Szkolenie: Micro Focus
Fortify Foundations - Application Security

FORMA SZKOLENIA	CENA	CZAS TRWANIA
E-learning	840 PLN NETTO*	1 dzień

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

Cel szkolenia:

This course introduces you to the basics of application security and the role of Fortify. You will learn how to exploit attacks, as well as formulate a threat model and risk assessment for your Application Development Life-Cycle for securing your organization’s applications.

Upon successful completion of this course, you should be able to:

- Recognize the basic concepts of application security
- Execute a variety of attacks against a web application to test vulnerabilities
- Describe the role of Threat Models and Risk Assessments in achieving application security
- Choose how to integrate typical security activities into a default secure SDLC
- Apply the appropriate data validation method to remediate given issues

Audience/Job Roles

This course is intended for those whose primary responsibilities include:

- Evaluating your organization's application security posture, quality, and compliance
- Application development and/or security testing web applications

Plan szkolenia:

- Introduction to Application Security
  - ABC Company Attack Scenario**
  - Application Security in Relation to Computer Security
  - Types of Application Security
  - Challenges in Application Security**
  - SQL Injection: Attack**
  - SQL Injection: Remediation

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- OWASP Top 10
  - Vulnerabilities in Web applications
  - Group and display OWASP issues
  - A1 – Injection
  - A2 – Broken Authentication and Session Management
  - A3 – Cross-Site Scripting
  - A4 – Insecure Direct Object References
  - A5 – Security Misconfiguration
  - A6 – Sensitive Data Exposure
  - A7 – Missing Function Level Access Control
  - A8 – Cross-Site Request Forgery
  - A9 – Using Known Vulnerable Components
  - A10 – Unvalidated Redirects and Forwards
  - Vulnerabilities in mobile applications
- Exploring application security attacks
  - OWASP Tools Hidden Fields**
  - Exploit Hidden Fields*
  - HTML Field Restrictions**
  - Bypassing HTML Field Restrictions*
  - SQL Injection**
  - Exploiting SQL Injection*
  - Cross-Site Scripting**
- Data Validation
  - Deciding Where to Implement Data Validation
  - Data Validation Types
  - Data Validation Techniques**
  - Example of Indirect Selection
  - Indirect Selection**
  - Indirect Selection - Trusting Server-Side Files
  - Whitelists**
  - Whitelists for Standard Input Types
  - Data Validation Library - OWASP ESAPI**
  - Blacklists**
  - Examples of Evading Blacklists
- Remediation - Security goals
  - Security Goals

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Challenges in Security Goals**
- The Concept of “Secure Enough”
- Deciding What to Fix
- Dangers of Requiring Proof of Exploitability**

- Remediation - Security activities
  - Threat Models**
  - Developing a Threat Model**
  - Identifying the potential sources of a breach**
  - Determining Remediation Strategies
  - Risk Assessment**
  - Classifying Attacks Using STRIDE
  - Evaluating Attacks Using DREAD
  - Risk Assessment – Example**
  - Scope of Risk Assessment**
  - Tips on Presenting a Vulnerability**
- Remediation - Security tools
  - Fortify Product Suite Overview Fortify Scanners
  - Fortify Server
  - Fortify Interface Options**
  - Dangers of Misuse**
  - Application Security and Scanners
  - Default Secure SDLC
  - Requirements Phase**
  - Development Phase**
  - QA-SecurityGate Phase**
  - Deployment Phase**
- SDLC Integration overview
  - Default Secure SDLC
  - Phased Deployment**

* Indicates a simulation (hands-on show me/try me)

** Indicates a scenario (practical examples)

Wymagania:

To be successful in this course, you should have the following prerequisites or knowledge:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Basic programming skills (able to read Java, C/C++, or .NET)
- Knowledge of Web and Application development practices
- Experience developing and/or managing software development for security
- Have an understanding of your organization’s compliance requirements

Poziom trudności

Certyfikaty:

The participants will obtain certificates signed by Micro Focus (course completion).

Prowadzący:

Authorized Micro Focus Trainer.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313