Web Application Hacking: Hands-On

Providing a solid grounding in web application security based on the renowned OWASP Top Ten

CSTP covers the fundamentals of the industry-recognised OWASP Top Ten – "the ten most critical web application security risks".

Web application flaws can leave an organisation and its customers vulnerable to attack. This is why knowledge of, and protection against, the 'OWASP Top Ten' is an essential component of modern information security strategies and a requirement of the Payment Card Industry Data Security Standard (PCI DSS).

On this course, practical exercises reinforce theory as candidates test functional ASP.NET and PHP applications. The course demonstrates hacking techniques with defence in mind and countermeasures are discussed throughout. The CSTP Exam (theory based) is included at the end of the course.

To Book Call:
+353 1 685 4942

Duration: 2 days
Cost: €1100.00

The course is ideally suited to anyone responsible for, or with an interest in, the security of web applications, such as: system administrators, auditors, IT security officers, information security professionals, budding penetration testers, QSAs and anyone subject to the requirements of PCI DSS. Web developers should note that the course discusses high-level countermeasures and as such is not primarily a secure coding course.

Prerequisites

A basic understanding of how a web page is requested and delivered, e.g.

- Are you familiar with the high-level components involved, e.g. browsers, web servers, web applications and databases?
- Do you have a basic understanding of HTTP?
- Do you have a basic understanding of HTML?

A basic understanding of databases and SQL would be an advantage, e.g.

- Do you understand the concept of data storage in tables within a relational database?
- Can you construct a simple SELECT statement to extract data from a table?

Together with CSTA helps prepare you for the CREST Registered Tester qualification

MSc Credits: 15

Course Content

A full list of practical exercises is available on our website: www.7safe.com/cstp

Principles

- Web refresher
- Proxies
- The OWASP Top Ten
- Web application security auditing
- Tools and their limitations
- HTTP request and response modification
- Logic flaws

Injection

- Types
- Databases overview – data storage, SQL
- SQL injection – data theft, authentication bypass, stored procedures
- Information leakage through errors
- Blind SQL injection

Cross-site Scripting (XSS)

- Email spoofing
- Phishing
- JavaScript – tabnabbing
- Reflected and Stored/Persistent XSS
- Cookies, sessions and session hijacking

Broken Authentication and Session Management

- Scenarios
- Attacking authentication pages

Insecure Direct Object Reference

- Direct vs indirect object references
- Authorisation

Cross-site Request Forgery (CSRF)

- Exploiting predictable requests

Security Misconfiguration

- Scenarios

Insecure Cryptographic Storage

- Identifying sensitive data
- Secure storage methods

Failure to Restrict URL Access

- Scenarios
- Information leakage through logs

Insufficient Transport layer protection

- Scenarios

Unvalidated Redirects and Forwards

- Scenarios

Conclusions

CSTP Exam

CPE Credits: 16