JWT Security Analysis Report

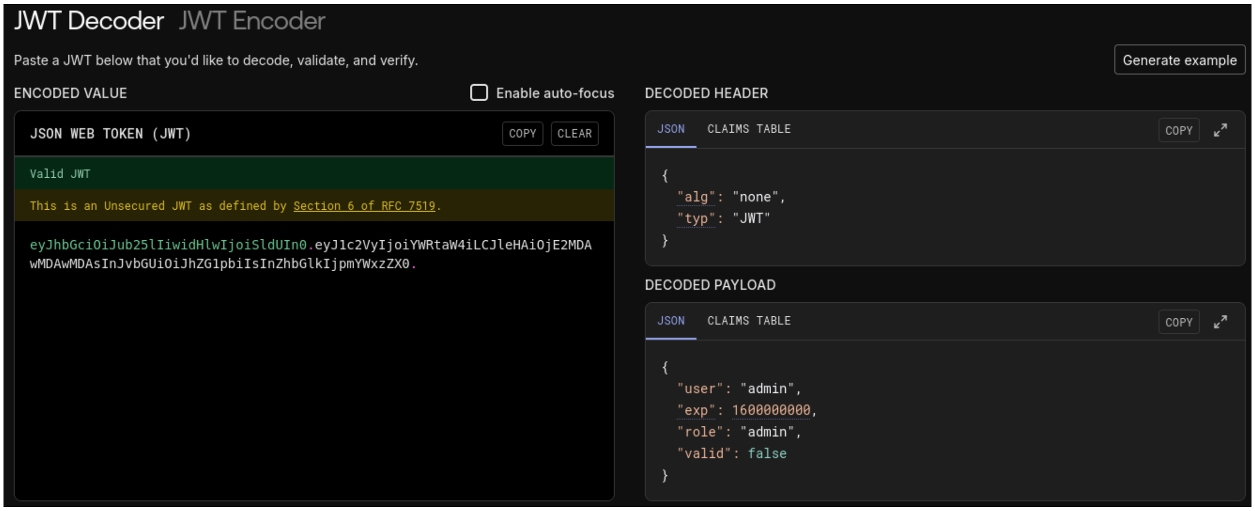
Prepared by: Falilat Owolabi
Date: Dec 1st, 2025
Analysis Window: November 30th 2025 - Dec 1st 2025
Testing Type: JWT analysis

1 Executive Summary.

This report documents the security analysis conducted on a json web token(JWT). The primary objective was to identify 5 security weaknesses in the JWT. Analysis is done using different tools to find security vulnerabilities in the token e.g. jwt.io xjwt.io burpsuite and OAUth.tool.
Some of the vulnerabilities discovered include:

- **No algorithm used for signature**
- **Token expiration time has elapse**
- **possible cross-service replay attack**
- **Missing Age Validation**

Sope:
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiYWRtaW4iLCJleHAiOjE2MDAwMDAwMDAsInJvbGUiOiJhZG1pbiIsInZhbGlkIjpmYWxzZX0.



Valid JWT

This is an Unsecured JWT as defined by Section 6 of RFC 7519.

```
eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiYWRtaW4iLCJleHAiOjE2MDA
wMDAwMDAsInJvbGUiOiJhZG1pbiIsInZhbGlkIjpmYWxzZX0.
```

```
{
  "alg": "none",
  "typ": "JWT"
}
```

```
{
  "user": "admin",
  "exp": 1600000000,
  "role": "admin",
  "valid": false
}
```

Output from jwt.io

Finding 1: No algorithm used for signature

Description: The token as shown in the result above indicates that no signature is effective in the JWT, this will cause the library used for signature verification to always return true, thus allowing signature claims being forged successfully within the token.

Business Impact: attacker can forge another valid signature claim that will be successful on the app and will use that against the system.

Fix: A token contains 3 parts, the header, The payload and the signature. In this target, the signature is not included and which is the key to holding a new claim from being forged by a malicious user who does not have the secret used in signing. So the token should include a signature to avoid a claim being forged.

Finding 2: Token expiration time has elapse

Description: This jwt as shown above expires in the timestamp 1600000000(Sun Sep 13 2020 13:26:40 GMT+1), as a result, this token should never be used on any app again to authenticate or authorise a user anymore.

Business impact: The token is not valid which if it was just issued will cause denial of service to users as most jwt libraries will reject it as an expired token.

Fix: Avoid token creation with expired timestamp and implement a valid expiration time which should not be valid for more than 10 minutes at most 15 minutes for best practices.

Finding 3: possible cross-service replay attack

Description: it is possible that an authentication server can serve multiple applications if the audience of the token is not verified by the application using it. If this claim is not verified, as the JWT itself is still regarded as valid through signature verification, it can have unintended consequences.

Business Impact: A token meant for application on a particular app can be used on another app if the audience claim is not verified by the app.

Fix: The audience claim should be verified when the token is decoded

Finding 4: Missing Age Validation

Description: the token has no iat(issued at) or nbf(not before) to indicate for how long the token has lived which makes it difficult to detect replay attacks on the token.

Business Impact: Possible replay attack can happen on the token

Fix: Add iat or nbf for new token validation

Finding 5: Missing issuer (iss) claim

Description: this token does not have an issuer in order to identify the token origin or lifecycle.

Business impact: the lack of an issuer claim means a token issued by one service could potentially be accepted as valid by another service that it was not intended for, leading to security vulnerabilities.

Fix: Add "iss" claim to identify token issuer (improves auditability)

Conclusion

The target token followed the standard of creating a token, while this might seem good, best practices should be followed to avoid unintended usage of the token, critical issues are discovered in which if exploited on the intended application will cause a very hazardous impact.

Challenges faced:

This is an analysis report and requires tools to decode the jwt given in scope. Some of the tools are able to identify the flaws in the token which made me understand what can make a token vulnerable and these tools helped also reduced the amount of research done to arrive at the report, overall I am able to understand better what a valid token should look like and what constitute an invalid token.

End of Report!