**Security and Authentication**

* Authentication, or AuthN, verifies users' identities before granting them access to a system or application.
* Authorization, also known as AuthZ, controls what a user can do once they're authenticated. In other words, it controls their access based on their role or permissions.
* User Manager is a component in ASP.NET Identity that is responsible for working with user accounts in your application.
* Sign-in Manager is a component in ASP.NET Identity that takes on the responsibility of managing user authentication, processing sign-ins and sign-outs, and ensuring that only users with valid credentials can log in.
* IdentityDB Context manages the secure storage of information related to users, roles, and claims.
* A session is a temporary state that securely maintains users' logged in status during their visit to a website.
* Sometimes, users want to stay logged in even after closing their browser. This is where cookies come into play, typically via a Remember Me option. A cookie is a small piece of data in a website saved in your browser to remember configurations between sessions. When enabled, cookies save login information on your device, letting you stay logged in across multiple visits. Unlike sessions, cookies persist on your device, so you don't have to log in each time you return to the site.
* Role-based access control, or RBAC, is a control mechanism that restricts system access to authorized users based on their roles within an organization.
* RoleManager gives you the admin access to manage products, update prices, and all customer orders.
* When an admin logs in, the system uses IdentityDB Context to check the database for their assigned role.
* Claims are name-value pairs that represent an attribute or characteristic of a user or entity.
* Claims-based authorization is a security model where access to resources or applications is determined by evaluating the claims associated with a user's identity.
* Authorization policies are rules that help us decide who can access certain areas of a system.
* Token-based authentication is a security method in which a user receives a token after logging in to authorize additional transactions.
* JSON Web Tokens, or JWTs, are a specific type of token that securely stores user information in a compact format called a JSON object.
* Stateless authentication is a way of verifying users without requiring the server to maintain any session data.
* This stateless approach keeps the system both efficient and secure.
* Typically, tokens are stored in the client's browser, either in a cookie for security or local storage.
* External Authentication Providers are third-party services or systems that manage the authentication process for an application, verifying a user's identity and using secure protocols.
* OAuth 2.0 is an authorization protocol that allows applications to grant limited access to users through External Providers.
* OpenID Connect, or OIDC, is an identity layer built on top of OAuth 2.0 protocol and is designed to authenticate a user's identity and provide information, or claims, about the user to the application.
* RBAC is a security model for restricting access to systems, data, or resources based on the roles of individual users within an organization. When using RBAC, instead of assigning individual permissions to each user, you assign users to roles, such as admin or employees, or users, each with predetermined permissions. This approach simplifies access management, especially when handling many users.
* The signature is created by encoding the header and payload and combining them with a secret key.
* Token expiration is the amount of time a token remains valid.
* They add security and convenience by issuing new JWTs without constant re-authentication.
* HTTP-only cookies are a special type of browser cookie that cannot be accessed by client-side scripts such as JavaScript, enhancing security by limiting access to the server only and keeping sensitive data safe from potentially harmful scripts.
* o protect JWTs, secure signing algorithms are used to make tokens tamper-proof, ensuring they can only be modified by the original issuer.
* Environment variables are system-level settings that store configuration data for applications.
* Integrity is the principle of ensuring that data remains accurate, consistent, and unaltered throughout its lifecycle.
* Availability is the principle of ensuring that systems, data, and resources are accessible to authorized users whenever they need.
* A Distributed Denial of Service (DDOS) attack is a cyber attack where multiple systems coordinate to flood a target with excessive requests, overwhelming its capacity to respond to legitimate users.
* Encryption is the process of converting readable text, known as plain text, into unreadable text, called ciphertext, to protect sensitive data.
* Symmetric encryption is a method of encryption where the same key is used for both encrypting and decrypting the data.
* Asymmetric encryption is a method of encryption that uses two keys, one for encryption and another for decryption.
* Advanced Encryption Standard (AES) is a fast, secure, and widely used symmetric encryption algorithm.
* Rivest-Shamir-Adleman (RSA) is a popular asymmetric encryption algorithm for securing data shared online, such as login credentials and other sensitive information.
* Data masking is the process of altering specific data elements, often by replacing sensitive information with fictional data.
* Static data masking involves creating a masked copy of data, typically for development and testing.
* Dynamic data masking hides information in real-time without altering the original data, displaying different versions based on user access.
* Data obfuscation is the deliberate process of making data difficult to interpret, ensuring its protection against unauthorized access.
* Tokenization is a data obfuscation method that replaces sensitive data with unique symbols or tokens, which hold no meaningful value outside of a secure system.
* Data scrambling is a data obfuscation technique that involves modifying data so that its original value is no longer recognizable, but its format and structure are preserved.
* Code obfuscation is a data obfuscation technique that makes software code to make it difficult to understand while preserving its original functionality.
* In contrast, data obfuscation transforms data into an unreadable format, ensuring its protection in non-secure environments or during storage in development systems.
* Data at rest refers to data stored in a physical or digital medium that is not actively moving through networks or being processed.
* Access controls are mechanisms that define who can access or modify stored information, granting permissions based on a user-specific role and responsibilities.
* Data redundancy involves creating backup copies of data to ensure its availability, in case of a failure in a storage location.
* Transport layer security, or TLS, ensures data is encrypted as it travels over the internet. TLS enables a secure encrypted connection between a customer's device and the company's server by encrypting the data in transit.
* A virtual private network, or VPN, creates a secure, encrypted connection between a user's device and a network, ensuring data remains private and protected over public networks.
* A firewall monitors and controls the data going in and out of your network, deciding what's allowed and what's blocked based on predefined security rules.
* Intrusion Detection System (IDS) detects and alerts IT teams to unusual or suspicious behavior that may indicate a potential threat, allowing them to respond quickly.
* Cross-site scripting, or XSS attacks, are a type of security vulnerability where attackers inject malicious scripts into your web pages that are subsequently loaded and executed in other users' browsers.