Web Application Fundamentals

Welcome to our Web Application Fundamentals program, a comprehensive journey into the core technologies behind web development with a strong emphasis on cybersecurity. This course covers essential protocols, client-side and server-side technologies, and database management, all while prioritizing best practices in secure coding. Prepare to dive deep into HTTP/HTTPS, HTML, CSS, JavaScript, PHP, and MySQL, as we build a solid foundation for developing secure and reliable web applications.

Program Code: XE107

Package: XE Basics

Course Information

Prerequisites

- Networking Knowledge
- Linux and Windows Operating System

Duration Options

- Self-paced: 2-4 weeks
- Trainer-led: 40 hours

Core Features of Cyberium

Labs
Enhance training with defense and attack tasks.

Books
Tailored coursebooks for cybersecurity studies.

Scenarios
Diverse situations mimicking real professional challenges.

Projects
Integrated projects to demonstrate acquired knowledge.

HTTP and HTTPS Basics

HTTP Fundamentals

Explore request/response headers, methods, and status codes

HTTPS Security

Learn secure headers and TLS/SSL principles

Practical Tools

Master cURL, Inspect Tool, and Wireshark for analysis

Understanding HTTP and HTTPS is crucial for web developers. These protocols manage data exchange, forming the backbone of web communication. We'll delve into interpreting headers, methods, and status codes, while exploring secure communication principles.

HTML, CSS, and Client-Side Security

HTML Basics

Learn document structure, elements, and attributes.

Practice viewing source code for vulnerability assessment.

CSS Styling

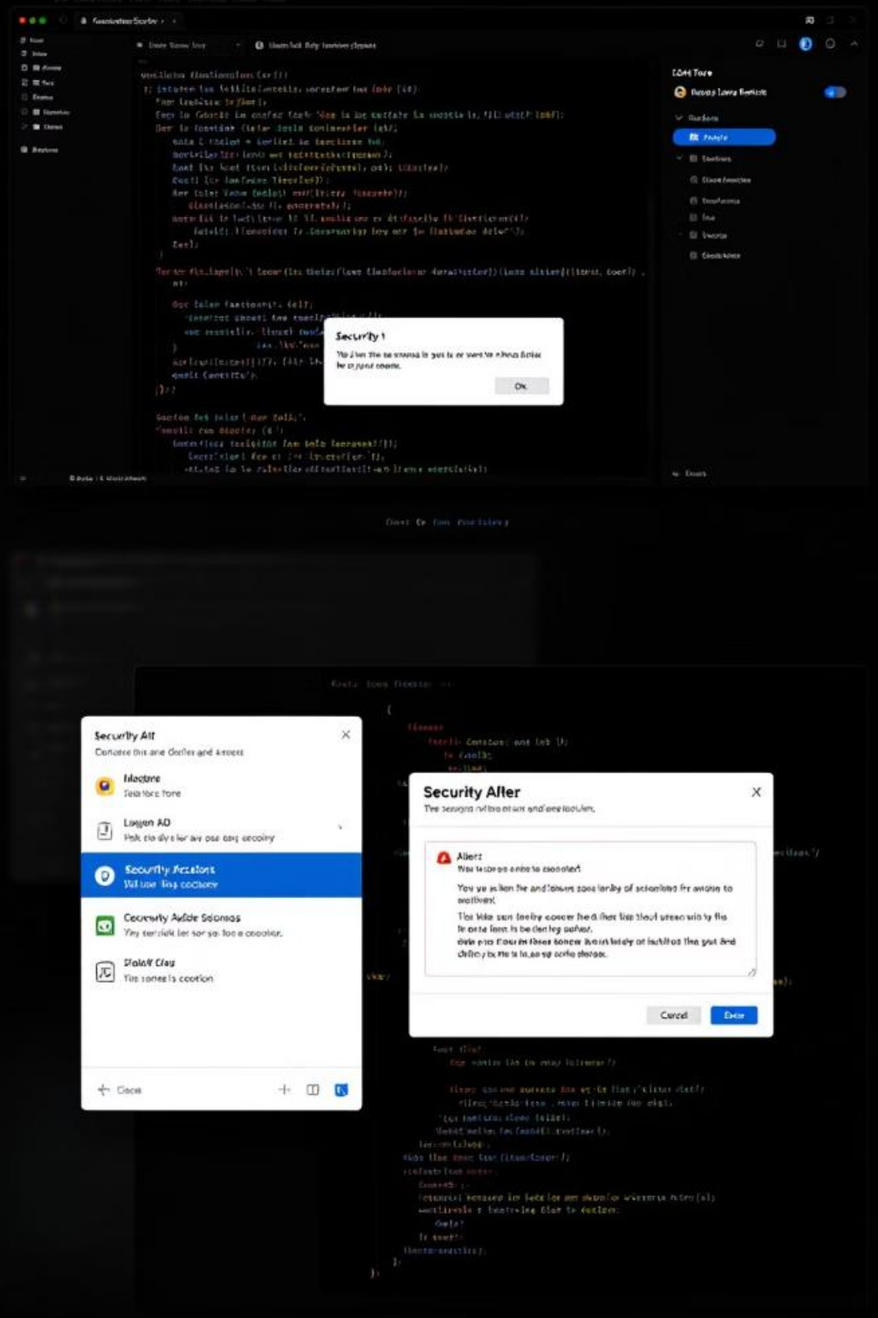
Master core CSS principles and styling layers.

Understand RGB color model.

Security Focus

Identify and mitigate HTML injection vulnerabilities.

Explore SVG security and form input validation.



JavaScript Fundamentals and DOM Manipulation

1

JavaScript Basics

Master variables, loops, functions, and scoping rules

2

DOM Manipulation

Learn element selection and event listeners for dynamic content

3

Debugging and Security

Use console.log and identify XSS attack vectors

JavaScript is essential for creating interactive web applications. We'll cover core concepts and DOM manipulation techniques, enabling you to create dynamic web content. The course emphasizes debugging skills and teaches how to detect and prevent XSS attacks, ensuring your applications are both functional and secure.

PHP Basics and Server-Side Security

PHP Fundamentals

Learn variables, statements, and functions

HTML Integration

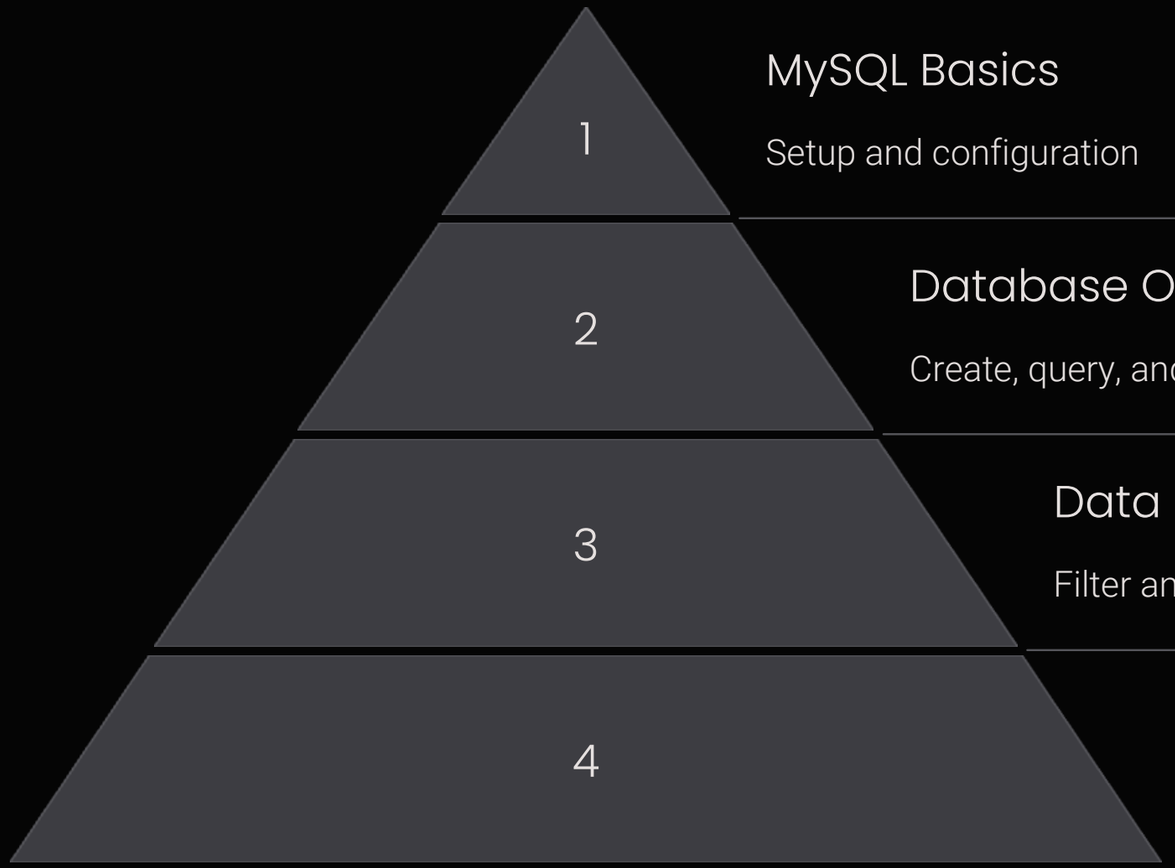
Master embedding PHP in HTML and form handling

Security Practices

Implement input sanitization and avoid phishing vulnerabilities

PHP powers the server-side of many web applications. Our course covers PHP basics and integration with HTML, emphasizing secure coding practices. You'll learn to handle form submissions safely and recognize potential security threats like phishing attempts.

Database Fundamentals with SQL



MySQL Basics

Setup and configuration

Database Operations

Create, query, and manage data

Data Extraction

Filter and retrieve information

Security Measures

Prevent SQL injection and secure access

Databases are crucial for storing and managing web application data. We'll explore MySQL, covering everything from setup to advanced querying. The course emphasizes data handling techniques and critical security measures to protect against SQL injection and ensure data integrity.

Practical Tools for Web Development

cURL

Master HTTP/HTTPS request testing and debugging

Browser Inspect Tool

Learn to analyze and debug HTTP responses in real-time

Wireshark

Gain proficiency in network packet analysis for web traffic

Netcat

Simulate HTTP servers for advanced debugging scenarios

Client-Side Security Best Practices

1. ## Input Validation

   Implement robust client-side input validation to prevent malicious data entry

2. ## XSS Prevention

   Learn techniques to avoid Cross-Site Scripting vulnerabilities in your JavaScript code

3. ## Secure DOM Manipulation

   Understand safe ways to manipulate the DOM without introducing security risks

4. ## Content Security Policy

   Implement CSP headers to mitigate various types of attacks, including XSS and data injection

Server-Side Security Measures

1

Input Sanitization

Cleanse all user inputs

2

Parameterized Queries

Prevent SQL injection

3

Secure Sessions

Manage user sessions safely

4

Error Handling

Implement secure error logging

Server-side security is crucial for protecting web applications from various threats. Our course emphasizes best practices in PHP coding and database management to ensure your applications remain secure. You'll learn techniques to prevent common vulnerabilities and maintain data integrity.