



Certified Application Security Tester



An advanced 3 day web hacking course designed for penetration testers, security researchers and security professionals who need to learn the art of hacking web applications.

This hands-on course helps you gain in-depth knowledge on how to identify security vulnerabilities and subsequently identify the real risk of these vulnerabilities by exploiting them. The course also covers the syllabus for the CREST Certified Tester exam (application).

The training provides attendees a collection of modern hacking tools required for conducting a complete web application security assessment.

Prerequisites

- Certified Security Testing Associate (CSTA)
- Certified Security Testing Professional (CSTP)

To Book Call:

0870 600 1667

Duration: 3 days

Cost: £1498.50 + VAT

Course Syllabus:

1. Introduction to Web Applications

- a. Authentication
- b. Authorisation
- c. Cookies
- d. HTTP protocol
- e. Overview of Google hacking

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. SSL and man-in-the-middle attacks
- b. TLS renegotiation, %00 byte issue
- 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. Hacking with Metasploit
- d. Insecure HTTP methods
- e. WebDAV issues

7. Cross Site Scripting

- a. Types of XSS
- b. Identifying XSS
- c. Exploiting XSS
- d. Advanced XSS exploitation with beef and XSS-Shell
- e. Secure cookie, HTTP-only

8. Advanced XSS

- a. Pitfalls in defending XSS
- b. 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

13. SQL Injection

- a. Introduction to SQL Injection
- b. Impact: Authentication bypass
- c. Impact: Extracting data (Blind SQL Injection, UNION tricks, OOB channels)
- d. OS Code Execution (MS-SQL, MySQL, Oracle)
- e. SQL Injection within stored procedures, parameterized 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

- a. Insecure cross-domain requests
- b. Flash XSS

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

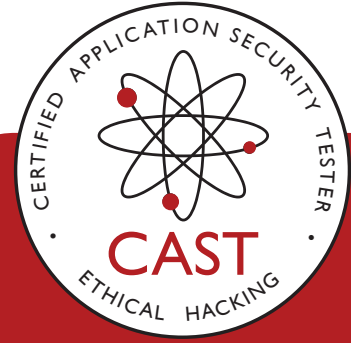
20. Capture The Flag Session

Professional Training Authored By Experts



CPE Credits: 24

Professional Penetration Tester Track



Helps prepare you for the
CREST Registered Tester qualification



Helps prepare you for the
CREST Certified Tester (Application) qualification

