INFOSECTRAIN

APPLICATION SECURITY ENGINEER

COURSE CONTENT

sales@infosectrain.com | www.infosectrain.com

Course Content

1. **Security Fundamentals : EC-Council CEH**
2. **Advanced Web Applications**
3. **Exploit Development Basics** (Python Shell Script)
4. **Application Security Governance**

Security Fundamentals : EC-Council CEH

- Essentials of security, touching base on various security terminologies
- Understanding various attack methodologies and techniques used by offenders/hackers in the real world
- In-depth understanding of various aspects of the cybersecurity field
- Hands-on experience on various industrial tools used for these purposes
- CEH
  - **Module 01:** Introduction to Ethical Hacking
  - **Module 02:** Footprinting and Reconnaissance
  - **Module 03:** Scanning Networks
  - **Module 04:** Enumeration
  - **Module 05:** Vulnerability Analysis
  - **Module 06:** System Hacking
  - **Module 07:** Malware Threats
  - **Module 08:** Sniffing
  - **Module 09:** Social Engineering
  - **Module 10:** Denial-of-Service
  - **Module 11:** Session Hijacking
  - **Module 12:** Evading IDS, Firewalls, and Honeypots
  - **Module 13:** Hacking Web Servers
  - **Module 14:** Hacking Web Applications
  - **Module 15:** SQL Injection
  - **Module 16:** Hacking Wireless Networks
  - **Module 17:** Hacking Mobile Platforms
  - **Module 18:** IoT Hacking
  - **Module 19:** Cloud Computing
  - **Module 20:** Cryptography

Advanced Web Applications

- Understanding and identification of vulnerabilities
- Techniques for the exploitation of vulnerabilities

  Understanding OWASP top 10
- Hands-on experience on various tools to develop deeper conceptual understanding by performing web-based attacks

- **Web Application Penetration Testing**
  - Web Application Assessment
    - OWASP Top 10 Vulnerabilities
    - Threat Modelling Principle
    - Site Mapping & Web Crawling
    - Server & Application Fingerprinting
    - Identifying the entry points
    - Page enumeration and brute forcing
    - Looking for leftovers and backup files
  - Authentication vulnerabilities
    - Authentication scenarios
    - User enumeration
    - Guessing passwords – Brute force & Dictionary attacks
    - Default users/passwords
    - Weak password policy
    - Direct page requests
    - Parameter modification
    - Password flaws
    - Locking out users
    - Lack of SSL at login pages
    - Bypassing weak CAPTCHA mechanisms
    - Login without SSL
  - Authorization vulnerabilities
    - Role-based access control (RBAC)
    - Authorization bypassing
    - Forceful browsing
    - Client-side validation attacks
    - Insecure direct object reference

- Improper Input Validation & Injection vulnerabilities
  - Input validation techniques
  - Blacklist VS. Whitelist input validation bypassing
  - Encoding attacks
  - Directory traversal
  - Command injection
  - Code injection
  - Log injection
  - XML injection – XPath Injection | Malicious files | XML Entity
  - bomb
  - LDAP Injection
  - SQL injection
  - Common implementation mistakes – authentication
  - Bypassing using SQL Injection
  - Cross Site Scripting (XSS)
  - Reflected VS. Stored XSS
  - Special chars – ' & < >, empty
- Insecure file handling
  - Path traversal
  - Canonicalization
  - Uploaded files backdoors
  - Insecure file extension handling
  - Directory listing
  - File size
  - File type
  - Malware upload
- Session & browser manipulation attacks
  - Session management techniques
  - Cookie based session management
  - Cookie properties
  - Cookies – secrets in cookies, tampering
  - Exposed session variables
  - Missing Attributes – httpOnly, secure
  - Session validity after logoff
  - Long session timeout
  - Session keep alive – enable/disable
  - Session id rotation

  - Session Fixation
  - Cross Site Request Forgery (CSRF) – URL
  - Encoding
  - Open redirect

- Information leak
  - Web Services Assessment
  - Web Service Testing
  - OWASP Web Service Specific Testing
  - Testing WSDL
  - Sql Injection to Root
  - LFI and RFI]
  - OWASP Top 10 Revamp

Exploit Development Basics (Python Shell Script)

Shell Scripting

- Shell script architecture, /bin/bash, ZSH, CSH
- Integrating Linux command with shell scripts, Batch files, Execute permission, chmod,
- Shell script with I/O operations, Loops and statements, Arrays
- Concept of piping, Working with functions, String Function, File Handling and Regular Expressions

Python Scripting

- Introduction to Python, Variables & Values
- Python Libraries-Scapy
- Concept of OOPs in Python
- Exception Handling
- Standard I/O operations, File Handling, Regular Expressions
- Loop and Conditional Statements, Functions and Command Line Arguments, Network Sockets

Application Security Governance

- SSDLC (Secure software development lifecycle)
- Risk Based approach in software development
- Understanding Business Logic Testing
- Stepping Beyond OWASP top 10
- SAST based Approaches
- DAST based approaches