OWASP Proactive Controls, Part 1 of 2: Controls 1 through 5

Meet the expert: Robert Hurlbut is a software security architect and trainer. He is a Microsoft MVP for Developer Security / Visual Studio and Development Technologies and he holds the (ISC)2 CSSLP security certification. Robert has 30 years of industry experience in secure coding, software architecture, and software development and has served as a project manager, director of software development, chief software architect, and application security champion for several companies. He speaks at user groups, national and international conferences, and provides training for many clients.

Prerequisites: The assumption is the student is familiar with web and/or mobile development plus basic application security principles. Also, it is highly recommended the student be familiar with the OWASP Top 10 project.
There are several other courses provided by LearnNowOnline which can prepare the student with knowledge of the OWASP Top 10 before taking this course. This course is about the OWASP Top 10 Proactive Controls, which is a supplement to the OWASP Top 10 for developers

Runtime: 01:56:24

Course description: In this course, you will learn about the OWASP Top 10 Proactive Controls document and the many guidelines it provides to help developers write better and more secure code. In particular, I provide an overview of the Proactive Controls and then I cover the first five security controls. These security controls include testing for security early and often, learning about parameterizing SQL queries, encoding data input that may be parsed as executable code, validating data input, and finally you will learn about identity and authentication techniques to make sure you know who is using your web applications. Join me in this course as we explore the OWASP Top 10 Proactive Controls.

Course outline:

Overview
- Introduction
- About This Course
- What Is a Security Control
- What are the OWASP Top 10 Proactive Controls
- OWASP Top 10 Proactive Controls
- Relation to OWASP Top 10
- History
- For Developers by Developers
- Demo: OWASP Top 10 Proactive Controls
- Summary

Verify Security
- Introduction
- C1 - Verfiy Security Early and Often
- The DevOps Challenge to Security
- Automated Tests in a Continuous Delivery Pipeline
- BDD - Security Testing Framework
- Demo: OWASP Top 10 Mapping
- Summary

Paramterize Queries
- Introduction
- C2 - Parameterize Queries
- Anatomy of an SQL Injection Attack
- The Perfect Password
- SQL Injection
- Demo: SQL Injection
- Demo: Attack Strategies
- Demo: Identity Membership
- Demo: Edit Posts
- Demo: Fixing SQL Injection
- Summary

Encode Data
- Introduction
- C3 - Encode Data
- Anatomy of an XSS Attack
- XSS Attack: Problem and Solution
- Microsoft Encoder and AntiXSS Library
- OWASP Java Encoder Project
- Other Resources
- Demo: Preventing XSS Attacks
- Demo: Sanitization
- Summary

Validate Inputs
- Introduction
- C4 - Validate All Inputs
- OWASP HTML Sanitizer Project
- File Upload
- File Upload Verification
- Summary

Identity and Authentication Controls
- Introduction
- C5 - Implement Identity and Authentication Control
- Password Cracking
- Password Management Best Practices
- Again, the Perfect Password
- User Authentication Best Practices
- User Authentication - Real-World Examples
- Summary