TRANCHULAS

Advanced Web Application Penetration Testing & Security Masterclass

Introduction

This hands-on, intensive course takes you from foundational web security concepts to advanced exploitation methodologies. Experience realistic attack scenarios faced by penetration testers and security professionals globally. Each learning phase builds upon practical labs using actual vulnerable applications, ensuring mastery of industry-standard tools and techniques.

Accreditations

Tranchulas Advanced Web Application Penetration Testing & Security Training is Assured Training in association with the National Cyber Security Centre (NCSC), UK. The course material has been rigorously assessed against the exacting standards of NCSC.

The quality of the trainers' delivery and the course administration has been quality checked and approved by APMG.

Additionally, Tranchulas is CREST Cyber Training Provider, further validating the excellence and credibility of our training offerings.

Assured Service Provider
in association with
National Cyber Security Centre
Training Course

CREST
CYBER
Training Provider

Course Objectives

By the end of this course, participants will be able to:

1. **Understand the foundations of web application security testing**, including penetration testing methodologies, ethical hacking principles, and industry best practices.
2. **Conduct systematic reconnaissance** of web applications using OSINT, architecture mapping, API endpoint discovery, and vulnerability scanning techniques.
3. **Identify and exploit common and advanced web vulnerabilities**, such as SQL injection, authentication bypasses, XSS, CSRF, server-side request forgery, and insecure file handling.

4. **Assess security in modern web technologies**, including REST/GraphQL APIs, cloud-native applications, and AI-driven platforms.
5. **Simulate real-world exploitation scenarios** by chaining vulnerabilities to achieve privilege escalation, data extraction, and full application compromise.
6. **Perform advanced manual testing for business logic flaws** that automated tools often miss.
7. **Document and communicate findings effectively**, producing professional reports that highlight both technical risks and business impact, tailored for executives and technical teams alike.

CWASP CERTIFICATION

This course leads to the **Tranchulas Certified Web Application Security Professional (CWASP)** certification. The CWASP exam is entirely practical. You will be placed in a controlled lab environment containing deliberately vulnerable web applications. To earn the certification, you must successfully exploit these applications, demonstrate a clear understanding of the attack vectors, and complete all required online lab exercises.

Course Outline

Module 1: General Concepts

- Introduction to the Web
- HTTP & HTTPS
- DNS and Domain Names
- Web Browser & Developer Tools
- Web Hosting & Web Standards
- Cookies and Sessions
- Burp Suite

Module 2: Kali Linux Installation & Vpn COnfiguration

- System Requirements
- VMWare Installation
- Kali Linux Installation
- VPN Configuration

Module 3: Introduction to Kali Linux

- Directory Structure & Files management
- Understanding Sudo in Linux
- Navigating the File System
- Network Services (ssh, vnc, apache, tftpd)
- File Transfers (SMB, Python3)

Module 4: Information Gathering

- Introduction
- Google Hacking
- Target Identification
- Subdomains & Subdomains Enumeration
- Shodan reconnaissance
- Site Mapping and Crawling
- Exercise: Attendees will do reconnaissance of target web application and build a profile, Attendees will identify entry points in target web applications running on Tranchulas Online Labs.

Module 5: Vulnerability Scanning

- Introduction
- Greenbone Vulnerability Scanner
- Nexpose LightVm Vulnerability Scanner
- Nessus Vulnerability Scanner
- Nuclei Vulnerability Scanner

Module 6: Command Injection

- Introduction to command injection vulnerabilities
- Detecting & Injecting commands
- Identifying and Bypassing Filters
- Command Injection Prevention
- Exercise: Attendees will execute attacks learned during this module on web applications in Tranchulas Online Labs

Module 7: File Inclusion

- Introduction to file inclusion
- Local File Inclusion (LFI)
- Bypassing Filters
- Remote File Inclusion (RFI)
- File Inclusion Prevention

Module 8: SQL Injection

- Introduction to SQL injection
- Error Based SQL Injection
- Union-Based Injection

- Time-Based Blind Injection
- NoSQL Injection
- SQL Injection Prevention
- Exercise: Attendees will exploit databases running on Tranchulas Online Labs

Module 9: File Upload Attacks

- Introduction to File Upload Attacks
- Identifying & Bypassing Filters
- LFI and File Uploads (RCE)
- File Upload Attacks Prevention
- Exercise: Upload a malicious file and get a reverse shell.

Module 10: Cross-Site Scripting (XSS)

- Introduction to Cross-Site scripting
- XSS Contents
- Reflected Cross Site-Scripting (XSS)
- Stored Cross Site-Scripting (XSS)
- DOM Cross Site-Scripting (XSS)
- Advance Techniques to Bypass WAF
- XSS Prevention
- Exercise: Attendees will plan and execute different XSS Attack Scenarios on target web applications in Tranchulas Online Labs

Module 11: XML External Entity (XXE) Injection

- Introduction to XML
- Exploiting XXE to read Server Files
- Bypassing Filters using PHP Wrappers
- XXE Prevention
- Exercise: Read files using XXE

Module 12: Login Brute Forcing

- Introduction to Login Bure Forcing
- Login Brute Forcing – Hydra
- Basic HTTP Authentication
- Login Brute Forcing – Burp Intruder
- Login Brute Forcing Prevention

- Exercise: Bypass authentication on Tranchulas Labs using login brute forcing.

Module 13: Cros-Site Request Forgery

- Introduction to CSRF
- How CSRF Works
- Delivering CSRF Exploit
- Exploiting CSRF
- Bypassing Filters
- Prevention Techniques
- Exercise: Reset a password on behalf of the victim
- Exercise: Command injection through CSRF

Module 14: Insecure Transport Layer Protection

- Understanding TLS/SSL Security
- Man-in-the-Middle (MitM) Attacks on HTTPS
- OpenSSL Heartbleed Attack (CVE-2014-0160)
- Mitigation & Best Practices

Module 15: Authentication & Authorization Attacks

- Understanding Authentication vs. Authorization
- IDOR Enumeration
- Bypassing Encoded References
- IDOR Prevention
- Exercise: Access profile of other users and fetch their data.

Module 16: Advance Web Attacks

- Introduction to SSRF
- Types of SSRF Attacks
- Exploiting SSRF Vulnerabilities
- Mitigation & Secure Development Practices

Module 17: Cloud Security Fundamentals

- Introduction to Cloud Security
- Cloud Service Models & Security Concerns
- Identity & Access Management (IAM) in Cloud
- Cloud Network Security

- Data Security & Encryption in the Cloud
- Cloud Threats & Attack Vectors
- Exercise: Investigating Cloud Security Breaches

Module 18: MFA Authentication Bypass

- Understanding Multi-Factor Authentication (MFA)
- Common MFA Bypass Techniques
- Advanced MFA Exploitation Techniques
- Mitigation & Defense Strategies
- Exercise: Analysis of successful MFA phishing campaigns.

Module 19: GraphQL API Security & Exploitation

- Introduction to GraphQL Security
- GraphQL Attack Surface
- Exploiting GraphQL APIs
- Mitigation & Secure Development Practices
- Exercise: Extracting Sensitive Data from GraphQL Endpoints

Module 20: LLM Web App Exploitation

- Introduction to Web LLM Security
- LLM Attacks Surface in Web Applications
- Exploiting Prompt Injection
- LLM Api Key Exposure
- Mitigation & Prevention

Module 21: JSON Web Tokens in Web Applications

- Introduction to JWT
- JWT Attack Surface
- Exploiting JWT Weakness
- Advance JWT Exploitation
- Mitigation & Prevention