Get live, expert instruction from anywhere.

Secure Coding in PHP Boot Camp

Learn how to make PHP applications resistant to attacks from security issues around JavaScript, Ajax and HTML5. This boot camp is designed for PHP developers t hat require effective, realworld, secure programming skills they can implement immediately at the workplace.

Course description

This comprehensive three-day Secure Coding for PHP Boot Camp discusses web vulnerabilities through PHP-based examples. You'll learn concepts beyond the OWASP Top Ten, tackling various injection attacks, script injections, attacks against session handling of PHP, insecure direct object references, issues with file upload and many others.

Both the introduction of vulnerabilities and the configuration practices are supported by a number of hands-on exercises demonstrating the consequences of successful attacks, showing how to apply mitigation techniques and introducing the use of various extensions and tools.

Who should attend

» PHP developers
» Managers, architects and technologists involved in PHP
» Anyone interested in learning more about secure PHP coding

Boot camp at a glance

🎓 What you'll learn

✓ Basic concepts of security, IT security and secure coding
✓ How to use various security features of PHP
✓ Information about vulnerabilities in the PHP framework

🖥 Delivery methods

✓ Online
✓ Team onsite

🕐 Training duration

✓ Immediate access to Infosec Skills
✓ 3-day boot camp
✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

» Three days of expert, live Secure Coding for PHP training
» 100% Satisfaction Guarantee
» Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
» 90-day extended access to all boot camp video replays and materials
» Hands-on cyber ranges and labs
» Knowledge Transfer Guarantee

Prerequisites

Basic to advanced knowledge of PHP, including experience developing PHP applications, as well as familiarity with Apache, MySQL and SQL.

What you'll learn

This boot camp teaches you how poor security practices leave applications open to attack and how to implement the necessary tools, techniques and best practices to write code in a secure manner. It will help develop your knowledge and skills around:

» Basic concepts of security, IT security and secure coding
» Web vulnerabilities beyond the OWASP
» Top Ten and know how to avoid them
» Various security features of PHP
» Recent vulnerabilities of the PHP framework
» Typical coding mistakes and how to avoid them
» Using security testing tools

Regularly updated training

Black hat hackers are always changing their tactics to get one step ahead of the good guys. We update our course materials regularly to ensure you learn about the latest threats — and how to write secure code to prevent those threats.

Skill up and get certified, guaranteed

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

INFOSEC Skills
LIVE BOOT CAMPS ▶

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real-world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

Secure Coding in PHP details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions!

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth boot camp prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

- » CIT security and secure coding
  - » Nature of security
  - » IT security related terms
  - » Definition of risk
  - » Different aspects of IT security
  - » Requirements of different application areas
  - » IT security vs. secure coding
  - » From vulnerabilities to botnets and cybercrime
  - » Classification of security flaws
- » Web application vulnerabilities
- » Basics of cryptography
  - » Cryptosystems
  - » Symmetric-key cryptography
  - » Other cryptographic algorithms
  - » Asymmetric (public-key) cryptography
  - » Public Key Infrastructure (PKI)
- » Client-side security
  - » JavaScript security
  - » AJAX security
  - » HTML5 security
- » PHP security services
  - » Cryptography extensions in PHP
  - » Input validation APIs
- » PHP environment
  - » Server configuration
  - » Securing PHP configuration

- » Environment security
- » Hardening
- » Configuration management
- » Advice and principles
  - » Matt Bishop's principles of robust programming
  - » The security principles of Saltzer and Schroeder
- » Input validation
  - » Input validation concepts
  - » Remote PHP code execution
  - » MySQL validation errors – beyond SQL Injection
  - » Variable scope errors in PHP
  - » File uploads, spammers
  - » Environment manipulation
- » Improper use of security features
- » Problems related to the use of security features
  - » Insecure randomness
  - » Weak PRNGs in PHP
  - » Stronger PRNGs we can use in PHP
  - » Password management – stored passwords
  - » Some usual password management problems
  - » Storing credentials for external systems
  - » Privacy violation
  - » Improper error and exception handling
  - » Classification of security flaws
- » Time and state problems
  - » Concurrency and threading
  - » Concurrency in PHP
  - » Preventing file race condition
  - » Double submit problem
  - » PHP session handling
  - » A PHP design flaw – open_basedir race condition
  - » Database race condition

- » Denial of service possibilities
- » Hashtable collision attack
- » Classification of security flaws
- » Using security testing tools
  - » Web vulnerability scanners
  - » SQL injection tools
  - » Public database
  - » Google hacking
  - » Proxy servers and sniffers
  - » Exercise – Capturing network traffic
  - » Static code analysis

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC