**Secure File Upload System Documentation**

Table of Contents

1. Introduction
2. System Requirements
3. Installation and Configuration
4. User Authentication
5. File Upload Functionality
6. Security Measures
7. Testing
8. Conclusion

1. Introduction

Purpose

The purpose of this document is to provide a comprehensive guide on how to use and test the secure file upload system developed in PHP.

Scope

This documentation covers the installation, configuration, usage, and testing of the secure file upload system.

2. System Requirements

Server Requirements

List the server requirements necessary to run the secure file upload system. Include information about the PHP version, database requirements, and any other dependencies.

File Upload Directory

Explain the importance of specifying a secure directory for file uploads outside the web server's root directory.

3. Installation and Configuration

Database Setup

Provide instructions for setting up the database tables (user, uploads, and logs). Include SQL scripts if applicable.

File Upload Directory Configuration

Explain how to configure the file upload directory in the system. Ensure that it's secure and inaccessible via the web.

Security Headers

Describe the configuration of security headers to mitigate potential security risks such as XSS and content sniffing attacks.

4. User Authentication

User Authentication System

Explain how to implement or integrate a user authentication system to restrict file uploads to authorized users only.

User Registration

If applicable, provide information on user registration, including account creation and password encryption.

5. File Upload Functionality

Uploading Files

Demonstrate how users can upload files to the system. Include information on the allowed file types, maximum file size, and any other relevant upload requirements.

Sanitizing File Names

Explain the mechanism used to sanitize uploaded file names, removing potentially harmful characters and ensuring unique names.

6. Security Measures

File Type Validation

Describe how the system verifies file types and accepts only valid file extensions.

File Size Limit

Explain how the system enforces a maximum file size limit for uploads.

Logging

Detail the system's logging capabilities, including what is logged (e.g., IP address, file name, timestamp) and how to access the logs.

7. Testing

Test Scenarios

Provide a list of test scenarios to evaluate the secure file upload system. Include scenarios for both successful file uploads and rejected upload attempts.

Test Steps

Outline the steps for performing each test scenario. Specify the expected outcomes and what to look for during testing.

8. Conclusion

Summary

Summarize the key points covered in this documentation, including the system's purpose, requirements, usage, and security features.

By following this documentation outline and providing detailed explanations and instructions for each section, users will have a clear understanding of how to use and test the secure file upload system. Additionally, they will be informed about the security measures in place to protect against potential threats and attacks.