



HP TRAINING

Php Security

Secure your PHP applications from common vulnerabilities. Learn to identify and mitigate threats to build robust, safe web solutions.

DURATION

Flexible

LEVEL

Intermediate

FORMAT

Instructor-Led

- Globally Recognized Certification

- Expert-Led Hands-On Training

- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This intermediate-level PHP Security course is meticulously designed for developers aiming to fortify their PHP applications against prevalent cyber threats. As web applications increasingly become targets for malicious actors, understanding and implementing robust security measures is paramount. This course delves deep into the common vulnerabilities found in PHP applications, providing you with the knowledge and practical skills to identify, prevent, and mitigate security risks. You'll explore essential security concepts, secure coding best practices, and the proper implementation of security features within PHP to build resilient and trustworthy systems.

Participants will gain hands-on experience with core security technologies and methodologies, including input validation, output encoding, secure authentication and authorization mechanisms, session management best practices, and protection against common attacks such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and insecure file uploads. By mastering these critical areas, you'll be equipped to safeguard user data, maintain application integrity, and comply with modern security standards. This expertise is crucial for any developer looking to advance their career in secure web development and contribute significantly to the security posture of their organization.

Level	Intermediate
Vendor	HP

COURSE CURRICULUM

01 Module 1: Foundations of Web Security and PHP Environment

- Overview of web application security landscape
- Common threats and attack vectors (OWASP Top 10 introduction)
- HTTP security fundamentals (headers, methods, status codes)
- PHP security configurations (php.ini hardening)
- Understanding PHP runtime environment and server security best practices

02 Module 2: Input Validation, Sanitization, and Output Encoding

- SQL Injection prevention techniques (prepared statements, PDO)
- Cross-Site Scripting (XSS) prevention (output encoding, HTMLPurifier)
- Command Injection and file inclusion vulnerabilities (LFI/RFI)
- Regular expressions for robust input validation
- Filtering and sanitizing user-supplied data

03 Module 3: Secure Authentication and Authorization

- Secure user registration and password management (hashing, salting, bcrypt)
- Multi-factor authentication (MFA) principles and implementation in PHP
- Implementing secure login and logout systems
- Role-Based Access Control (RBAC) and permission management strategies
- Preventing brute-force and credential stuffing attacks

04 Module 4: Session Management and CSRF Protection

- Secure session handling (session fixation, hijacking prevention)
- Session management best practices (session IDs, cookies, secure flags)
- Understanding Cross-Site Request Forgery (CSRF) attack vector
- Implementing CSRF tokens and other protection mechanisms
- HTTP Security Headers for enhanced client-side protection (CSP, X-Frame-Options, HSTS)

05 Module 5: File Security, Error Handling, and Cryptography

- Secure file uploads and downloads (validation, storage)
- Preventing directory traversal vulnerabilities
- Secure error and exception handling for production environments
- Logging sensitive information securely
- Introduction to cryptography in PHP (encryption, hashing, digital signatures)

06 Module 6: API Security, Secure Deployment, and Testing

- Securing APIs in PHP applications (API keys, OAuth, JWT)
- Secure deployment practices (server hardening, patching, dependency management)
- Security considerations for third-party libraries and frameworks
- Basic security testing methodologies (penetration testing overview, vulnerability scanning)
- Continuous Security Integration concepts

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

- > **Secure PHP Developer**
- > **Application Security Engineer (PHP Focus)**
- > **Web Security Consultant**

FREQUENTLY ASKED QUESTIONS

Q: How will this course specifically prepare me to tackle the OWASP Top 10 vulnerabilities in real-world PHP applications?

This course provides targeted modules on each major vulnerability category from the OWASP Top 10, such as SQL Injection, XSS, and CSRF. You'll learn the underlying attack vectors, understand how to identify them in existing PHP code, and gain practical skills in implementing robust prevention and mitigation strategies using secure coding practices and PHP's built-in security features to protect your applications effectively.

Q: What prerequisites are expected for this intermediate PHP Security course, particularly regarding my existing PHP development experience?

This course assumes you have a solid foundational understanding of PHP syntax, object-oriented programming (OOP) in PHP, and experience building basic web applications. While knowledge of specific frameworks isn't mandatory, a general familiarity with web development concepts (HTTP, databases) will be highly beneficial. The course focuses on building security principles upon your existing PHP development skills.

Q: Beyond preventing common attacks, what advanced security concepts or tools will I be introduced to that are relevant to enterprise-level PHP applications?

In addition to fundamental attack prevention, this course delves into advanced topics crucial for enterprise environments, including secure API design with authentication mechanisms like OAuth and JWT, implementing robust Role-Based Access Control (RBAC), secure cryptography practices for data protection, and understanding secure deployment strategies. You'll also touch upon basic security testing methodologies relevant for larger, complex PHP applications.

ABOUT COMPUTER PRIDE



East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+

Years of Excellence

10,000+

Professionals Trained

50+

Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location

1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email

info@computer-pride.co.ke

Phone

+254 705 900 900

www.computer-pride.co.ke