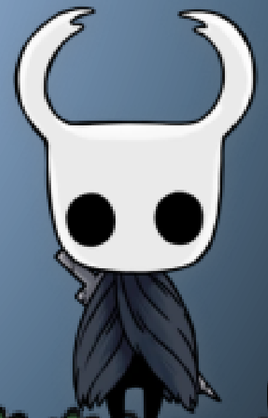
HOLLOW DEV BOOTCAMP

AUTHENTICATION SYSTEM



MICRO CLUB

SESSION CONTENT

- Auth
- JWT
- Hashing encryption
- bcrypt

WHAT IS AUTHENTICATION

Authentication is the process of verifying the identity of a user or system. It ensures that the entity trying to access a service or resource is who it claims to be. This is typically done by checking credentials like passwords, security tokens, or biometric data (e.g., fingerprints).

- Username/email and Password : Users provide a unique username and a secret password that are checked against stored credentials.
- Multi-Factor Authentication (MFA) : Requires multiple forms of verification, such as a password and a code sent to a mobile device.
- OAuth : Uses tokens to grant users access without sharing passwords, often seen in integrations with third-party services like Google or Facebook

MICRO CLUB

WHAT IS JWT

JWT, or JSON Web Token, is a compact, URL-safe token used for securely transmitting information between parties as a JSON object. It is widely used in web applications for authentication and data exchange. A JWT consists of three components:

1. **Header** : Specifies the token type (JWT) and the signing algorithm used, such as HMAC SHA256.
2. **Payload** : Contains the claims, which are statements about an entity (typically the user) and additional data, like user ID or expiration time.
3. **Signature** : Created by encoding the header and payload using the specified algorithm and a secret key, ensuring the token's integrity and authenticity.

MICRO CLUB

JWT EXAMPLE

eyJhbGciOiJIUzM4NCIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoiQWJkZXJyYWhtYW5lIiwiQWdlIjoxOX0.XVHOUQ4e0g1il9iBUILDPOnBiPxkET3P4HsnpkfnS5lkHDJhPTiRTJ1Kv4MwuwXP

Header

Payload

SIGNATURE

MICRO CLUB

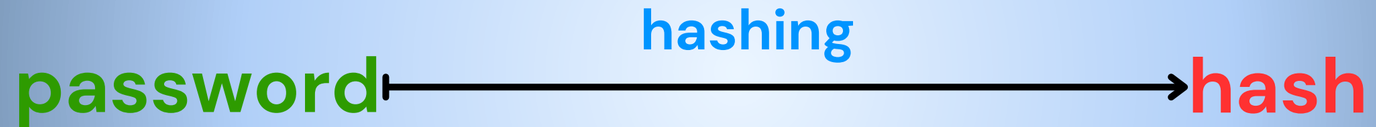
WHAT IS HASHING

Hashing is the process of converting data, such as a password or message, into a fixed-size string of characters, which typically appears as a sequence of numbers and letters. The output, called a hash, is unique to the original data, making it a one-way function that cannot be easily reversed. Hashing is commonly used for securely storing passwords, ensuring data integrity, and creating digital signatures. By applying a hash function to data, you can verify the data's authenticity without revealing the original content. Popular hash algorithms include SHA-256, MD5, and bcrypt.

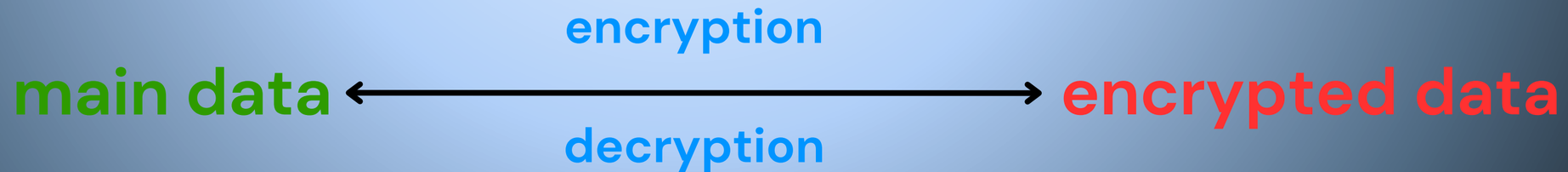
MICRO CLUB

HASHING VS ENCRYPTION

- Hashing converts data into a fixed-size string (hash) that cannot be easily reversed, commonly used for data integrity and secure password storage with algorithms like SHA-256, MD5, and bcrypt.



- Encryption transforms data into a different format that can be reversed with a key, ensuring data confidentiality and that only authorized parties can read the information, using algorithms such as AES, RSA, and DES



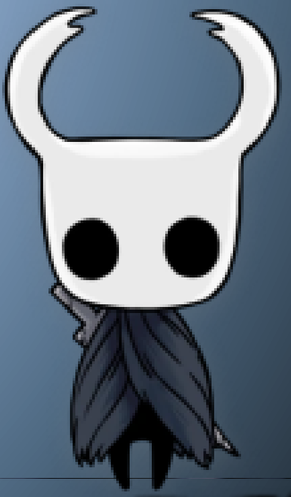
MICRO CLUB

WHAT IS BCRYPT

Bcrypt is a security tool used to safely store passwords. It takes a password and turns it into a scrambled string, making it very hard for someone to figure out the original password. Bcrypt adds extra protection by mixing in a random "salt" with each password, making it even harder for attackers to guess passwords using common techniques. It's a popular choice for websites and applications to keep user passwords safe from theft or hacking attempts.

MICRO CLUB

THANK YOU !



MICRO CLUB