Authentication and Authorization in PHP

ACCESS CONTROL LISTS

Matthew Setter
PHP SECURITY ENGINEER
@settermjd matthewsetter.com

Module Overview

- Learn about Access Control Lists
- What they are
- How they work
- Their advantages and disadvantages
- How to implement them in PHP

What Are 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 is permitted to perform.”

Access Control Lists - Techopedia

> “Is a means of restricting access to information based on the identity of users and/or membership in certain groups. Access decisions are typically based on the authorizations granted to a user based on the credentials they presented at the time of authentication. In most typical DAC models, the owner of the information or any resource can change its permissions at their discretion.”

Discretionary Access Control - OWASP

Access Control List Key Advantages

- Quickly audit user permissions
- Know what users should not be able to do
- Used for years in computer security
- Used in the major operating systems
- Used in network security

Core Concepts

Roles

Resources

Rights

Core Concepts

Roles

Resources

Rights

Core Concepts

Roles

Resources

Rights

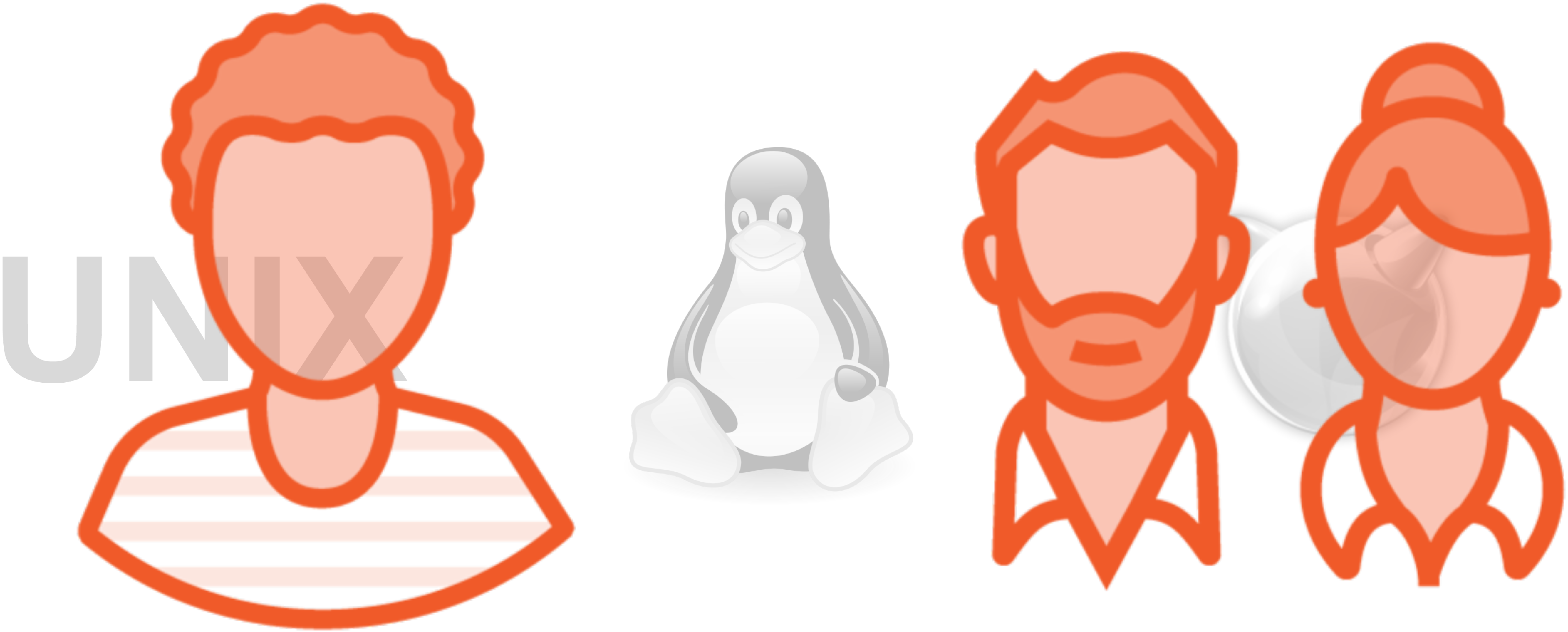
Core Concepts

Roles

Resources

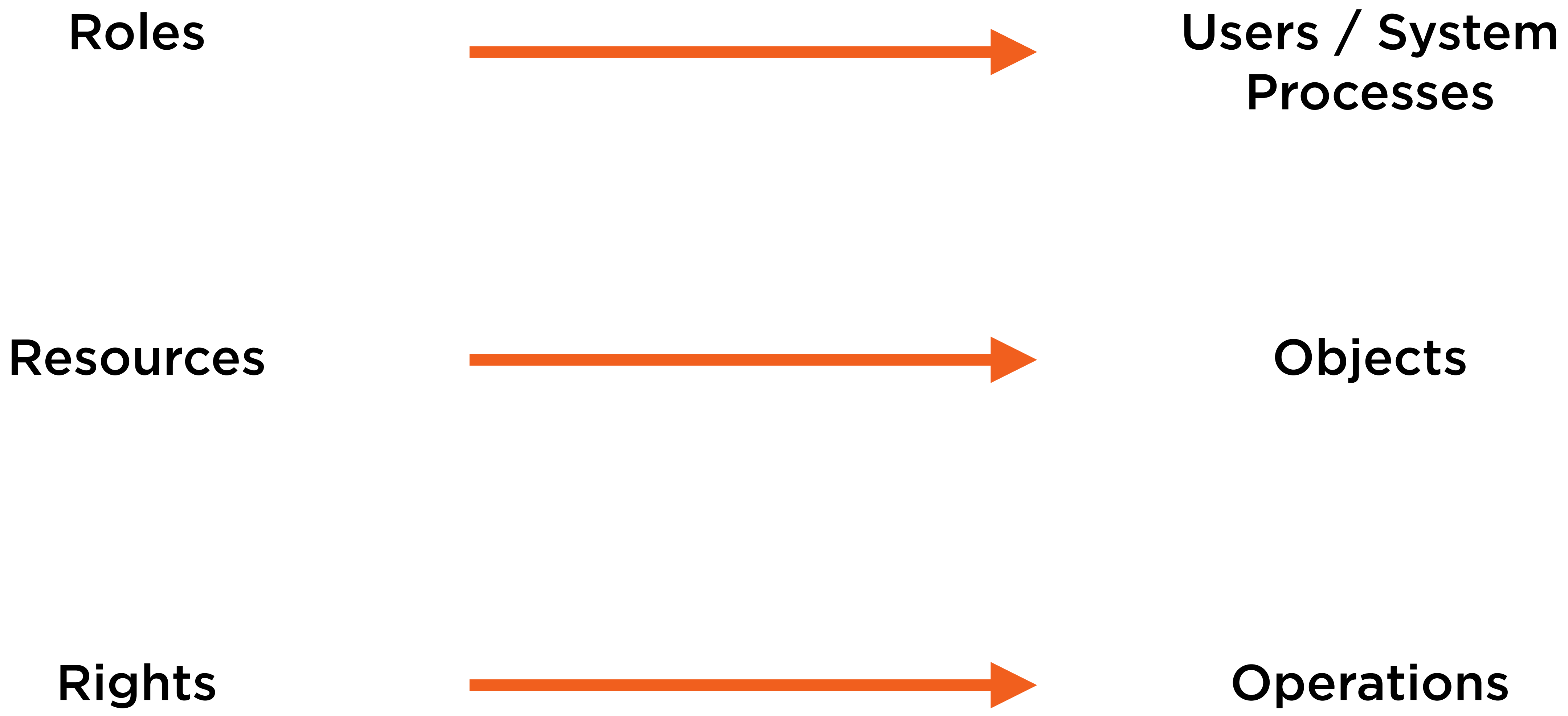
Rights

UNIX



Owner

Group



Roles → Users / System Processes

Resources → Objects

Rights → Operations

Quick ACL Demonstration

User	Object	Permission

Quick ACL Demonstration

User	Object	Permission
Paul	User	Login, Logout, Manage Own Account

Quick ACL Demonstration

User	Object	Permission
Paul	User	Login, Logout, Manage Account
Mary	User	Login, Logout, Manage Own Account, Suspend User, Change Password

Quick ACL Demonstration

User	Object	Permission
Paul	User	Login, Logout, Manage Account
Mary	User	Login, Logout, Manage Account, Suspend User, Change Password
Terri	User	Login, Logout, Manage Account, Suspend User, Change Password, Add User, Edit User, Delete User

Quick ACL Demonstration

User	Object	Permission
Paul	User	Login, Logout, Manage Account
Mary	User	Login, Logout, Manage Account, Suspend User, Change Password
Terri	User	Login, Logout, Manage Account, Suspend User, Change Password, Add User, Edit User, Delete User
Peter	User	All Permissions

Advantages and Disadvantages

Advantages

- They are conceptually simple
- Relatively simple to create and manage
- Quite granular in nature
- Don’t require a lot of computing overhead

Disadvantages

- Suitable for smaller organizations
- The larger they are the more difficult they are to manage

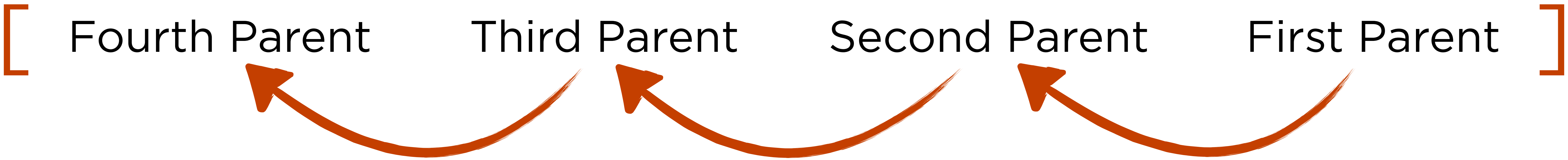
Quick Recap

- Access Control List essentials
- ACLs are a form of Discretionary Access Control
- Advantages and disadvantages
- Saw a conceptual Access Control List

Up Next:
Implementing Access Control Lists in PHP

Implementing Access Control Lists in PHP

The Parent Roles List is a LIFO Stack



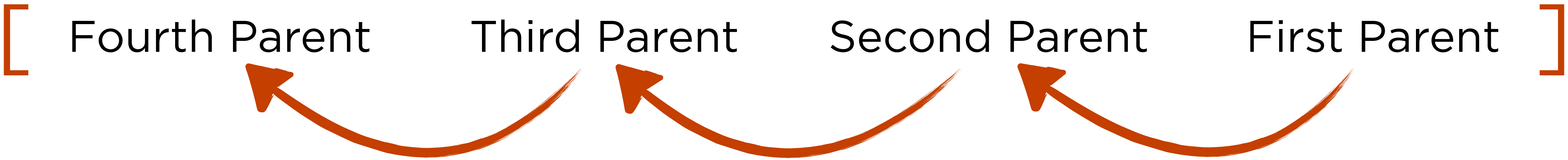
Fourth Parent

Third Parent

Second Parent

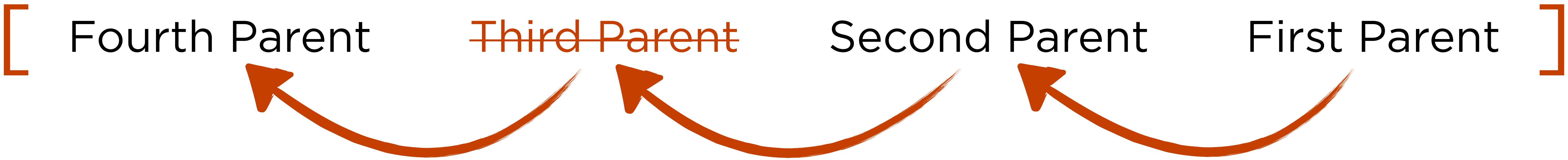
First Parent

The Parent Roles List is a LIFO Stack



[Fourth Parent Third Parent Second Parent First Parent]

The Parent Roles List is a LIFO Stack



[Fourth Parent ~~Third Parent~~ Second Parent First Parent]

Dynamic Assertions

Ownership Assertions
Ensure that a resource is owned by a given role

Expression Assertions
Check if a property on a role equates to a property on a resource

Callback Assertions
Use custom logic to determine if a permission should be granted

Module Recap

Module Recap

- Learned about Access Control Lists
- What they are
- How they work
- Advantages and disadvantages
- How to implement them in PHP

Up Next:
Role-based Access Control