

logon

Web Exploitation

Description:

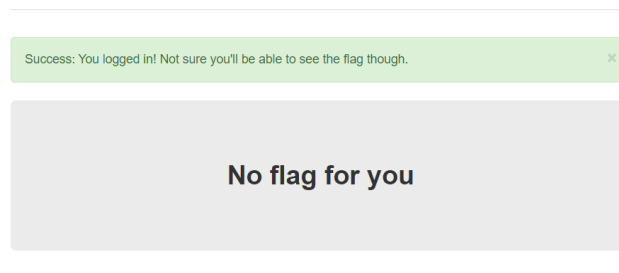
The factory is hiding things from all of its users. Can you login as Joe and find what they've been looking at?

<https://jupiter.challenges.picoctf.org/problem/13594/>

Hints:

- 1) Hmm it doesn't seem to check anyone's password, except for Joe's?

Solution:



Name	Value	Domain	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition Key	Prio
admin	False	jupiter.chal...	/	Session	10					Med
username	Vik	jupiter.chal...	/	Session	11					Med
__cf_bm	9SzgvP.Ol6bmGZVPiskfanWhxpdBtjsC0flw7eDBGME-1704919402-...	.picoctf.org	/	2024-01-1...	152	✓	✓	None		Med
_ga_l6FT52K063	GS1.2.1704915634.21.1.1704919158.0.0.0	.picoctf.org	/	2025-02-1...	52					Med
cf_clearance	wNai2EQEn7uXt15nuMxJpgpqyulgYRCPA3v298r4xbw-1704826160...	.picoctf.org	/	2025-01-0...	112	✓	✓	None		Med
password	1234	jupiter.chal...	/	Session	12					Med

- 1) You can login as any user except Joe using any password.
- 2) We do that and inspect the cookies where we see a admin cookie which is set to false.

	Value
	True
	Vik
	9SzgvP.OI6bmGZvPlskfanWhxpdBtjsC0flw7eDBGME-170491
	GS1.2.1704915634.21.1.1704919158.0.0.0
	wNai2EQEn7uXt15nuMxJpgpqyulgYRCPA3v298r4xbw-17049

3) We change the value of this to true to get the flag.

Flag:

picoCTF{th3_c0nsp1r4cy_l1v3s_d1c24fef}

Flag:

picoCTF{th3_c0nsp1r4cy_l1v3s_d1c24fef}