



TRANCHULAS

WORKSHOPS AND TRAININGS

**HANDS-ON WEB APPLICATION
PENETRATION TESTING TRAINING
COURSE**

TRANCHULAS

Tranchulas is a multinational cyber security company having its offices in UK, USA, Australia and Pakistan. We are global provider of information security assessment, compliance, managed security and training services.

ABOUT THE TRAINER

Tranchulas training and workshops are conducted by world's top information security experts. Our instructors are featured speakers at renowned security conferences such as Hack in the Box Malaysia, InfoSek Slovenia, Hack.lu Luxembourg, CONFidence Krakow, Troopers, Shakacon, OWASP Europe and BruCON Belgium.

AUDIENCE

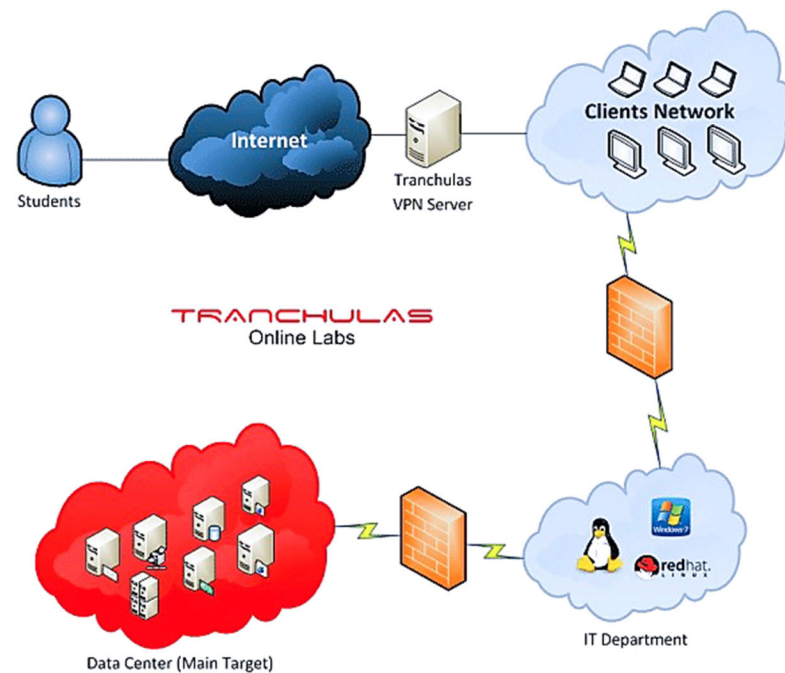
- Application Developers
- Application Security Managers
- Security Consultants
- QA Testers
- IT Managers
- Penetration Testers
- Any security professional who is interested in learning about web application security

PRE-REQUISITES

- Basic knowledge of HTML and Java Script
- Participants must bring their own laptops

TRANCHULAS ONLINE LAB

Tranchulas Online Labs are available 24x7 for practicing web attacks learnt during the training course. Online labs have several web applications based on real-world scenarios which can be exploited and have different difficulty levels. Vulnerabilities include but are not limited to XSS, SQL Injection, CSRF, cookie manipulation, local file inclusion. Students are required to discover and exploit vulnerabilities in order to pass online labs and receive Tranchulas Certified Web Application Security Professional (CWASP) Certification.



CWASP CERTIFICATION

Certified Web Application Security Professional (CWASP) is an exclusive certification which will test your technical skills on a live but simulated web application where you are expected to discover and exploit security vulnerabilities. Students are required to pass our online lab test in order to receive CWASP.

CWASP

Certified Web Application Security Professional

SUPPORT

You can connect with Tranchulas Online labs for 90 days to practice your hacking kung-fu after the training course. During this time our technical team will provide you email/phone/skype support in order to ensure the skills acquired on the training course are being applied correctly. This will also assist you in resolving questions that have arisen in the workplace after applying newly acquired penetration testing skills. We'll be your super hero, rescuing you from the confusion and frustration of learning. We'll be your super hero, rescuing you from the confusion and frustration of learning.

COURSE OUTLINE

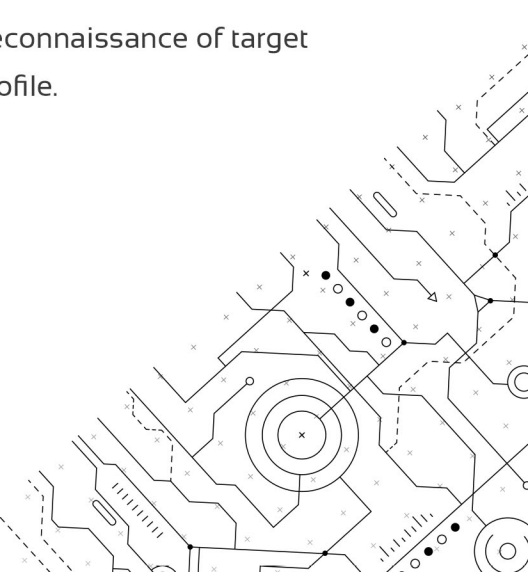
MODULE 1 - GENERAL CONCEPTS

- Web application Test Scope and process
- Overview for the development of secure Web applications
 - Tainted variables
 - Sensitive sinks
 - Validation functions
- Analysis
 - Black box testing
 - Gray box testing

MODULE 2 - INFORMATION GATHERING

- Site Mapping and Crawling
- Fingerprinting
 - Exercise:** Attendees will identify entry points in target web applications running on Tranchulas Online Labs
- File Extensions Handling
- Page enumeration
- Error messages and exceptions
- Path Disclosure
- Google Hacking
- Email Harvesting
- Maltego

Exercise: Attendees will do reconnaissance of target web application and build a profile.



COURSE OUTLINE

MODULE 3 - VULNERABILITY SCANNING

- Introduction to Vulnerability Scanners
- Scanning with OWASP Zap
- Scanning with Acunetix
- Scanning with Burp Suite pro

MODULE 4 - SQL INJECTION VULNERABILITIES

- Introduction to SQL Command
- Inserting and deleting data through SQL injections
- SQL Injection using SQLMap.
- A look at different solutions for SQL injection

Exercise: Interact with server through SQL Injection.

MODULE 5 - CROSS SITE SCRIPTING (XSS) VULNERABILITIES

- Introduction to Cross site scripting attacks
- Stored XSS Attacks
- Reflected XSS Attacks
- Understanding blacklist, stripping and other tricky XSS solutions
- Understanding the best solutions and how they apply to real life development

Exercise: Attendees will plan and execute different XSS Attack Scenarios on target web applications in Tranchulas Online Labs.

Exercise: Attendees will use BeEF (Browser Exploitation Framework) to conduct advanced cross site scripting attacks.

COURSE OUTLINE

MODULE 6 - IMPROPER INPUT VALIDATION

- Techniques to validate Input
- Local file read
- Local file inclusions
- Path Traversal and Null Bytes
- Encoding Attacks
- OS Command Injection
- CSV Injection
- XML Injection
- Open Redirects
- Directory Traversal

Exercise: Attendees will download restricted files from server using Directory Traversal

Exercise: Attendees will execute attacks learned during this module on web applications in Tranchulas online labs

MODULE 7 - INSUFFICIENT TRANSPORT LAYER PROTECTION

- A look at WiFi and ARP poisoning with network sniffing
- Using tools to sniff passwords

MODULE 8 - OPENSSL HEARTBLEED VULNERABILITY

- An introduction to OpenSSL Attacks
- HeartBleed vulnerability
- Exploitation

COURSE OUTLINE

MODULE 9 - AUTHENTICATION VULNERABILITIES

- Authentication Types and Scenarios
- User Enumeration
- Brute Force Attacks
- Direct Page requests
- Cookie Manipulation
- Parameter Manipulation

Exercise: Attendees will execute attacks learned during this module on web applications in Tranchulas Online Labs

MODULE 10 - BROWSER MANIPULATION

- Cross Site Request Forgeries / Session Riding
- Approaches to CSRF Prevention Techniques

MODULE 11 - INSECURE SESSION MANAGEMENT

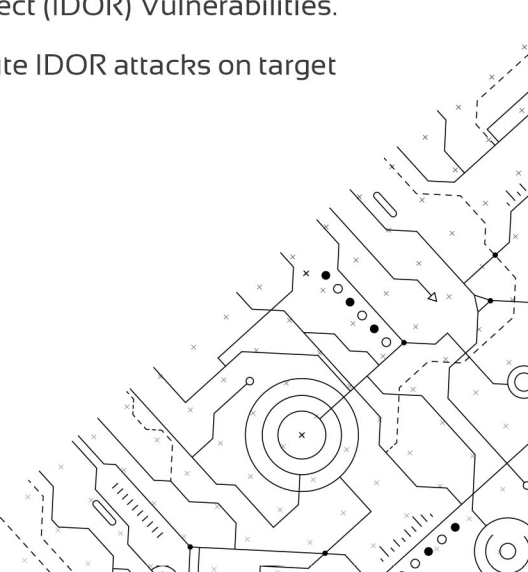
- Session Management Techniques
- Cookie Information Leakage
- Phishing Attacks
- Session Fixation

Exercise: Attendees will execute attacks learned during this module

MODULE 12 - AUTHORIZATION BYPASS

- Introduction to Authorization Bypass
- No Authorization mechanism in place
- Insecure Direct Reference Object (IDOR) Vulnerabilities.

Exercise: Attendees will execute IDOR attacks on target application.



COURSE OUTLINE

MODULE 13 - MASS ASSIGNMENTS

- Introduction to Mass Assignment attack
- User Role management on Signup
- Exploiting Mass Assignment issue

MODULE 14 - SERVER-SIDE REQUEST FORGERY

- Introduction to SSRF
- Impact of SSRF attacks
- Exploiting SSRF vulnerability

MODULE 15 - LOOKING AT THE BIG PICTURE

- A discussion of user interface issues and how to help end users make secure decisions
- Virtual hosts, how they may compromise your secure application
- A practical look at how hackers identify non- public systems
- Keeping oneself up to date with security
- The importance of focusing on secure code rather than security flaws.



CONTACT US

UNITED KINGDOM

TRANCHULAS LTD
20-22 WENLOCK ROAD
LONDON, ENGLAND, N1 7GU
TEL: +44 (20) 755-88924

UNITED STATES

TRANCHULAS LLC
1 HALLIDIE PLAZA, 2ND FLOOR
SAN FRANCISCO, CA, 94102
TEL: +1 (415) 689-9588

SYDNEY

TRANCHULAS PTY LTD
LEVEL 10 & 11
66 CLARENCE ST
SYDNEY NSW 2000
TEL: +61 (2) 8011-3356

PAKISTAN

TRANCHULAS PVT LTD
2ND FLOOR, EVACUEE TRUST
COMPLEX
SIR AGHA KHAN ROAD, F-5/1
ISLAMABAD, 44000

GENERAL INQUIRES:

INFO [AT] TRANCHULAS [DOT] COM

TRAINING SERVICES:

TRAINING [AT] TRANCHULAS [DOT] COM