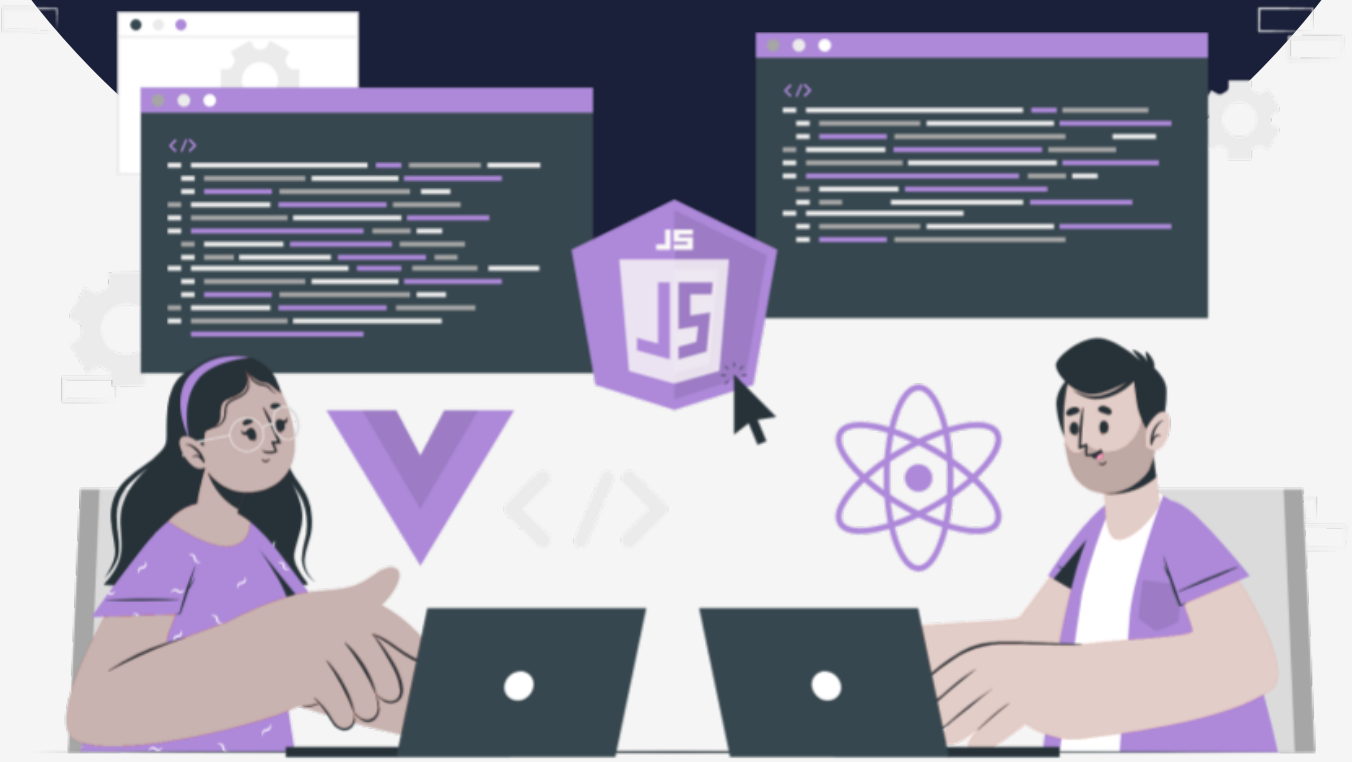
Lesson:

Authentication and Authorization



PW SKILLS

Topics

- What is Authentication?
- Common Types of Authentication.
- What is Authorization?
- Which Comes First, Authentication or Authorization?
- Real-world example.

What is Authentication?

Authentication is a process that verifies that someone or something is who they say they are. Technology systems typically use some form of authentication to secure access to an application or its data. For example, when you need to access an online site or service, you usually have to enter your username and password. Then, behind the scenes, it compares the username and password you entered with a record it has on its database. If the information you submitted matches, the system assumes you are a valid user and grants you access.

Common Types of Authentication

Systems can use several mechanisms to authenticate a user. Typically, to verify your identity, authentication processes use: - **something you know - something you have** - or **something you are.**

Something you know: Passwords and security questions are two authentication factors that fall under this category. As only you would know your **password** or the **answer** to a particular set of security questions, systems use this assumption to grant you access.

something you have: Physical devices such as **smart cards, USB security tokens,** and **mobile phones** fall under this category. For example, when you access a system, and it sends you a One Time Pin (OTP) via SMS or an app, it can verify your identity because it is your device.

something you are: Biometric authentication mechanisms fall under this category. Since individual physical characteristics such as fingerprints are unique, verifying individuals by using these factors is a secure authentication mechanism.

What is Authorization?

Authorization is the process of determining whether a user or system is allowed to access a particular resource or perform a particular action. In other words, authorization is the process of granting or denying access to protected resources based on the permissions and privileges of the user or system.
For example, in a web application that allows users to create and edit content, the authorization system might

require that a user be logged in and have the necessary permissions before allowing them to create or edit content. The authorization system might also implement role-based access control (RBAC), which allows administrators to grant or deny permissions based on the user's role or level of access.

Which Comes First, Authentication or Authorization?

Authentication and authorization both rely on identity. As you cannot authorize a user or service before identifying them, authentication always comes before authorization.

For example, imagine a user attempting to access a protected resource on a website without being authenticated. If authorization is performed first, the user may be granted access to the resource even though they have not been verified as a legitimate user. This could potentially allow an attacker to gain unauthorized access to sensitive information.

On the other hand, if authentication is performed first, the user's identity can be verified before any authorization decisions are made. This ensures that only authorized users are granted access to protected resources, reducing the risk of unauthorized access and data breaches.

Real-world example

Authentication is the process of verifying the identity of a user, while authorization is the process of granting or denying access to resources based on the authenticated identity and permissions.

For example, when you login to your email account, you are required to provide your username and password to authenticate yourself. Once you are authenticated, the email server will check your permissions to determine what resources you can access. You might be authorized to read and send emails, but not to delete them or change settings.

Another example is a bank website, where you have to authenticate yourself with a username and password to access your account information. Once authenticated, the website will check your authorization to see what transactions you are authorized to perform, such as viewing account balances, transferring money, or paying bills.

In both cases, authentication ensures that only the authorized user can access the account, while authorization determines what actions the user is allowed to perform.