Fortify Foundations Application Security

Course Data Sheet

Course No.: FT3E0034*
Category/Sub Category: Application Security

For software version(s): 17.1
Software version used in the labs: 17.1
Course length: Approximately 4 hours

Delivery formats: eLearning
Training is available online.

To order visit: Enterprise Security University

* This course replaced “Developing with Fortify for Application Security”

Course Description
This course introduces you to the basics of application security and the role of Fortify products play to help you achieve secure applications. 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.

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

Course Objectives
Upon successful completion of this course, you should be able to:
- Recognize the basic concepts of application security
- Configure Fortify to group and display issues according to the OWASP Top 10 list.
- Execute a variety of attacks against a web application to test vulnerabilities
- Apply the appropriate data validation technique for a particular situation.
- 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.

Prerequisites / Recommended Skills
To be successful in this course, you should have the following prerequisites or knowledge:
- Basic programming skills (able to read Java, C/C++, or .NET.)
- Basic understanding of web technologies: HTTP Requests and Responses, HTML tags, JavaScript, and server-side dynamic content (JSP, ASP or similar)
- Computer desktop, browser, and file system navigation skills
# Learning Path

<table>
<thead>
<tr>
<th>Modules</th>
<th>Objectives</th>
</tr>
</thead>
</table>
| **Module 1: 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 |
| **Module 2: 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 |
| **Module 3: 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** |
| **Module 4: 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 |
| **Module 5: Remediation - Security Goals** | • Security Goals  
  • Challenges in Security Goals** |
### Module 6: Remediation - Security Activities

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

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Models**</td>
<td>Developing a Threat Model**</td>
</tr>
<tr>
<td>Identifying the potential sources of a breach**</td>
<td>Determining Remediation Strategies</td>
</tr>
<tr>
<td>Risk Assessment**</td>
<td>Classifying Attacks Using STRIDE</td>
</tr>
<tr>
<td>Evaluating Attacks Using DREAD</td>
<td>Risk Assessment – Example**</td>
</tr>
<tr>
<td>Scope of Risk Assessment**</td>
<td>Tips on Presenting a Vulnerability**</td>
</tr>
</tbody>
</table>

### Module 7: Remediation - Security Tools

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortify Product Suite Overview</td>
<td>Fortify Scanners</td>
</tr>
<tr>
<td>Fortify Server</td>
<td>Fortify Interface Options**</td>
</tr>
<tr>
<td>Dangers of Misuse**</td>
<td>Application Security and Scanners</td>
</tr>
<tr>
<td>Default Secure SDLC</td>
<td>Requirements Phase**</td>
</tr>
<tr>
<td>Development Phase**</td>
<td>QA-SecurityGate Phase**</td>
</tr>
<tr>
<td>Deployment Phase**</td>
<td></td>
</tr>
</tbody>
</table>

### Module 8: SDLC Integration Overview

<table>
<thead>
<tr>
<th>Topic</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Secure SDLC</td>
<td>Phased Deployment**</td>
</tr>
</tbody>
</table>

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