ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Web Application Security Essentials (.NET)

Course Summary

Description

This class teaches developers how to protect against the most dangerous, costly, and prevalent threats to the security of websites, both internal and external. Students will not only learn to identify these threats but will also leave the class with practical and workable defenses for each one.

You'll be given an e-commerce website to practice on. After learning about each attack type, you'll carry out the attack. Then you'll harden your website using what was learned in the lecture and watch the attack fail the second time. This hands-on approach will anchor your understanding of web application security.

The lectures are packed with interesting stories from newspaper headlines and videos as practical examples of each of the attacks. You will learn how the hackers successfully carried out those attacks, including the tools used so that we know precisely how to defend our sites against these attacks and ones like them.

We will focus on OWASP's Top Ten Security Threats, seeing examples, learning hackers' methods, and the best practices for protecting our sites against similar attacks.

Objectives

After taking this course, students will be able to:

- Identify and understand the most prevalent and dangerous security threats in today's web applications including the OWASP Top 10 and CWE/SANS Top 25.
- Know how to defend his or her organization against each one of them.
- Explain cryptographic ciphers like SHA1, MD5, Blowfish, and RSA and know which ones are stronger.
- Get and use certain hacker tools like vulnerability scanners and how to protect their sites against those same tools

Topics

- Overview of web security
- Overview of the OWASP top ten vulnerabilities
- Overview of the CWE/SANS top 25 vulnerabilities
- Clickjacking
- Phishing
- Denial of service attacks
- A10 Underprotected APIs
- A9 Using components with known vulnerabilities
- A8 Cross-site request forgery
- Cryptography overview
- A7 Insufficient attack protection
- A6 Sensitive data exposure
- Password management
- A5 Security misconfiguration
- A4 Broken access control
- Padding oracle attack
- Information leakage and improper error handling
- A3 Cross site scripting
- A2 Broken authentication and session management
- A1 Injection flaws
- Bringing the top ten together – best practices for security overall.

Web Application Security Essentials (.NET)

Course Summary (cont'd)

Audience

This class is most appropriate for intermediate to advanced developers who want to enhance their knowledge of security threats and who want to know the practical steps on how to protect their web applications.

Prerequisites

There are no prerequisites for this course.

Duration

Five days

ProTech protechtraining.com *"Charting the Course ...*

... to Your Success!"

Web Application Security Essentials (.NET)

Course Outline

I. Overview of web security
- A. OWASP publications and projects
- B. Overview of the OWASP top ten vulnerabilities
- C. Overview of the CWE/SANS top 25 vulnerabilities

II. A10 Underprotected APIs
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves
- D. Whitelists and mapping

III. Denial of service attacks
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves

IV. A9 Using components w/known vulnerabilities
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves
- D. AJAX, web services

V. ClickJacking
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves

VI. A8 Cross site request forgery
- A. Real-world example
- B. How attackers do it
- C. Demo of a CSRF attack
- D. How NOT to protect against CSRF
- E. How we protect ourselves
- F. Synchronizer token pattern made easy

VII. Cryptography overview
- A. Vulnerability examples
- B. History
- C. Functions of cryptography
- D. Types of encryption with ciphers
- E. When to use each type
- F. Which ciphers to avoid
- G. How SSL/TLS works

VIII. A7 Insufficient attack protection
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves

IX. Phishing attacks
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves

X. A6 Sensitive Data Exposure
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves
- D. AJAX, web services
- E. War stories of lost & stolen data
- F. How we protect ourselves
- G. How to encrypt web.config
- H. Demo of cracking passwords

XI. Password management
- A. Real-world story of bad password policies
- B. Easy and secure user controls
- C. Best practices for security architects

XII. Threat Risk Modeling
- A. Proper analysis of a web project
- B. STRIDE
- C. DREAD
- D. Threat Trees
- E. How to predict attack vectors

XIII. A5 Security misconfiguration
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves
- D. Best practices for installation
- E. Internal attackers

XIV. Information leakage and improper error handling
- A. Real-world example
- B. How attackers do it
- C. How we protect ourselves

XV. A4 Broken access control
- A. Real-world examples
- B. How attackers do it
- C. How we protect ourselves
- D. Mapping references

Web Application Security Essentials (.NET)

Course Outline (cont'd)

XVI. A3 Cross site scripting
- A. Real-world example
- B. How attackers do it
- C. Live demo of a XSS attack
- D. Reflected vs. stored attacks
- E. How we protect ourselves
- F. Installing and using the Anti-XSS Toolkit

XVII. A2 Broken authentication and session management
- A. Real-world example
- B. How sessions & cookies work
- C. How attackers exploit
- D. How we protect ourselves

XVIII. Secure Coding Principles
- A. Systemic views to security
- B. Bolted-on security
- C. Baked-in security
- D. Best practices

XIX. A1 Injection flaws
- A. Sample attack vectors
- B. How attackers do it
- C. How we protect ourselves
- D. Parameterized queries
- E. ORMs (LINQ-to-SQL, EF, NHibernate)
- F. Stored procedures
- G. Whitelisting vs. blacklisting

XX. Web services security
- A. Real-world example
- B. How it differs from web site security
- C. Special considerations for XML web services
- D. How attackers do it
- E. How we protect ourselves

XXI. Bringing the top ten together – best practices for security
- A. Review of the top ten (and more)
- B. Handout: Checklist for protecting against all top ten attacks
- C. Handout: Many links to tools, articles, and further study