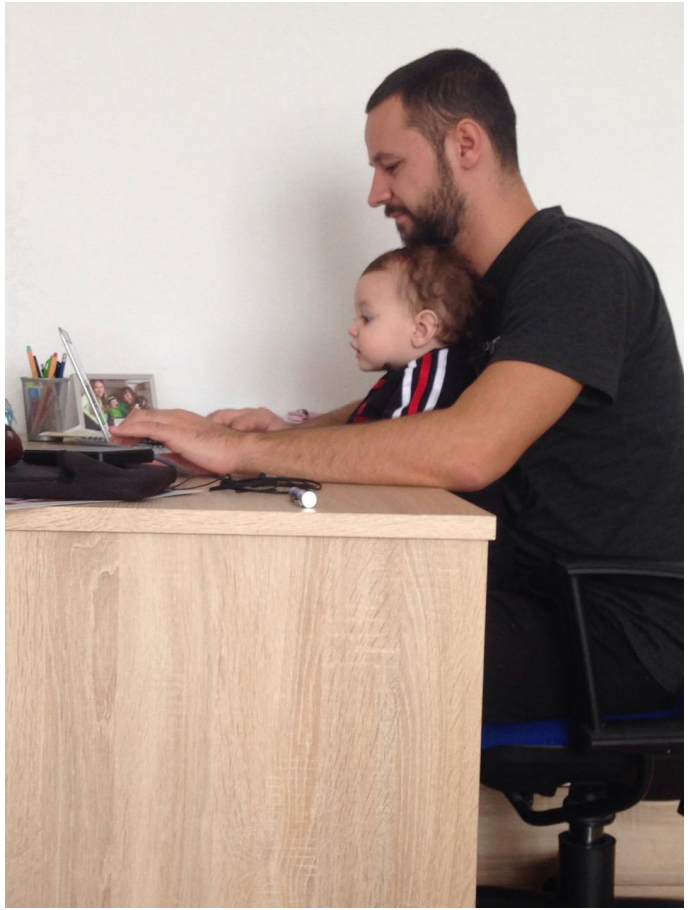
Running a Bug Bounty Program

What you need to know

Shpend

- TU - Master in Software Engineering
- Senior AppSec Engineer & Team Lead @ Bugcrowd
- Bug bounty Hunter
- Video Games

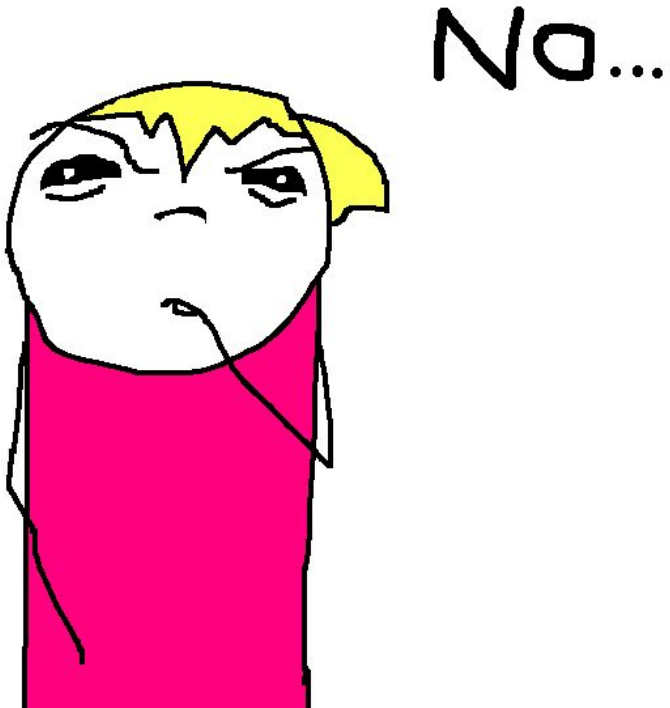


Agenda

- What & Why
- Pre-launch
- Post-Launch
- Notable findings

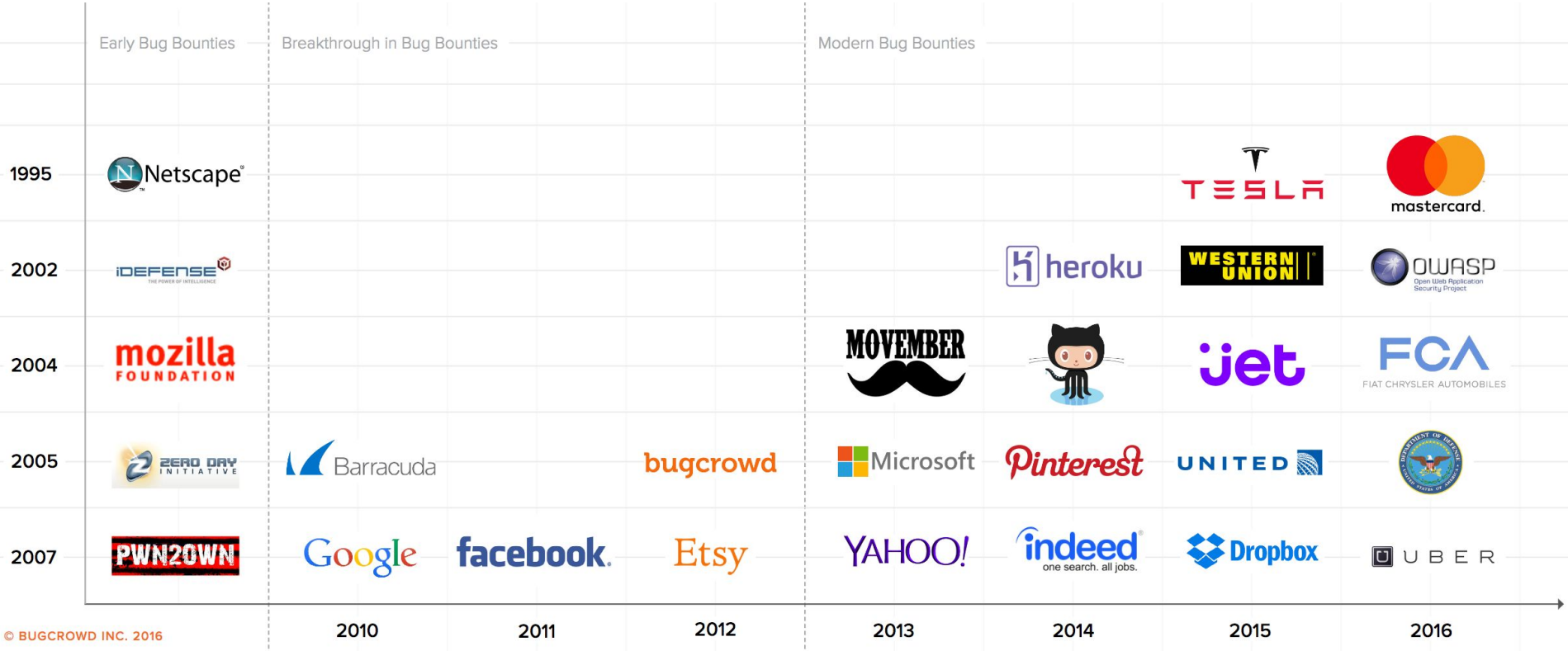
Bug Bounty Programs

Audience survey: Do you know what Bug Bounty means?



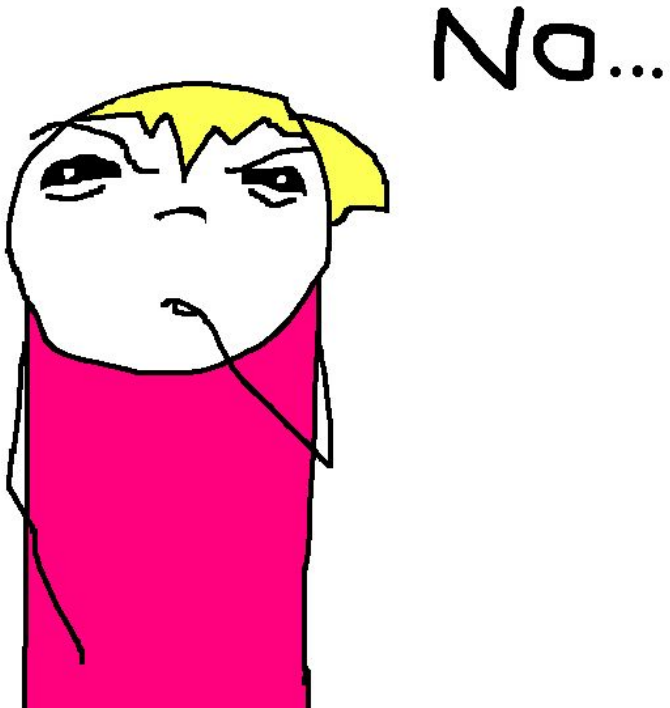
Source (Hyperbole and a Half)

The History of Bug Bounties: Abbreviated Timeline from 1995 to Present



Why?

Should I invite random people to hack on my systems?



Source (Hyperbole and a Half)

Benefits to running a Bug Bounty Program

- Lots of Eyes
- Pay for results model
- Shows a more advanced security posture
- Better reputation

Source (ESRB)

Case Study: Instructure

	2013 (Pentest)	2014 (Bug Bounty)	2015 (Bug Bounty)
Critical	0	0	0
High	1	25	3
Medium	1	8	2
Low	2	16	5

https://www.canvaslms.com/security

Source (Canvas)

Who are these people?

- All ages
- All levels of experience & skillsets
- All over the world
- Users and and non-users
- Passionate about security!

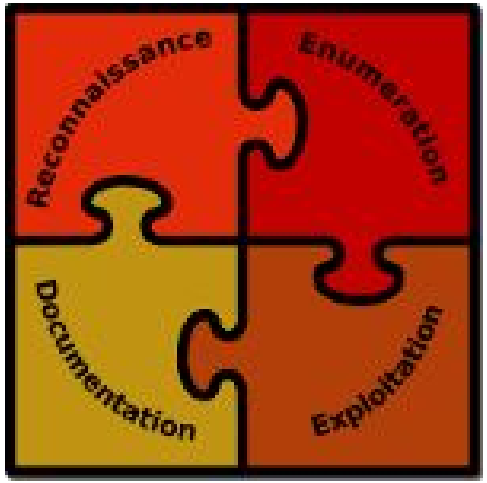
Source (ESRB)

Researcher Incentive

- Cash!
- Reputation (Hall of Fame)
- Ranking (platforms)
- Passionate about security!

Source (ESRB)

The Value of Crowdsourced Testing



Source (RedTeam Pentesting)

How?

Before and After

- Pre-Launch as a Program Owner
  - Scope
  - Exclusions
  - Environment
  - Access
- Post-Launch as a Program Owner
  - Handling Submissions (Manpower)
  - Communicating Effectively
  - Defining a Vulnerability Rating Taxonomy

“Make a change, pay the researcher.”

Source (Get A Life)

Pre-Launch

Scope

- Define target(s).
  - Only webapp (www.example.com)
  - All subdomains (careful) (*.example.com)
  - All products & acquisitions (more careful)
  - Mobile? (Android, iOS, Windows Phone? j/k)
  - Human & physical

Source (Accurate Shooter)

Scope

- Define non/rewardable findings
  - No security impact (Logout csrf)
  - Best practice (Session management)
  - Full/partial poc? (XXE, SSRF,SQLI)
- Define reward range
  - Min and Max
  - Table based on vuln types
- Define Disclosure
  - Allowed or not

Source (Accurate Shooter)

Exclusions

- You might *not* care about:
  - (Low-impact) “low hanging fruit”
  - Intended functionality
  - Known issues (call out!)
  - Accepted risks
  - Issues based on pivoting

Source (Meme Generator)

Environment

- Production vs. staging
- Make sure it can stand up to testing!
  - Scanners
  - Contact forms
  - Pentesting requests
- Special bounty types
  - IoT/devices
- Researcher environments

Source (The Daily Mail)

Access

- Easier = better (self-signup)
- Provide adequate resources for success
  - E.g. sandbox credit cards
- No shared credentials

Source (Demotivation)

Post-Launch

Be Prepared

- High volume of submissions
- Scanners
- Manpower
- Communication

Source (Meme Generator)

Tips: Triage submissions

- Work oldest to newest
- Push back if unclear (ask more info)
- Tag valid findings
- Experience -> faster triage

Source (Meme Generator)

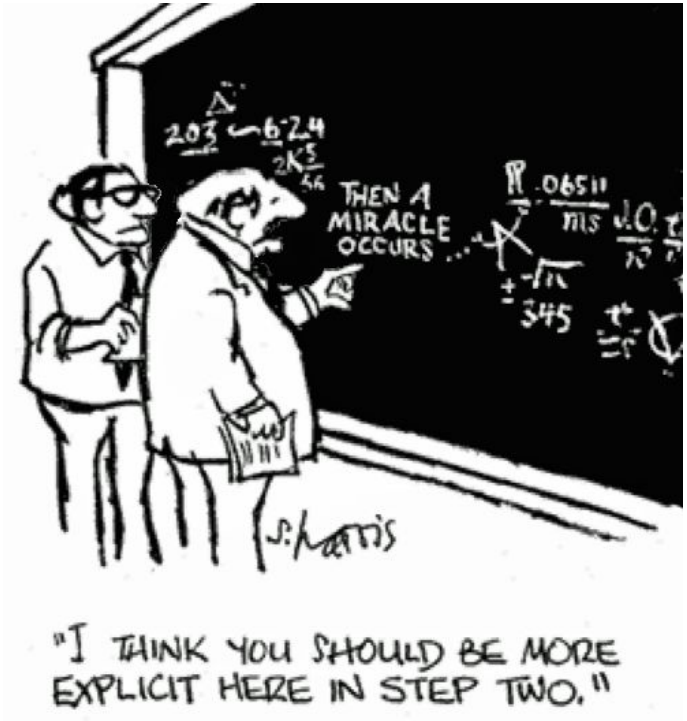
Tips: Triage submissions efficiently

- Check Domain/Bug for in scope
- Check for duplicates
- Reproduce (Replication steps)
- Have accounts (with diff roles) ready
- Have multiple browsers ready
- Keep burp open (you'll need it)
- Have environment ready (XXE oob via ftp)
- Keep scope handy

Source (Meme Generator)

Communication is Key

- Researchers like:
  - Concise, unambiguous responses
    - ESL
  - Short response time
  - Predictable reward time
- Communicate issue being looked at
- Reply to researcher questions.



Source (Profielwekstuk)

Define a Vulnerability Rating Taxonomy

- For program owners:
  - Speeds up triage process
  - Track your organization's security posture
  - Arrive at a reward amount more quickly
- For researchers:
  - Focus on high-value bugs
  - Avoid wasting time on non-rewardable bugs
  - Alongside brief, helps build trust

Discuss the VRT at a Roundtable

- Priority will change as your organization does
- Establish a regular meeting
  - Review interesting bugs
  - Discuss additions
  - Propose changes
- This is an ongoing process!
- Great learning opportunity

Source (Wikipedia)

Notable Findings

Kernel Panic

- 2 Remote BoF kernel level (Cifs/NSF)
- Found in custom kernel modules
- Rewarded $10k each
- Timeframe: 2 weeks

Source (Meme Generator)

“You can’t see me” exposed!

- POS tablet (Android)
- Shipped to researchers for testing
- Winner takes all ($15k)
- Hacked via flashing
- Bonus bug: admin backdoor

Source (Meme Generator)

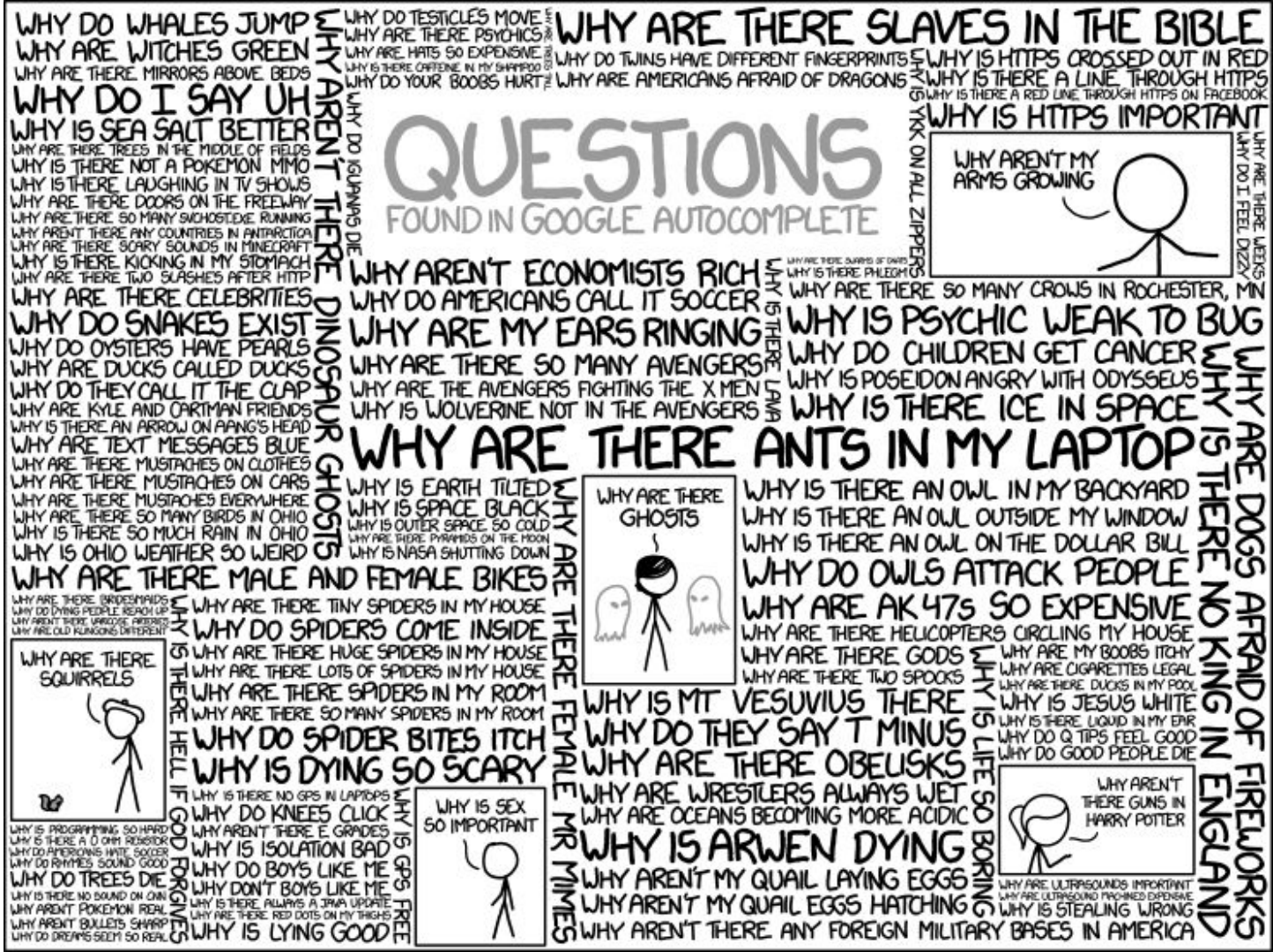
Login as anyone

- SSO available for setup
- Domain no verified
- Attacker set ups SSO
- Attacker adds ANY email address in their SSO account
- Attacker available to login using that email address
- Reward: $10k

Source (Meme Generator)

Thanks!

Shpend Kurtishaj
me@shpendk.com
@shpendk



Source (xkcd)