



[Back to Product Page](#)

Pen. Testing Websites and Databases Course

1 Sessions -

3 Hours of Interactive Training

Pen Testing Websites and Databases training course is the 4th course in the CPTEngineer series which is based on 5 key elements of Pen Testing; information, gathering, scanning, enumeration, exploration and reporting. In this course you will; learn to understand SQL Injections and SQL Injection enumeration. Learn Metasploit and other database direct attack tools. This course is part four of five training series that will help prepare you to pass the CPTEngineer Certification Exam, formerly known as CPTS.

Benefits

- Learn and master SQL Injections
- Learn and master tools like; N-Stalker, NTO Spider and other web assessment tools
- Learn how attackers use specific techniques to retrieve sensitive information

About The Author

Session 1

Section A: The Essence of SQL Injection

- Databases
- Vulnerabilities / Common Attacks
- SQL Injections
- Impacts of SQL Injection
- Business Impacts of SQL Injection
- Using SQL Injection
- SQL Injection Enumeration
- Extended Stored Procedures
- Lee Lawson Video

Section B: Direct Attacks and Protection

- Direct Attacks
- Attacking Database Servers
- Obtaining Sensitive Information
- Hacking Tools
- Oracle Security Tips
- Metasploit
- Metasploit Demo
- Finding and Fixing SQL Injections
- Hardening Databases

Section C: SQL Injection in Action

Section E: Most Common Attacks Illustrated

- Vertical Privilege Escalation
- XSS: Cross-Site Scripting
- Business Impacts of XSS
- Finding/Fixing XSS
- Injection Flaws
- Unvalidated Input
- Unvalidated Input Illustrated
- Business Impacts of Unvalidated Input
- Finding/Fixing Unvalidated Input
- Attacks Against IIS
- Unicode

Section F: Tools of the Trade Part I

- N-Stalker
- NTOSpider
- Free Web Assessment Tools
- N-Stalker Demo
- HTTPTrack
- Wikto

Section G: Tools of the Trade Part II

Duane Anderson, for the last two decades, has been working in the IT Security Training and Consulting Arena. He has worked with US and foreign military branches, U.S. government agencies, banking and regulated industries and fortune 500 companies. Duane has contributed to mile2's security curriculum with Certified Penetration Testing Engineer, Certified Digital Forensics Examiner and Certified Wireless Security Engineer. In addition, he has coordinated and executed IT counter-hacking & security courses for the US Marine Corps, US Army, US Air Force, U.S. Treasury, Sprint, IBM, Washington Mutual and Service Canada. Duane brings a vast wealth of experience and holds the following professional qualifications -- Security+, CPTS, CPTE, CDFE, CEH and Mile2 Certified Instructor.

- Injection Attack
- Injection Attack Demo
- Joel Helkason Video

Section D: Attack Methods

- Web Server Market Share
- Common Web App Threats
- Progression of the Professional Hacker
- Anatomy of a Web Application Attack
- A Generic Web Application System
- Query Strings
- URL Mappings to Web Application Systems
- Penetration Methodologies

- Paros Proxy
- Paros Proxy Demo
- Burp Proxy
- Dictionary Maker/ Cookies
- Acunetix Web Scanner
- Eclipse for Code Review
- OWASP WebScarab
- Samurai Web Testing