Truephers Certified Web Application Penetration Tester

Web Application Penetration Testing Training

40 hours Training Course

Introduction to Web App Penetration Testing

- What is web 2.0
- Protocols
- Web Server
- Web Programming Languages
- Verb Tampering
- Netcat

Tools and Toys

- Firefox Hackers Browser
- Installing Add-ons
- Foxy-proxy
- Cookie editor
- HTTP--request-response interceptor
- Tamper monkey
- Greasemonkey
- Hackers bar
- Firebug
- Noscript
- UserAgent Switcher

Enumeration

- Mapping the Web Application
- OS Fingerprinting
- Web Server Fingerprinting
- Whois Enumeration
- Wayback Machine
- Reverse IP Domain Check

Call: 73 994 994 73 www.truephers.com info@truephers.com

- Email harvesting
- Sub-domain finding
- Active port scanning
- Nmap port scanning

Proxy Interceptor

- Burp Suite Introduction
- Burp Suite Configuration
- Burp Suite Interceptor
- Burp Suite Repeater
- Burp Suite Intruder
- Burp Suite Comparer
- Burp Suite Decoder
- Burp Suite Sequencer
- OWASP ZAP Proxy tool
- Using OWASP ZAP Proxy tool

Google Hacking Database

- Using Google Dorks
- Finding Open Cameras
- Finding files types, pages on particular Website
- Finding backup and log files
- Finding default configured Routers
- SHODAN (Search Engine for IOT)

Attacking Authentication

- Understanding Web Authentications
- HTTP-Basic Authentications
- HTTP-Digest Authentications
- Attacking HTTP-form based Authentications
- Bypassing Login forms
- Fuzzing Login forms

Attacking Session Management

- Understanding Session Management

- Understanding Cookies
- Fuzzing Session Management
- Finding weak session tokens
- Session token manipulation
- BurpSuite Sequencer

HTML Injection

- HTML Injection Basics
- HTML Injection in parameters
- Bypassing filters

Command Injection

- Command Injection
- Command Injection filter bypass
- Command Injection with commix
- Command Injection to reverse shell on box.

File Uploads Vulnerabilities

- Basics File Uploads Vulnerabilities
- Content-Type check bypass
- Bypassing blacklist uploads.
- Bypassing with PHPx
- Bypassing using double extension
- Bypassing getimagesize() check
- Null byte injection
- File upload to reverse shell

RFI / LFI

- Remote file Inclusion
- RFI to shell on box
- Local file inclusion
- LFI filter bypass
- LFI to shell on box or complete server takeover.
- LFI with null byte injection
- Remote code execution with LFI and Apache logs poisoning.

- Remote code execution with LFI and SSH logs poisoning.

SQL Injection

- Understanding SQL Injection
- Login bypass with SQL Injection
- Union based SQL Injection
- Blind SQL Injection
- Error based SQL Injection
- SQL Injection with SQLMap

HTTP Sniffing

- Sniffing
- ARP Poisoning
- HTTP, FTP Password Capturing
- Cain and Able
- Etter-cap sniffing
- Degrading HTTPS to HTTP with SSL-strip and sniff data.

Basics JavaScript for Penetration Tester

- Introduction to JavaScript
- Syntax, Comments, Variables, Functions, Events, Strings, Numbers
- Modifying HTML with JavaScript
- Modifying all links with JavaScript
- Modifying forms with JavaScript
- Event Listeners
- Internal/ External JS
- XMLHttpRequest
- HTML Parsing
- XML Parsing
- JSON Parsing

Cross Site Scripting

- Basics of JavaScript
- Basics of Cross site scripting (XSS)
- DOM based XSS

- Cross Site Request Forgery
- CSRF token bypassing
- Multi-Step CSRF
- Beef Framework