Week 16 Research

By: Patrick Corcoran

Hashing and salting data is a crucial security measure to prevent hacking and system intrusion. Hashing involves converting sensitive information, like passwords, into irreversible ciphertext using hash algorithms. This ensures that even if data is accessed, the original content cannot be easily deciphered. Salting adds an extra layer of defense by introducing random data before or after the sensitive information before hashing. This randomness disrupts pre-calculated tables used by hackers, making it significantly more challenging to deduce the original data. Together, hashing and salting enhance the security of sensitive data, safeguarding against unauthorized access and potential system breaches.

A JWT is comprised of three parts: a header, payload, and signature. The header specifies the token type and the algorithm used. It is encoded using Base64Url to form the initial part of the JWT. The payload contains claims, including registered ones like issuer, expiration time, subject, and audience. While not mandatory, these claims are recommended for interoperability. Custom claims, like an employee's role, can also be included. The payload is encoded using Base64Url to form the second part of the JWT. The signature is created by signing the encoded header and payload using the algorithm specified in the header. This signature verifies the issuer's identity and ensures the message hasn't been altered during transmission.

<https://www.pingidentity.com/en/resources/blog/post/encryption-vs-hashing-vs-salting.html#:~:text=Hashing%20is%20a%20one%2Dway%20process%20that%20converts%20a%20password,to%20obfuscate%20the%20actual%20password>.

<https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-json-web-token-jwt>