Ice task 2

Research

What is JWT?

Information can be securely transferred between parties as a small, URL-safe, digitally signed JSON object using the JWT (JSON Web Token) open standard (RFC 7519). (GeeksforGeeks, 2025)

- Usually, a JWT consists of three parts:
  header. payload.signature
- Web applications frequently use it for authorisation and authentication. (GeeksforGeeks, 2025)

What makes JWT crucial for safe online apps?

JWT assists with: (GeeksforGeeks, 2025)

- Authentication ← Verifies a user's identity without requiring credentials to be checked each time.
- Stateless Sessions: Tokens carry their own data, eliminating the requirement for server-side session storage.
- Based on assertions in the token, authorisation either permits or prohibits access to resources.
- Integrity & Security → If properly implemented, the signature guards against manipulation.

How do HTTP headers and JWT interact?

Typically, the Bearer scheme is used to pass JWTs in the Authorisation header:

Authorisation: <JWT> Bearer

An example of a flow:

- A signed JWT is issued by the server after the user logs in.
- JWT is stored by the client (in local storage or memory).
- The client includes the JWT in the HTTP header for every request.
- Access is granted or denied when the server confirms the signature and claims.

Real-World breach Example: (Stytch Team, 2024) Auth0 JWT Vulnerability (2015–2017)

- A serious JWT vulnerability that affected multiple libraries, including those used in Auth0, was discovered by researchers between 2015 and 2017.
- The problem: Attackers were able to change the JWT algorithm from RS256 (asymmetric) to HS256 (symmetric) by using certain libraries.
- By doing this, attackers might avoid authentication by using the public key as the HMAC secret and creating legitimate tokens.
- Proof-of-concept attacks took advantage of this vulnerability, demonstrating how inadequate JWT validation could allow attackers to pose as users or administrators.

Summary

In contemporary apps, JWTs are essential for safe authorisation and authentication. They operate through HTTP headers, but as demonstrated by the Auth0 JWT algorithm confusion issue, incorrect settings or inadequate validation can result in serious breaches.

References

GeeksforGeeks, 2025. *JSON Web Token (JWT)*. [Online]
Available at: https://www.geeksforgeeks.org/web-tech/json-web-token-jwt/
[Accessed 22 Sept 2025].

Stytch Team, 2024. *Auth0's Security Incidents: How JWT Vulnerabilities Have Repeatedly Impacted the Platform*. [Online]
Available at: https://stytch.com/blog/auth0-security-incidents/
[Accessed 22 Sept 2025].