TRAINING

MWR CYBERSEC

Proactive Web Defence

A three-day training course in web application security and secure coding practices, helping to ensure that your software is resilient to attacks from even the most advanced threats

PWD is an exercise-driven training course that will guide you through exploiting vulnerabilities in a realistic website. Step-by-step tutorials will ensure that you gain a thorough understanding of a modern attacker's mind-set and capabilities. Equipped with this understanding, we will move our attention back to secure coding best practice and defensive programming techniques that can be used to make our applications robust and resilient to attacks.

Who should attend?

The course is aimed primarily at web developers although it is also suitable for technical project managers. The content caters for beginners with limited or no security knowledge and gradually progresses to advanced topics. Prior to attending Proactive Web Defence, it is recommended that you:

- Can build a dynamic web application that can communicate with a database
- Have a basic understanding of relational databases and SQL
- Can read basic JavaScript (even if you can't write it)
- Understand the basic principles of web servers and HTTP

Course highlights

- How to identify, exploit and remediate all the common web application security flaws, over and above the **OWASP Top Ten**
- How to **build secure web applications** that can withstand advanced attacks
- How hackers attack web applications, web servers and database servers
- How to **deploy secure web and database servers** that can withstand an attack
- The most up to date and effective **secure coding practices**

Benefits to your organization

- Helps to ensure that your software is resilient to an attack, against even the most **advanced threats**
- Increases levels of **trust and reputation** when developing for external organizations
- **Increases your organization's overall understanding** of security, reducing the time and cost of remediating vulnerabilities
- **Stimulates a positive attitude** and an understanding of the importance of security within the development team
- Fulfils secure coding requirements for **PCI DSS**

How is this course different?

The course is delivered by experienced security professionals, who perform web application security assessments on a daily basis.

We focus on teaching offensive security techniques, so that you can fully understand the capabilities of modern attackers and therefore how to defend against them.

This is a practical, exercise driven course. We've developed a realistic web application with common flaws which allows us to show you how attackers would exploit these vulnerabilities in the real world.

We teach you how to introduce security in your development lifecycle in a practical manner, by combining secure coding principles, design and source code reviews

MWR CYBERSEC

Topics / Syllabus

Foundation

- Hackers - Culture and Motives
- A History of Hacking
- Firewalls Pitfalls
- The CIA Triad
- HTTP Protocol Refresher

Authentication & Authorization

- Authentication Issues
- Username Enumeration
- Brute Force Attacks
- Account Lockout
- Multi-Factor Authentication
- Forgotten Password Functionality
- Session Hijacking
- Session Fixation
- Authorization Issues

Injection Attacks

- SQL Injection for Authentication Bypass and Data Extraction
- XML Injection
- LDAP Injection
- XPath Injection
- CRLF Injection
- SMTP Injection
- OS Command Injection
- XML eXternal Entity Processing (XXE)
- XML Denial of Service

Client-Side Attacks

- Cross-Site Scripting (XSS)
- Advanced XSS Attacks
- Output Encoding
- Cross-Site Request Forgery (CSRF)
- JSON Hijacking
- Cross-Site Redirects
- Clickjacking Attacks

Infrastructure Level Attacks

- Directory Traversal
- Insecure File Upload
- LFI and RFI
- Web Server Hardening
- Buffer Overflows
- Dangerous HTTP Methods
- Database Server Hardening
- Attacking the Database Server

Encryption & Data Storage

- Fundamentals of Encryption
- Common Encryption Flaws
- Secure Socket Layer (SSL)
- Stored Data
- Cracking Password Hashes
- Data Leakage

HTML 5

- XSS Filter Considerations
- Cross-Origin Resource Sharing
- Cross-Window Messaging
- Web Local Storage

Integrating Security

- Current State of the Industry
- Secure Software Development Lifecycle
- Security Requirements
- Security Coding Standards
- Conducting a Design Review
- Conducting a Code Review
- Vulnerability Scanning Tools
- Penetration Testing
- Logs and Alerts
- Vulnerability Management

For more information visit www.mwrcybersec.com or email us on info@mwrcybersec.com