

Szkolenie: Rogue Wave
Building Security into your PHP applications

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Cyfrowe	525 EUR NETTO*	1 dzień
Stacjonarne	Tablet CTAB	675 EUR NETTO*	1 dzień
Metoda dlearning	Cyfrowe	525 EUR NETTO*	1 dzień
Metoda dlearning	Tablet CTAB	525 EUR NETTO*	1 dzień

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00

Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

Cel szkolenia:

Security is paramount when developing applications for the web. Every year we hear about high profile companies losing sensitive data to intruders, and mainly compromises originate from their web presence. The best way to achieve a truly secure web application is to build that application with security in mind from the start. Join us as we investigate common mistakes and failing in web security, and teach you how to build truly secure web applications from the ground up.

What will I learn:

- After completing this course, you will be prepared to incorporate standard, best practice security measures into your PHP applications. You will be able to identify the most common types of vector attacks and industry experienced vulnerabilities allowing you to monitor and fortify your application code against them.

What will I be able to achieve?

- Building truly secure web applications with confidence and aptitude.
- Ensure that your application and company avoid an embarrassing hack or data breach.
- Be sure that you understand and can mitigate the most common web security failings, and understand why "Security First" is the best possible way to code.

Audience:

- This course is designed for intermediate to experienced PHP application developers who are looking to enhance their skills and be able to learn or implement security best practices. It is

also appropriate for intermediate PHP and professional developers who are interested in studying early on how to build security into the applications as part of their learning process.

Plan szkolenia:

- CONCEPTS
 - What is Security
 - Defense in Depth
 - Basic Security Rules
 - Building Secure Web Applications Guidelines
 - Open Web Application Security Project (OWASP)
 - Web Application Exploits
 - Risk Management
 - Injection
- ATTACKS
 - SQL Injection
 - XSS Injection
 - Cross-site forgeries (CSRF)
 - Brute Force
 - Broken Authentication and Session Management
 - Insecure Direct Object References
 - Security Misconfiguration
 - Insufficient Cryptographic Storage
 - Missing Function-Level Access Control
 - Using Components with Known Vulnerabilities
 - Invalidated Redirects and Forwards
- PREVENTION
 - Secure Configuration
 - Authentication Techniques
 - Password Cryptography
 - Hermetic Filtering/Validation/Escaping Techniques
 - Handling Asynchronous Web Calls (AJAX)
 - Lock down Database Security
 - Employing Access Controls and Handling Account Lockouts (ACL)
 - White Listing Techniques
 - Using an API Framework (Apigility)
 - Creating a Standard Review Process

- Captchas, Tokens and Session Management
- Cryptographic Storage Techniques
- Extension Evaluation
- Securing File Uploads
- Logging
- Web Server Security
- RESOURCES
 - Additional Learning Resources
 - Security Standards
 - Penetration Testing
 - Performance Tools

Wymagania:

Basic to advanced knowledge of PHP 5 is recommended including experience developing PHP 5 applications.

Poziom trudności



Certyfikaty:

The participants will obtain certificates signed by Rogue Wave Zend.

Prowadzący:

Rogue Wave Zend Certified Trainer.