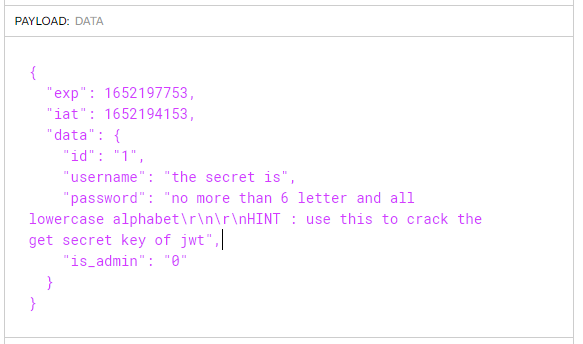
SOAL

Ini merupakan soal berupa API yang memiliki celah, apakah kamu bisa menemukan celah dan flagnya?

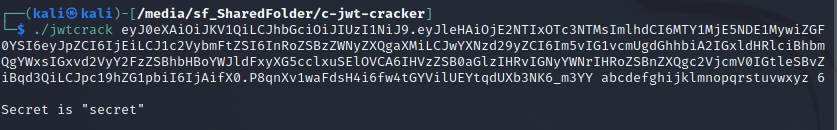
\*link\_website

WriteUp

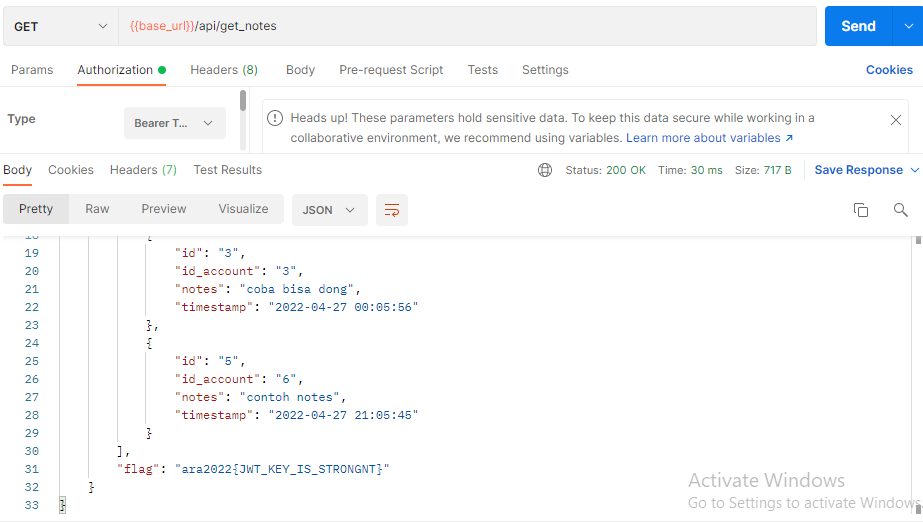
1. Kita bisa mencoba – coba API yang ada
2. Ternyata API login bisa di sqlinjection sederhana seperti ‘ OR 1=1 –
3. Lalu saat kita dapat tokennya, kita dapat mendecode nya pada <https://jwt.io/> dan hasilnya akan seperti ini



1. Dari situ kita tahu bahwa kita bisa mendapatkan secret key dari jwt yang didapat
2. Bisa menggunakan tools jwt crack dari tools yang ada di google



1. Setelah itu kita bisa mengubah “is\_admin” menjadi “1”
2. Dan kita akan menggunakan JWT admin untuk mencari flag tersebut yang tersimpan dalam endpoint
3. Dan didapatkan flagnya



Link tools jwtcrack = https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/JSON%20Web%20Token/README.md