Application Security Testing Workshop

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

Laptop Required | Aligned with OWASP (Web & Mobile) 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
- SOAP/XML, REST/JSON, AJAX Security Testing
- Reconnaissance, Scanning & Fingerprinting
- A.A.A. & Session Management Flaws
- SQLi Attack Types & Testing Methods
- XSS Attack Types & Testing Methods
- XSRF Attack & Testing Methods
- SSL/TLS: Handshake & Testing Methods
- IPSec Protocol & Usage; SSL/IPSec VPN
- Buffer Overflow Attacks
- Web Application Filters & Firewalls
- Python & JavaScript for Web Security Testing
- Nikto, XSSer, SQLMap, W3af
- Nmap, Netcat, Recon-Ng

What You Will Receive

- **Instructor Led Classroom Sessions**
- **Soft Deliverables**
  - Program Slides & Lab Guides
  - Reference Documents
- **Online Lab Access** [30 Days]
- **WASD & ASTECertificate 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 and Testers
  - Application Security Analyst
  - Security Managers, Consultants, Auditors
- Research &Development Team
  - Architects, Developers
  - Software Testing Team (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

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

Laptop Required | Aligned with OWASP (Web & Mobile) Application Security Testing Requirements

Detailed Curriculum

Module#1: Application Security Testing: Introduction

- Understanding the Web
- Importance of Application Security Testing
- Application Security Testing :Current Approach
- HTTP Protocol
  - History, Versions, Status Codes
  - Request Methods **[LAB]**
- HTTPS Protocol
  - Introduction, PKI, SSL/TLS Handshake
  - Testing Methods **[LAB]**
- Proxy Servers
  - Burp Suite **[LAB]**
  - Zed Attack Proxy **[LAB]**

Module#2: Introducing OWASP

- About OWASP
- OWASP Top10 (2017) Web Security Risk**[LAB]**
- OWASP Top10 (2016) Mobile Security Risk**[LAB]**
- OWASP Testing Guides: Walkthrough

Module#3: Securing Web Services

- About Web Services & Testing Requirements
- SOAP/XML, REST/JSON
  - Features, Usage and Concerns
  - Testing Attack Scenarios **[LAB]**
- AJAX Technologies
  - About, Features and Security Concerns
  - Testing Attack Scenarios **[LAB]**
- Possible Threats on Web Services
- Security Best practices

Module#4: Reconnaissance

- Why Information Gathering
- DNS Protocol
  - Overview, Zone Transfer
  - Analysis & Scan **[LAB]**
- Exploring Google Search **[LAB]**
  - Keywords & Filters
  - Google Hacking Database (GHDB)
- Website Mirroring **[LAB]**
- Internet Connected Devices [**LAB: Shodan**]
- The-Harvester, Recon-Ng **[LAB]**

Module#5: Looking for Entry Point

- Scanning
  - Identify Ports, Services **[LAB]**
- Fingerprinting Web Server **[LAB]**
- Spidering/Crawling **[LAB]**
- Fuzzing
  - About, What to Look for
- Directory Browsing **[LAB]**

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

- Authentication
  - About, Password Policies
  - Different Schemes **[LAB]**
  - Username Harvesting **[LAB]**
  - Cracking Weak Passwords **[LAB]**
- Authorization
  - About, Access Control Types
  - Privilege Escalation due to HTTP Header **[LAB]**
  - Directory Traversal Attacks **[LAB]**
  - Insecure Direct Object Reference **[LAB]**
- Accountability
  - About, Secure Logging practices

Module#7: Session Management Flaws

- Stateless Nature of HTTP
- “Sessions” & Tracking Methods
- Attacks on Sessions
  - Fixation, Hijacking, Tampering **[LAB]**
- Securing Cookies & Headers**[LAB]**
- Testing Session Security **[LAB]**

Module#8: Injection Attacks

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

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

Laptop Required | Aligned with OWASP (Web & Mobile) Application Security Testing Requirements

Module#9: Cross Site Scripting (XSS)

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

Module#10: Cross Site Request Forgery (XSRF)

- XSRF Attack:
  - What, Why & How
- Defensive Measures like CSRFToken etc
- XSRF Scenarios in
  - Web & Mobile Applications**[LAB]**
  - Rich Interface Application [HTML5] **[LAB]**
- Security Best Practices

Module#11: IPSec & VPN

- IPSec: About, Usage
- SSL & IPSec VPN

Module#12: Buffer Overflow Attacks

- Heap & Stack Overflow
- Format String Vulnerabilities **[LAB]**

Module#13: Scanners & Frameworks

- W3af **[LAB]**
- Metasploit Framework **[LAB]**

Module#14: Web Application Filters and Firewall (WAF)

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

Module#15: Python & Scapy

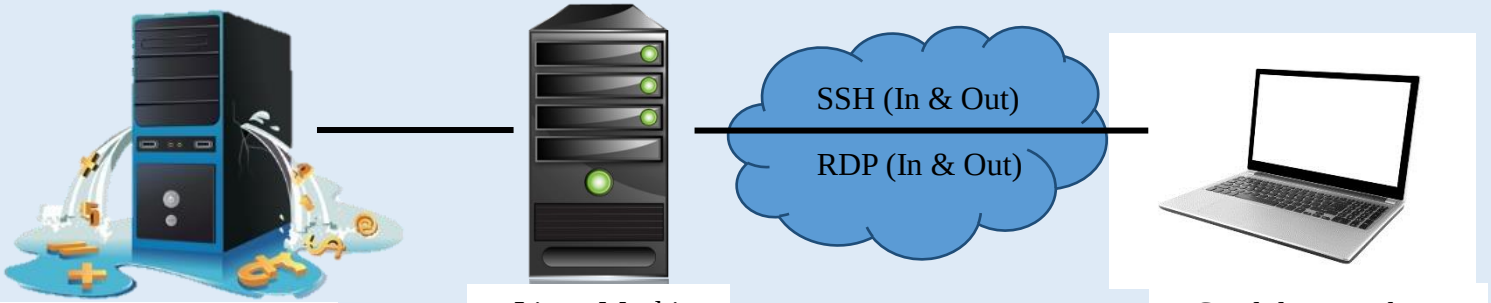
- Python for Web Security Testing
- Crafting Network Packets with Scapy

Module#16: Application Threat Modeling

- About S.T.R.I.D.E
- Threat Modeling
  - Process & Workflow
  - Threat Considerations in an Application
- Threat Modeling Demo **[LAB]**

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 SecurityTesting Certification

Web Application Security Defender (WASD)

Globally Available | Proctored | 180 mins. | 90 MCQ | Passing Grade: 60% | Exam Language: English

Hack2Secure

Web Application Security Defender

Application Security Testing Expert (ASTE)

Globally Available | Proctored | 180 mins. | 90 MCQ | Passing Grade: 60% | Exam Language: English

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 TestingTraining Program from Hack2Secure

1 Attempt | 6 months Voucher Validity

Delivered globally at Pearson VUE Authorized Test Centres

Pearson | VUE

To Schedule WASD& ASTE Exam,
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 in-

Security 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
- Vendor Independent programs aligned with Industry Security Practices and Requirements

Security Certification

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

End-to-End Security 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.
- Network/Infrastructure Risk Assessment.
- Consulting

skype **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

About Vértice Infosystems

Vértice Infosystems, a growing IT application and services providing company, based in Pune, India.

Vértice Infosystems teams excels in multiple domains and offers development of customized IT Applications, Mobile Applications, Software Testing, and IT Services & Solutions.
Vértice Infosystems also provides Security trainings and certification courses under partnership program with Hack2Secure.

Corporate Training

Vértice Infosystems provides corporate trainings in following field

- Application Security (**Accredited Training Partner – Hack2Secure**)
- Agile Methodology
- SAS
- CRM
- Team Edifice Programs
- Life Coaching

Training Programs for Institutions

- Security Lab Workshop
- Soft Skill Development
- Student Counselling
- Virtualization Technologies

Training Programs For Individual

- Oracle
- Big Data – Hadoop
- Application Security
- CRM
- SAS

IT Services & Solutions

Vértice Infosystems teams excels in multiple domains and offers development in following fields

- Business Development
- Information Technology
- Mobile Technology
- Web Designing and Web Hosting
- Software Testing

Phone: +91 88301 17402
Web : www.verticeinfosystems.com