STACK the Codes

6 OCT 2022 - 6 NOV 2022

CONTENTS:

Presented by CSG

GOVTECH
GOVERNMENT TECHNOLOGY AGENCY OF SINGAPORE

PROBLEM STATEMENT 1

As the Cybersecurity operations manager, I would like to proactively scan the World Wide Web (WWW) to identify and take down phishing sites acting as authorities of the Singapore Government. Doing so should stop malicious sites from claiming more victims in Singapore.

To enable this proactive hunt, I need help with engineering two main components*:

a) To efficiently and cost effectively crawl, scrape, and screenshot URLs at scale to handle more than 1 million pages / day on continuous basis.

b) To Classify crawled webpage using ML and/or statistical models to identify a few broad categories like (Offensive Content, Cyber malicious, and Scam / Phishing, potentially illegal activity, etc)

Highly recommend the use native cloud capabilities*

PROBLEM STATEMENT 2

The downside to a centralized ID management means that it is susceptible to a single source of failure. In event that the central ID provider is made unavailable and rendered non-recoverable, the central ID provider/agency will not be able to perform trust attestation or authentication of users and devices.

Thus, the solution has to explore adopting a decentralised model of doing trust attestation such as using blockchains, smart contracts and immutable user profiles to ensure that users and devices connecting to government networks are authorised, authenticated, secured and security posture validated constantly. New users and devices can also be added to the blockchain via peer-to-peer validation.

PROBLEM STATEMENT 3

mTLS is a much needed baseline for Zero-Trust as a whole. However, its PKI setup requires heavy operational investment and resources from agencies which also includes the management of the key lifecycle from provisioning to renewal to revocation.
If any of the stages are not handled timely, the impact is rippled to the web services and may bring down the business in worst case.

The emergence of SPIFFE issuing X.509 SVID also means that whole setup need some form of “transformation” into mesh network and sidecar driven setup (towards a K8 architecture). Challenge is whether there is an optimal (and yet secure) translation from existing PKI to SPIFFE or an alternative to achieve a reasonable identity-based attestation level.

PROBLEM STATEMENT 4

As a DevSecOps specialist, I would like to ensure that developers are able to develop features quickly, while being prevented from introducing common vulnerabilities into the application, such as those listed in OWASP Top 10. The solution should secure a common web framework (e.g. Django, Express.js, Spring), to prevent developers from introducing specific classes of vulnerabilities (e.g. XSS, SQLi, command injection, IDOR).

PROBLEM STATEMENT 5

As a developer, I would like a tool to provide an abstraction layer on top of Terraform, to enable developers to connect pre-defined Terraform modules (e.g. modules for s3, alb) easily (e.g. through visualisation and automating away "glue" code).

PROBLEM STATEMENT 6

With AI being more prevalent in systems, as part of adversarial AI, I would like to develop a tool leveraging on AI (model, expert rules, statistical analysis, optimisation algorithms) and automation to assess the efficacy of cybersecurity products (e.g. NexGen F/W, WAF).

SUBMISSION CRITERIA

1. STACK the Codes recommends participants to submit technical solutions for any of the problem statements listed above. Teams **can only** select **(1)** problem statement and submit **(1)** solution for the selected problem statement.

2. Submissions **must** include a hosted **code repository** (Github) containing a **fully-functional prototype** and its **full source code**. The repository should also include a detailed documentation either in the form of a **readme/wiki.**

3. Submissions **must** also include a **video demonstration of core functionalities** of your solution (**maximum 5 mins**). This video can be embedded with your documentation (hosted on youtube/gdrive or other platforms).