

Certified Network Security Professional – Securing Web Applications



Course Overview

Securing Web Applications is the latest module of the hugely popular Certified Network Security Professional training programme.

The course has been designed to provide IT Professionals responsible for the security and development of web applications with practical skills, which can be used to improve and maintain the security of their web applications.

Why CNSP - Securing Web Applications?

Insecure web applications are among the main threats to an organisation today. Web applications, ranging from dynamic news pages through to fully blown eCommerce applications, have been adopted by many organisations to enable them to share information and provide products and services to clients.

The implications of insecure web applications led to the formation of The Open Web Application Security Project (OWASP), an open-source application security project set up to assist organisations in the securing of their web applications.

The OWASP top ten is a list of the top ten current web application vulnerabilities.

Organisations that regularly ensure they are protected against this top ten greatly reduce the threat of their web applications being exploited. Jeremiah Grossman, CTO of White Hat and leading network security commentator, recently stated that:

- “The vast majority of websites have at least one serious vulnerability”
- “Many websites are being broken into, but no one knows about them and this will increase exponentially over the next few years”
- “The standard mandated by the credit card industry, PCI-DSS, makes little difference to the security of a website”
- “Web application vulnerability scanners miss as many of the most common issues as they find”

Your business... is your business.

Course outcomes

During this essential one-day course attendees will experience ten hands-on lab sessions where they learn to discover, exploit and fix each of the top ten security threats as defined by the Open Web Application Security Project.

All attendees are also trained how to use the Sec-1 Scanner, and will receive the Sec-1 Scanner Lite free of charge for use within their own organisation. The course includes:

- Introduction to web application security
- Introduction to Sec-1 Scanner Lite
- The OWASP Top Ten (includes hands-on labs)

About Sec-1

Sec-1 is a dedicated network security solution provider based in Leeds, dealing with clients throughout the UK. Our three step approach to best practice in network security consists of:

- Assisting clients to move their organisation towards industry best practice
- Providing detailed information advising on any gaps between current practice and industry best practice
- Partnering with clients to attain industry best practice through solution provision

About the Certified Network Security Programme

The Certified Network Security [CNSP] Programme has been developed to provide IT Professionals with a structured and modular approach to attaining the knowledge required to secure an organisation in today's ever changing environment. The CNSP Programme is constantly under development, other modules include:

- CNSP – Ethical Hacking and Countermeasures**
- CNSP – Wireless Hacking and Countermeasures**
- CNSP – Internal Security Auditing**

Who Should Attend

The CNSP – Securing Web Applications is designed for IT Professionals responsible for or with an interest in Web Application Security.

Prerequisites

Attendees should have knowledge of TCP/IP and the Windows operating system.

Each Candidate Will Benefit From:

- Attainment of the skills required to test against the OWASP Top Ten
- Free use of the Sec-1 Scanner Lite
- Free CNSP - Securing Web Applications Tool Kit
- Free access to the Sec-1 Security Portal

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