Web Security & Bug Bounty: Learn Penetration Testing

For more courses, resources and workshops, visit zerotomastery.io

Here are the resources we use in the course and you can use the links below for more information in each section:

Creating Virtual Lab:

- 1) Virtual Box - https://www.virtualbox.org/
- 2) Kali Linux - https://www.kali.org/
- 3) OWASPBWA -https://sourceforge.net/projects/owaspbwa/
- 4) TryHackMe Platform - https://tryhackme.com/
- 5) HackTheBox Platform(Optional) - https://www.hackthebox.eu/

Website Enumeration & Information Gathering

- 6) Google Dorking - https://www.exploit-db.com/google-hacking-database
- 7) WhatWeb - https://tools.kali.org/web-applications/whatweb
- 8) Dirb - https://tools.kali.org/web-applications/dirb
- 9) Nmap - https://nmap.org/
- 10) Nikto - https://tools.kali.org/information-gathering/nikto

Introduction To Burpsuite

- 11) Burpsuite - https://portswigger.net/burp
- 12) Burpsuite Usage - https://portswigger.net/burp/documentation/desktop/penetration-testing

HTML Injection

- 13) What is HTML Injection - https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/03-Testing_for_HTML_Injection

Command Injection

- 14) What is Command Injection - https://owasp.org/www-community/attacks/Command_Injection

Broken Authentication

- 15) Broken Authentication - https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Bruteforce Attacks

- 16) Hydra - https://tools.kali.org/password-attacks/hydra

Broken Access Control

- 17) What is Broken Access Control - https://hdivsecurity.com/owasp-broken-access-control

Security Misconfiguration

- 18) Problem With Default Credentials - https://www.techrepublic.com/article/how-to-find-and-fix-vulnerable-default-credentials-on-your-network/

Cross Site Scripting - XSS

- 19) Useful XSS Cheatsheet - https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

SQL Injection

- 20) Useful SQL Injection Cheatsheet - https://portswigger.net/web-security/sql-injection/cheat-sheet

XXE

- 21) What Is XXE ? - https://portswigger.net/web-security/xxe

Components With Known Vulnerabilities

- 22) What is the danger of CWKV ? - https://hdivsecurity.com/owasp-using-components-with-known-vulnerabilities

Logging & Monitoring

- 23) Why We Perform Logging & Monitoring - https://www.appdynamics.com/product/how-it-works/application-analytics/log-analytics/monitoring-vs-logging-best-practices

Bug Bounty/Penetration Testing Platforms

- 24) BugCrowd - https://www.bugcrowd.com/
- 25) HackerOne - https://www.hackerone.com/
- 26) SynAck - https://www.synack.com/
- 27) Intigriti - https://www.intigriti.com/