The Bug Bounty scene (and how to start)

Who am I?

Twitter: @nijagaw
Keybase: keybase.io/nijagaw
Blog: Sheepsec.com
In: /in/njgawronski/

- Nicodemo Gawronski (Nico)
- Bug Hunter & Security Researcher (Ranked 11th on Bugcrowd)
- Ex Pentester (@Sec1Ltd), now freelancer
- Love travelling and reading!

DC151

My Career

- Classics Diploma (Latin, ancient Greek, philosophy, physics, maths, ...)
- Hacking degree at Glasgow Caledonian University
- Intern then Security Consultant @Sec1Ltd
- Currently, Bug Hunter and Pentest Freelancer

DC151

What is a bug bounty program?

- A treasure hunt where everybody can participate and win prizes:
  - Scope: e.g. *.yahoo.com and infrastructure included
  - Rules (hack all the things, leave users alone, no DoS)
  - Rewards (pay per bug based on impact & first come, first served; Kudos points; swags)
  - Find a bug & report it (Internal SSRF: description, demonstrate impact, POC steps, POC screenshots/video)
  - Reward (Well done Reward! $2000)

DC151

Compared to a Pentest for a hunter - 1

- Bigger scope*
- Ongoing*
- Performance based
- Gamification (rewards, points, swags, badges)
- Time and competition (e.g. submitted LFI after 5 min)
- No direct contact with customer

DC151

Compared to a Pentest for a hunter - 2

- Many programs (choose what you like)
- New features?
- No Credentials for critical targets*
- No White listing
- Some bugs are not considered important (username enumeration)
- Rewards vary
- No bruteforce, escalation or automated scanning*

DC151

Compared to a Pentest for a hunter - 3

- Reporting is a challenge:
  1. Quality
  2. Speed
  3. Triage team
- Can rules be broken? (ban or higher reward)
- Time between triage and reward
- You need to dig deeper

DC151

Compared to a Pentest for a customer - 1

- Rewards VS fixed price
- Quality findings and flood of duplicates
- Triaging can be out sourced
- Program interest (Is your program interesting enough?)
- White hat VS Black hat
- Continuous assessment

Bug Bounty Program Types

- Private & cash rewards (Google, Facebook)
- Private & no reward (Amazon)
- Hybrid (Microsoft)
- Bounty platforms (Bugcrowd, Hackerone, Synack, etc.)

DC151

Private & Cash Rewards

- Scope include new acquisitions
- High rewards
- High competition
- Difficult target
- Quick response and they really care about security
- Public hall of fame

DC151

Private & no rewards

- Probably more vulnerabilities (no $$$, no swags)
- Public hall of fame (good for your CV)
- Chance for public disclosure (good for your CV)
- Challenge to hack an important target

DC151

Hybrid (Microsoft)

- Part of the scope == $$$
- Part of the scope == hall of fame & swags
- Not good for your wallet, great for training

Bug Bounty Platforms - Overview

- Public programs (entry point & the tip of the iceberg)
- Report bugs and you get points
- Private programs (few selected are invited)
- Different platform = different rules and entry level
- Payouts, points, bonus, swags, badges

DC151

Bug Bounty Platforms

- Hackerone
- Bugcrowd
- Synack
- Cobalt
- Zerocopter
- Intigriti & Dvuln

Hackerone (hackerone.com)

- 1st platform ($22M in bounties)
- Free subscription: ~178 public programs
- Mostly web and mobile apps ^
- Good: quantity of public programs, high rewards, great triage team, points for duplicates
- Bad: Doesn’t always manage bounties, a couple of fake programs
- Main programs: Twitter, Yahoo, Uber, Pornhub

DC151

Bugcrowd (bugcrowd.com)

- 2nd platform (hackerone direct competitor)
- Free subscription: 72 public programs (45 rewards, 27 points)
- Mostly web & mobile apps, few hardware bounties ^
- Good: manage bounty, good support, no fake programs & points system (points for duplicate), top 3 of the month receive bonus
- Bad: reward time vary, issues with triage team (write good reports!)
- Main programs: Tesla, Netgear, Jet2 (medium/high rewards)

DC151

Synack (synack.com)

- 3rd platform
- Free subscription with CV, interview & exams
- Only private programs (infra, web, mobile, hardware)
- Manage bounty & points are not so relevant (afaik)
- Good: support, no fake programs, quick payouts, bonus, learning experience
- Bad: long time to report & traffic is recorded and used by Synack

DC151

Cobalt (cobalt.io)

- A mix between pentest and bug bounty
- Free subscription with CV & interview
- Few old public programs; more private programs (web apps)
- Almost no management for bounty & points are not relevant
- Good: support, no fake programs, learning experience, team work
- Bad: fixed Payout

DC151

Zerocopter (zerocopter.com)

- Developed by bug hunters
- Free subscription with cover letter then maybe accepted
- Only private programs
- Good: Manage bounty, support, no fake programs, payouts are known
- Bad: fewer programs

Dvuln (dvuln.com) & Intigriti (intigriti.be)

- New platforms
- Free subscription for Intigriti, screening process for Dvuln
- Few private programs
- Manage bounty & points are not relevant
- Good: Lower competition
- Bad: fewer programs at the moment

When to start?! It depends on your goals

If your goal is:

- Learning: start now, it doesn't matter if you are a student or have a job
- Challenge: same as above. Do it seriously.
- Money: how much do you want to make? You won't see money at first. Lot of competition and you won’t receive private invitations.
- Career: not suggested if you are a beginner; stressful if you are not a beginner. You need to better and/or faster of the competition

DC151

How to start?! First steps

- Read the Web App Hacker's Handbook
- Follow interesting people on Twitter (twitter.com/nijagaw/following)
- Download vulnerable VMs (vulnhub.com) and Burp Suite
- Select a public program with *.domain
- Work with others! Start from main domain and move to subdomains (usually more vulnerable)
- Report, learn, repeat.

DC151

How to start?! Which program?

Any public programs with *.domain is good BUT:

- Preferably on Bugcrowd (duplicate points can help) and
- Amazon and Microsoft websites (in scope for their bug bounty but no cash rewards) (Time for a POC video?)
- Enjoy the hunt!

DC151

Video Time

- The app: *Redacted*
- The vulnerability: Stored XSS + SSRF (phantomjs) == LFI
- The answer: Thank you, ok fixed, bye!
- Achievement unlocked

DC151

Thank you! Grazie! ☺

- Any Questions?

Twitter: @nijagaw
Blog: Sheepsec.com
In: /in/njgawronski

DC151