



*BugHuntersVillage*

# **UNLOCKING THE SECRETS:** **HOW TO GET STARTED IN** **BUG BOUNTY HUNTING**

*Presented by: Anzil*



# Overview

---

- *Introduction*
- *My Story*
- *Writeups and Blogs*
- *Tools for Recon*
- *How to choose a program*
- *Conclusion*



# Introduction

- Bug bounty hunting is a dynamic and rewarding field where skilled individuals, like you, proactively search for security weaknesses in applications and platforms. By responsibly disclosing these vulnerabilities to the concerned organizations, you not only help them improve their security but also earn rewards and recognition for your efforts.
- In this video we'll cover the fundamental building blocks for success in bug hunting. We'll explore key concepts such as understanding the bug bounty landscape, selecting target platforms, and leveraging various testing methodologies.



## My Story

I am started bug hunting just reading blogs and trying it out on target that's how i earned my first bounty and then i continued reading disclosed reports and writeups and trying that on my target , reading is the key to knowledge when we encounter an issue it will helps you to understand how to approach this type of issue.

---



# Writeups & Blogs

## Disclosed Reports

- Hackerone Hacktivity has an unlimited stream of disclosed vulnerabilities on the Hackerone platform. Reading through them is a great way to see what kinds of things people are finding and inspiring your own hacking.
- Crowdstream is the Bugcrowd equivalent of Hackerone's Hacktivity. Although there are far less disclosed reports there, it's worth reading through them!



# Blogs

- Inti De Ceukelaire is a great bug bounty hunter and the Head of Hackers at bug bounty platform Intigriti. He has a knack for finding critical systemic bugs that affect a lot of organisations, and doing great write-ups!
- DOnut's blog is a total mixed bag with lots of gems.
- Intigriti's Medium Publication is filled with great bug bounty conte
- Pentesterland has a huge, curated list of bug bounty writeups and resources for beginner hackers.

# Tools for Recon

## Subdomain Enumeration

- Subfinder
- Assetfinder
- Amass
- httpx
- Aquatone

# Directory Fuzzing

- ffuf
- feroxbuster
- wfuzz
- dirsearch

# Identify Technologies

Wappalyzer

# Intercepting Requests

Burp suite



# Dorks and search engine

## Google dorks

examples:-

- `site:target.com -www`
- `site:target.com intitle:"test" -support`
- `site:target.com ext:php | ext:html`
- `site:subdomain.target.com`
- `site:target.com inurl:auth`
- `site:target.com inurl:dev`

## Search Engine

- `Shodan.io`
- `cencys.io`

# Misc

- Waybackurls
- Arjun
- Sqlmap
- Ghauri
- Confused
- Dlafox
- Nuclei

And some more will discuss on upcoming videos

# Choose Platform

- Hackerone
- Bugcrowd
- Intigrity
- Open bug bounty

## How to choose a Target

- Check the program Scope
- check the program Responsiveness
- Program launch date
- Rewards

# Conclusion

Hi , Hope you enjoyed the introduction , Stick with reading blogs and writeups will help you to earn bounties. Join communities and collaborate with other hackers share knowledge. Try to focus on one target at a time , Enumerate the target and create an approach to the target , go for the vulnerabilities you learned from reading blogs , try and repeat , focus on yourself don't demotivate yourself after getting duplicates or informational just keep reporting until you reach your limit



*BugHuntersVillage*

# THANK YOU

*For watching this Video*



*muhammedanzil.h1@gmail.com*



*<https://alone-breecher.github.io/>*