Running A Successful Crowdsourced Security Program:

Tips On How Not To Fail...

Grant McCracken @ ISC^2 - 10/10/19

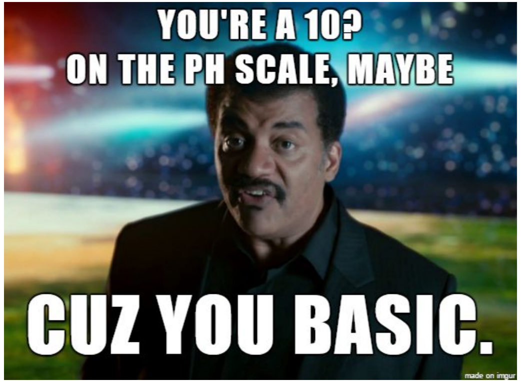
Agenda

- About
- Crowdsourced security?
  - What is it?
  - Flavors
    - Bug bounty
    - VDP (Vulnerability Disclosure Program)
- Components of a program
- What makes for an (un)successful program?
- Things to think about
- Thought exercises/recap
- Questions?

About

- Grant McCracken
  - Director of Solutions @ Bugcrowd
    - Done a *lot* of bug bounty...
  - Past appsec engineer; OSCP
  - Appsec USA/EU, misc bsides and meetups, etc

First, the basics



Crowdsourced security:

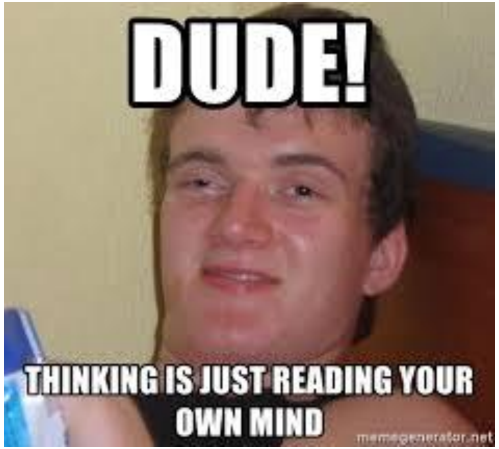
- **What is it?**
  - Strength in numbers
  - With a large enough pool, the right people are out there
- **Bug Bounty** (active)
  - Pay per bug/impact
  - Public/private
- **VDP** (passive)
  - See something, say something
- **The future...**
  - Using the crowd for more

Components to a crowdsourced program

Setting clear expectations from the get-go around...

- **Scope**
  - What can/cannot researchers test?
  - Where do they report everything else?
- **Rewards**
  - How much can a researcher expect to get paid for what?
- **A centralized place to ingest/track vulnerabilities**
  - Internal process(es)
- **Ratings**
  - Taxonomy
- **Information**
  - Including any details needed to be successful.
  - We *want* to find bugs!
  - Safe harbor

Setting up for success



- **Build a competitive and engaging program**
  - Competitive rewards + leveraging the VRT
  - A clear and attractive program scope (pretend you're the researcher)
  - Ensure adequate resources are assigned for rapid rewards/validation
- **Understand how your program will grow over time**
- **Remember: we *want* researchers to find bugs!**
  - Ensure that we're giving testers the tools to succeed (e.g. credentials/access/PII)
  - Work **with** researchers; not against them.
  - Providing fresh meat/changelogs, etc.
- **Where to report findings against other assets?**

Tips for program ownership

F-R-U-I-T

- **F**air
  - Rewarding in line with set expectations.
  - The brief is a contract!
- **R**esponsive
  - Quick to reward and answer questions.
- **U**nderstanding
  - Recognizing researchers are here to help, and are human.
- **I**nvested
  - The program is a priority; not a burden.
- **T**ransparent
  - Honest, open, and clear with researchers

Worst Practices...

- Slow to review, respond, and reward findings (months, if ever). Age subs like a fine wine.
- List a massive reward range, and then only pay out at the low end.
- Low-key sneak-fix bugs and claim they never existed.
- Run a “black box” program. No scope = no vulns; no vulns = super secure!
- Leave the brief as ambiguous as possible. Keep em’ guessing.
- Sneak-edits to the rules of engagement “nope, the rules say...” (great way to get out of paying)
- Never update the program or show appreciation.
- Be sure to remember researchers are the enemy - they’re hackers, right?
- Threaten to sue everyone. Who doesn’t love getting sued?
- Forget that you have a program.
- Give broken documentation or credentials. They’re hackers, they can figure it out...
- Forget to tell researchers about things that you know about (systemic issues).
- If it’s not critical, who cares?
- Include obtuse and arbitrary restrictions on involvement. The harder it is to participate, the less vulns will be found, and less vulns - more secure!
- Ignore researchers; they don’t have feelings.

Thought exercises/recap...

Imagine you’re:

- **A researcher…**
  - Does this make sense to you?
  - Are there good expectations around what to test, and compensation?
  - Would you be incentivized to test against this target? If not, why? Be sure to address those points before asking why researchers won’t.
- **An attacker…**
  - How would you realistically attack your org/assets? When considering scope, it helps to put things into perspective. Bad actors rarely come in through the front door.
- **A contractor…**
  - Do you want to work for the group that pays quickly and fairly, or for slow and unfairly?
- **If exploited in the wild...**
  - When questioning the dollar value of a finding, ask yourself what it would cost if this got exploited in the wild. Odds are that learning about it as part of a bounty is cheaper than in the wild.

Questions?