ONE PAGE SUMMARY

IT & Software › Full Stack Development › Authentication Systems

Introduction to Authentication Systems

Mastering Authentication Systems for Secure Applications

DEFINITION

> Authentication systems verify user identities before granting access to applications. They ensure security by confirming that users are who they claim to be.

KEY CONCEPTS

Authentication vs. Authorization

Authentication verifies identity, while authorization determines access levels for authenticated users.

Multi-Factor Authentication (MFA)

MFA enhances security by requiring two or more verification methods from different categories.

Tokens

Tokens are digital keys issued after successful authentication, allowing users to access resources without re-entering credentials.

Session Management

Session management tracks user activity and maintains their authenticated state during interactions with the application.

Password Hashing

Password hashing transforms passwords into a secure format, making it difficult for attackers to retrieve the original password.

EXAMPLES

→ Logging in with a username and password.

→ Using a mobile app to receive a one-time code for MFA.

→ Accessing a secure area of a website after successful login.

MEMORY TIPS

★ Remember 'A' for Authentication and 'A' for Access - they go hand in hand.

★ Think of MFA as 'More Factors, Always' for enhanced security.

★ Use the acronym 'TIPS' for Tokens, Identity, Passwords, and Sessions.

COMMON MISTAKES

✗ Confusing authentication with authorization.

✗ Neglecting to implement MFA for sensitive applications.

✗ Using weak passwords or failing to hash them properly.

QUICK RECAP

Authentication systems are crucial for verifying user identities and securing applications. Key concepts include MFA, tokens, and session management. Remember to differentiate between authentication and authorization for better security practices.