Logon picoCTF

logon 🔖   👤 | 100 points ✕

Tags: picoCTF 2019   Web Exploitation

AUTHOR: BOBSON

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/44573/ (link) or http://jupiter.challenges.picoctf.org:44573

Hints ❓

1

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

46,704 solves / 49,312 users attempted (95%)   👎 88% Liked 👍

🚩 picoCTF{FLAG}   Submit Flag

I opened up the link and came to a login screen.

Factory Login   Home   Sign Out

Username

Password

Sign In

© PicoCTF 2019

Upon entering Joe's name for the username and blank password I was greeted with this message.
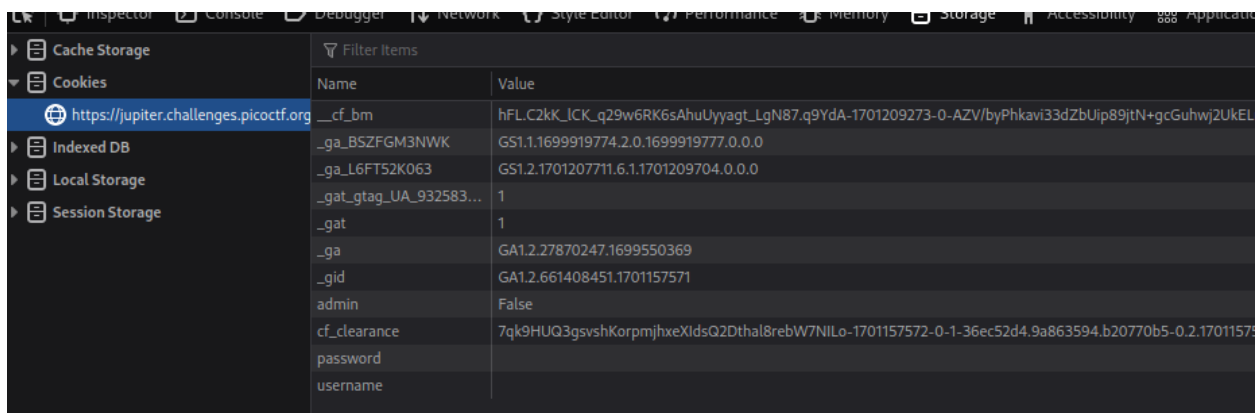
I'm sorry Joe's password is super secure. You're not getting in that way.   ✕

After a few common password tries I saw that this method would not work and tried clearing out the entries and signing in and got this message.

Success: You logged in! Not sure you'll be able to see the flag though.   ✕

No flag for you

From here I decided to inspect the page. I began going through all the tabs and saw in the cookies that the admin tab was set to false.

Name	Value
__cf_bm	hFL.C2kK_lCK_q29w6RK6sAhuUyyagt_LgN87.q9YdA-1701209273-0-AZV/byPhkavi33dZbUip89jtN+gcGuhwj2UkEL
_ga_BSZFGM3NWK	GS1.1.1699919774.2.0.1699919777.0.0.0
_ga_L6FT52K063	GS1.2.1701207711.6.1.1701209704.0.0.0
_gat_gtag_UA_932583...	1
_gat	1
_ga	GA1.2.27870247.1699550369
_gid	GA1.2.661408451.1701157571
admin	False
cf_clearance	7qk9HUQ3gsvshKorpmjhxeXldsQ2Dthal8rebW7NILo-1701157572-0-1-36ec52d4.9a863594.b20770b5-0.2.17011575
password	
username	

I changed the value to True and refreshed the page and got the flag.

Flag:

picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}