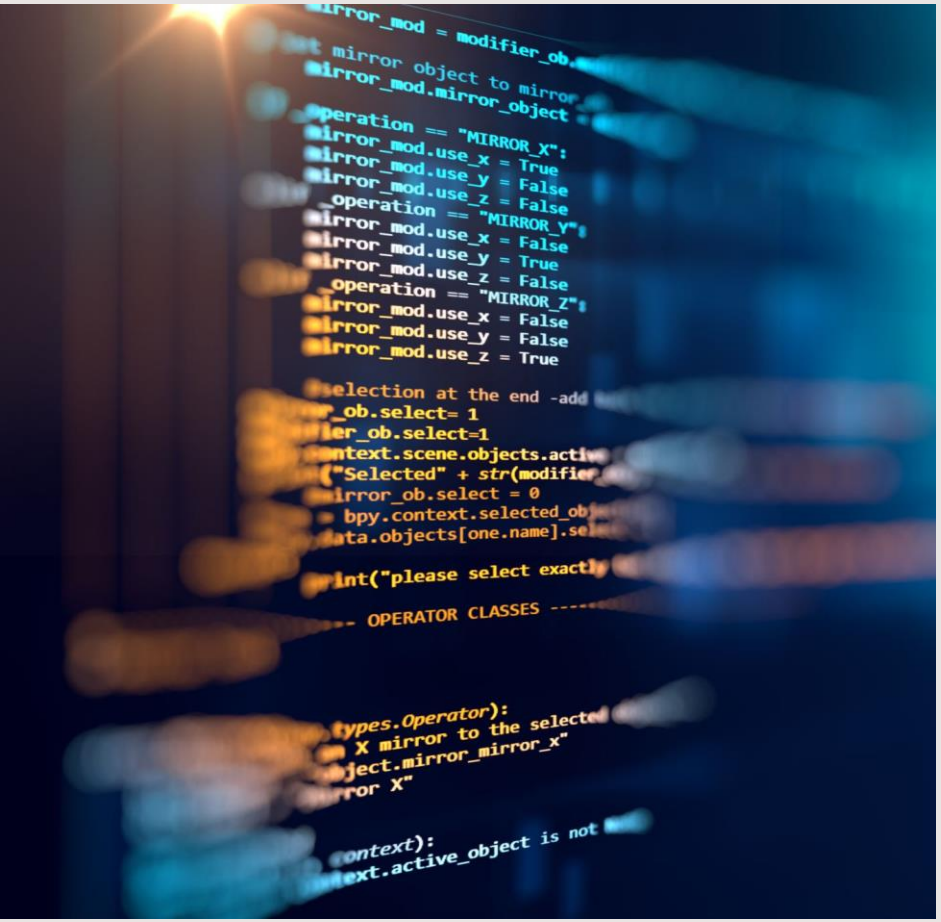
ARMOURINFOSEC

@harshbothra_

GETTING STARTED WITH BUG BOUNTY

By: Harsh Bothra



~Whoami~

Security Engineer/Analyst

Cobalt Core Pentester

Synack Red Team Member

Bugcrowd TOP 150 All Time

Lazy Bug Bounty Hunter

Author @Multiple Hacking Books

Speaker @Multiple Security Conferences

Creator @Project Bheem

Agenda

- Introduction to Bug Bounty
- Bug Bounty Platforms
- Bug Bounty Landscape in 2021
- Selecting a Program
- Application Testing Methodology
- Security Issues to Look for in 2021
- Tips & Tricks

Introduction to Bug Bounties

- Ethical/White Hat Approach to Responsibly Disclose Security Vulnerabilities to the Organizations, usually in exchange of Rewards.
- Rewards can be a Thanks to $$$$$
- Gives you Reputation, Constant Learning Opportunity, Thrills to face new challenge & a beautiful community

Bug Bounty Platforms

HackerOne	BugCrowd	Intigriti
YesWeHack	Synack {Private}	Yogosha {Private}
CESPPA	Vendor Specific/Self Hosted Programs	Zerocopter {Private}

@harshbothra_

BUG BOUNTY LANDSCAPE IN 2021

Selecting a Program

SCOPE

REWARDS

ACCEPTANCE RATIO

ACCEPTANCE/REWARD TIME

COMPLEXITY

Application Testing Methodology

Define	Define Target Scope
Understand	Understand Application Business Logic
Prepare	Prepare Threat Map
Perform	Perform Scope Based Recon
Perform	Perform Manual Pentest
Perform	Perform Application Specific Attacks
Learn	Learn what you lack & hit back on the target

Threat Mapping

Navigate	Navigate Application
List	List All Component & Functionality
Write	Write Theoretical Attack Scenario for Each Function
Create	Create Possible C.I.A. & C.R.U.D Impact Scenario
Verify	Verify all these test cases while you perform assessment

Manual Testing Approach

- Understand Application Flow
- Figure Out various possible Flows of same feature
- Try to break the application flow
- Test every possible test case for each individual functionality
- Do not miss any test case even if it’s complicated
- Rely less on tools, Proxy tool is good go.
- Learn and Hack

Recon 101

What is Recon ?

- Way to discover & create a better attack surface!

Why Recon?

- Increased Attack Surface == More Security Issues
- Looking at less travelled road == More Success
- Digging assets of your target to the deepest point possible.
- Recon != Security Issues but increases probability of getting >> Security Issues.

Security Issues to Look for in 2021

- GraphQL Security Issues
- WebSocket Vulnerabilities
- Business Logic Abuse
- Broken Access Controls
- Cloud Misconfiguration
- Known Vulnerable Softwares
- SSO/OAUTH/SAML Implementations
- Cross-Site Scripting
- SSRF, XXE & Command Injection
- Hardcoded Information & Data Exposure
- Misc. Security Issues & New Research ;)

TIPS & TRICKS

Get in Touch

Website – https://harshbothra.tech

Twitter - @harshbothra_

Instagram - @harshbothra_

Medium - hbothra22.medium.com

LinkedIn - @harshbothra

SpeakerDeck - @harshbothra

Email – hbothra22@gmail.com

THANK YOU