Web Application Security Testing

42+ Hours | Online Lab Access | 'Web Application Security Defender' Cert Attempt

Aligned with OWASP Top 10 (2017) Risk, Testing Guide (v4) & Recommended Practices

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 Application Security Risk and Security **Testing Guide,** these intensive practical oriented sessions provide deep-dive on required testing tips and tricks to evaluate, test and assess Web Application Security flaws.

Key Take Away

- Injection Attacks | SQL, Command, OS Inj.
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (XSRF)
- Broken Authentication & Access Control
- Session Management and related Attacks
- Vulnerable External Entities (XXE)
- Client-Side Attacks

- Web Reconnaissance Methods
- Google Hacking
- Spidering, Finger Printing & Scanning
- Web Application Filters & Firewalls
- Burp Suite & Zed Attack Proxy (ZAP)
- Nmap, NetCat, Recon-Ng
- XSSer, SqlMap, Nikto, W3af

What You Will Receive

- **Instructor Led Sessions**
  - Live Online | Class Room
- **Soft Deliverables**
- **WASD Cert Attempt Voucher**
  - 1 Attempt, 6 months Validity
  - Globally Delivered and Proctored across PearsonVUE Test Centers

- **Online Lab Access**
  - Cloud Based
  - 24X7, 30 Days Access
- Access to **Self-Paced Online Sessions**
- **Training Completion Certificate**
- **Post Session Technical Support**

For more details on Web Application Security Testing (WAST)

www.hack2secure.com/wast

Program Scope & Curriculum

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

- Web Application Security: Introduction
- Proxy Servers
  - Burp Suite, Zed Attack Proxy (ZAP)
- HTTP Protocol
  - History, Versions, Status Codes
  - Request & Response Analysis
- SSL/TLS Protocol
  - PKI: Introduction, Digital Certificates
  - About SSL/TLS, Handshake Process
  - Testing methods
- About OWASP
  - Top 10 Web Application Security Risk
    - Root Cause, Practical Analysis
    - Recommended Best Practices
  - Application Security Testing Framework
  - Web Application Testing Guide
    - Component & Scope

Module#2: Casual Leakage Points [Reconnaissance]

- Importance of Information Gathering
  - DNS Protocol: Overview, Analysis & Scan
- Open Source Intelligence
- Exploring Google Search (Google Hacking)
  - Keywords & Filters, Hacking Database
- Website Mirroring: Httrack
- Exploring Internet Connected Devices: Shodan
- Web Reconnaissance Tools
  - TheHarvester, Recon-Ng

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

- Web Scanning: Identify Ports & Services
  - NMap, Nikto
- Fingerprinting, Spidering/Crawling
- Web Application Fuzzing: Directory Browsing

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

- Authentication
  - About, Types, Different Schemes
  - Password Policies, Cracking Passwords
- Authorization
  - About, Access Control Types
  - Privilege Escalation Attack
  - Insecure Direct Object References
- Accountability
  - About, Secure Logging Practices

Module#5: Session Management

- "Sessions" & Tracking Methods
- Attacks on Sessions
  - Fixation, Hijacking, Tampering
- Securing Cookies & Headers
- Cross Site Request Forgery
  - About, how it happens, Attack Scenarios
  - Myths & Defensive Measures
    - CSRF Tokens, Double Submitted Cookies

Module#6: Injection Attacks

- SQL Query: Primer
- SQL Injection (SQLi)
  - About, Root Cause, Types & Analysis
  - Different Attack Scenarios
  - Automated Tool: SQLMap
- Command Injection:
  - About, Root Cause, Attack Scenarios
- [Local/Remote] File Inclusion Vulnerability

Module#7: Cross Site Scripting (XSS)

- JavaScript: Primer
- Same Origin Policy, Document Object Model
- XSS
  - Overview, Types & Analysis
  - Different Attack Scenarios
  - Automated Tool: XSSer
- HTML Injection
  - About, Root Cause, Attack Scenarios

Module#8: Web Services & APIs

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

Module#9: Web Filters and Firewall (WAF)

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

Module#10: Buffer Overflow Attacks

- Stack & Heap Overflow
- Format String Vulnerability

42+ Hours | Online Lab Access | 'Web Application Security Defender' Attempt

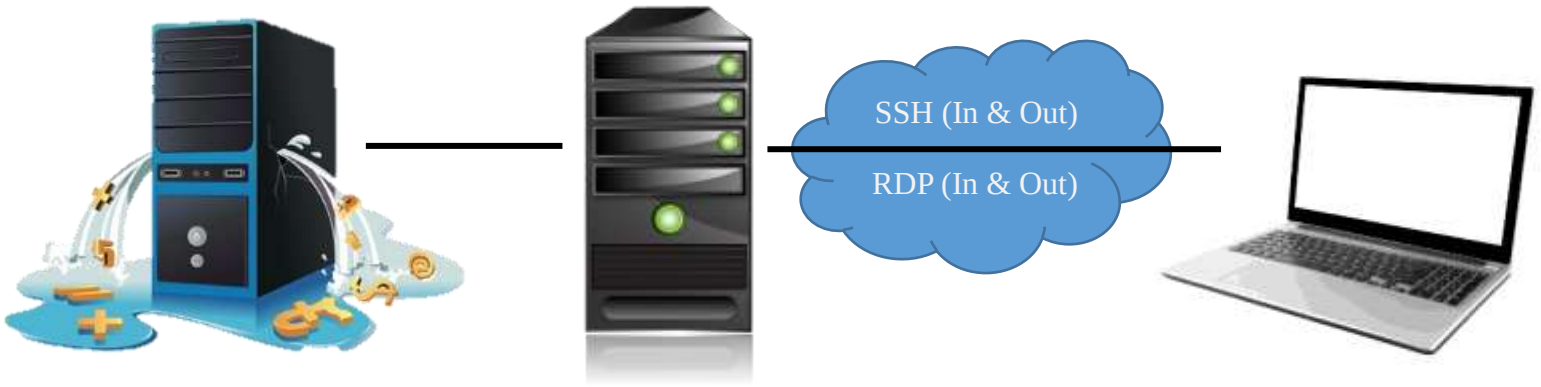
Aligned with OWASP Top 10 (2017) Risk, Testing Guide (v4) & Recommended Practices

Who Should Attend

- **Working Professional**
  - Looking to explore and adopt Web & Software Security Testing Practices
  - Looking to learn Web and Software Security Testing Tools, Techniques & Practices
- **Fresh College Graduate / Student**
  - Looking to learn skills & build career in Web Security Domain
- **Anyone**
  - Looking to explore Web Security concerns and attack scenarios
- **Software/Application Development Team**
  - Testing Team
    - QE/QA, Leads, Managers
  - Developers
    - Looking to get awareness on different Attack Scenarios
  - Analyst, Architects, Consultants
    - Looking to explore Web Security Risk & Impact analysis
- **Security Team/Office**
  - Penetration Testers, Auditors
  - Engineers, Analyst

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

For more details on Web Application Security Testing (WAST)

www.hack2secure.com/wast

Web Application Security Defender

Evaluate your Web Security Essential Knowledge & Skills

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 Testing Training 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

For more details, visit **www.hack2secure.com/wasd**

www.hack2secure.com | **certificate@hack2secure.com**

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.

Hack2Secure
INSPIRE • INDUCE • INNOVATE

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.

InfoSec Certification

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

End-to-End 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
- 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

EXCELLENCE IN SECURITY TRAINING PROGRAMMES
Source: GDS Review Magazine