WIST

Put your bounty where your bug is...



An Introduction to bug bounty hunting...

root#whoami

Hilary Soita

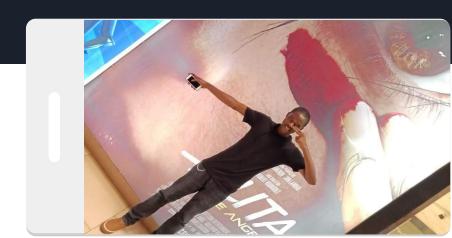
Information security Analyst, Cellulant

Bug Bounty hunter

@bit3c0de

www.sylarsec.com

Affiliation: Africa Hackon



Definition

• Bug bounty hunting is the art of being paid/compensated to finding bugs in softwares, web application, websites, mobile apps and other platforms.

- The Companies make this available for users who sign up to do this on some well known platforms like:
 - HackerOne
 - BugCrowd
 - Intigriti
 - Synack
 - etc...

What it means for...

Companies

Decentralized security testing

More Bugs to be reported

Better reputation

Hackers

Competition

Variety of platforms to test

Flexibility in testing

Money

More Money

What can make you a better bug hunter?

- O Programming knowledge
- A deep understanding of web and web technologies
- Be good at writing PoCs
- O4 Study up on attack methodologies and practice more
- Have good and concise reports

What to respect in a program

O Terms and condition

O2 Program scope

O3 Confidentiality



Testing Environments

Web

BWAPP

<u>Webgoat</u>

OWASP Juicy Shop

Hacker101

<u>HackTheBox</u>

Mobile

Damn Vulnerable iOS App (DVIA)

<u>Damn Vulnerable Android Application</u>

Damn Insecure and Vulnerable Application

Damn Vulnerable Hybrid Mobile Application,

Resources to get you going (videos)

- How to shot web Jason Haddix, 2015
- <u>Bug hunters methodology v3</u> Jason Haddix, 2018
- Hunting for Top Bounties Nicolas Grégoire, 2014
- O4 Finding Bugs with Burp Plugins & Bug Bounty 101, Bugcrowd, 2014
- The secret life of a bug hunter Frans Rosen, 2016

Resources to get you going (books)

- The Web Application Hacker's Handbook
- O2 OWASP Testing Guide v4
- The Hacker Playbook 3: Practical Guide To Penetration Testing
- O4 The Tangled Web: A Guide to Securing Web Applications
- 05 Web Hacking 101
- 06 <u>Mastering Modern Web Penetration Testing</u>

Resources to get you going (blogs)

- Ol Brutelogic @brutelogic
- O2 <u>Bugbountynotes</u> @zseano
- NahamSec @NahamSec
- 04 <u>Jasonhaddix</u> @Jhaddix
- 05 <u>Edoverflow</u> @EdOverflow

Find interesting bounty info

- https://twitter.com/search?src=typd&q=%23BugBountyTips
- O2 https://twitter.com/search?q=%23bugbounty&src=typd
- $\label{eq:com/search} O3 \qquad \text{https://twitter.com/search?f=tweets\&q=\%23togetherwehitharder\&src=t} \\ \text{ypd}$
- Site:hackerone.com "reports" intext: "SQL injection"

Empower the browser

- Hackbar sidebar that aids in web pentesting by aids in testing for SQLi and XSS.
- **JS toggle** enable/disable javascript in a single click
- **Hackbar** use this to switch the user agent to different strings
- **Firebug** edit and debug HTML, CSS and JavaScript live in any webpage
- Webdeveloper Tools adds various web development tools in the browser
- **Useragent switcher** switches the user agent in a single click
- Live HTTP Headers displays live http headers for each http request and responses to/from servers
- Tamper data displays headers and responses, but also has the abilities to edit the headers
- Cookie Manager + adds and edit cookie data in your browser

Best Approach

- Ol Develop your own way of thinking
- O2 Understand/ stick to the scope
- Focus more on doing good recon
- O4 Understand the application's logic
- O5 Assemble a good testing platform

Avoiding duplicates (hunters' nightmare)

- Test more on subdomains instead of main domain
- Use a standard template for reporting. This saves time
- Hunt for business logic flaws. Understand the application better.
- Hit hard. Go for the critical bugs. I.e SQli, RCE, SSRF etc...

What should a report contain

- **O** Vulnerability title/name
- O2 Vulnerability Description
- 03 Vulnerability Impact
- 04 Vulnerable link
- O5 PoC (screenshot, video, exploit code)

Any questions?



