Web Application Security Testing (WAST)

Hands-On | 42 Hours, 7 Days |WASD Exam Attempt | Online LAB Access

Laptop Required | Aligned with OWASP Top10 (2017) & Testing Guide (v4)

Hack2Secure's Workshop on Web Application Security Testing provides hands-on exposure using Simulated Lab Environment required for understanding and analysis of different Web Security Risk and Attack vectors. Scoped around **OWASP Top 10 (2017) Web Security Risk** and **Security Testing Guide (v4)**, these intensive practical oriented sessions provide deep-dive on required practical tips and tricks to evaluate, test and assess Web Application Security flaws.

Key Take Away

- Active and Passive Reconnaissance methods
- SSL/TLS Handshake and Testing methods
- Scanning, Fingerprinting and Spidering
- Exploring A.A.A. Concerns
- Session Management and related Attacks
- SQL & Command Injection
- Cross Site Scripting (XSS)
- Cross Site Request Forgery
- Exploiting Web Services & APIs
- Buffer Overflow Attacks
- Web Application Filters & Firewalls
- Burp Suite and Zed Attack Proxy (ZAP)
- Metasploit Framework, W3af
- Nikto, XSSer, SQLMap
- NMAP, NETCAT, Recon-ng
- Python and Java Script for Security Testers

What You Will Receive

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

Who Should Attend

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

Detailed Curriculum

Module#1: Building the Base [Concepts, Processes & Methodologies]

- Understanding the Web
- Importance of Web Application Security
- Web Application Security Testing (WAST): Current Approach
- Proxy Servers
  - Burp Suite **[LAB]**
  - Zed Attack Proxy **[LAB]**
- HTTP Protocol
  - History, Versions, Status Codes
  - Request & Response Analysis **[LAB]**
- HTTPS Protocol
  - Introduction, SSL/TLS handshake
  - Testing Methods**[LAB]**
  - Vulnerability Case Study: HeartBleed
- About OWASP
  - OWASP Top10 (2017) Web Application Security Risk **[LAB]**
  - OWASP WAST Guide: Walkthrough

Module#2: Casual Leakage Points [Reconnaissance]

- Why Information Gathering
- DNS Protocol:
  - Overview, Zone Transfers
  - Analysis & Scan **[LAB: Whois, Nslookup]**
- Open Source Intelligence
- Exploring Google Search**[LAB]**
  - Keywords & Filters
  - Google Hacking Database (GHDB)
- Website Mirroring**[LAB: Httrack]**
- Internet Connected Devices**[LAB: Shodan]**
- TheHarvester & Recon-Ng **[LAB]**

Module#3: Looking for Entry Point [Scanning, Fingerprinting & Spidering]

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

Module#4: Analyzing A.A.A. Concerns

- Authentication
  - About, Password Policies
  - Different Schemes**[LAB]**
  - Username Harvesting**[LAB]**
  - Cracking Weak Passwords**[LAB]**
- Browser Cache Weakness
- Authorization
  - About, Access Control Types
  - Privilege Escalation Attack **[LAB]**
  - Insecure Direct Object References**[LAB]**
  - Directory Traversal Attacks**[LAB]**
- Accountability
  - About, Secure Logging Practices

Module#5: Session Management

- Stateless Nature of HTTP
- “Sessions” & Tracking Methods
- Attacks on Sessions
  - Fixation, Hijacking, Tampering**[LAB]**
- Securing Cookie& Headers**[LAB]**
- Testing Session Security**[LAB]**
- Cross Site Request Forgery
  - About & How it happens
  - Myths & Defensive Measures
  - Attack Scenario **[LAB]**

Module#6: Injection Attacks

- SQL Query: Primer
- SQL Injection (SQLi)
  - About, Root Cause, Analysis, Types
  - Attack Scenarios **[LAB]**
  - SQLMap **[LAB]**
- Command Injection:
  - About, Root Cause
  - Attack Scenario **[LAB]**
- [Local/Remote] File Inclusion Vulnerability**[LAB]**

Module#7: Python & Java Script for Web Security Testing

- Python & Java Script for WAST
- Python & Java Script to Craft Attacks **[LAB]**
- Explore SCAPY for Packet Crafting**[LAB]**

Hands-On | 42 Hours, 7 Days |WASD Exam Attempt | Online LAB Access

Laptop Required | Aligned with OWASP Top10 (2017) & Testing Guide (v4)

Module#8: Cross Site Scripting (XSS)

- Same Origin Policy
- Document Object Model (DOM)
- XSS
  - Overview, How it Works, Types
  - Testing Methods, Attack Scope**[LAB]**
- HTML Injection**[LAB]**

Module#9: Web Services & APIs

- About Web Services& Testing Requirements
- Explore JSON & AJAX: Usage and Features
- Web Security Attacks with SOAP Queries
  - SQLi & Command Injection **[LAB]**
- XSS in AJAX & JSON Objects **[LAB]**

Module#10: Buffer Overflow Attacks

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

Module#11: Scanners & Frameworks

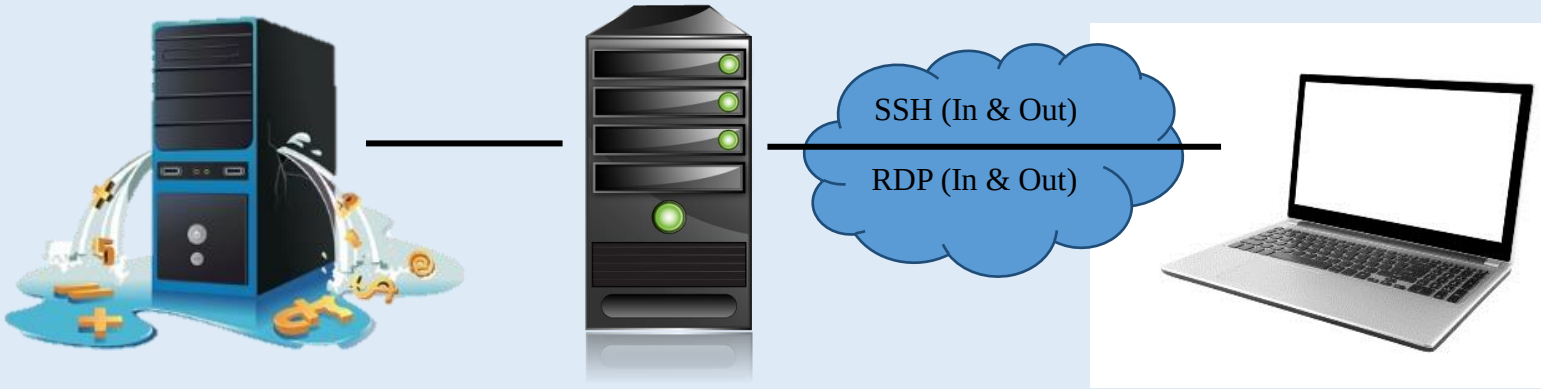
- W3af **[LAB]**
- Metasploit Framework **[LAB]**

Module#12: Web Application Filters and Firewall (WAF)

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

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

Web Application Security Defender

Evaluate your Skills in Web Application Security Assessment

Hack2Secure

Web Application Security Defender

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

Web Application Security Defender (WASD) Certificate program evaluates individual's implementation level skills required for Web Application Security Assessment.This program ensures candidate's awareness on Application Security Challenges, Risk, Tools, Techniques and methodologies along with hands-on practical level knowledge and skill-sets.

WASD is based on Application Security Industry Standards and Best Practices and ensures Knowledge and Understanding of Secure Web Application Assessment requirements. It walks through different phases/domains of Application Security Testing and provide required practical strategies and methodologies to evaluate Security at every level.

Benefits

- Validates your practical expertise and knowledge in Web Application Security Assessment
- Get Global Recognition and Credibility
- Ensures Real Time skills required to handle Web Application Security Risk
- Demonstrate knowledge of Industry Standards and Best Practices
- Ensures effective skills to measure and implement Security Controls

Attempt to WASD Exam is **included** as part of Web 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 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