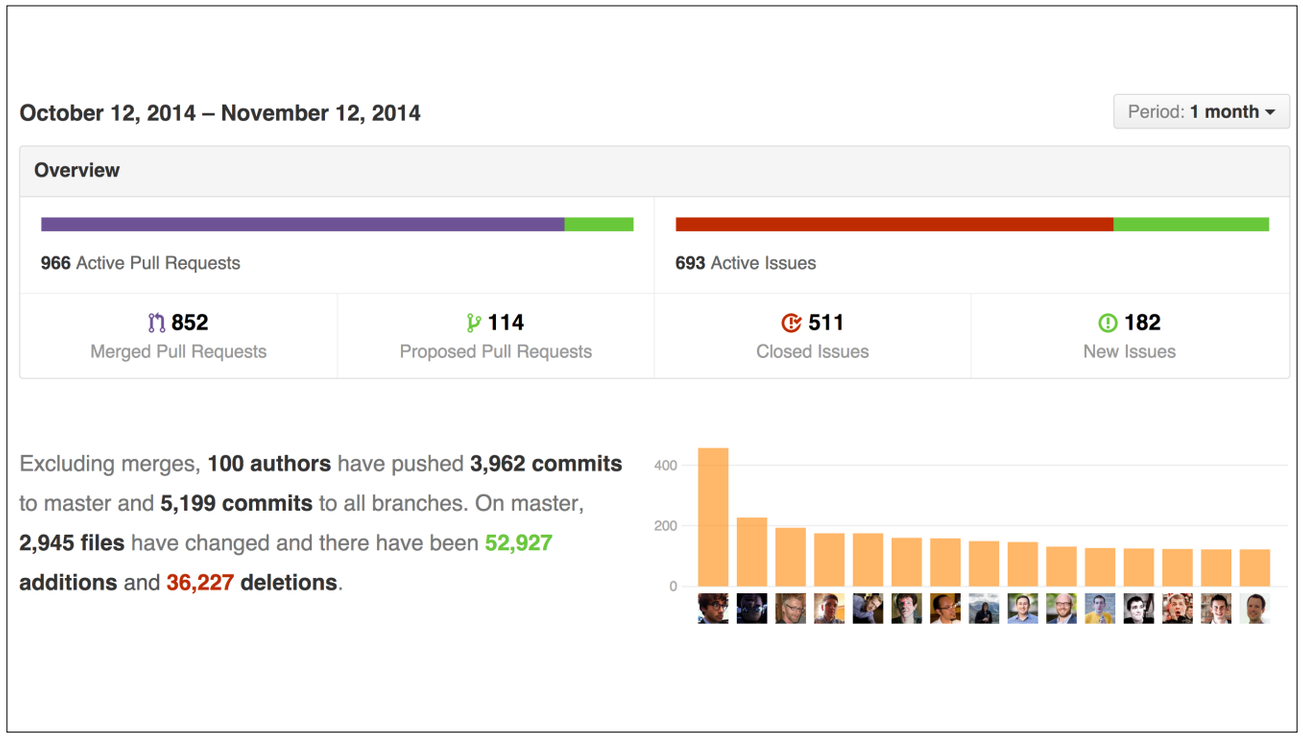
- Started 2 years ago
  - had fun pwning shit for a month
  - doesn’t scale


Ben Toews

- GitHub writes lots of code
- Culture of shipping



- That’s just github/github though
- Across all repos
    - 23089 commits
    - 3607 pulls

stats as of 2014/11/11

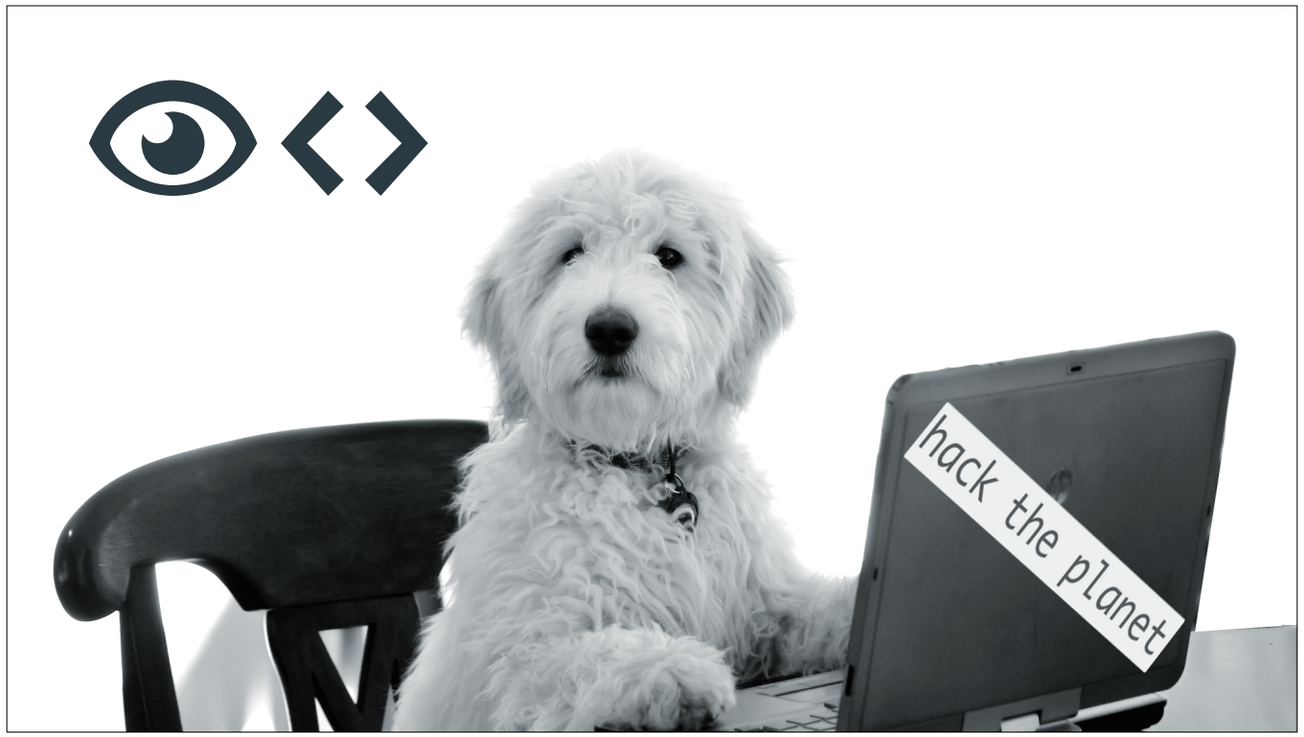
- GitHub culture is very opposed to friction
- Can’t stop people’s work for security

https://www.flickr.com/photos/j-maxx/10312338993/

- With those limitations in place, how do we do appsec?

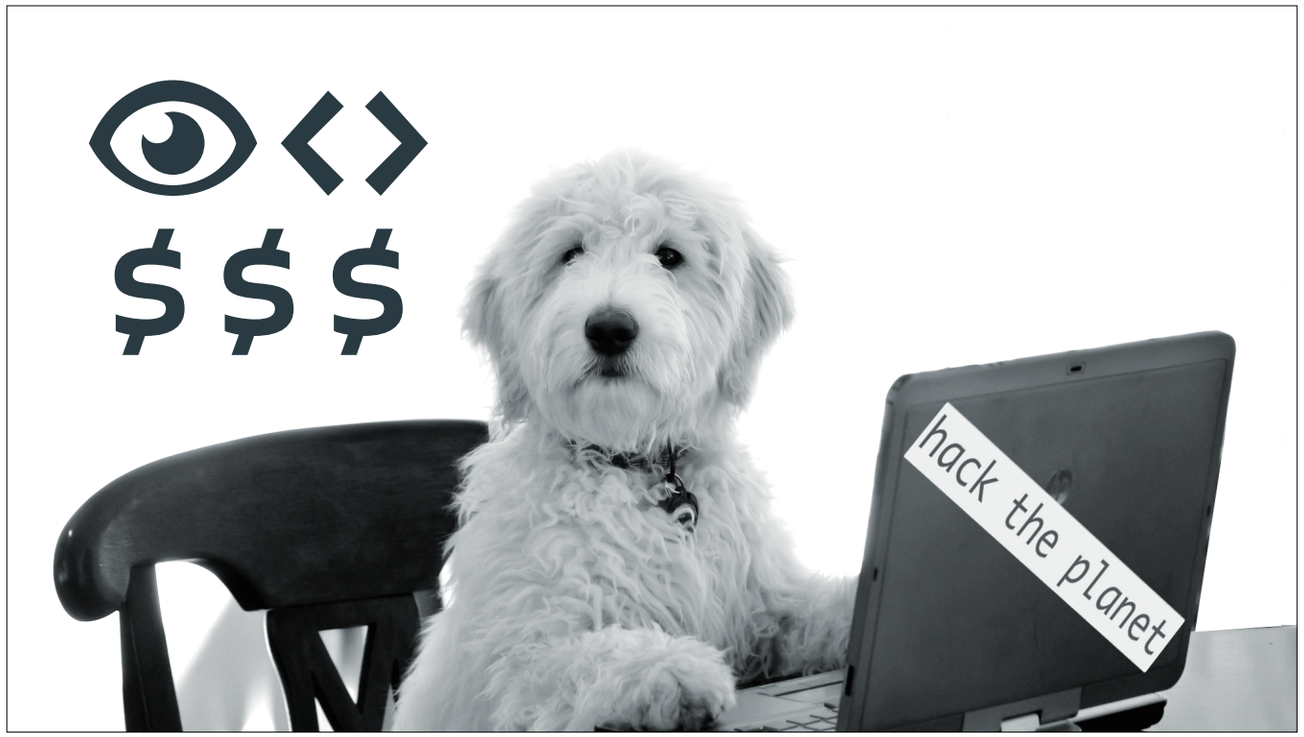
- We start out with the best developers
    - Senior people
    - We treat them like adults
- Always had a culture of security
    - Leadership cares about security
    - Devs care about security
- We build a culture of trust
    - We encourage questions and CCs
    - No formal developer training
        - We write docs
    - We defer to devs where they’re the experts
        - We aren’t afraid of saying “we don’t know”

https://www.flickr.com/photos/27147/3210109272



- Manual code review
    - People ask us for review
    - Production readiness reviews
    - Things flagged by static analysis

https://www.flickr.com/photos/revamptramp/7418429900



- Consultants
    - Helps to scale manual review
    - Why do it yourself when you can pay someone else 10x to do a worse job
    - Seriously though, fresh eyes are good
    - Can hire experts (Golang) for small jobs

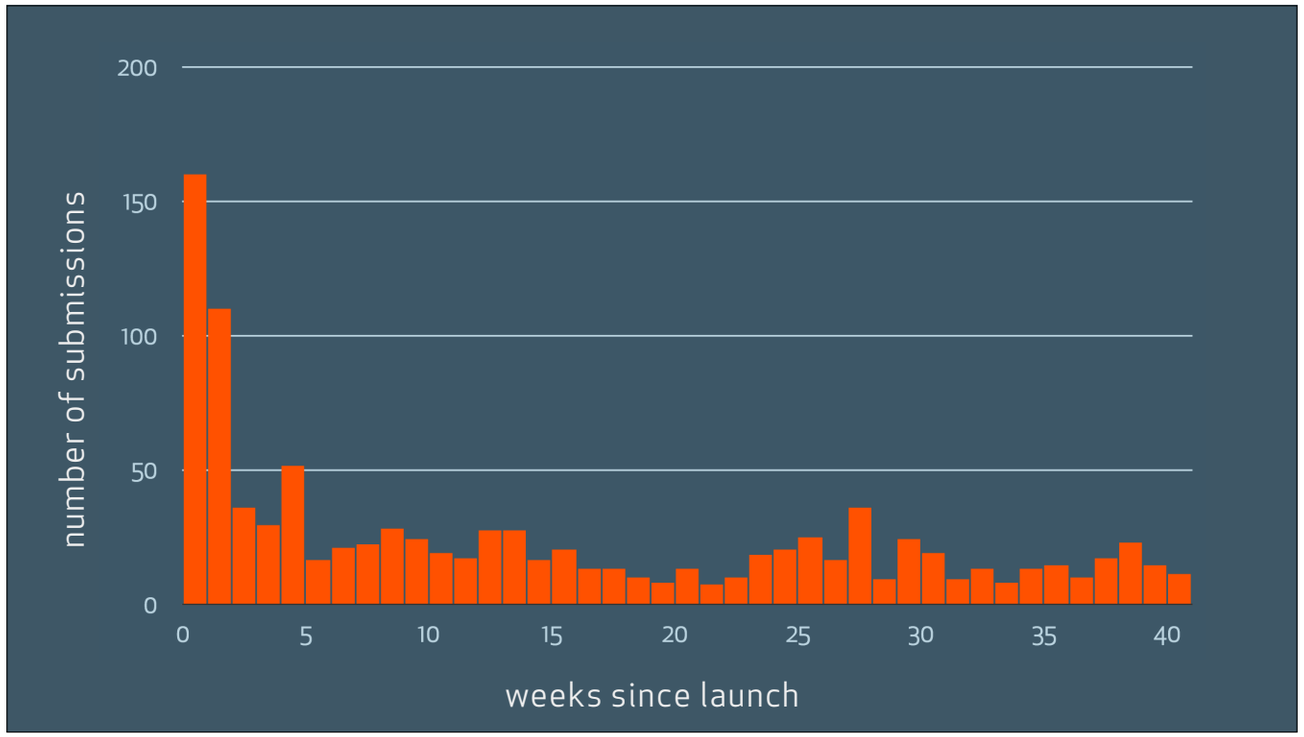
https://www.flickr.com/photos/revamptramp/7418429900

- Bounty Program
    - January 30, 2014

https://www.flickr.com/photos/sergioavatara/3415238118

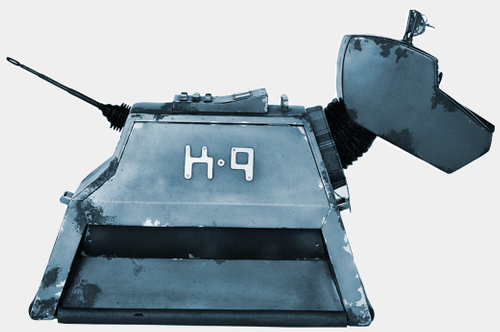
- Bounty Program
    - January 30, 2014 - 9.3 months
    - ~600 *flagged as* spam

stats as of 2014/11/11
https://www.flickr.com/photos/sergioavatara/3415238118



- 2 weeks of hell
- *totally* worth it

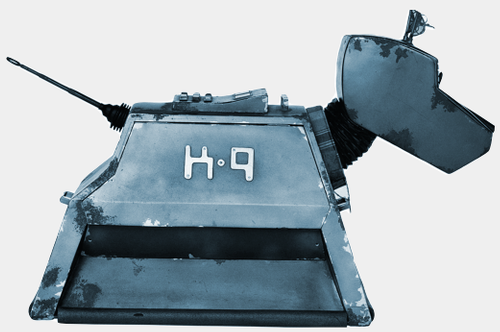
they're coming...



- Robots will inherit the earth
- Static analysis
- Sentinel
    - Brakeman
    - Regexes
    - Push hooks
    - Diffed between commits
    - Inline diff comments

http://www.famouscutouts.com/images/detailed/1/952-K-9.jpg

demo



- Demo sentinel diff comments

http://www.famouscutouts.com/images/detailed/1/952-K-9.jpg

security is hard

- Review
    - good devs
    - manual review
    - static analysis
    - bug bounty
- Decent coverage

@mastahyeti

- Thanks