HOW TO START

BUG BOUNTY ??

01

●○○○○○○○○

DON'T START BUG BOUNTY BECAUSE YOU FEEL LIKE IT'S EASY MONEY. THERE IS TOO MUCH HARD WORK AND CONTINUOUS LEARNING THAT MOST PEOPLE CANNOT SEE.

Do bug bounty only if it entertains you and you're passionate about it. Otherwise the only thing you'd earn is "disappointment".

Digitokawn

02

○●○○○○○○○

UNDERSTAND THE FLOW AND MAKE A MIND-MAP

If you're one of those passionate people(as mentioned in point (1), then start understanding the flow.

Make your own mind-map and if you don't have one use Kathan Patel's Repository, here is the link:

https://github.com/KathanP19/HowToHunt

03

○○●○○○○○○

SOLVE LABS & GAIN SOME REAL-LIFE EXPERIENCE

Digitokawn

Initially you can solve labs but I personally did not do it so recommend directly jumping on live sites as it gives you confidence and real world experience.

04

○○○●○○○○○

PICK A TARGET WITH WIDE SCOPE

As a beginner you need to pick a target with wide scope and you have to test everything that you have learned so far on each target subdomain, doesn't matter vulnerability is found or not but it will make you feel confident that yes you know the methodology.

→

05

○○○○●○○○○

HUNT LESS, READ MORE

Digitokawn

Yes you heard me right! Read as many articles as you can on a daily basis. Intially you need to do this.

06

○○○○○●○○○

GIVE ENOUGH TIME TO RECON

Give sufficient time to recon when you hunt on a target, use different tools for the same purpose, make your unique wordlist, find as many login panels as you can, enumerate technology versions and their public CVE information, find hidden hosts using Shodan, censys etc.

Once you have gathered enough information about the target then it won't take much efforts from you to find vulnerabilities.

"If I only had an hour to chop down a tree, I would spend the first 45 minutes sharpening my axe." - Abraham Lincoln..

→

07

○○○○○○●○○

USE RESOURCES

If you are stuck somewhere, refer this Bible of Ethical Hacking:

https://book.hacktricks.xyz/welcome/readme

Watch as many POC's as you can. You can simply find POC's on YouTube or you can find Hackerone POC's using Google Dorks like this:

- site:hackerone.com
- intext IDOR site:hackerone.com
- intext Business Logic Error etc.

08

○○○○○○○●○

READ-WRITE MODE ON

Observe weird things, anything with a harmful impact to either the site or it's user is a Vulnerability.

Keep the Read-Write Mode ON. Make sure whatever you learn, quickly perform a practical of it otherwise you'll never be able to master it.

Digitokawn

LOVE THIS POST?

Don't forget to share and save this post if you love it!