The intricacies of bug bounties

BY UNCLE RAT

Agenda

- Basic tips
- What bug bounty platform to pick
- What target to pick
- How to get Invites to private programs

Basic tips

Basic tips

- Bug bounties is NOT pen testing
  - Bug bounty targets have been tested before
  - Internally by the company
  - By pentesters before us
  - Probably by automatic tools
- Spend time picking a good target
  - As much as you need
  - It can be the difference between finding a bug and finding frustation

Basic tips

- Finding a valid bug requires
  - Speed
  - Creativity
  - Or both
- We can either be
  - The first to find and scan a subdomain
  - The one to outsmart everyone
  - Or both

Basic tips

- Don't follow a methodology, it doesn’t help
    - Build an intuition for bugs instead
- Don't mourn for dupes
    - They are also valid bugs, be faster next time or think different
- Don't forget to take notes
    - We want to test our target over multiple days
    - We want to retest our target often
        - Agile release cycles are 2 weeks!! (Not all companies use agile)
    - We want to test complicated scenario's

Picking a platform

Picking a platform

- 4 Types of platforms
  - Major platforms, well known
  - Regional platforms, less known
  - Private platforms, can only join by application
  - Self hosted bug bounty programs such as google or security.txt

Picking a platform

- Major platforms (Intigriti, bugcrowd, hackerone)
  - More competition
  - More programs to pick from
  - Intigriti also doesn't have negative karma
- Regional platforms (Yeswehack,yogosha,…)
  - Less competition
  - Smaller selection of programs
  - Mostly regional languages, use translator plugins
  - Less hardenedt targets due to less competition

Picking a platform

- Private platforms (Synack)
  - You have to apply to join
  - Way less competition
  - Quality targets
- Self hosted platforms (Google, firebounty.com,google dorking)
  - Quality is highly dependant on the program
  - Usually less hackers
  - Usually less hardened since most are VDP

Picking a target

Picking a target – different categories

- We can notice several properties when we look at targets
  - B2B vs B2C target
  - Wide scope vs main app
  - Web app vs mobile vs desktop vs ip range vs iot vs …
  - VDP vs PAID
  - Public vs private program

Picking a target – different categories

- Uncle rat usually goes for
  - B2B target such as invoicing application
  - main app
  - Web app
    - Mobile is harder but also has less competition
  - PAID but I recommend starting with VDP
    - Get those invites for private programs before you get cash
  - Private program, but first you need to get invites
  - Programs where I can create or receive different users of different priviledge levels

Picking a target – What to avoid when starting out

- Avoid high payouts, usually more hardened
- Avoid news papers, usually very little functionality
- Avoid banks, usually more hardened
- Avoid mobile, learn API testing first via web and then expand to mobile
- Avoid webshops unless you are willing to spend money
    - You need to test ALL the functionality including buying, returning,…
- Avoid programs that don't give you credentials and don't let you self register
- DO TAKE THESE BACK UP LATER WHEN YOU KNOW MORE

Getting invites to private programs

Getting invites to private programs

- Be active
- Report valid bugs
- Bug bounty platforms will
  - Keep stats on your reports
  - Keep stats on your skills
  - Invite you if they see fit
- Participate in the CTFs hackerone and bugcrowd sometimes host
  - They give private invites of lower quality