Certified Web Application Security Tester (C-WAST)

COURSE OUTLINE

Module 1 Web Application Testing Software - Part 1

- Web Application testing software Preview
- Tamper Data
- Live HTTP header
- Firebug
- Hackbar
- HCON STF Framework Preview
- BurpSuite
- Google Hacking
- Google Hacking Practical

Module 2 Web Application Security - Part 2

- XSF Theory
- XSF DEMO
- Insecure Direct Object Reference (IDOR)
- Insecure Direct Object Reference Demo
- SQL injection Preview
- SQL Injection DEMO
- File Inclusion Preview
- File Inclusion LFI
- File Inclusion RFI
- DOM XSS Presentation
- DOM XSS DEMO

Module 3 SQL Protection - Bypass Attacks

- SQL Injection Bypass

Module 4 Web Application Shell Detection Bypass

- Bypassing File get type method
- Bypassing htaccess protection
- FileSize Protection Mechanism - Bypass

Module 5 Shell Upload Bypass (Firewall - Modsecurity & Antivirus Bypass)

- Modsecurity Bypass
- Web server Antivirus Bypass

Module 6 Symlink Bypass Attack

- Symlink Bypass Attack

Module 7 Xenotix - Cross Scripting Scanner & Exploiter

- Xenotix Theory Preview
- Xenotix Practical

Module 8 IronWasp - Web Apps Scanner Theory

- Ironswasp theory Preview
- Ironwasp Demo

Module 9 Web Exploitation Software

- D2 Elliot - Vulnerability Scanning and Exploitation Tool – Installation
- D2 Elliot - Vulnerability Scanner - Exploitation

Module 10 Anonymous Browsing and Testing using TOR

- Anonymous Browsing and Testing using ToR

Module 11 OWASP Top10 Introduction

- OWASP Top10 - Introduction