Authentication and Authorization in PHP

WHAT IS AUTHORIZATION?

Matthew Setter
PHP SECURITY ENGINEER

@settermjd matthewsetter.com

Module Overview

- Learn about authorization
- What it is
- How it compliments authentication
- Three authorization types

What is Authorization?

“Authorization is the function of specifying access rights/privileges to resources. More formally, to authorize is to define an access policy.”

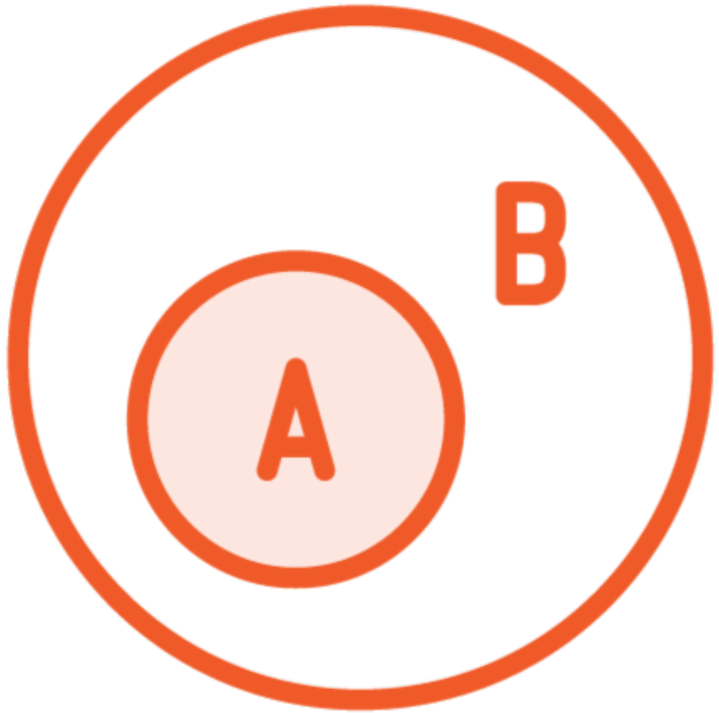
Authorization - Wikipedia

What is Authorization?

- A compliment to authentication
- Determines what the user can and cannot do

Authorization Types

Authorization Types



1. Access Control Lists
2. Role-based Access Control
3. JSON Web Tokens

Access Control Lists

“Access Control Lists refers to the **permissions attached to an object** that specify **which users are granted access to that object and the operations it is allowed to perform**. Each entry in an access control list specifies the subject and an associated operation that it is permitted to perform”

Access Control Lists - Techopedia

Access Control Lists (ACLs)

Advantages

- Excellent for smaller requirements
- Small organizations
- File-based access control
- Network access

Access Control Lists (ACLs)

Disadvantages

- Does not scale well
- Managing permissions becomes cumbersome
- Difficult to audit and update access

Role-based Access Control

“Role-based access control (RBAC) systems assign access and actions **according to a person's role within the system**. Everyone who holds that role has the same set of rights. Those who hold different roles have different rights.”

Role-based Access Control - Okta

Role-based Access Control

Advantages

- Suits large organizations
- Uses roles, not resources
- Roles and responsibilities determine access

Role-based Access Control

Who

What

When

Where

What Order

What Circumstances

JSON Web Tokens

“They are a **compact** and **self-contained** way for **securely transmitting information** between parties using JSON objects.”

What is a JSON Web Token - JWT.io

“This information can be **verified** and **trusted** because it is **digitally signed** (and can be **encrypted**). JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.”

What is a JSON Web Token - JWT.io

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvbG9jYWxkb21haW4uZGV2IiwiYXVkIjoiaHR0cHM6XC9cL2xvY2FsZG9tYWluLmRldiIsImlhdCI6MTYwMTU4MDcwOSwibmJmIjoxNjAxNTgwNzY5LCJzdWIiOiJhZG1pbiJ9.qvVcdbKmmXJxEqz4xbrAcOT2KbAtBi3GQbfexL713eM

JSON Web Tokens

Composed of three parts:

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvbG9jYWxkb21haW4uZGV2IiwiYXVkIjoiaHR0cHM6XC9cL2xvY2FsZG9tYWluLmRldiIsImlhdCI6MTYwMTU4MDcwOSwibmJmIjoxNjAxNTgwNzY5LCJzdWIiOiJhZG1pbiJ9.qvVcdbKmmXJxEqz4xbrAcOT2KbAtBi3GQbfexL713eM

JSON Web Tokens

Composed of three parts:

1. **A header**

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvbG9jYWxkb21haW4uZGV2IiwiYXVkIjoiaHR0cHM6XC9cL2xvY2FsZG9tYWluLmRldiIsImlhdCI6MTYwMTU4MDcwOSwibmJmIjoxNjAxNTgwNzY5LCJzdWIiOiJhZG1pbiJ9.qvVcdbKmmXJxEqz4xbrAcOT2KbAtBi3GQbfexL713eM

JSON Web Tokens

Composed of three parts:

1. A header
2. A payload

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJodHRwczpcL1wvbG9jYWxkb21haW4uZGV2IiwiYXVkIjoiaHR0cHM6XC9cL2xvY2FsZG9tYWluLmRldiIsImlhdCI6MTYwMTU4MDcwOSwibmJmIjoxNjAxNTgwNzY5LCJzdWIiOiJhZG1pbiJ9.qvVcdbKmmXJxEqz4xbrAcOT2KbAtBi3GQbfexL713eM

JSON Web Tokens

Composed of three parts:

1. A header
2. A payload
3. A signature

Module Recap

- Learned about authorization
- What authorization is
- How it compliments authentication
- Three authorization types

Coming Up Next

- Access Control Lists
- How they work
- Advantages and disadvantages
- Implement them in PHP