

Scavenger Hunt



Easy

Web Exploitation

picoCTF 2021

AUTHOR: MADSTACKS

Description

There is some interesting information hidden around this site. Can you find it?

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

[Launch Instance](#)

81,390 users solved

67% Liked

picoCTF{FLAG}

[Submit Flag](#)

Hint :

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

Solusi :

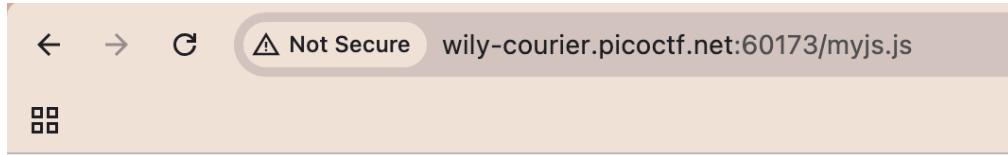
Kita buka web problemnya, lalu langsung inspect untuk melihat code utama yang terlihat setelah inspect. disitu kita melihat ada potongan flag seperti berikut.

```
<!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>
    <div class="container">
      <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>
      <div id="tabintro" class="tabcontent" style="display: block;">
        <h3>How</h3>
        <p>How do you like my website?</p>
      </div>
      <div id="tababout" class="tabcontent" style="display: none;">
        <h3>What</h3>
        <p>...</p>
        <!-- Here's the first part of the flag: picoCTF{ -->
        ...
    </div>
  </body>
</html>
```

Setelah itu, aku coba cari file lain karena menurut hint mungkin menyindir kita untuk mencari file lain. Kita lihat ada 2 file di head, yaitu mycss.css dan [myjs.js](#). kita coba buka melalui URL dengan menambah /{file} seperti berikut. dan ini hasil dari membuka mycss.css

```
div.container {  
    width: 100%;  
}  
  
header {  
    background-color: black;  
    padding: 1em;  
    color: white;  
    clear: left;  
    text-align: center;  
}  
  
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 */
```

Disitu ada potongan ke-2 dari flag. setelah itu kita cari lagi potongan lain dengan membuka file [myjs.js](#) melalui URL. hasilnya seperti berikut.



```
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? */
```

Jika kita lihat, ada hint baru di paling bawah yang membuat kami untuk ingin melanggar HINT (jangan brute force) tapi kami ngeyel lupa kalo itu cuma hint bukan peraturan dari kompetisi atau picoctf. seperti ini brute forcenya.

```
~ % brew install dirsearch
```

Kita download dulu tools nya yaitu tools dirsearch

```
dirsearch % ls
CHANGELOG.md      config.ini      setup.cfg
CONTRIBUTORS.md   db              setup.py
Dockerfile         dirsearch.py    static
README.md          lib             testing.py
__init__.py        requirements.txt tests
dirsearch % pwd
/Users/user/dirsearch
dirsearch % python3 dirsearch.py -u http://wily-courier.picoctf.net:60173/
[...]
v0.4.3
Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25
Wordlist size: 12294

Target: http://wily-courier.picoctf.net:60173/

[22:15:59] Scanning:
[22:16:13] 200 - 65B - /DS_Store
[22:16:17] 200 - 96B - /.htaccess
[22:17:59] 200 - 961B - /index.html
[22:18:40] 200 - 124B - /robots.txt
[22:18:43] 403 - 292B - /server-status
[22:18:43] 403 - 292B - /server-status/

Task Completed
dirsearch %
```

Kita melihat ada beberapa file disana. kita coba lihat dan akses robots.txt dengan menambahkan url /robots.txt hasilnya sebagai berikut.

← → ⌂

⚠ Not Secure

wily-courier.picoctf.net:60173/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?
```

Ada intruksi disallow /index.html, berarti jangan buka index.html.

← → ⌂

⚠ Not Secure

wily-courier.picoctf.net:60173/.htaccess



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

← → ⌂

⚠ Not Secure

wily-courier.picoctf.net:60173/.DS_Store



Congrats! You've completed the scavenger hunt! Part 5: _9588550}

picoCTF{th4ts_4_l0t_0f_pl4c3s_2_lO0k_9588550}