

Local Authority



Easy Web Exploitation picoCTF 2022 inspector

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

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](#)

79,089 users solved

95% Liked

1

picoCTF{FLAG}

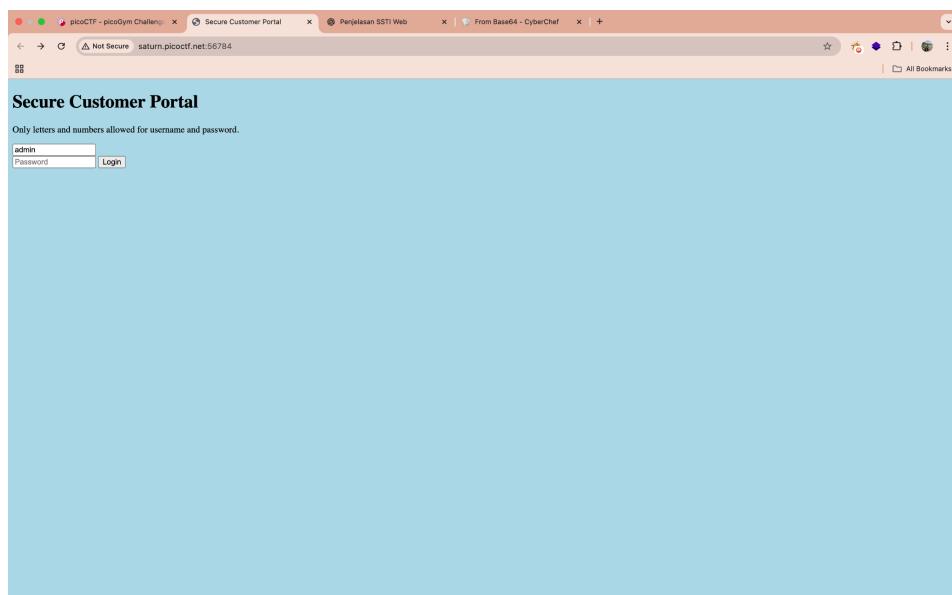
[Submit Flag](#)

Hint :

1. How is the password checked on this website?

Solusi :

Kita coba untuk launch instance, setelah launch instance akan ada link web yang dituju dengan tampilan berikut.



Web ini berisi form username dan password untuk diinput (login), dan bayangan kita mengacu pada injeksi SQL, namun ketika lihat hint, kami menyadari bahwa hint tersebut menginstruksikan kita untuk dapat mengerti cara password login ini dicek.

Kami coba untuk langsung inspect sebelum mensubmit username dan password untuk memicu perubahan pada program di inspect.

The screenshot shows the Network tab in the Chrome DevTools developer tools. The URL is `saturn.picoctf.net:55831`. The page title is "Secure Customer Portal". A form is visible with fields for "username" containing "asdawd" and "password" containing "*****". A "Login" button is present. The Network tab shows a single request to "login.php" with a status of 200 ms. The table below lists the request details:

Name	Status	Type	Initiator	Size	Time
login.php	200	document	Other	1.0 kB	316 ms

At the bottom, it says "8 requests | 9.6 kB transferred | 10.2 kB resources | Finish: 7.20 s". A message at the bottom right says "Currently recording network activity" and "Perform a request or reload the page by using the "Reload page" button or by pressing ⌘ R. Learn more". A "Reload page" button is shown.

Ini adalah tampilan page ketika belum mensubmit username dan password yang ada pada form.

The screenshot shows the Network tab in the Chrome DevTools developer tools. The URL is `saturn.picoctf.net:55831/login.php`. The page title is "Log In Failed". The Network tab shows multiple requests: "login.php" (status 200), "style.css" (status 200), "secure.js" (status 200), "js.js" (status 200), "dom.js" (status 200), "js.js" (status 200), and "dom.js" (status 200). The table below lists the request details:

Name	Status	Type	Initiator	Size	Time
login.php	200	document	Other	1.0 kB	316 ms
style.css	200	stylesheet	login.php:7	(memory ...)	0 ms
secure.js	200	script	login.php:11	(disk cac...)	1 ms
js.js	200	script	content.js:43	1.4 kB	2 ms
dom.js	200	script	content.js:43	2.0 kB	2 ms
js.js	200	script	content.js:43	1.4 kB	1 ms
dom.js	200	script	content.js:43	2.0 kB	1 ms

At the bottom, it says "7 requests | 7.7 kB transferred | 8.8 kB resources | Finish: 2.04 s | DOMContentLoaded: 476 ms | Load: 569 r".

Setelah dilakukan submit, network memberikan beberapa file js dan kami terpacu pada file [secure.js](#), langsung saja kita buka.

Name	Headers	Preview	Response	Initiator	Timing
login.php					
style.css					
secure.js					
js.js					
dom.js					
js.js					
dom.js					
js.js					

```
1
2
3
4 function checkPassword(username, password)
5 {
6     if( username === 'admin' && password === 'strongPassword098765' )
7     {
8         return true;
9     }
10    else
11    {
12        return false;
13    }
14}
15
16
```

Dan ternyata disana terdapat validasi username dan password beserta isi username dan password dengan role sebagai admin. Jadi kita coba input saja di form login tadi.

Secure Customer Portal

Only letters and numbers allowed for username and password.

picoCTF{j5_15_7r4n5p4r3n7_05df90c8}

Benar saja, kami menemukan flagnya.