A7

Axpino Technologies

PHP + Security

COURSE CURRICULUM

Course Description

- PHP + Web Securities Boot Camp

- Course Type: Boot Camp
- Total Time: 30 hours
- Days: 15 Days
- Daily Classes: 2 hours

Axpino Technologies

PHP Programming

What is PHP

- Introduction to PHP
- PHP usage
- Open Source
- Cross Platform
- Easy Development

Getting Started with PHP

- Software Requirements
  - Web Server
  - Database Server
- Text Editors

PHP Document Structure

- Code Beginning
- Code Ending
- Output Parsing
- Separate Commands

- Comments
  - Single Line
  - Multiple Line
-
- Variables
- Variable Reference
- Constants
- Data Types
  - Integer
  - Double
  - Strings
  - Booleans
  - Array
  - Objects
  - Resources
  - Data Types Functions

Axpino Technologies

PHP Programming

Working with Arrays

- Array positions
- Associative array
- Multi Dimensional Array

Working with Operators

- Operands
- Operators
- Assignment Operator
- Arithmetic Operator
- Concatenation Operators
- Combined Operators
- Comparison Operators
- Logical Operators
- Auto Increment Operators

Control Flow statement

- **Branching statement**
- **Nested Branching Statement**
- **Loops**
- **Interrupting Loops**
- **Nested Loops**

Functions in PHP

- Introduction to Functions
- Types Of Function
- working with functions

Axpino Technologies

PHP Programming

Object Oriented Programming in PHP

- Class
- Object
- Multiple Objects
- Inheritance
- Access Modifiers
- Constructors
- Destructors

Handling Files and Directories

- Working with file handling
- Writing and reading files
- File permissions
- Directory handling
- File handling functions

Database Interaction

- Connecting MYSQL
- Closing MYSQL
- Selecting MYSQL database
- Executing MYSQL queries

PHP HTTP Methods

- GET Method
- POST Method

Axpino Technologies

PHP Programming

Working with HTML forms

- **Introduction to HTML forms**
- Server Side Handling
- Self Action Script

Other PHP Topics

- PHP global variables and arrays
- HTML File Uploading
- Sessions
- Ajax

Axpino Technologies

Web Application Security

Injection Based Attacks

- SQL Injection
- Types of SQL Injection
  - Form Based
  - URL Based SQL Injection
  - Union Based SQL Injection
- HTML Injection (Cross Site Scripting) – XSS
- Types of XSS Attacks
  - Stored XSS or Persistent XSS
  - Reflected XSS or Non-Persistent XSS
  - DOM Based XSS
- Code Injection
  - Remote Code Execution

Setting Up Web Application Penetration Testing Lab

- Collecting and Installing PenTest Tools
- Flexible Browser with Security Add-ons
- Setting up Browser Proxies

Introduction to other Miscellaneous Web Based Attacks

- Web Based Brute Forcing
- Insecure Cryptographic Storage
- Broken Authentication and Session Management
- Basics of Cookies Stealing/Session Hijacking
  - What is Cookies Stealing/Session Hijacking
  - Session Hijacking: Threats
  - Attack the Victim
- HTTP Referrer Attack
- MITM Attack
- Man-in-the-Browser Attack
- Remote File Inclusion
- Local File Inclusion
- Directory Traversal
- Parameter Tampering
- Shell Injection

Secure Programming

Use Cryptography for Application Security

- Hashes
- Secure Key Storage
- Weak Practices in Cryptography

Data Validation Strategies

- Where to include Data Validation
- Prevent Parameter Tampering
- Hidden Fields
- Encoded Strings
- HTML and URL Encoding
- Delimiter and Special Characters

Session Management

- Session ID Generation
- Session Handling
- Regeneration of Session Tokens
- Session Validation
- Session Bruteforcing
- Session Termination