TRANCHULAS

TRANCHULAS WORKSHOPS AND TRAININGS

Certified Web Application Security Professional (CWASP)

About the Training

This training course is a series of educational interactive training sessions where the attendees will gain hands on experience. They will be able to identify security flaws in web applications customized or built for the training course. They will also be able to exploit those security flaws to fully understand the value of fixing those flaws.

Audience

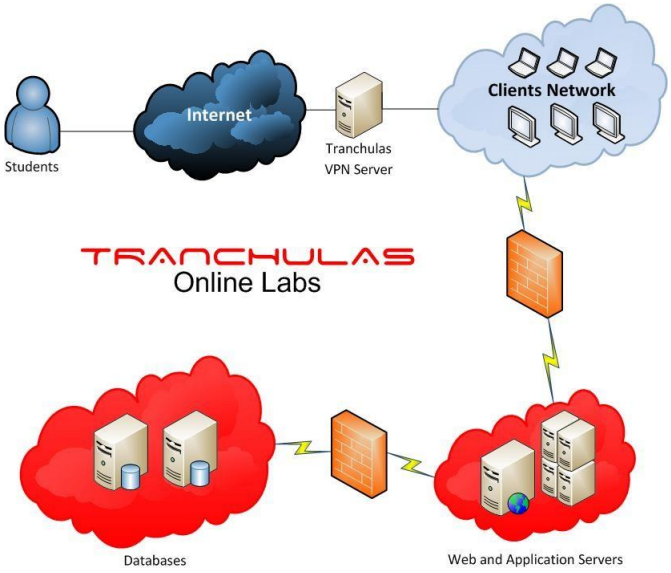
- Application Developers
- Application security managers
- Security consultants
- QA testers
- IT managers
- Penetration testers
- Any security professional who is interested in learning about web application security

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.

Tranchulas Online Labs

Tranchulas Online Labs are available 24x7 for practicing web attacks learnt during 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.



Post Training 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.

Pre-Requisites

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

CWASP
Certified Web Application Security Professional

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
- Common configuration and development errors
  - HTML comments and versioning
  - Backup files
  - Local databases
  - HTML hidden fields
  - Directory enumeration
  - Directory Indexing
- Analysis
  - Static code analysis
  - Black box testing
  - Gray box testing
- Encoding Schemes, URL Encoding, Unicode Encoding
- Bypassing Client-Side Controls

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

Module 3: Authentication Vulnerabilities

- Authentication Types and Scenarios
- User Enumeration
- Brute Force Attacks
- Attacking Password Change Functionality & Forgotten Password Functionality
- Tricks on password and lockout policies
- Direct Page requests
- Authentication Bypassing: SQL Injection, LDAP Injection, XPATH Injection
- Exercise: Attendees will execute attacks learned during this module on web applications in Tranchulas Online Labs

Module 4: Improper Input Validation

- Techniques to validate Input
- Local file read
- Local file inclusions
- Path Traversal and Null Bytes
- Encoding Attacks
- OS Command Injection
- XML Injection
- Open Redirect
- Directory Traversal
- Exercise: Attendees will download restricted files from server using Directory Traversal
- HTTP Response Splitting
- Exercise: Attendees will execute attacks learned during this module on web applications in Tranchulas Online Labs

Module 5: SQL Injection Vulnerabilities

- Introduction to SQL Command
- Using SQL injection to bypass authentication, extract information from database using UNION and errors

- Inserting and Deleting data through SQL Injections
- SQLMap Hands on
- Local system access and Escalation of privilege using SQL injection
- Blind SQL injection techniques
- A look at different solutions for SQL injection
- Exercise: Attendees will exploit databases running on Tranchulas Online Labs
- Exercise: Interact with server through SQL Injection

Module 6: File Uploading Vulnerabilities

- Uploading malicious code/shells on web server.
- Using shells to perform different level of functions
- (executing os level commands, view source code, copy/move data, delete data, pivoting)
- Prevention of these vulnerabilities through application code.

Module 7: 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
- Cookie Stealing using XSS
- 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

Module 8: Browser Manipulation

- Cross Site Request Forgeries / Session Riding
- Approach to CSRF
- Exercise: Reset a password on behalf of the victim
- Exercise: Command injection through CSRF
- Failure to restrict URL access
- Clickjacking
- Prevention Techniques

Module 9: Insufficient Transport Layer Protection

- A look at WiFi and ARP poisoning with network sniffing
- Using tools to sniff passwords
- Sidejacking, i.e. hijacking sessions by stealing cookies

Module 10: Insecure Session Management

- Session Management Techniques
- Cookie Information Leakage
- Phishing Attacks
- Session Fixation
- Exercise: Attendees will execute attacks learned during this module

Module 11: Insecure cryptographic Storage

- A look at insecure usage of hashing algorithms (md5 /sha1)
- XOR encryption and its weaknesses
- Exercise: Attendees will use publicly available online and offline tools for cracking passwords

Module 12: Assessing Application Architectures

- Attacking Tiered Architectures
- Exploiting Trust Relationships between Tiers
- Subverting Other Tiers
- Attacking Other Tiers

Module 13: HeartBleed OpenSSL Attack

- An introduction to HeartBleed and OpenSSL
- Approach for exploiting HeartBleed.

Module 14: HTML Injection Attack

- An introduction to HTML Injection
- How it can be used.

Module 15: Server-Side Request Forgrey Attack

- An introduction to SSRF Attack
- How it can be used.

Module 16: CSV Injection Attack

- An introduction to CSV Injection Attack
- Exploiting CSV Injection.

Module 17: 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 Tranchulas

United Kingdom

Tranchulas Limited
Suite 15091, 2nd Floor, 145-157 ST John Street
London, England, EC1V 4PW
Tel: +44 (20) 755-88924

United States

Tranchulas LLC
Skyline Tower, 10900 N.E. 4th St, Suite 2300
Bellevue, Washington 98004
Tel: +1 (408) 512-1113

Pakistan

Tranchulas Private Limited
2nd Floor, Evacuee Trust Complex Sir
Agha Khan Road, F-5/1 Islamabad,
44000
Tel: +92 (51) 287-1433

General Inquires: info [at] tranchulas [dot] com
Training Services: training [at] tranchulas [dot] com