EDGE X FOUNDRY™

SAST for EdgeX Foundry

James Gregg / EdgeX DevOps

Wednesday July 17, 2019

Static Application Security Testing (SAST) (Fuji scope)

Initial evaluation focused on tools / languages / cost / ease of integration

- *Missing requirements from Security WG*

Tool Selection

What's the right SAST tool for EdgeX Foundry?

- *Define the criteria for tool selection*

Implementation / Integration

What should happen if the scan finds a vulnerability?

- Define Build Behavior
  - Break the build, Continue build but Alert, Scan outside of Build separately
  - How to Alert and Who receives notification? Slack, Email

Developer Feedback Loop / Remediation

What happens after tool is up and running scans?

- Code remediation timelines based on severity
- Roles and Responsibility of Code Reviewer within tool
- Measurement of improved security of code base over time (ties into certification)

Seeking input, recommendation and direction from EdgeX Security experts

Initial Analysis of SAST Tools

- Previous discussions and review of findings in EdgeX DevOps WG meetings
- Focused on tools that were FOSS and supported EdgeX Foundry code base including Go language support

Tools \ Languages	GoLang	C	C++	JavaScript	Python	Groovy
Fortify	✓	✓	✓	✓	✓	✓
Coverity	✓	✓	✓	✓	✓	✓
Kritika		✓	✓	✓	✓	
SonarQube / **SonarCloud**	✓			✓	✓	
Checkmarx	✓			✓		
Snyk	✓			✓	✓	
Guardrails	✓			✓	✓	
Whitehat				✓		

Recordings / Meeting Minutes are available online (WW26-28)

https://wiki.edgexfoundry.org/display/FA/DevOps+Working+Group?preview=/329486/31588576/StaticCodeAnalysis.pptx

Analysis / Ranking and Rating

Based on the previous table, the analysis are captured for the tools which supports GoLang.

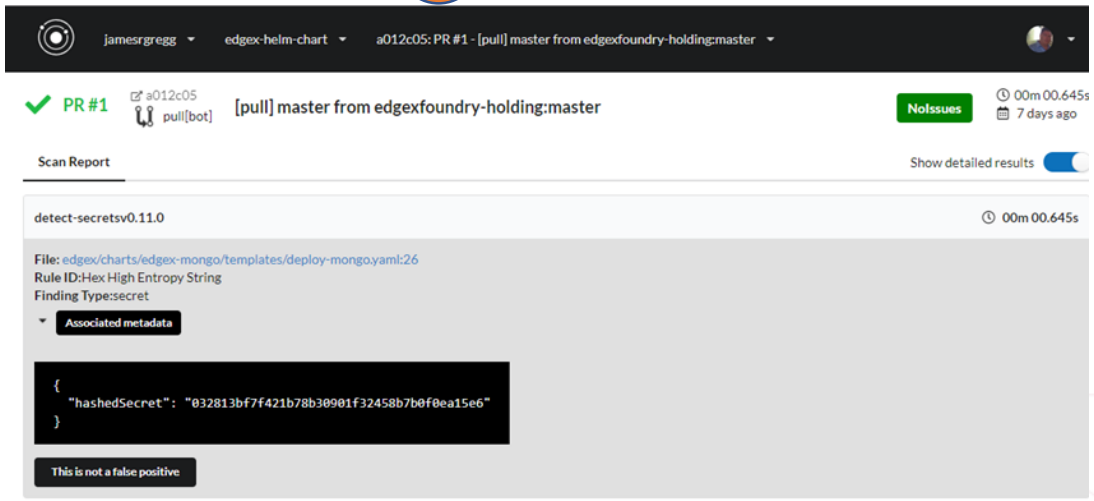
Rank	Tools	Github Integration	Support for Docker	Cost	Open Source	SCM Support	SaaS	Rules config	Remarks
1	Guardrails	Need to see how this could work for EdgeX Foundry.		Free for open source project Pricing	No	Yes	Yes	Yes	Paid clients have additional functionality for CLI and PR support
2	SonarQube *SonarCloud*	Easy github plugin Scanner Info Server Info	Yes Docker	Free for open source project, except for C, C++ Pricing	Yes	Yes • Get Started • Jenkins Configuration • Sonar Scanner	Yes	Yes	It supports GoLang, but C/C++ scanning works only on Developer / Enterprise version. Additional overhead to implement with LF resources needed to enable by FUJI.
3	Snyk	Integration not supported for GoLang (Details)	~~No for GoLang~~	Free for open source project Pricing	No	Yes Documentation	Yes	Yes	Snyk supports testing and monitoring Go projects that have their dependencies managed by dep or govendor. Go support is currently supported via the Snyk CLI and Git Integrations ~~Seems like limited support for GoLang – need supplier roadmap~~ Reporting requires paid plan = $$$
4	Fortify	Don't see the proper documentation	Couldn't find it	Cost involved	No	Yes Data Sheet	Yes	Yes	It supports on demand scanning, but it is expensive.

Updates

- Snyk now supports Go with go modules using CLI
- Coverity not considered in this initial analysis
- Linux Foundation doesn't support SonarQube instances but offers SonarCloud

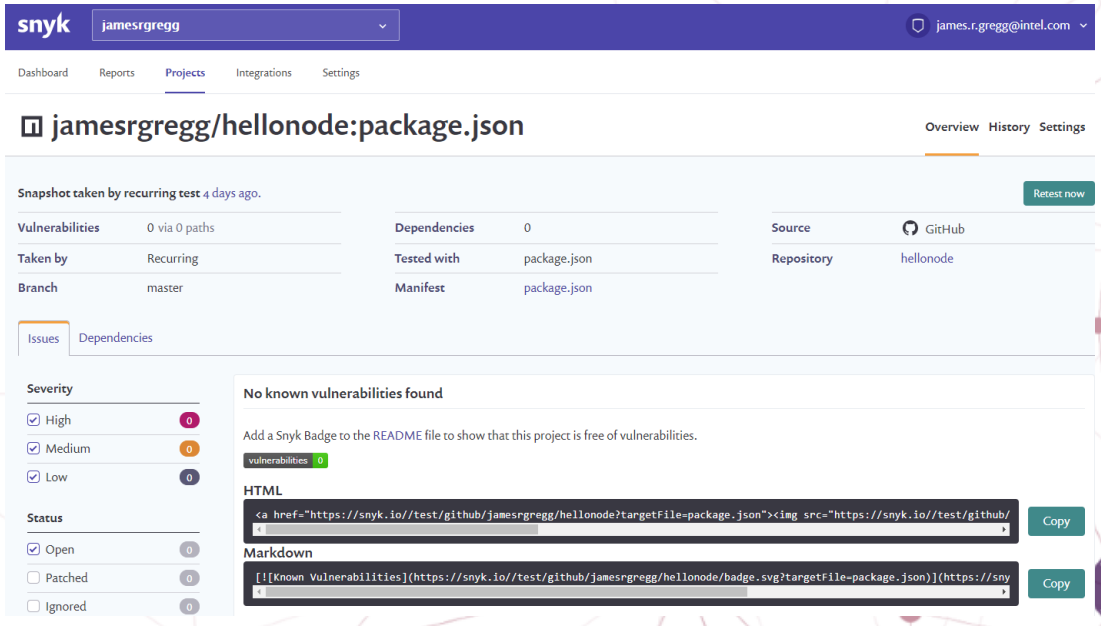
POC Recap

Guardrails 1



Initial Findings:
Not the right solution for this project.
Oriented towards web based applications, not microservices.

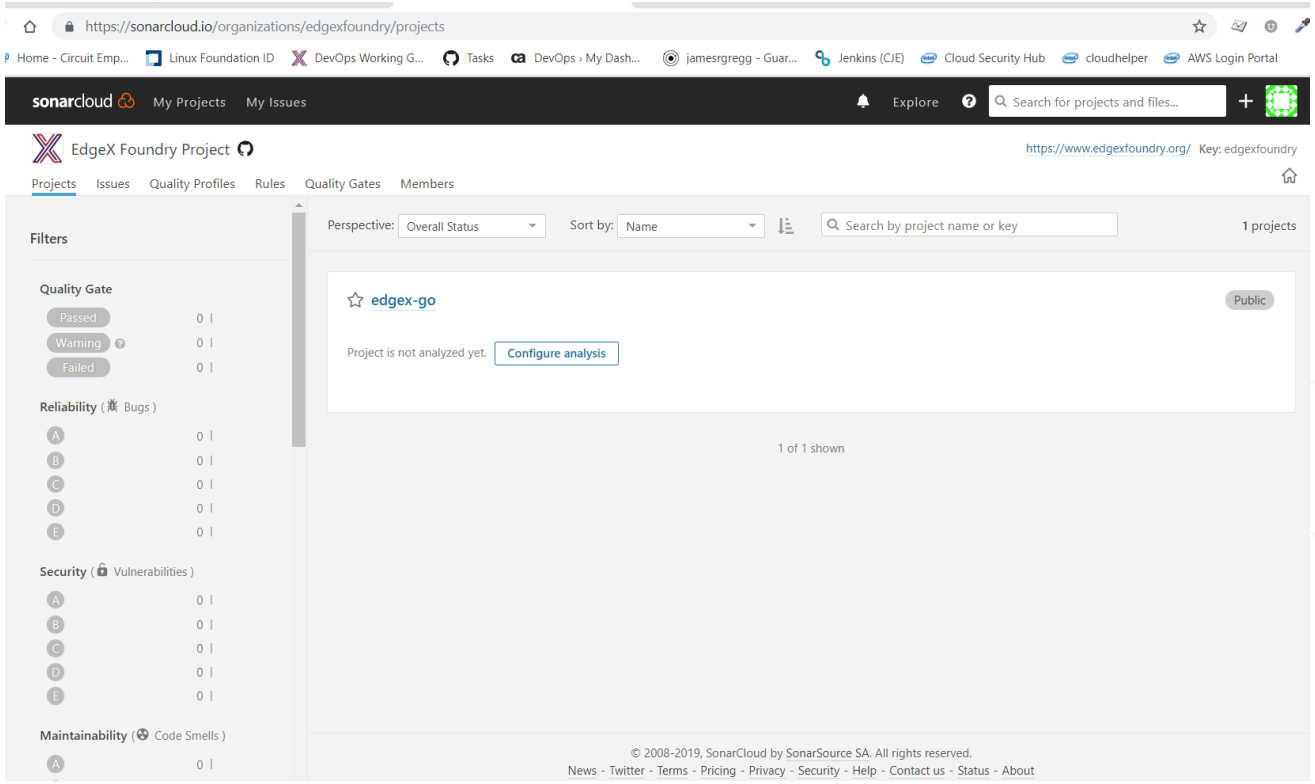
Snyk 3



Initial Findings:
Ruled out due to lack of Go Lang support with go modules.
There now appears to be a Snyk Docker based CLI that supports scan based on go.mod

SonarCloud 2

(Linux Foundation service offering)



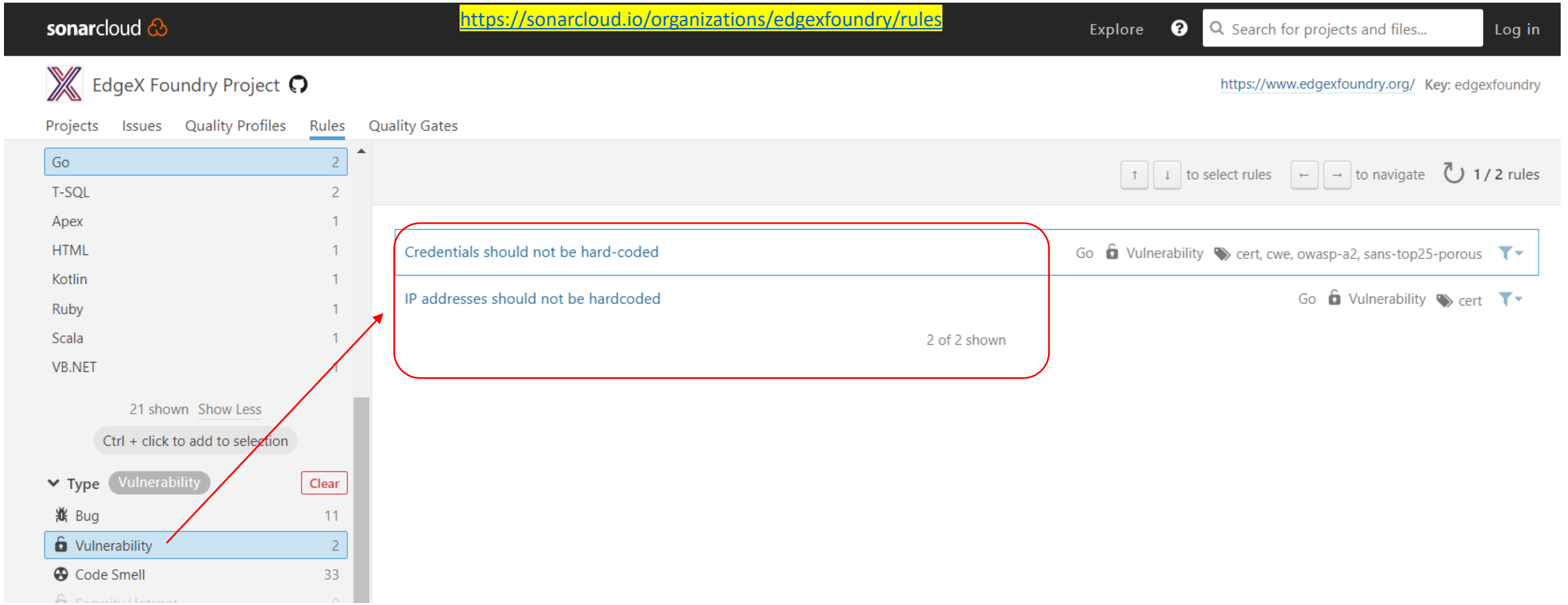
- SonarCloud SaaS version
  - Free for Linux Foundation (Open Source)
  - Easy implementation
  - Offers Code Quality / Code Coverage / Code Smells
    - Same capability already in place now with Codecov.io for Code Coverage reporting
  - Very Limited Security Checks for Go (see rules next slide)
  - Other Languages include (mostly web oriented)
    - OWASP Top 10
    - Sans Top 25
    - CWE

Currently enabled on edgex-go repo but hasn't been scanned to date

SonarCloud Vulnerability Rules for Go

Rules

https://sonarcloud.io/organizations/edgexfoundry/rules



Wrap Up

- Discussion
  - Developer Workflow should include recommendation from Security WG on developer tool for local scan

  Malini suggestion to take a closer look at https://github.com/golangci/golangci-lint and go-sec

  Try - gometalinter with gosec

  - Resourcing for role for reviewing would be handled within SIR team
  - Need to focus on tools that provide true static code analysis
  - Image scanning is addressed with Clair as pre and post release reporting process

- Next Steps / Recommendation
  - Look at output from different tools
    - SonarCloud
    - Snyk
    - Coverity
    - Checkmarx
  - James to coordinate a demo with Snyk within this forum
  - Enable the SonarCloud integration using sonar.properties
  - Bring reports into Security WG for review