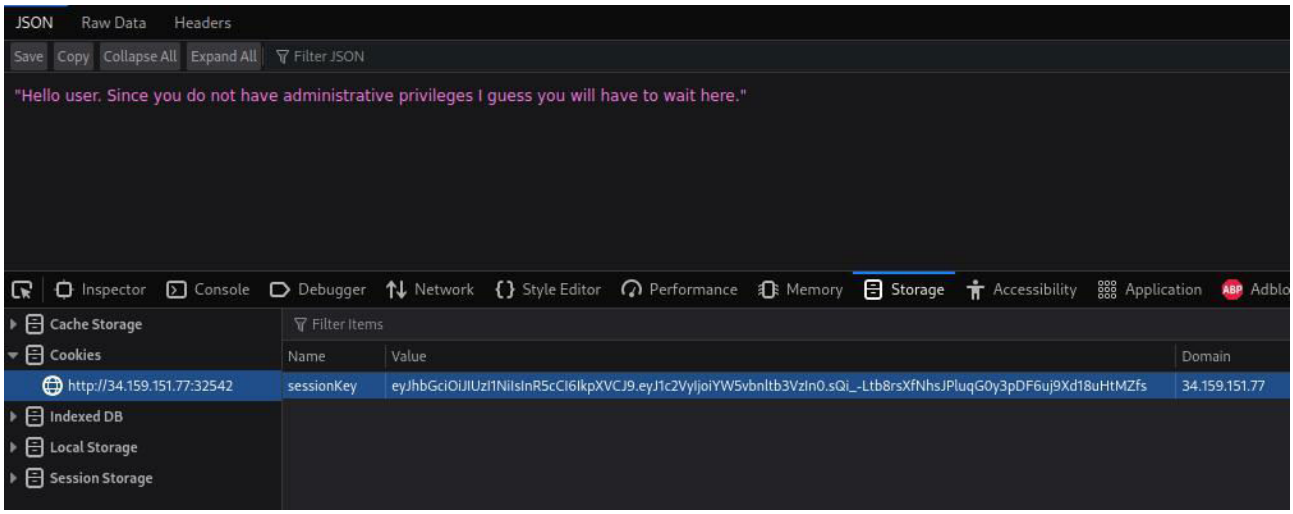
you-can-trust-me

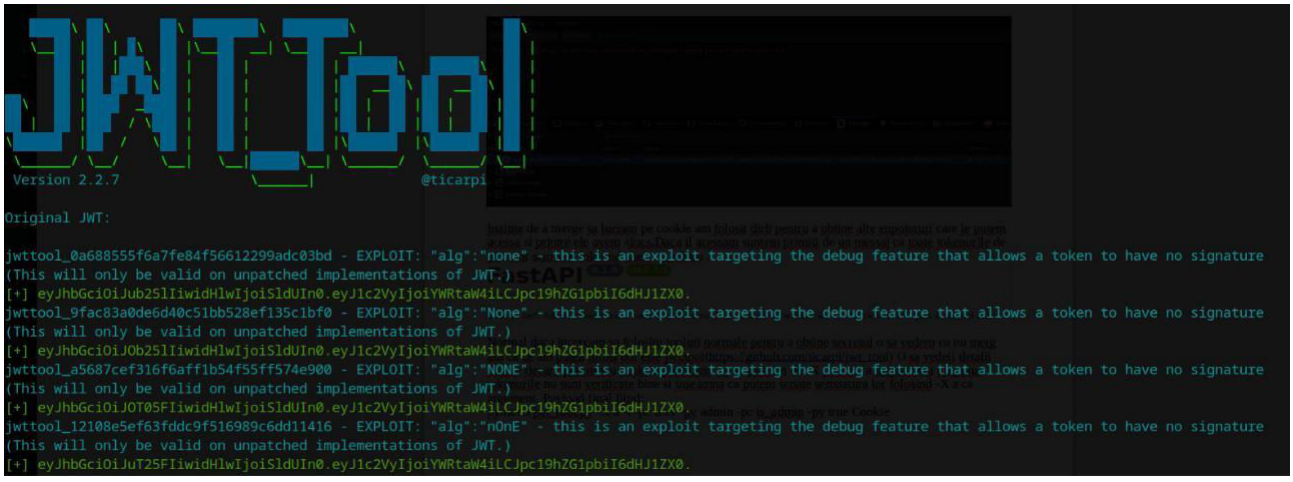
Din descriere este clar ca avem de aface cu manipulare de cookies asa ca daca aruncam o privire pe site vedem un mesaj care ne zice ca avem nevoie de privilegii de admin asa ca daca ne uitam la cookie observam ca este un jwt tipic .



Inainte de a merge sa lucram pe cookie am folosit dirb pentru a obtine alte enpointuri care le putem acessa si printre ele avem /docs.Daca il acessam suntem primiti de un messaj ca toate tokenurile de jwt sunt semnate folosind cheia is_admin .

Note to self: Admin tokens must have the is_admin key defined otherwise we will know that it is just a normal user.

Normal daca incercam sa folosim tooluri normale pentru a obtine secretul o sa vedem ca nu merg asa ca ce am putea folosi noi este jwt.tool(https://github.com/ticarpi/jwt_tool) O sa vedeti detalii despre fiecare parametru acolo si incercam sa ne folosim de -X pentru ca majoritatea timpului tokenurile nu sunt verificate bine si inseamna ca putem scoate semnatura lor folosind -X a ca argument. Payload final fiind:
python3 jwt_tool.py -X a -I -pc user -pv admin -pc is_admin -pv true Cookie



Dupa ce obtinem cookie-ul il schimbam pe site in storage dar primim mesaj ca flagul lipseste...Well din nou mergem la jwt.io si incercam sa adaug la payload flag si il setam true(adica exista) :

python3 jwt_tool.py -X a -I -pc user -pv admin -pc is_admin -pv true -pc flag -pv true cookie

Deci am terminat nu?Nici pe aproape acum primim la raspuns missing pin.Well we give or or try harder?Ez response so incercam sa adaugam si pinul 123456 de exemplu:

python3 jwt_tool.py -X a -I -pc user -pv admin -pc is_admin -pv true -pc flag -pv true -pc pin -pv 123456 cookie

Problema aici este ca primim ca response faptul ca nu este cel bun si ca este format din 4 cifre.Well aici este o problema pentru ca avem 10^4 posibilitati pentru acest pin deci….? Un script o sa ajute normal doar ca de obicei in ctf exista 2 numere magice de 4 cifre care sunt folosite mai mereu:1337 (leet) si 7331. Deci daca incercam pe ambele o sa vedem ca primim ca response flagul.Payloadul folosit in final:

python3 jwt_tool.py -X a -I -pc user -pv admin -pc is_admin -pv true -pc flag -pv true -pc pin -pv 7331 cookies

Desigur un approach mai corect era un bruteforce de pinuri folosind un script doar ca asta dureaza mult timp plus ca trebuie modificat astfel incat cookie-ul sa aibe signatura : none.

Flag:

CTF{2965f7e9fcc77fff2bd869db984d…….6781edb382cc34536904207a53d}

Trolled by masquerade8077