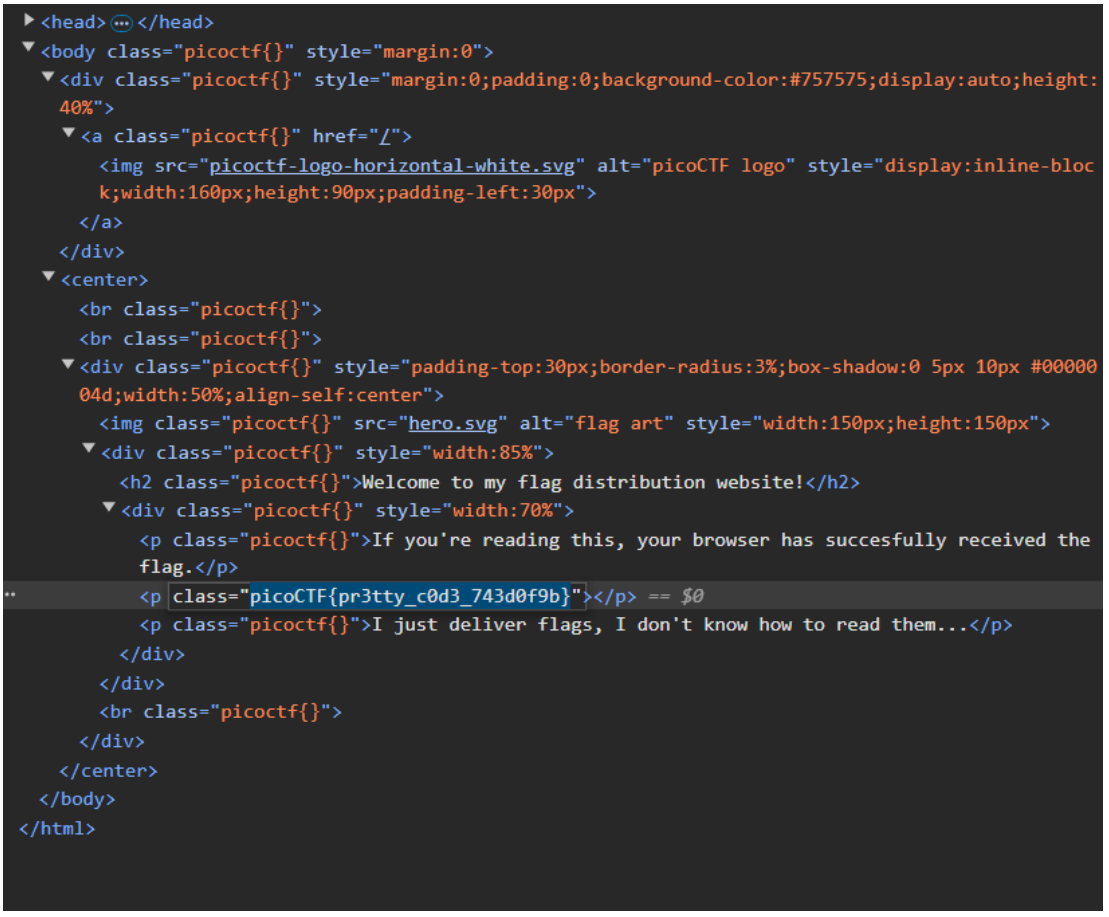
WebDecode

Inspect and Decode the "*sus*" parameters from base64 decoding



Unminify

Inspect directly see the source .php file



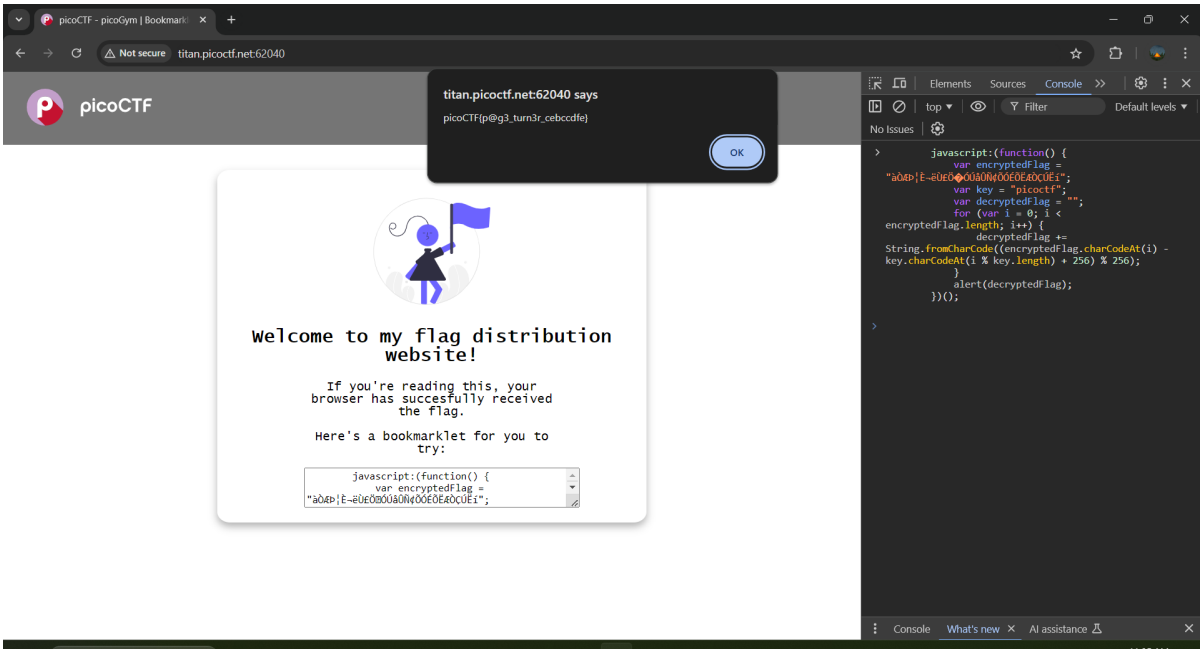
IntroToBurp

after submitting the first login, intercept the otp request pages `Content-type` 's value to `plain/text` ' or any other invalid value

Weak or Improper Server-Side input validation ➡️ at this challenge the website only getting designed to validate properly formatted requests with Contect-Type: application/x-www-form-urlencoded (Missing Logic) || changing the value will bypass this validation filter (Content-Type error makes otp validation getting passed)

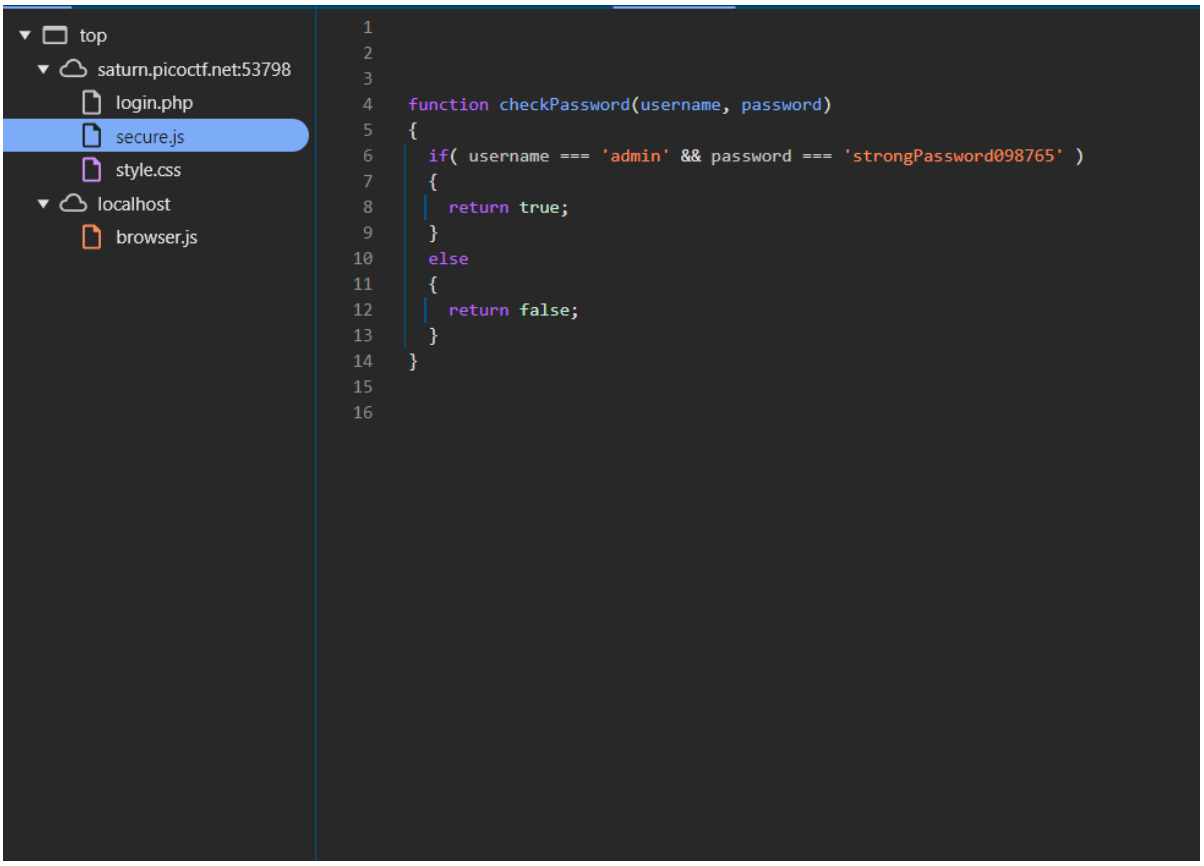
BookMarklet

Directly use the leaked javascript function to the web console and print out the flag directly



Local Authority

After attempting with random password, the secure.js will appear and leaked the real admin username and password



Inspect HTML

Directly inspect .html

Includes

Directly see the sources file and combine the flag

Cookies

Since submitting the form have a Cookie format of `Cookie: name=-1` try adjusting from 1 to max of 28 by using web browser Cookie editor or burp Suite (One of the cookie lies there ~17)

Scavenger Hunt

This one is to explore the websites directory

part 1 = index.php

part 2 = mycss.css

part 3 = robots.txt + *clue: apache server*

part 4 = .htaccess + clue: storing web files at mac || **.htaccess** is for web directory level configuration (Authentication, Access Control)

part 5 = .DS_Store || **.DS_Store** is macOS's hidden file storing custom attributes of a folder primarily a system file (reveal hidden directories within that folder)

get aHEAD

Directly change the request method to HEAD (**HEAD** : commonly used to check the availability of the specific resource), and check the network tab for the response (flag)

dont-use-client-side

```
function verify() {
  checkpass = document.getElementById("pass").value;
  split = 4;
  if (checkpass.substring(0, split) == 'pico') {
    if (checkpass.substring(split*6, split*7) == '706c') {
      if (checkpass.substring(split, split*2) == 'CTF{') {
       if (checkpass.substring(split*4, split*5) == 'ts_p') {
        if (checkpass.substring(split*3, split*4) == 'lien') {
          if (checkpass.substring(split*5, split*6) == 'lz_b') {
            if (checkpass.substring(split*2, split*3) == 'no_c') {
              if (checkpass.substring(split*7, split*8) == '5}') {
                alert("Password Verified")
                }
              }
            }

          }
        }
      }
    }
  }
  else {
    alert("Incorrect password");
  }

}
```

Directly align the order (split, split*2), (split*2, split3), ...

logon

Intercept the post requests from the login, and change the cookie information about the admin to **True**

Insp3ct0r

inspect and explore all source file

where are the robots

go to robots.txt and access the vulnerable directory