

Includes 



Easy

Web Exploitation

picoCTF 2022

inspector

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

Go to this [website](#) and see what you can discover.

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **14:07**

Restart Instance

Hints

1

79,695 users solved



84% Liked



picoCTF{FLAG}

Submit Flag

Hint :

1. Is there more code than what the inspector initially shows?

Solusi :

Melihat hint tersebut, berarti kemungkinan flag ada di code lain selain apa yang terlihat pada hasil inspect utama. Tapi kita bedah dulu apa isi inspect utama.

```
<!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>On Includes</title>
  </head>
  <body>
    <script src="script.js"></script>
    <h1>On Includes</h1>
  </body>
</html>
```

... <p> == \$0

"Many programming languages and other computer files have a directive, often called include (sometimes copy or import), that causes the contents of a second file to be inserted into the original file. These included files are called copybooks or header files. They are often used to define the physical layout of program data, pieces of procedural code and/or forward declarations while promoting encapsulation and the reuse of code."

</p>

<p> Source: Wikipedia on Include directive </p>

<button type="button" onclick="greetings();">Say hello</button>

</body>

</html>

Sekilas kita tidak melihat yang janggal. Namun aku coba lagi dengan metode lain melalui network dengan memicu respon berbeda, ternyata hasilnya juga null. coba cara lain lagi hasilnya null. Dan akhirnya kami kembali lagi di tampilan code inspect utama dan sedikit melihat keanehan yaitu ada 2 file lain pada directory yang sama / alamat yang sama yaitu file style.css dan [script.js](#) yang artinya bisa dibuka melalui URL secara langsung dengan menambahkan `{file_lain}`. Kita coba dulu untuk style.css dan hasilnya sebagai berikut.

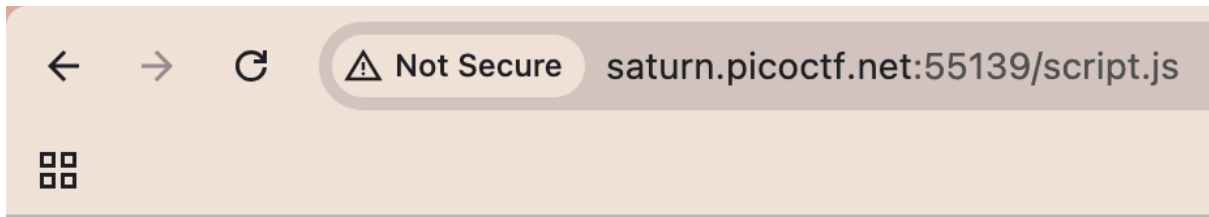
```
← → ↻ ⚠ Not Secure saturn.picocft.net:55139/style.css
```

☐☐☐

```
body {
  background-color: lightblue;
}

/* picoCTF{1nclu51v17y_1of2_ */
```

Flagnya mungkin terpisah, mungkin bisa kita temukan di file 1 nya sebagai berikut.



```
function greetings()  
{  
  alert("This code is in a separate file!");  
}  
  
// f7w_2of2_6edef411}
```

Alhasil flagnya diteukan.