Web Security & Bug Bounty: Learn Penetration Testing in 2022

**Section 1 - Introduction to bug bounty**

1.Course outline

* Create virtual lab
* Enumeration and info
* Burp suite
* Html injection
* Command injection + execution
* Broken authentication
* Brute force attacks
* Access control
* XSS
* SQL injection
* Xpath, XEE
* Logging + monitoring
* Bug Hunting

2.Join Our online classroom

* ZeroToMastery discord channel.

3.Exercise: Meet Your classmates and instructor

4.What is penetration Testing?

* Penetration testing is also known as pen testing or ethical hacking.

It describes the intentional launching of simulated cyberattacks that seek

out exploitable vulnerabilities in computer systems, networks, websites, and applications.

5.What is Bug Bounty ?

* Mostly bug hunting happens in webpages.
* Common vulnerabilities : Password vulnerabilities, Database vulnerabilities, device vulnerabilities
* Things to do: 1.Virtualization , 2.Installing Kali Linux, 3. Basic knowledge of web structure.

**Section 2 - Our Virtual Lab Setup**

1.Installing VirtualBox and kali Linux

2.Important - New kali Linux categories

3.OWASPBWA Installation

4.Creating TryHackMe Account

**Section 3 - Website enumeration & Information Gathering**

1.Website Enumeration - Theory

* Input fields are the places where most vulnerabilities are found
* Common tools used are Nmap,Nikto,Google,BurpSuite.

2.Google Dorks

* "site: <website> filetpe:pdf" will display all the pdf files in tesla.com.
* Pattern searching : ""@tesla.com" -site:tesla.com"
* Google dorks website / exploit-db

3.Ping,host,Nslookup

* "ping" command will check whether a site,ip is online or not. Some websites might not ping back which doesn't necessarily mean its offline.
* "host <website>" command will lookup for IP address.
* "nslookup <website>" command will display details of target address ip and info.
* "whois <website>" command will show many details.
* Information gathering can be done using google.

4.Whatweb

* "whatweb" command will display the technologies used in the website.
* Options : --aggression <number> - show more details

5.Dirb

* "dirb <website>" This command will print all the directory under it.

6.Nmap

* This tool is used to map out the network
* "nmap <website>" will show the details about the ports.
* "nmap --script <vulnerability> <website>" To run vulnerability script for a website.
* "nmap --script vuln <website>" checks for any vulnerability in that website.
* "nmap --script http-stored-xss <website>" checks for XSS vulnerability in that website.

7.Nikto

* This tool is used for comprehensive tests against web servers for multiple items.
* "nikto -host <web address>" to scan the website.
* "nikto -host <web address> -port <port>" to scan the website for that particular port.