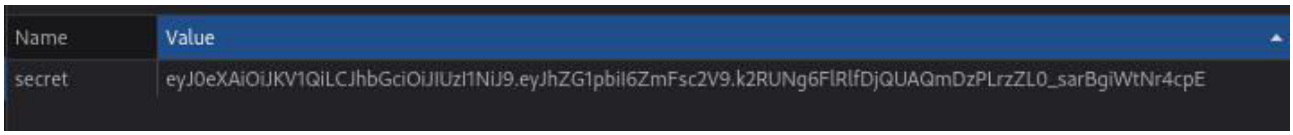
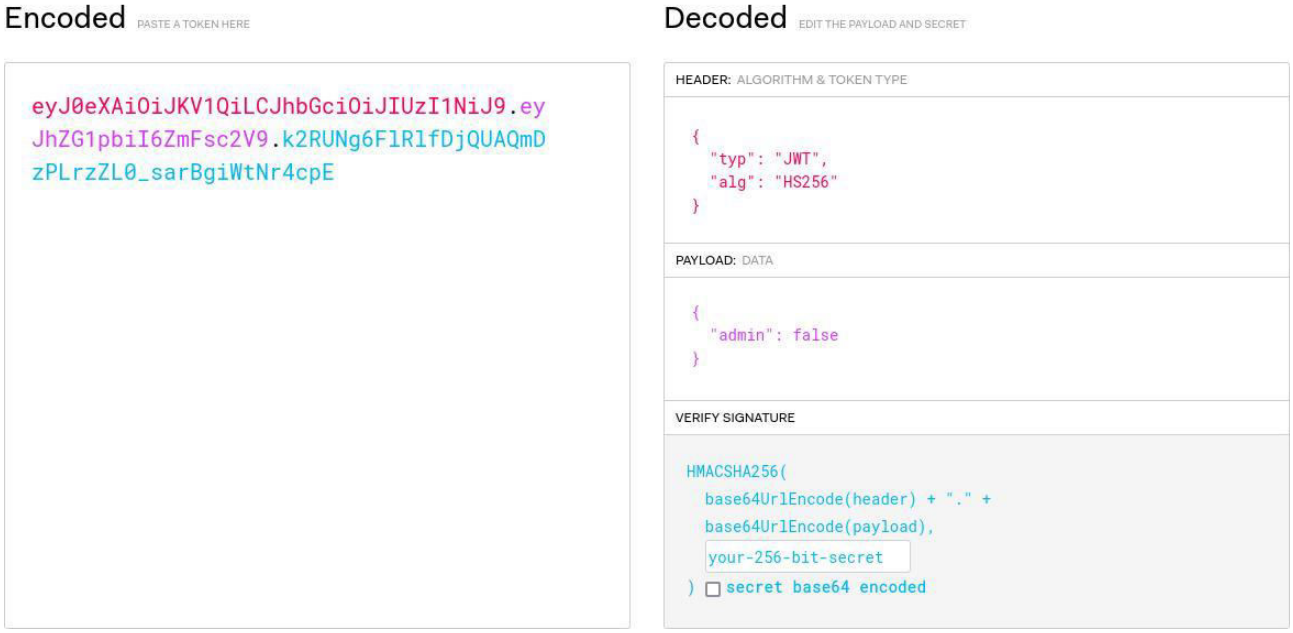
Cat-button

Din descriere ne putem da seama ca avem nevoie de privilegii de admin ca sa putem lua flagul.Daca aruncam o privire suntem primiti de o pisica :)).Aruncand o privire peste site nu se observa nimic special adica avem cookie cu scor si asa mai departe da nu ne ajuta cu nimic ca sa obtinem alte privilegii sau sa primim flagul.Dupa o perioada de timp am observat in coltul paginii un button alb “Reveal Secret” care ma trimis la http://35.246.139.54:31153/secret.php .Primim un mesaj interesant aici cum nu avem cookie de administrator asa ca sa aruncam o privire la cookies (Inspect / Q ==> Storage si Cookies)

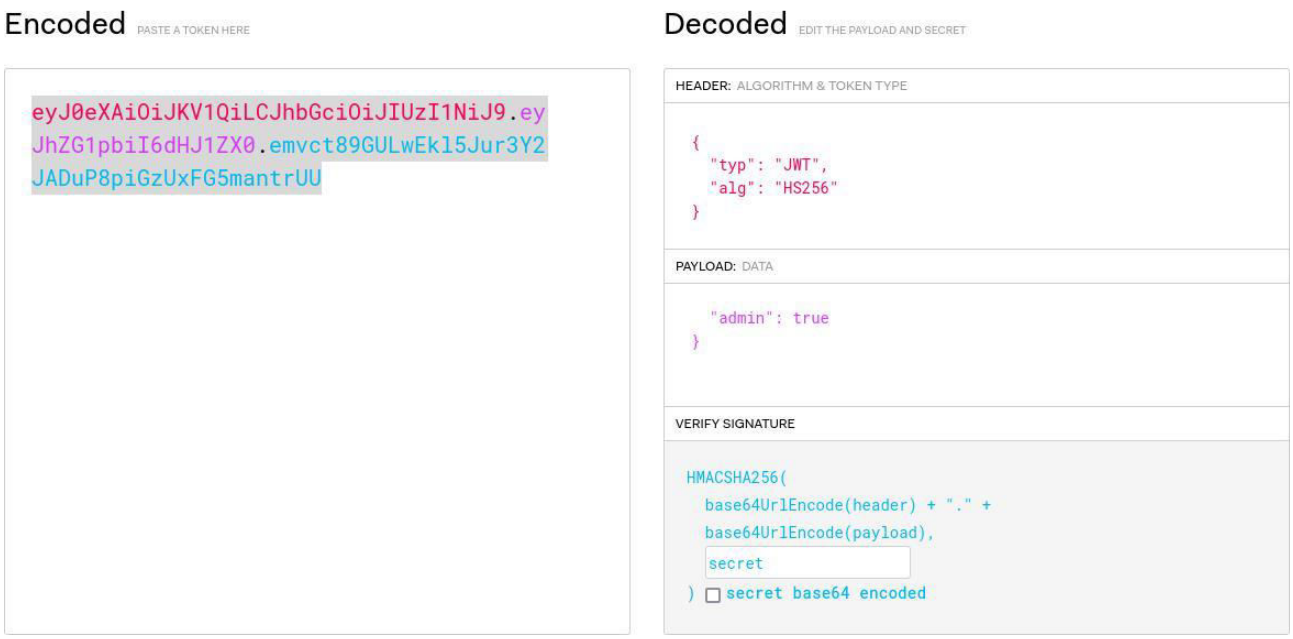


Acest șir de caractere dat este un **JSON Web Token** (JWT). JWT (JSON Web Token) este folosit pentru **autentificare și autorizare** într-un mod sigur și compact. **Prima parte (Header):** `eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9`
A doua parte (Payload): `eyJhZG1pbiI6ZmFsc2V9`
A treia parte (Signature): `k2RUNg6FlRlfDjQUAQmDzPLrzZL0_sarBgiWtNr4cpE`
De aici putem folosi un tool ca jwt.io sa vedem ce contine acest cookie:



Daca ne uitam la payloadul pe care il contine are “admin” setat pe fals.Deci singurul lucru care trebuie sa il facem este sa il setam pe true si sa luam flagul nu?Suna destul de simplu doar ca fiecare token este semnat de catre un secret deci fara acel secret nu putem sa acessam site -ul cu cookie de admin.Aici putem folosi un approach de brute-force cu diverse tooluri.Eu folosesc de obicei un tool numit jwt-cracker(https://github.com/brendan-rius/c-jwt-cracker).O sa ai nevoie de un wordlist ca acesta sa functioneze deoarece noi incercam parole astfel incat una sa fie valida pnetru acest cookie(rock you este pritenul tau,doar cauti rock you wordlist o sa fie primul link)

Dupa aplicare descoperim ca sercretul folosit pentru a cripta acest cookie este “secret” . Asa ca setam admin pe true, punem la signature “secret” si o sa primim un nou cookie bazat pe informatiile oferite:



Singurul lucru ramas acum este sa copiezi acest cookie nou sa il introduci in loc de cookie-ul vechi si o vezi cum pe pagina o sa primesti flagul.

CTF{98ed1dfbddd3510841cdeb99……e9841758708046540237987}

Trolled by masquerade8077