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

Hints

1

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.

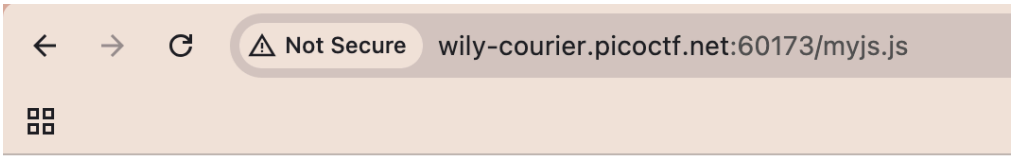
Solusi :

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

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 */
```

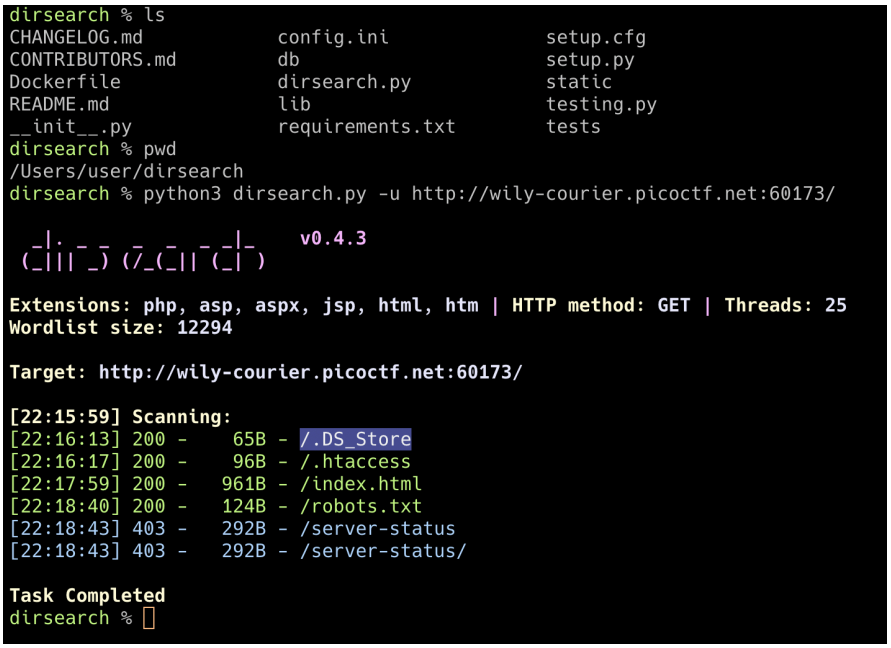
Disitu ada potongan ke-2 dari flag. setelah itu kita cari lagi potongan lain dengan membuka file myjs.js melalui URL. hasilnya seperti berikut.



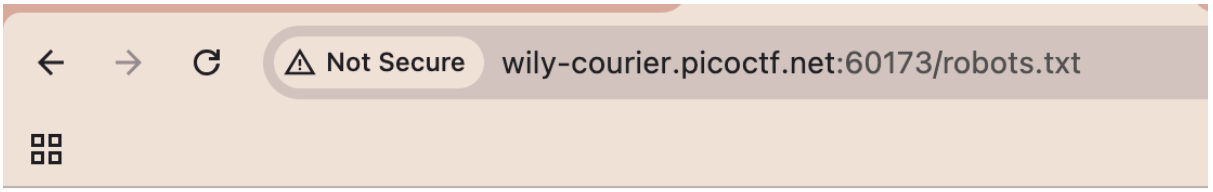

```
function openTab(tabName,elmnt,color) {
    var i, tabcontent, tablinks;
    tabcontent = document.getElementsByClassName("tabcontent");
    for (i = 0; i < tabcontent.length; i++) {
        tabcontent[i].style.display = "none";
    }
    tablinks = document.getElementsByClassName("tablink");
    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.

Kita download dulu tools nya yaitu tools dirsearch

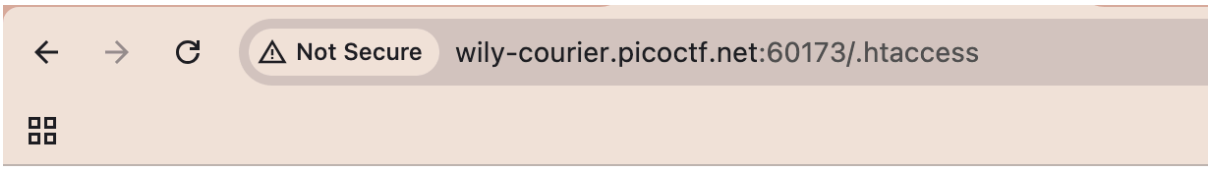


Kita melihat ada beberapa file disana. kita coba lihat dan akses robots.txt dengan menambahkan url /robots.txt hasilnya sebagai berikut.

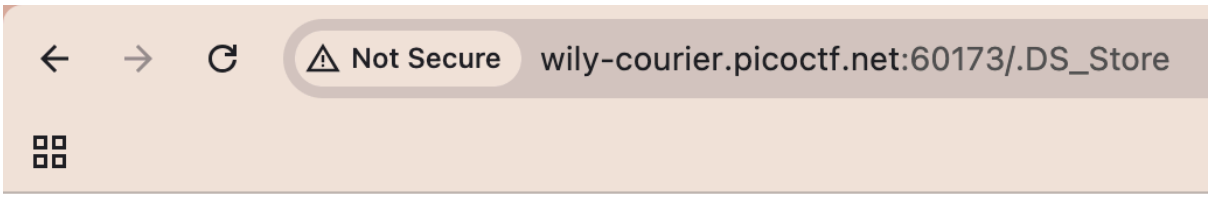



```
User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

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




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




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

picoCTF{th4ts_4_l0t_0f_pl4c3s_2_lO0k_9588550}