



Call us on...  
**0113 257 8955**



## Securing Web Applications Training

### Part of the Sec-1 Training Programme

#### Course Overview

Insecure web applications are among the main threats to organisations today. To counter these threats Sec-1 has developed the Securing Web Applications training course.

The course is a one day module from Sec-1's training programme and has been designed to provide IT Professionals and Web Developers with the skills and tools required to effectively protect their web applications from exploitation.

#### Course Outcomes

During this essential one day course attendees will experience ten hands on lab sessions where they are shown how to discover, exploit and fix each of the OWASP top ten security vulnerabilities.

Each attendee is provided with the AppCheck Web Application and Infrastructure Scanner which they are also able to trial, free of charge, upon completion of the course.

#### Key Benefits

This training module provides attendees with the following benefits:

- Learn to protect your Web Applications from the most common vulnerabilities
- Free use of the AppCheck Web Application and Infrastructure Scanner
- Attain the skills required to test against the OWASP (Open Web Application Security Project) Top Ten
- Free Securing Web Applications Tool Kit

#### What do our clients say about the course?

*Excellent course, very practically biased, and a good thorough overview of attack methods against Web Applications.*

ICT Manager  
Local Regional Government

*I can attest to the excellent standards of training, communication and practical hands on training.*

IT Specialist  
Engineering Sector

*Very interesting and information, presenter knows his stuff, well worth attending.*

DBA Security Specialist  
Defence & Energy Sector

#### Accreditations



## Course Schedule

### Introduction to Web Application Security

- Web Application attack trends and high profile examples
- Web Application Architecture
- Introduction to the Sec-1 App Testing Tool kit

### Authentication & Session Management

- Authentication Technologies & Strategies
- Session Management
- Assessing Session ID Strength
- Common Security Flaws
  - LAB: Attacking Form Based Authentication
  - LAB: Attacking Session Management
- Authentication & Session Management Best Practices

### Cross Site Scripting (XSS) & Cross

#### Site Request Forgery (CSRF)

- Introduction to XSS and CSRF attacks
- Persistent XSS vs Reflective XSS
- CSRF Examples
- Discovering XSS and CSRF Vulnerabilities
- Exploiting XSS and CSRF Vulnerabilities
  - LAB: Discovering XSS Vulnerabilities
  - LAB: Hijacking Authenticated Sessions via XSS
- Preventing XSS and CSRF attacks

### Malicious File Execution

- "File Include" vulnerabilities
- Discovering File Include Vulnerabilities
- Exploiting File Include Vulnerabilities
  - LAB: Discovering and exploiting file include vulnerabilities
- Preventing Malicious File Execution attacks

### Insecure Direct Object Reference &

#### Failure to Restrict URL Access

- Parameter Tampering
- Discovering "Insecure Direct Object Reference Vulnerabilities"
  - LAB: Parameter Tampering
- Defeating Parameter tampering via Database Association Proxies

### Insecure Cryptographic Storage &

#### Insecure Communications

- Encryption Algorithms
- Common Encryption implementation vulnerabilities
- SSL and TLS
  - LAB: Assessing SSL Strength
- Recommended Best Practices

### Injection Flaws

- SQL Injection, XPATH injection and OS Command Injection
- Discovering Blind and Error based SQL Injection Vulnerabilities
- Using SQL injection exploit frameworks
- Reading Table Data Via SQL injection (Blind and Error Based)
  - LAB: Discovering and exploiting SQL injection Vulnerabilities
  - LAB: Gaining remote Code Execution & Reading Table Data
  - LAB: Exploiting Blind SQL injection Vulnerabilities
- Coding against SQL injection.

### Information Leakage and Improper

#### Error Handling

- Error handling overview
- HTTP Error Codes
- Implementing secure Error handling

### OWASP Top 10 Recap and Q & A

## The Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) was established to assist organizations with web applications security. The OWASP top ten is a list of the most serious web application vulnerabilities, and information on how to eradicate them.

Organisations that protect against the OWASP top ten vulnerabilities greatly reduce the threat of their applications being exploited.

Leading Network Security commentator Jeremiah Grossman\* has stated that:

- The majority of websites 'have at least one vulnerability'
- Many websites are hacked without their owners knowledge, and this 'will increase exponentially over the next few years'
- The standard mandated by the credit card industry, PCI-DSS, makes little difference to a websites security

\*CTO White Hat

## Who Should Attend

Sec-1's Securing Web Applications course is designed for IT Professionals responsible for or with an interest in Web Application Security.

## Prerequisites

Attendees should have:

- A working knowledge of Web Application technologies and programming languages
- A working knowledge of TCP/IP and common networking technologies
- A basic knowledge of common databases (e.g. Microsoft SQL Server)

## About the Sec-1 Training Programme

Sec-1 has developed a training programme to provide IT professionals a structured approach to learning.

The training programme is constantly under development.

Other courses include:

- Ethical Hacking and Countermeasures
- Wireless Hacking and Countermeasures

Call Sec-1 now, on **0113 224 8092** to book your place.

