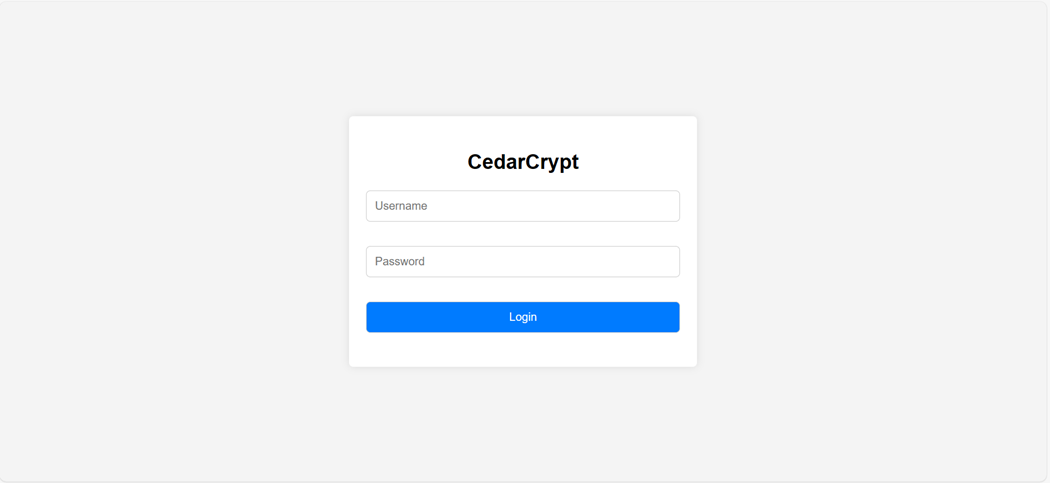
# ***Challenge Name :- CedarCrypt***

**Description:** Welcome to the CedarCrypt Adventure! Your journey begins in a mystical realm where you'll encounter the secrets of ancient trees and the power of JSON Web Tokens (JWT). Embark on this quest to unveil the hidden flag encoded within the depths of the forest.

**Level:** Hard

**Solution:**

**Step-1:** You will get a login page.



**Step-2:** You have to put SQLi payload for auth bypass.

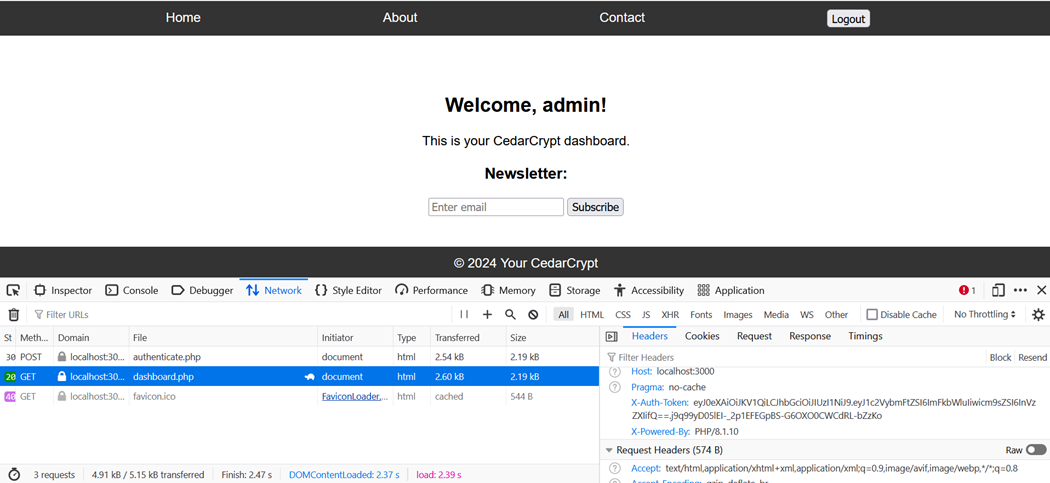
**Payload:** Username: admin

Password: "1"="1"--

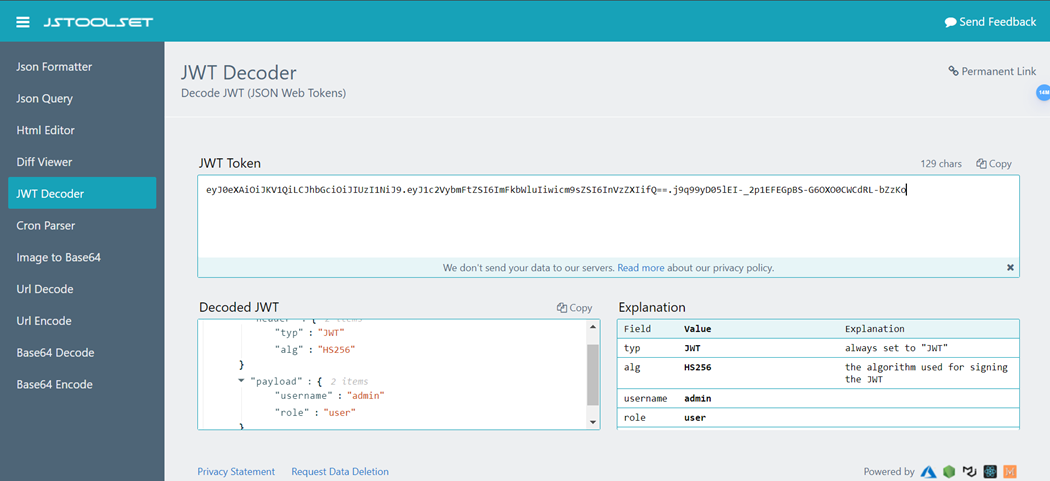
**Step-3:** You will redirect to dashboard , In response header you will see

x-auth-token: with jwt token .

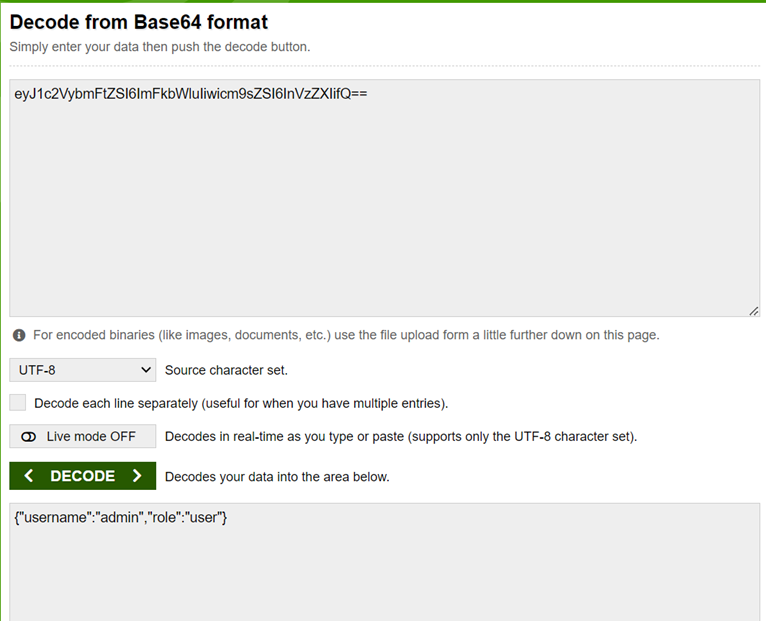
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZSI6InVzZXIifQ==.j9q9 9yD05lEI-\_2p1EFEGpBS-G6OXO0CWCdRL-bZzKo



**After decoded:** in <https://www.jstoolset.com/jwt>

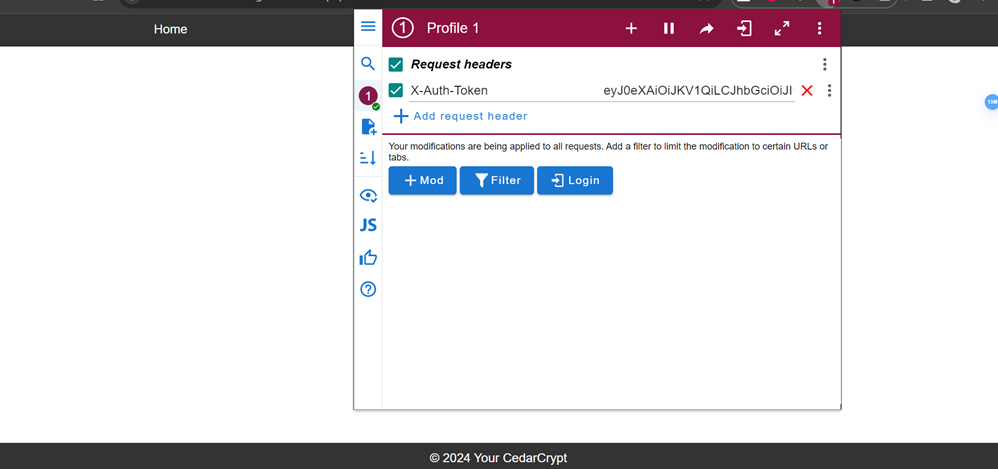


Use base64 Decoder for payload: in JWT header.payload.signature **Payload:** eyJ1c2VybmFtZSI6ImFkbWluIiwicm9sZSI6InVzZXIifQ== **Decoded:**



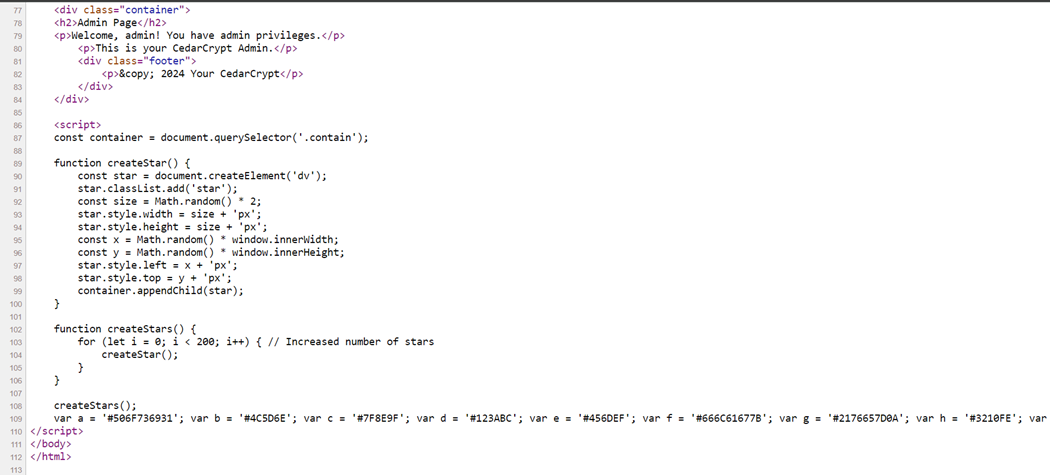
Change role user to admin and again encode and put back .

**Step-4:** For header modification I use mod header extension .



After that hit enter or simple refresh you will redirect to admin page.

**Step-5:** Do view page source and follow flag alphabet in JS . Every character have hex value simple arrange By flag .



f: 666C61677B l:247461795F

a:506F736931

g: 2176657D0A

flag❼ 66 6C 61 67 7B 24 74 61 79 5F 50 6F 73 69 31 21 76 65 7D 0A ❼ **flag{$tay\_Posi1!ve}**

This page is intentionally left blank