How To Become A Bug Bounty Hunter?

MUFF1N Follow
Apr 13 · 6 min read

First , What is A Bug Bounty Program?

- A **bug bounty** program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting **bugs**, especially those pertaining to exploits and vulnerabilities.
- A reward offered to a perform who identifies an error or vulnerability in a computer program or system.
  'The company boosts security by offering a bug bounty

. . .

How To Become a BUG BOUNTY HUNTER ?

Step 1) Start reading! — There are some go-to books that you can buy to help you learn the basics and essentials of penetration testing and bug hunting. Since bug bounties often include website targets, we'll focus on getting you started with Web Hacking and later we'll branch out.

Note ->It's very important to focus on an area of hacking that is interesting & exciting to you. Focus on that one area and pick up new things as you go, but don't try to be the "ultimate hacker" and learn everything.

Hacking is a lifelong journey of learning.

Two Books I Suggest are -

The Web Application Hacker's Handbook
This is an absolute must-read and considered the web-app hacker's 'bible'. This book starts from square one, walking you through getting Kali Linux installed all the way through using tools and finding exploits.

OWASP Testing Guide v4
Highly suggested by Bugcrowd

For more reading :**Penetration TestingThe Hacker Playbook 2: Practical Guide to Penetration Testing**

For Mobile hacking :**The Mobile Application Hacker's HandbookiOS Application SecurityStep**

. . .

2) Practice what you're learning! — While you're learning it's important to make sure that you're also understanding and retaining what you learn. Practicing on vulnerable applications and systems is a great way to test your skills in simulated environments. These will give you an idea of what you'll run up against in the real world.

Hacksplaining

This is a great site to learn a bit more about various web hacking techniques and how they're done. It's actually more of a practical walk-through. Super useful!

Penetration Testing Practice Labs
This site has a massive list of practice apps and systems for several hacking scenarios. Use this list to find new testing labs and sites to practice your skills.

. . .

Step 3) Read bounty write-ups and POCs (Proof of Concepts) from other hackers on Medium and watch tutorials on YouTube!
—

Its Very Important To Understand How Other hackers are Finding Bugs.

Bugcrowd Researcher Resources: Tutorials
Collection of great tutorials from the Bugcrowd community and beyond.

/r/Netsec on Reddit
Netsec on Reddit is almost exclusively tech writeups and POCs from other researchers.

JackkTutorials on YouTube

Jackk has created many tutorials that walk you through CSRF, XSS, SQL Injection, Target Discovery and much more.

DEFCON Conference videos on YouTube

Watch all of the talks from DEFCON over the years. Very useful resource.

Hak5 on YouTube

Hak5 typically focuses on hardware hacking, but in addition to that they also have the 'Metasploit Minute' show, HakTip: NMap and much more.

Awesome-Infosec

This is a curated list of helpful security resources that covers many different topics and areas.

. . .

Step 3-A) Gather your arsenal of tools

Bugcrowd community has curated an extensive list of tools that you can add to your bag of tricks

Bugcrowd Researcher Resources - Tools

Step 4) Join the community! — You're joining a global community

of tens of thousands of hackers.

Join the #Bugcrowd IRC channel to talk to over 100 security researchers

Step 5) Start learning about bug bounties — Okay, now you're at the point where it's almost time to start hunting for bounties. But first, let's learn how bug bounties work and how to get started, just to make sure we maximize our chances of success.

How to approach a target
Advice from other bug hunters that will help you find more success when approaching a bug bounty.

How to write a Great Vulnerability Report
This will walk you through how to write a great vulnerability report. The better your report, the higher chance you will get a bounty!

How to write a Proof of Concept
Proof of Concepts show the customer how your bug is exploited and that it works. This is crucial to being rewarded successfully.

HackerOne POC

Bug Bounty World

How to Report a Bug
Our walkthrough for reporting a bug via the Bugcrowd platform.

Bug Bounty Disclosure Policy
These are the rules of the road. It's very important that you understand the bounty program's bounty brief and disclosure policy.

. . .

Step 6) Get hacking! — It's time to start hacking! When you're new and getting started, it's probably best not to try hacking the most popular bug bounties out there. Trying to hack Tesla Motors, Facebook, Pinterest and others will likely end in frustration for beginners, as those companies are very popular and are more secure because they receive many bug reports.

Go for the Kudos only programs — Instead focus on bug bounties that have likely been overlooked by others. These are often bug bounties that don't pay rewards but instead offer kudos points on Bugcrowd. These 'kudos points only' programs are a fantastic way to get started with bug bounties and to show your skills to Bugcrowd. After you've submitted some valid bugs to Bugcrowd, even if they're kudos rewards only, you will likely start receiving invites to private bounty programs. The private bounty programs are invitation only and restricted to a small number of people, which means less competition and a higher likelihood of successfully finding a bug

. . .

Step 7) Always Be Learning — Like we mentioned earlier, hacking is a lifelong journey of learning. This is what makes this field so exciting! There are always new articles and presentations to learn from, interesting people to meet at conferences or local meetups, and new opportunities to pursue.Bug bounties are a fantastic way to enter the InfoSec community and build your career. Use bug bounties as a way to make extra money, improve your skills, meet new people, and even build out your resume.Remember, always act professional and treat people well. This is a small community and we like to take care of each other - you never know who you might meet!

. . .

Bug Bounty Platforms :

Bugcrowd

HackerOne

HackTrophy - Recently launched for Czech republic & Slovakia (Central Europe)

BountyGraph - For free and open-source software dependencies.

PlugBounty - A Bugbounty Platform for Plugins, Extensions, Libraries

Synack

Zerocopter

cobalt.io -(Private)

SlowMist - (Blockchain Ecosystem Security)

Independet Bug Bounty programmes:

Google Vulnerability Reward Program (VRP)

Public talks (YouTube):

Bug Bounty Hunting Methodology v3 - Jason Haddix | Bug Bounty Hunting Methodology v2 - Jason Haddix

Giving Back to the Bug Bounty Community - ZSeano

Finding Hidden Gems in Old Bug Bounty Programs - Yappare

Bounty Hunters - GrrCON 2018 - J Wolfgang Goerlich

Interesting blogs:

PortSwigger Web Security Blog

Offensive Security by Automation

Tutorials by zseano

Bugcrowd’s blog

HackerOne Blog

http://blog.orange.tw/

Vulnerability Prioritization

Bugcrowd’s Vulnerability Rating Taxonomy

PortSwigger's Issue Definitions

OWASP Testing Guide

Most common vulnerabilities (Tutorials):

Open Redirect Vulnerability

A Guide To Subdomain Takeovers

Exploiting CORS misconfigurations for Bitcoins and bounties

Popular Google Dorks Use(finding Bug Bounty Websites)

site:.eu responsible disclosure
inurl:index.php?id=
site:.nl bug bounty
“index of” inurl:wp-content/ (Identify Wordpress Website)
inurl:”q=user/password” (for finding drupal cms)

Browser Plugin’s:

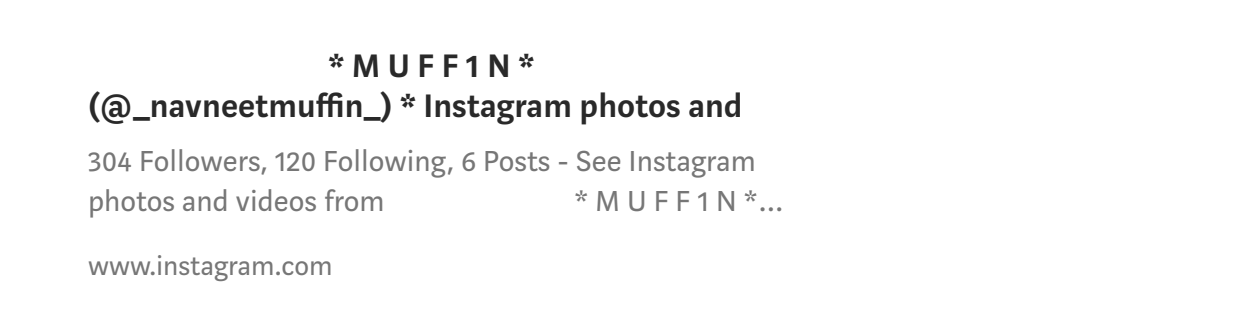
Chrome : http://resources.infosecinstitute.com/19-extensions-to-turn-google-chrome-into-penetration-testing-tool/

Firefox : http://resources.infosecinstitute.com/use-firefox-browser-as-a-penetration-testing-tool-with-these-add-ons/

. . .

Follow me :

Instagram —



Download :

Vikash Chaudhary's Bug Bounty Hunting - Offensive Approach to Hunt Bugs!!

Source : Google | BugCrowd

If You Have Any Query , Feel free to contact me!!

And , If You Have any Suggestion Comment it.