GitHub for Security Testing

Steve Swiss
Solutions Architect

Agenda

- Problem Statement
- Approach
- Alternatives
- Future Opportunities
- References

Problem Statement

- Must Haves
  - Need to test candidate code updates for security issues
  - Testing should be automatic (not depend on developer or tester manual process)
  - Testing should be easy to scale for many repositories
- Other Opportunities
  - Dynamic security testing for major releases (pen testing, etc.)

Approach

- Trigger security testing on commits to protected branches
- Use GitHub advanced security testing feature (vulnerability, secrets, etc.) on COMMITS
- When new repositories are created
  - Update repo to enable advanced security using repository API
  - Check for README (indicates that repo has at least one branch)
    - If no README, UPDATE repo by pushing default README)

Alternates to GitHub Advanced Security

- Use existing testing resources when COMMITs to protected branches occur
- Can use GitHub Actions in place of custom web hook listener
  - Easy to configure via yaml file to define testing
  - Runs on separate platform - does not burden dev platforms
  - Can easily be tailored to use existing security testing tools or other third party

Future Opportunities

- Adding dynamic security testing for major releases
  - Start with GitHub Actions alternative to static testing, but trigger on RELEASE event
  - Target code can create test environment (Docker, e.g.) and initiate third party DAST

References

- GitHub Repository for this demo: https://github.com/orgs/SMSwissGitHubDemo/repositories
- GitHub Webhooks, and setting up local listener server: https://docs.github.com/en/developers/webhooks-and-events/webhooks/about-webhooks and subsequent pages. The Ruby local server using ngrok is easy to set up and run.
- GitHub Actions: start with https://docs.github.com/en/actions/learn-github-actions/understanding-github-actions#overview and subsequent pages for configuring a repository to send events, and how to set up workflows when events occur
- GitHub Advanced Security: https://docs.github.com/en/get-started/learning-about-github/about-github-advanced-security
- Dynamic security testing (DAST): https://en.wikipedia.org/wiki/Dynamic_application_security_testing for a Wikipedia intro to the topic. We can provide recommendations for third party DASTs if needed.
- CVE website: https://cve.mitre.org for known cybersecurity vulnerabilities, community sourced and maintained
- NVD website: https://nvd.nist.gov maintained by the US government, and is synced with CVE