# How to Get Started into Bug Bounty Complete Beginner Guide

( Part 1 Web Pentesting )

Hello guys, after a lot of requests and questions on topics related to Bug Bounty like how to start. I researched a lot for collecting best resources for you Bug bounty. I am starting from basic as prerequisites to tips and labs along with report writing skills. I have also included some of my personally recommend tips.

## Let's get started 🔥🔥

Hacking is now an accepted profession in which He/She can earn an honest and decent living. Not only are there many pen testing jobs within organizations, providing these "startup" hackers with a place to legitimately fine-tune those skills and abilities , but we also have a new breed of testing –Bug Bounties.

## 1) What is Bug Bounty ?

Let me explain you in a very simple way .. A reward or money offred to a person who finds the bugs (error) or vulnerability in a website or computer program and report it to the company in a responsible way.

## 2) What you need to know before starting a bug bounty program

- Scope - *.example.com
- Focus - payment processing
- Exclusions - 3rd party sites
- Organization-wide awareness
- Environment - prod vs staging
- Access - shared credentials or self-signup
- Decide - Private or Public?

Learn - Internet, HTTP, TCP/IP , Networking ,Command-line,

Linux , Web technologies, java-script, PHP, java ,

At least 1 programming language

## 3) Skills required to be a bug bounty hunter

Some of the key areas to focus that are part of OWASP Top 10 which are:

- Information gathering
- SQL Injection
- Cross-Site Scripting (XSS)
- Server Side Request Forgery (SSRF)
- Local & Remote file inclusion
- Information Disclosure
- Remote Code execution (RCE)

After understanding these vulnerabilities you can begin reading others reports ,POCs on the bug bounty platforms like Hackerone to figure out the common testing techniques.

**Tip** – Go for Owasp testing Guide

[Version 4.2] - 2020-12-03 - Download the v4.2 PDF here

## 4) Resources

Writeup – Pentester.land

Infosecwriteups.com

Daily news – Portswigger daily

Books - The Web Application Hacker's Handbook

Web hacking 101

Real-world bug hunting

Usefull Tools - 100 Hacking tools and Resources

Cheet Sheet –Edoverflow bugbounty cheetsheet

Gowsundar bug bounty tips

Labs – Portswigger academy

Confrences - Blackhat Defcon zeronight

Youtube Channels for the latest content –

Nahamsec

Jhaddix

Stok

Codingo

Red team Village

The Cyber Mentor

liveoverflow

InsiderPhD

Farah hawa

Do Subscibe my Youtube Channel Hackittech

Follow these guys on Twitter -

[+]nahamsec

https://twitter.com/NahamSec

[+]TomNomNom

https://twitter.com/TomNomNom

[+]stokfredrik

https://twitter.com/stokfredrik

[+]Jensec

https://twitter.com/_jensec

[+]cybermentor

https://twitter.com/thecybermentor

[+]Harsh Jaiswal

https://twitter.com/rootxharsh

[+]Rahul Maini

https://twitter.com/iamnoooob

[+]aditya Shende

https://twitter.com/adityashende17

[+]Harsh Bothra

https://twitter.com/harshbothra_

## 5) Bug Bounty Program:

- Open For Signup
- Hackerone
- Bugcrowd
- hackenproof
- Bugbountyjp
- Intigriti
- Open Bug Bounty

## 6) Tips for report writing –

- A detailed description of how the vulnerability is triggered
- Information outlining what happens when it is triggered – this helps us know if we've reproduced it correctly
- Simple steps to reproduce the vulnerability
- A description of the impact of the vulnerability

To take it a few steps forward, here's what makes a great report:

- Details about the specific code causing the vulnerability
- Scripted (Bash, Ruby, etc.) reproduction steps if it makes sense for that bug
- For complex bugs, a video can aid understanding, but this should not replace the written steps to reproduce
-

## 7) Sample format of the report:

- Vulnerability Name
- Vulnerability Description
- Vulnerable URL
- Payload
- Steps to Reproduce
- Impact
- Mitigation

## 8) Looking for more programs using Google Dorks

- inurl:”bug bounty” and intext:”€” and inurl:/security
- intext:bounty inurl:/responsible disclosure
- intext:”BugBounty” and intext:”reward“
- intext:”BugBounty” inurl:”/bounty” and intext:”reward

## 9) Some usefull tips –

- Do not expect someone will spoon feed you everything.
- PATIENCE IS THE KEY don’t expect you will get bounty in a single day or a month. It take a year to master so stay focused.

**Support me** if you like my work! Do Subscribe my Youtube Channel and **Follow me** on Instagram.