GitHub Auditor

Team So Far So Good in partnership with Xenon

Team So Far, So Good

Project name: GitHub Auditor

Mentors: Jason Gilmore and Donnie Hasseltine

Chris Yang

Nico Wong

Kyle Stubbs

Edward Thai

Thomas Zhang

Problem

- No efficient way to review possible security issues of multiple Github organizations and repositories.
  - 2FA
  - Outside Contributors
  - Sensitive Information (ie. Api Keys)
- Top-level managers have to audit all of their company's github organizations.
  - No time!
    - Having multiple employees constantly give updates.
    - Thoroughly reviewing multiple orgs and repos one by one.

Solution: Demo

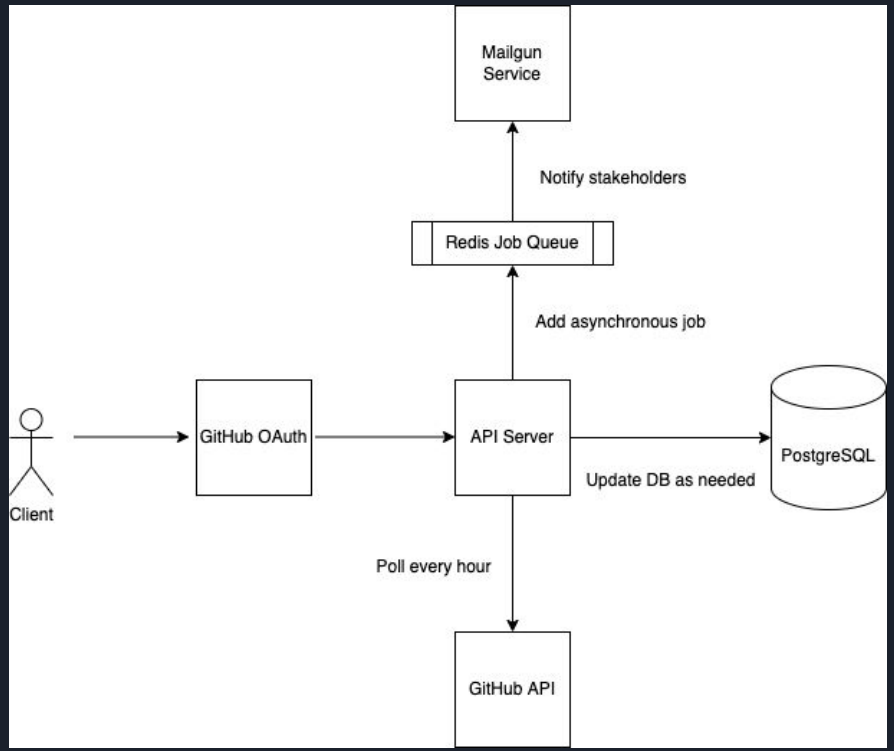
The Current Solution:

- Two Factor Authentication: Organization -> Settings -> Organization Security
- Outside Contributors: Organization -> People -> Outside collaborators
- Dependabot alerts: Organization -> Repository -> Security -> View Dependabot Alerts
- Pull Requests lacking assigned reviewers: Organization -> Repository -> Pull Requests
- Sensitive Information in the Code: Organization -> Repository -> Security -> Code Scanning Alerts (if enabled). Otherwise, not much recourse outside of manual code review

Our Solution:

- Open GitHub Auditor. Recording: https://youtu.be/9AeUV-bzaT8

Technical details



Novelty and challenges

- Setting up the development environment
- Difficult learning the OAuth process and workflow
- Interacting with GitHub API
- Ruby on Rails
  - API development
  - Interacting with PostgreSQL
- React
  - Designing UI/UX
  - Routing on the client side

Next steps

- Display exposed API keys
- Display specific Dependabot alerts per repository
- Set-up Mailgun alerts

Thank You