OWASP Proactive Controls, Part 2 of 2: Controls 6 through 10

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: 55:43

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 will cover the last five controls. These include implementing access control to verify what a user is allowed to do in a system, methods of protecting data at rest and in transit, implementing logging and intrusion detection, and finally I will talk about using existing security frameworks and libraries as well as best practices for error and exception handling. Join me in this course as we continue our exploration of the OWASP Top 10 Proactive Controls.

Course outline:

Implement Access Controls
- Introduction
- C6 - Implement Appropriate Access Controls
- Access Control Anti-Patterns
- Role-Based Access Control
- ASP.NET Roles vs. Claims Authorization
- Apache Shiro Permission-Based Access Control
- Summary

Protect Data
- Introduction
- C7 - Protect Data
- Encrypting Data in Transit
- HSTS (Strict Transport Security)
- Certificate Pinning
- Browser-Based TOFU Pinning
- Pinning in Play (Chrome)
- Forward Secrecy
- Google KeyCzar
- Libsodium
- Summary

Logging and Intrusion Detection
- Introduction
- C8 - Implement Logging and Intrusion Detection
- Tips for Proper Application Logging
- Detection Points Examples
- Summary

Security Frameworks and Exception Handling
- Introduction
- C9 - Leverage Security Frameworks and Libraries
- Security Frameworks and Libraries
- C10 - Error and Exception Handling
- Best Practices for Error and Exception Handling
- Summary