

Secure Coding for Web Developers



The aim of this training course is to make web developers aware of common insecure coding practices and how these can be addressed to make secure applications.

The attendees will have access to web applications specifically designed to demonstrate these vulnerabilities. Besides learning about the vulnerabilities which arise from insecure coding, the attendees will also learn the hacking techniques which attackers use to subvert an application's programming/business logic for their advantage. This will also help developers adopt the defence-in-depth approach and ensure they have all aspects of security in consideration while developing applications.

Course Outline

1. Introduction to Web Applications

- Authentication
- Authorisation
- Cookies
- HTTP protocol
- Overview of Google hacking

2. Attacking Authentication

- Types of authentication
- Clear text HTTP protocol
- Username enumeration
- Security through obscurity

3. Web Server Issues

- IIS/Apache exploits and introduction to hacking tools such as metasploit
- Insecure HTTP methods

4. Cross Site Scripting

- Types of XSS
- Secure cookie, HTTP-only
- Complicated XSS

5. Cross Site Request Forgery

- Demo
- Complicated XSRF with POST requests
- XSRF in web services

6. Session Fixation

7. CRLF Injection

- Proxy poisoning, XSS with CRLF injection

8. Clickjacking

9. SQL Injection

- Introduction to SQL injection
- Authentication bypass
- Extracting data
- OS code execution
- Overview of advanced SQL injections

10. Malicious File Uploads

11. Vulnerable Flash Applications

12. Parameter Manipulation Attacks

13. Business Logic Bypass.

- Authentication bypass
- Other logical flaws

14. SSL Misconfigurations

- SSL and man-in-the-middle attacks
- Screenshots

15. Security Problems with Thick Client Applications

To Book Call: 0870 600 1667

Duration: 2 days

Cost: £999.00 + VAT