Running a bug bounty

Crowdsourcing security

Collin Greene
Also known as..
What is a bug bounty program

- Essentially bribing strangers to tell us their facebook 0days
- Sometimes blows up in our face, most of time works pretty well
- Storytime – 21 year old Collin + bank
- The common scenario obviously pretty broken
Security at facebook

Set the ~scene~

- Targeted external audits, internal audits, cc'd on diffs
- Tools – code reviews, static/dynamic analysis, HACK
- Bug bounty is a complimentary security system
- Good security bugs are rare gems to us
Our haul of bugs
Facepalm group

- Don’t click cancel
- &makeprofile=1
- Overly large emoticon posts in a group shut it down
Privacy

- Big deal (DIY bug was expensive)
- Forgetting privacy checks. Read vs mutate
- Detect secret groups
Unknown unknowns

- One fine day…
- These bugs lead to deep dark forgotten parts of your code
- <CENSORED USERNAME> bug goldmine
Corporate 0day reckoning

- Outside researchers don’t know what code you wrote and what you purchased
- This will happen
- Always a total bloodbath
“Logic”

- Groups + Blocking = ???
- Any picture is an xss. DNS shenanigans
- Javascripts Math.random() not random enough.
Wacky

- Poke
- Brokenness in the world at large
- To be or not to mp3
Stay on your toes

Report a Security Vulnerability

If you believe you have discovered a security vulnerability in Facebook, please fill out the form below with a thorough explanation of the vulnerability.

If you are attempting to report spam, abuse, or other account issues, please visit the Facebook Security Page for further assistance.

Vulnerability Type ▼ Vulnerability Scope ▼

Description and impact

asdf

Collin Greene fake@asdf.org

Submit
Components of bug bounty program

- Complimentary security system
- Bug bounty programs a good thing for both sides
So does it work?

- HELL YES

- Didn’t expect it to work. We had a bet…
  - Ended up getting 20+ good bugs in first 24 hours

- Alternative outlet to black market (big topic)

- Contrast bug bounty vs code review
Fake graph

- Inputs (time, $$). Output: Good security bugs
- This is the best deal in the universe
Deetz

- Started July 2011
- Received a BOATLOAD of legit bugs. Frontloaded less than one would expect.
- ~ %14 “unbreak now” over last 3+ years
- Paid out over TWO MILLION DOLLARS (dr evil)
Some reasons to start a bug bounty

- It is already happening, embrace it
- “Paying for success” – incentives are aligned
- Driving signal for future deeper security audits
- Can be used to find the teams having security issues and offer to help them more
- Even playing field, anyone can submit and get paid
- Makes vendors quake in their boots
The REAL reason to start a bug bounty

- The one(s) that got away
- It is illuminating to see the issues that slipped passed everything you threw at them
- Harnessing the creativity of lots of people attacking you
Whats the day to day like

- We read about 100 reports before we get an actionable one. This can feel like taking a facebook quiz
- Read reports, triage, verify, dig, fix, diff, pay, communicate to researcher, look for similar bugs, find out why it slipped through
- Nontechnical considerations: PR, legal, etc.
- Language barrier. English skill != HaxOring skill.
- Must love bugs!
Essential tensions

▪ You are bribing someone who has an 0day

▪ Can be confrontational, some things seems like bugs but are not, you get to convince external people who are upset to hear it that they are wrong

▪ Is a customer service and PR job in addition to technical (I don’t always do great at this…)

▪ Anyone can turn around and use bug on zuck then call up cnn
Pitfalls

- Scattershot – people go for easiest stuff first
- Must be responsive with emails and fixes
- Jokers testing bugs on the CEOs account
- Might not work for traditional software companies
- Stressful – messing up a single report has high consequences.
Lessons learned / cool facts

- “It works”
- People don’t argue with you much
- Being generous and putting ego aside
- Direct effort via incentives and gatekeeper
- Most good bugs come from a small % of submitters
The submitters

- 21% are native english speakers
- All types - youngest was 15 year old
- Hired people from this program
- best possible interview question is "Do you know about our bug bounty program?"
- Since been running 2 years it has helped start lots of security careers (consulting, etc)
The system working – stories of two people
Questions