COURSE OUTLINE

ETHICAL HACKING
Certified Application Security Tester (CAST)

SPECIALIST-LEVEL COURSE | **Cost: £2,600.00 + VAT** | **Duration: 4 days**

This specialist four-day web hacking course is for people in a wide range of application development and testing roles. It is designed to give you an in-depth knowledge of how to identify security vulnerabilities and an understanding of the real risk that these vulnerabilities pose by exploiting them.

"Had a fantastic time on the course, well delivered, useful and eye opening to say the least. Heading off to take the CREST exam shortly! Thanks for all your help."
CAST Delegate MarketingSource Ltd

COURSE OVERVIEW

An advanced web hacking course designed for experienced penetration testers, developers and security professionals who need to extend their knowledge of hacking web applications. The course covers the syllabus for the latest CREST Certified Web Application Tester (CCT App) exam and therefore you will be expected to demonstrate that you are able to find a range of security flaws and vulnerabilities, including proving the ability to exploit and leverage the flaws to ascertain the impact of the issues found.

THE SKILLS YOU WILL LEARN

- You will be led through a range of state-of-the-art hacking tools and techniques to allow you to conduct a complete web application security assessment
- Once able to identify and exploit vulnerabilities, you will learn a range of defensive counter measures, allowing you to develop applications that are more resistant to attack and provide a better protection for data assets

KEY BENEFITS

This course will give you:

- Security vulnerability identification and avoidance
- An industry recognised qualification
- Essential preparation for the CREST Certified Web Application Tester (CCT App) exam

WHO SHOULD ATTEND

This course is ideally suited to individuals that have been working in an application testing (security assessment/administration) or developer environment for some time and who have hands-on experience with web application security administration
and testing, including experienced:

- Penetration testers
- Application developers
- Security professionals

PREREQUISITES

CAST is an advanced application security training course and it is highly recommended that you have completed the PA Consulting CSTP course, or already possess equivalent knowledge. It is important that you have knowledge of networking and a practical experience of modern web application technologies (e.g. HTML, JavaScript, PHP, ASP, MSSQL, MySQL). Hands-on experience of modern hacking trends, tools and technologies would also be an advantage.

WHAT QUALIFICATION WILL I RECEIVE?

Those delegates successfully passing the exam at the end of the course will be awarded PA Consulting's Certified Application Security Tester (CAST) qualification.

To find out if our cyber training is right for you, and to make a booking, contact our education team on 01763 285 285 or email

COURSE OUTLINE

ETHICAL HACKING
Certified Application Security Tester (CAST)

●●●● SPECIALIST-LEVEL COURSE | Cost: £2,600.00 + VAT | Duration: 4 days

SYLLABUS

1. **Introduction to web applications**
   - **a.** HTTP protocol
   - **b.** Authentication
   - **c.** Authorisation
   - **d.** Cookies

2. **Authentication**
   - **a.** Types of authentication
   - **b.** Clear text HTTP protocol
   - **c.** Advanced username enumeration/brute force issues
   - **d.** Security through obscurity

3. **Authorisation**
   - **a.** Session management issues
   - **b.** Weak ACLs
   - **c.** Cookie analysis

4. **SSL misconfigurations**
   - **a.** Attacks on SSL
   - **b.** TLS renegotiation
   - **c.** MD5 collisions

5. **Security problems with thick client applications**
   - **a.** Insecure design
   - **b.** Echo Mirage, MiTM, replaying traffic etc.

6. **Web/application server issues**
   - **a.** IIS/Apache/OpenSSL exploitation
   - **b.** Oracle application server exploits (bypass exclusion list etc)
   - **c.** Insecure HTTP methods
   - **d.** WebDAV issues

7. **Cross-site scripting**
   - **a.** Types of XSS
   - **b.** Identifying XSS
   - **c.** Exploiting XSS
   - **d.** Secure cookie, HTTP-only

8. **Advanced XSS**
   - **a.** Advanced XSS exploitation
   - **b.** Pitfalls in defending XSS
   - **c.** Fixing XSS

9. **Cross-site request forgery**
   - **a.** Identifying/exploiting CSRF
   - **b.** Complicated CSRF with POST requests
   - **c.** CSRF in web services
   - **d.** Impact
   - **e.** Fixing CSRF

10. **Session fixation**
    - a Cookie fixation
    - **b.** Faulty log-out functionalities

11. **CRLF injection**
    - **a.** Proxy poisoning
    - **b.** XSS with CRLF injection

12. **Clickjacking**
    - a Impact of clickjacking and proof of concept

13. **SQL injection**
    - **a.** Introduction to SQL injection
    - **b.** Impact: Authentication bypass
    - **c.** Impact: Extracting data (Blind SQL Injection, UNION injection, OOB channels)
    - **d.** OS code execution (MS-SQL, MySql)
    - **e.** SQL injection within stored procedures, parameterised statements
    - **f.** Places where you never thought SQLI could occur
    - **g.** Pitfalls in defending SQL injections
    - **h.** Fixing SQL Injections

14. **Malicious file uploads**
    - **a.** File uploads
    - **b.** IIS zero-day
    - **c.** Hacking unprotected application servers

15. **Vulnerable flash applications**

16. **Business logic bypass**
    - **a.** Authentication bypass
    - **b.** Insecure coding
    - **c.** Other logical flaws

17. **OS code execution**

18. **Remote/local file inclusion**
    - **a.** File inclusion
    - **b.** OS code execution

19. **Direct object reference**

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, and to make a booking, contact our education team on 01763 285 285 or email