**BTLO — Secrets|writeup**

# Scenario:

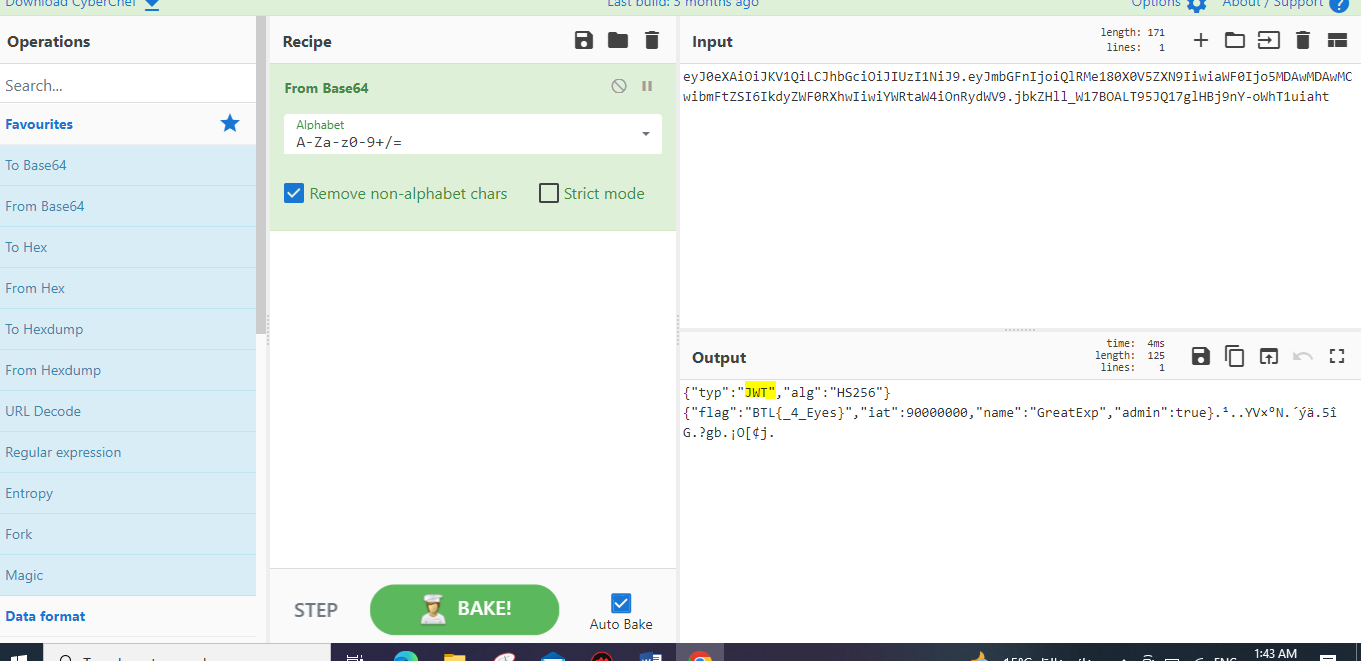
You’re a senior cyber security engineer and during your shift, we have intercepted/noticed a high privilege actions from unknown source that could be identified as malicious. We have got you the ticket that made these actions.

You are the one who created the secret for these tickets. Please fix this and submit the low privilege ticket so we can make sure that you deserve this position.

Here is the ticket:

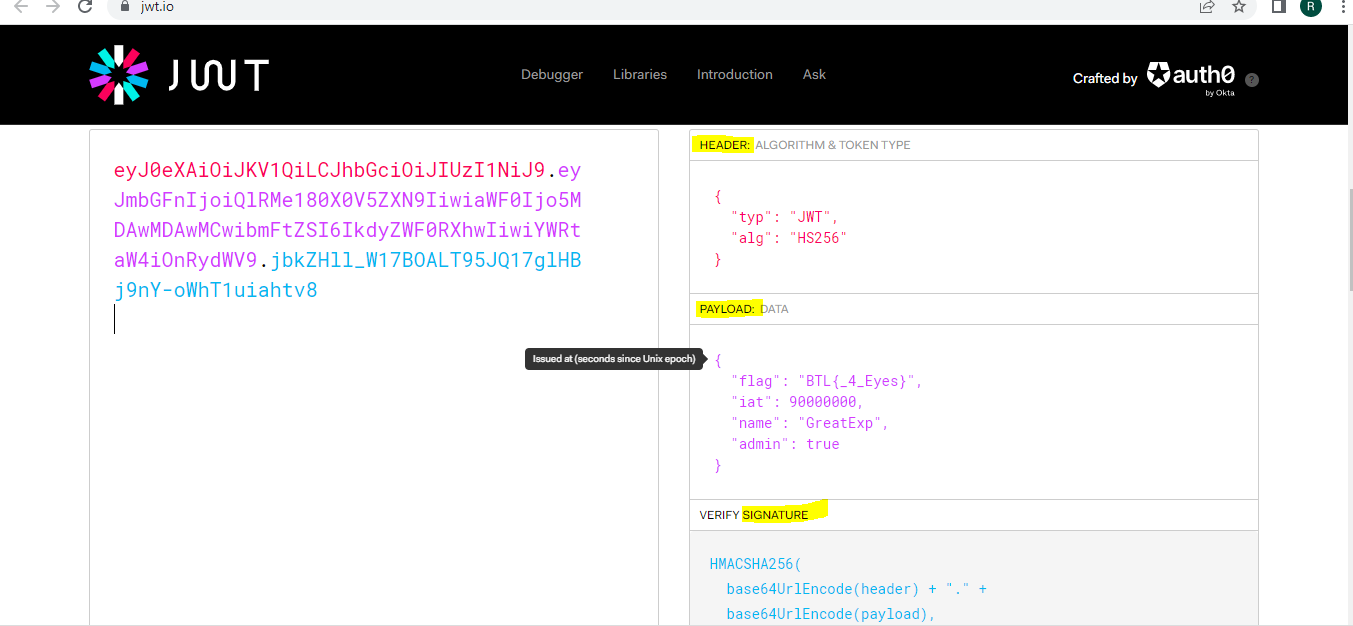
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJmbGFnIjoiQlRMe180X0V5ZXN9IiwiaWF0Ijo5MDAwMDAwMCwibmFtZSI6IkdyZWF0RXhwIiwiYWRtaW4iOnRydWV9.jbkZHll\_W17BOALT95JQ17glHBj9nY-oWhT1uiahtv8

1.Can you identify the name of the token?

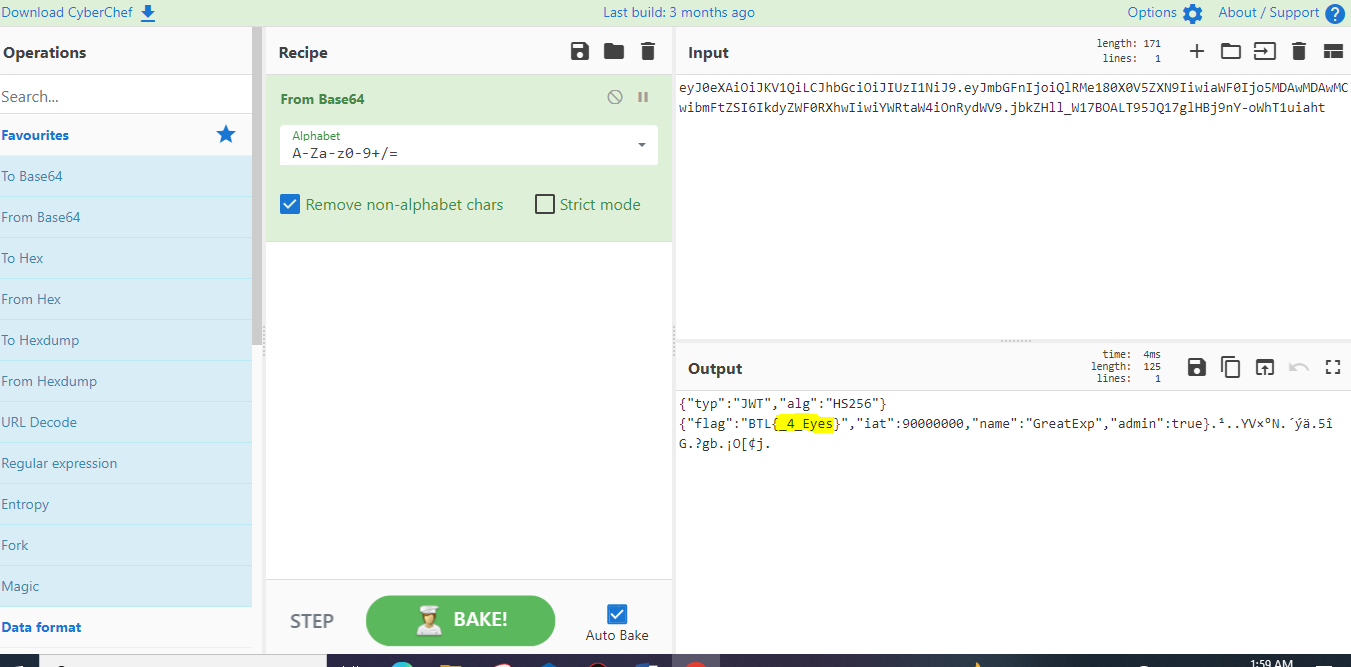
The given Ticket is encrypted in base64 you can decode the given token online on CyberChef since it’s JWT token key.

2. What is the structure of this token?

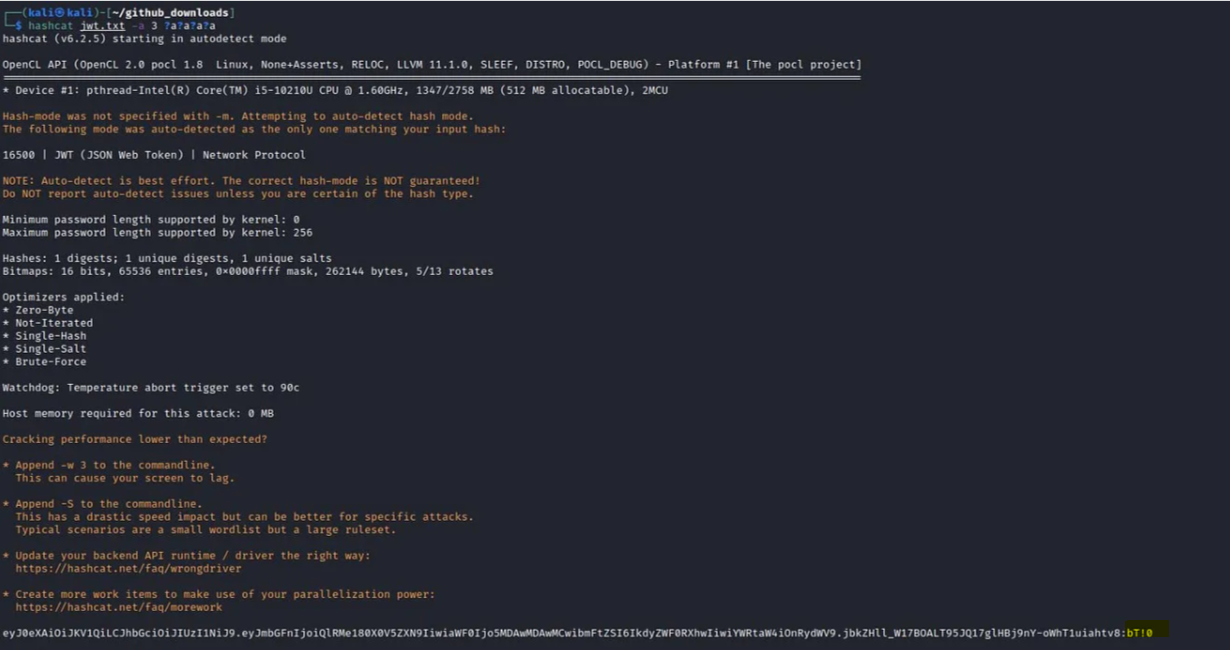
The given ticket generate a new verified signature ticket with a low privilege i generated it from <https://jwt.io/>



3. What is the hint you found from this token?



4. What is the Secret?

To get the Secret key you have to crack the provided token so to crack the JWT token I use Hashcat. At first save the given Token in a text file, I have save it as jwt.txt.

5. Can you generate a new verified signature ticket with a low privilege?

generate a new verified signature ticket with a low privilege i generated it from https://jwt.io/. You have to change admin value as false and add secret key.

