

# 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

## Hints ?

1

79,089 users solved



95% Liked



picoCTF{FLAG}

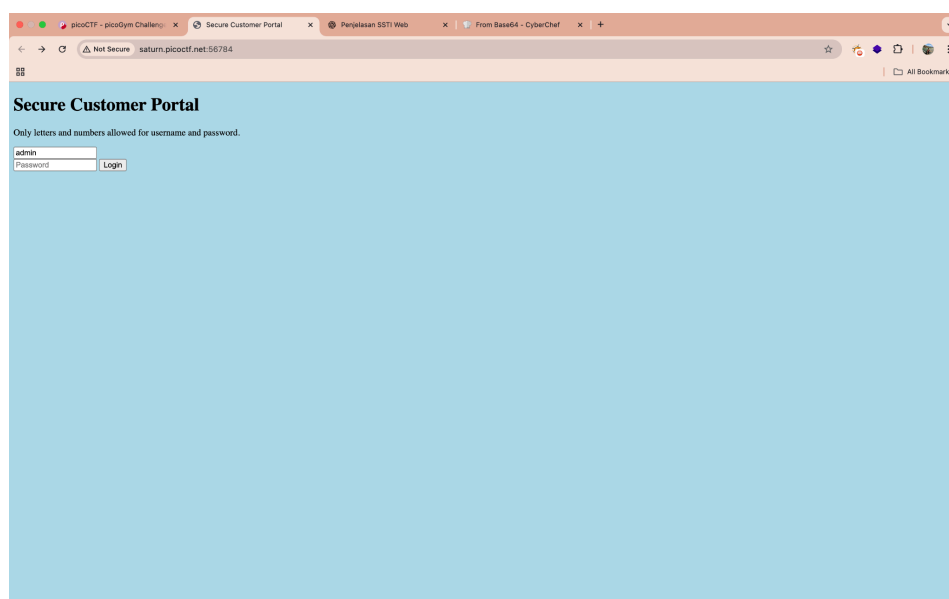
Submit Flag

Hint :

1. How is the password checked on this website?

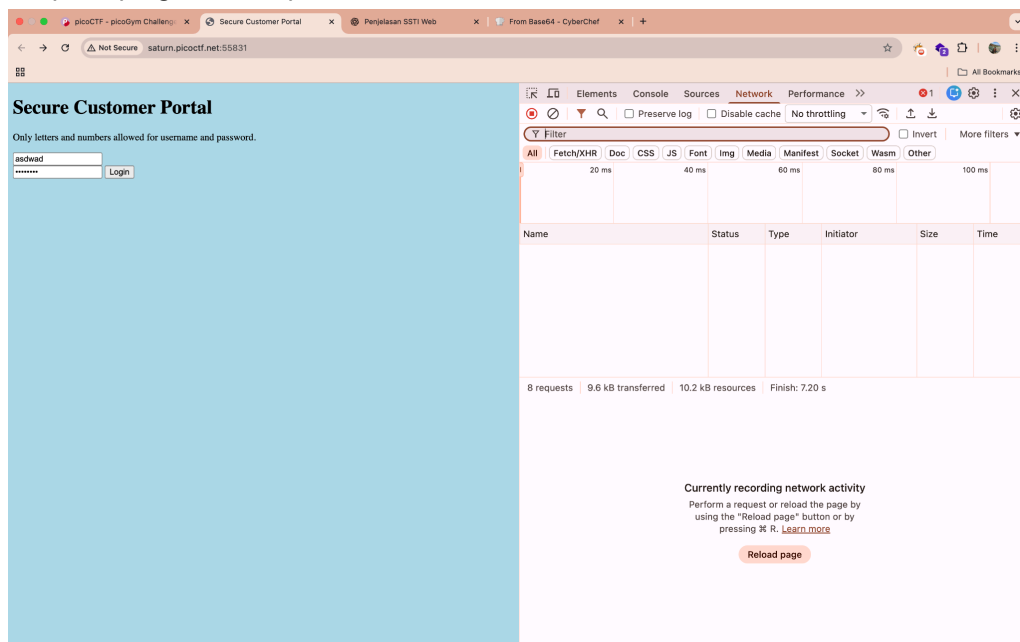
Solusi :

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

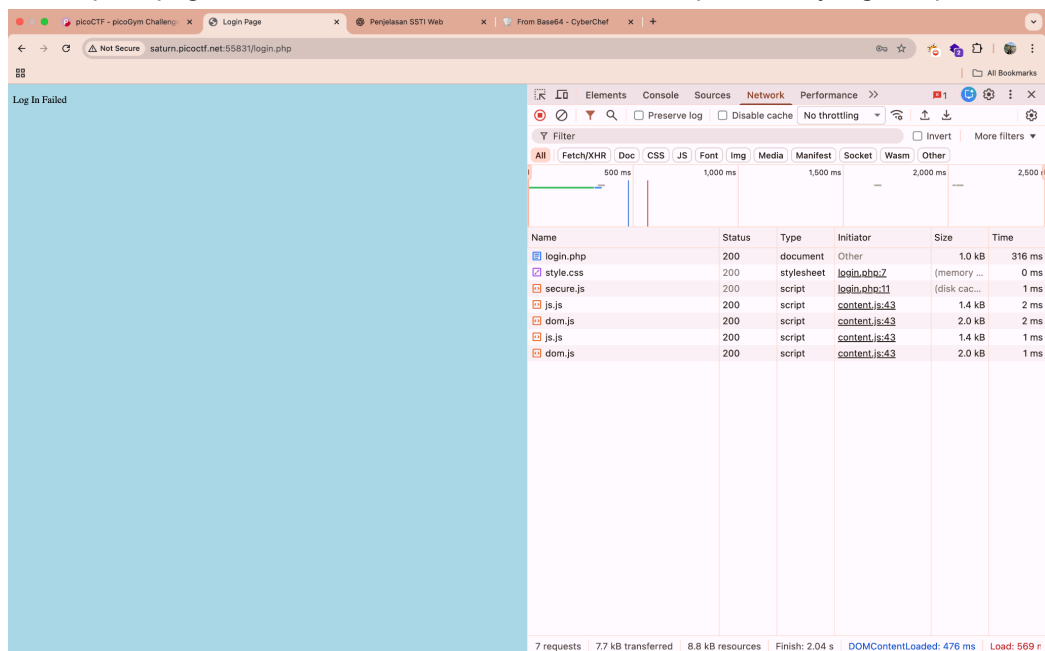


Web ini berisi form username dan password untuk diinput (login), dan bayangan kita mengacu pada injeksi SQL, namun ketika lihat hint, kami menyadari bahwa hint tersebut menginstruksikan kita untuk dapat mengerti cara password login ini dicek.

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



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



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

Name	X	Headers	Preview	Response	Initiator	Timing
login.php	1					
style.css	2					
secure.js	3					
js.js	4		<pre>function checkPassword(username, password)</pre>			
dom.js	5		<pre>{</pre>			
js.js	6		<pre>  if( username === 'admin' &amp;&amp; password === 'strongPassword098765' )</pre>			
dom.js	7		<pre>  {</pre>			
js.js	8		<pre>    return true;</pre>			
dom.js	9		<pre>  }</pre>			
js.js	10		<pre>  else</pre>			
	11		<pre>  {</pre>			
	12		<pre>    return false;</pre>			
	13		<pre>  }</pre>			
	14		<pre>}</pre>			
	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.