Application Security Testing

Hands-On | 60+ Hours, 10 Days | "WASD" & "ASTE" Exam Attempt | Online LAB Access

Laptop Required | Aligned with OWASP Application Security Testing Requirements

Hack2Secure's Workshop on Application Security Testing provides hands-on exposure using Simulated Lab Environment required for understanding and analysis of different Application Security Risk and Attack vectors.

Scoped around **OWASP Web & Mobile Application Security Testing Requirements** along with **Web Services**, these intensive practical oriented sessions provide deep-dive on required practical tips and tricks to evaluate, test and assess Application Security flaws.

Key Take Away

- OWASP Top10 (Web & Mobile) Security Risk
- Web Services & API Security Testing
- Application Reconnaissance, Scanning and Fingerprinting
- Authentication & Authorization Risk
- Common Application Security Risk
    - SQL Injection
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Session Management Flaws
- Application Security Tools:
    - Burp Suite & Zed Attack Proxy
    - Nikto, XSSer, SQLMap, W3af
    - Nmap, Netcat, Recon-Ng
- SSL/TLS: Handshake & Testing Methods
- IPSec Protocol & Usage
- Buffer Overflow Attacks
- Web Application Filters & Firewalls
- Threat Modeling for Secure Design

What You Will Receive

- **Instructor Led Classroom Sessions**
- **Soft Deliverables**
    - Program Slides & Lab Guides
    - Reference Documents
- **Online Lab Access** [30 Days]
- **WASD & ASTE Certificate Attempt Voucher**
    - 1 Attempt, 6 months Validity
    - Globally Proctored and Delivered by Pearson VUE
- Access to **Self-Paced Online Sessions** on Application Security Testing
- **Training Completion Certificate**

Who Should Attend

- Security Team/Office
    - Security Engineers, Testers, Analyst
    - Security Managers, Consultants, Auditors
- Research & Development Team
    - Architects, Developers, Testers (QA)
    - Software Consultants, Research Engineers
    - Team Leads, Technical Managers
- Students
    - Looking to pursue career in Application Security Assessment/Testing
- Anyone
    - who wants to explore Application Security Testing Tools, Techniques and Practices

Detailed Curriculum

Module#1: Application Security Testing: Introduction

- Understanding the Web
- Application Security Testing
  - Importance, Current Approach
- HTTP Protocol
  - History, Versions, Status Codes
  - Request Methods
- HTTPS Protocol
  - Introduction, PKI, SSL/TLS Handshake
  - Testing Methods
- Proxy Servers
  - Burp Suite, Zed Attack Proxy (ZAP)

Module#2: Introducing OWASP

- About OWASP
- Top10 Web & Mobile Security Risk
- Testing Framework
- Testing Guide: Walkthrough

Module#3: Securing Web Services

- About Web Services & Testing Requirements
- SOAP/XML, REST/JSON
  - Features, Usage and Security Concerns
  - Attack Scenarios
- AJAX Technologies
  - About, Features and Security Concerns
  - Attack Scenarios
- Security Best practices

Module#4: Reconnaissance

- Why Information Gathering
- DNS Protocol
  - Overview, Zone Transfer, Analysis & Scan
- Exploring Google Search
  - Keywords, Filters, GHDB
- Website Mirroring, Httrack
- Internet Connected Devices, Shodan
- The-Harvester, Recon-Ng

Module#5: Looking for Entry Point

- Scanning & Fingerprinting
  - Nmap: Identify Ports, Services
  - Netcat
- Spidering/Crawling
- Fuzzing: About, What to Look for
- Directory Browsing

Module#6: Analyzing A.A.A. Concerns

- Authentication
  - About, Schemes, Password Policies
  - Security Attacks
    - Username Harvesting
    - Cracking Weak Passwords
  - Best Practices, Case Studies
- Authorization
  - About, Access Control Types
  - Security Attacks
    - Privilege Escalation Attack
    - Directory Traversal Attack
    - Insecure Direct Object Reference
  - Best Practices, Case Studies
- Accountability
  - About, Secure Logging Practices
  - Case Studies

Module#7: Session Management Flaws

- Stateless Nature of HTTP
- “Sessions” & Tracking Methods
- Attacks on Sessions
  - Fixation, Hijacking, Tampering
- Securing Cookies & Headers
- Best Practices, Case Studies

Module#8: Injection Attacks

- SQL Query: Primer
- SQLi Attack:
  - About, Root Cause, Types, Analysis
- Command Injection
  - About, Root Cause, Analysis
- Injection Scenarios in
  - Web & Mobile Applications
  - Rich Interface Application [HTML5]
- SQLMAP
- Local/Remote File Inclusion Vulnerability]
- Security Best practices & Mitigation Controls

Module#9: Cross Site Scripting (XSS)

- JavaScript: Primer
- Same Origin Policy, Document Object Model
- XSS Attack:
  - About, Root Cause, Types, Analysis
- XSS Scenarios in
  - Web & Mobile Applications
  - Rich Interface Application [HTML5]
- HTML Injection
- Security Best practices & Mitigation Controls

Detailed Curriculum

Module#10: Cross Site Request Forgery (XSRF)

- XSRF Attack:
  - What, Why & How, Myths
- Implementing Defensive Measures
  - CSRFToken, Double Submission Cookies
- XSRF Scenarios in
  - Web & Mobile Applications
  - Rich Interface Application [HTML5]

Module#11: Buffer Overflow Attacks

- Heap & Stack Overflow
- Format String Vulnerabilities

Module#12: Scanners & Frameworks

- W3af, Metasploit Framework

Module#13: Web Application Filters and Firewall (WAF)

- Web Application Defenses: Filtering & Firewall
- Filtering
  - .NET & ESAPI Filtering Options
- Web Firewall
  - Types, Detection & Attack methods

Module#14: Python for WAST

- Python: Primer
- Python to craft HTTP Packets & Attacks
- Scapy
  - About, Usage
  - Network Packet Crafting & Analysis

Module#15: Application Threat Modeling

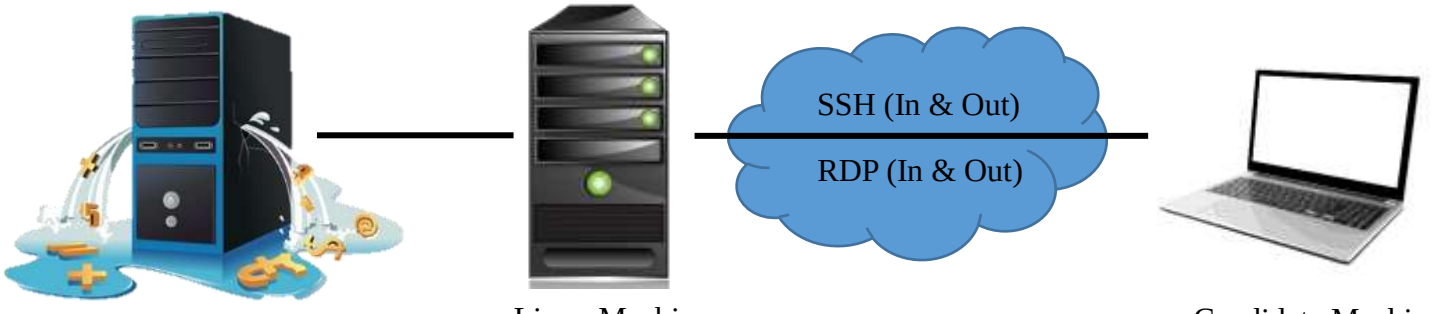
- About S.T.R.I.D.E
- Attack Surface Analysis
- Threat Modeling
  - Process & Workflow
  - Threat Considerations in an Application
    - Web & Mobile Clients
    - API Communication
  - Threat Modeling: Workshop

Module#16: IPSec & VPN

- IPSec
  - About, Usage
- SSL & IPSec VPN

Online Lab Layout

Cloud Based | Independent Setup for Each Participant | Accessible for 30 Days



Vulnerable Web Server
(Target Machine)

Linux Machine
(Client/Attacker)

Candidate Machine

Application Security Certification Programs

Web Application Security Defender (WASD)

Globally delivered & Proctored with PearsonVUE | 180 mins, 90 MCQ | Passing Grade: 60%

Hack2Secure

Web Application Security Defender

Application Security Testing Expert (ASTE)

Globally delivered & Proctored with PearsonVUE | 180 mins, 90 MCQ | Passing Grade: 60%

Hack2Secure

Application Security Testing Expert

Benefits

- Validates your practical expertise and knowledge in Application Security Risk and Testing measures
- Get Global Recognition and Credibility
- Ensures Real Time skills required to detect, test and mitigate Application Security flaws
- Demonstrate knowledge of Industry Standards and Best Practices
- Ensures effective skills to measure and implement Security Controls

Attempt to WASD & ASTE Exam is **included** as part of Application Security Testing Training Program from Hack2Secure

1 Attempt | 6 months Voucher Validity

Delivered globally at Pearson VUE Authorized Test Centres

Pearson | VUE

For more details, **www.hack2secure.com** | **www.pearsonvue.com/hack2secure**

About Hack2Secure

Hack2Secure excels in "Information Security" Domain and offers customised IT Security programs, including Training, Services and Solutions. Our programs are designed by industry experts and tailored as per specific needs. We help students, professionals and companies with knowledge, tools and guidance required to be at forefront of a vital and rapidly changing IT industry.

InfoSec Training

Vendor Independent, Customizable, Across Domains

Hack2Secure excels in delivering intensive, immersion security training sessions designed to master practical steps necessary for defending systems against the dangerous security threats. Our wide range of fully customizable training courses allow individual to master different aspects of Information Security as per their industry requirement and convenience.

- Delivered Training to more than 15k+ Professionals Globally
- Customizable Security Training Programs, aligned with Business Requirements

InfoSec Certification

- Globally delivered and Proctored Security Certification programs with **PearsonVUE**
- Vendor Independent Programs based on Industry Security Standards and Practices

InfoSec Services

Hack2Secure offers IT Security Professional Services to provide ways to stay ahead of Security Threats through adaptive and proactive Security methods like

- Secure Software Development Lifecycle
- Secure Application Design & Threat Modeling
- Application Security Testing
- Risk Assessment, Consulting

hack2secure

+91 (80) 49 58 32 99
+91 (80) 49 58 33 99

Hack2Secure featured as:

25 FASTEST GROWING CYBER SECURITY COMPANIES IN INDIA
Source: The CEO Magazine, India

10 BEST SECURITY COMPANIES in INDIA: 2017
Source: Silicon Review Magazine, India

EXCELLENCE IN SECURITY TRAINING PROGRAMMES
Source: GDS Review Magazine