COURSE OUTLINE

ETHICAL HACKING
Certified Security Testing Professional (CSTP)

●●●○ **CORE-LEVEL COURSE** **Cost: £1,950.00 + VAT** Duration: **3 days**

Web application flaws can leave an organisation and its customers vulnerable to attacks. This web application ethical hacking course will give you the knowledge of, and protection against, the 'OWASP Top Ten Web Application Security Vulnerabilities', an essential component of modern information security strategies and a requirement of the Payment Card Industry Data Security Standard (PCI DSS).

COURSE OVERVIEW

This three-day course is designed to give you the skills you need to undertake an application penetration test in order to ensure valuable data and assets are effectively protected. You will have access to a functional ASP.NET and PHP application through which theory is reinforced by way of practical exercises in order to demonstrate hacking techniques with defensive countermeasures always in mind.

THE SKILLS YOU WILL LEARN

- A number of methodologies for undertaking a web application penetration test
- How to exploit vulnerabilities to access data and functionality
- A range of defensive countermeasures as well as sufficient knowledge as to how to counter these attacks

KEY BENEFITS

This course will enable you to:

- Learn effective techniques to identify exploits and vulnerabilities
- Improve your ability to respond effectively to cyber threats
- Gain valuable preparation for the CREST Registered Penetration Tester (CRT) examination and the knowledge required to join our CAST course (advanced web application security)
- Acquire the skills and understanding to progress to the next stage in your career as a security professional

WHO SHOULD ATTEND

Anyone with responsibility for, or an interest in, the security of web applications, including:

- System administrators
- Software developers
- Budding penetration testers
- Anyone subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS)

PREREQUISITES

An understanding of how a web page is requested and delivered:

- Are you familiar with the high-level components involved, e.g. browsers, web servers, web applications and databases?
- What are HTTP and HTML?

An understanding of databases and SQL would also be an advantage:

- 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?

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA's Certified Security Testing Professional (CSTP) qualification.

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com

COURSE OUTLINE

ETHICAL HACKING
Certified Security Testing Professional (CSTP)

●●●○ **CORE-LEVEL COURSE** **Cost: £1,950.00 + VAT** Duration: **3 days**

> *"The course content helped to reinforce my existing knowledge and give real world examples and practical exercises for the key features of the content and syllabus."*
> ***CSTP Delegate***
> ***NewVoiceMedia Ltd***

SYLLABUS

1. Principles
a. Web refresher
b. Proxies
c. The OWASP Top Ten
d. Web application security auditing
e. Tools and their limitations
f. HTTP request and response modification
g. Logic flaws

2. Injection
a. Types
b. Databases overview – data storage, SQL
c. Exploiting SQL injection – e.g. data theft, authentication
d. Exploiting Blind SQL injection
e. Exploiting stored procedures and Bypass
f. Exploiting leaked information through errors
g. Exploiting Server-Side Template Injection (SSTI)
h. Exploiting Server-Side Request Forgery (SSRF)
i. Exploiting Application Programming Interface (API)

3. Broken Authentication
a. Attacking authentication pages
b. Exploiting predictable requests
c. Session management - cookies

4. Sensitive Data Exposure
a. Identifying sensitive data
b. Secure storage methods

5. XML External Entities (XXE)
a. Identifying XXE
b. Scenarios

6. Broken Access Control
a. Insecure Direct Object Reference
b. Direct vs indirect object references
c. Cross-site Request Forgery (CSRF)
d. Missing Function Level Access Control
e. Unvalidated Redirects and Forwards

7. Security Misconfiguration
a. Identifying misconfiguration
b. Scenarios

8. Cross-site Scripting (XSS)
a. JavaScript
b. Email spoofing
c. Phishing
d. Reflected and Persistent XSS
e. Cookies, sessions and session hijacking

9. Insecure Deserialization
a. Identifying insecure object
b. Scenarios

10. Using Components with Known Vulnerabilities
a. Identifying well know vulnerabilities with components
b. Scenarios

11. Insufficient Logging & Monitoring
a. Scenarios

12. Additional Web Auditing Tool and Conclusions
a. Scenarios

PA Consulting
Global Innovation & Technology Centre Back
Lane, Melbourn
Herts, SG8 6DP, United Kingdom
tel: +44(0) 1763 285285
email: cybereducation@paconsulting.com
www: cybereducation.paconsulting.com

To find out if our cyber training is right for you, or to make a booking, call our education team on 01763 285 285 or email cybereducation@paconsulting.com