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: AfricaHackon

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?

01 Programming knowledge

02 A deep understanding of web and web technologies

03 Be good at writing PoCs

04 Study up on attack methodologies and practice more

05 Have good and concise reports

What to respect in a program

01 Terms and condition

02 Program scope

03 Confidentiality

Testing Environments

Web

- BWAPP
- Webgoat
- OWASP Juicy Shop
- Hacker101
- HackTheBox

Mobile

- Damn Vulnerable iOS App (DVIA)
- Damn Vulnerable Android Application
- Damn Insecure and Vulnerable Application
- Damn Vulnerable Hybrid Mobile Application

Resources to get you going (videos)

01 How to shot web - Jason Haddix, 2015

02 Bug hunters methodology v3 - Jason Haddix, 2018

03 Hunting for Top Bounties - Nicolas Grégoire, 2014

04 Finding Bugs with Burp Plugins & Bug Bounty 101, Bugcrowd, 2014

05 The secret life of a bug hunter - Frans Rosen, 2016

Resources to get you going (books)

01 The Web Application Hacker’s Handbook

02 OWASP Testing Guide v4

03 The Hacker Playbook 3: Practical Guide To Penetration Testing

04 The Tangled Web: A Guide to Securing Web Applications

05 Web Hacking 101

06 Mastering Modern Web Penetration Testing

Resources to get you going (blogs)

01 Brutelogic - @brutelogic

02 Bugbountynotes - @zseano

03 NahamSec - @NahamSec

04 Jasonhaddix - @Jhaddix

05 Edoverflow - @EdOverflow

Find interesting bounty info

01 https://twitter.com/search?src=typd&q=%23BugBountyTips

02 https://twitter.com/search?q=%23bugbounty&src=typd

03 https://twitter.com/search?f=tweets&q=%23togetherwehitharder&src=typd

04 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

01 Develop your own way of thinking

02 Understand/ stick to the scope

03 Focus more on doing good recon

04 Understand the application’s logic

05 Assemble a good testing platform

Avoiding duplicates (hunters’ nightmare)

01 Test more on subdomains instead of main domain

02 Use a standard template for reporting. This saves time

03 Hunt for business logic flaws. Understand the application better.

04 Hit hard. Go for the critical bugs. I.e SQli, RCE, SSRF etc...

What should a report contain

01 Vulnerability title/name

02 Vulnerability Description

03 Vulnerability Impact

04 Vulnerable link

05 PoC (screenshot, video, exploit code)

Any questions?

DEMOS