CWE REST API Working Group Meeting – May 5, 2022

1) Call to order
2) Agenda approval
3) Regular order
   - Update on email list reflector: CWE-CAPEC REST API Working Group cwe-capec-rest-api-working-group-list@mitre.org
   - Note - GitHub: https://github.com/CWE-CAPEC/REST-API-wg
   - MITRE infrastructure update
     - CVE team also is updating an API
     - 2 different WGs: REST, schema
   - DB/tool chain – deferred to later meeting
     - STIX 2.1
       - Has an extension for an additional schema (for the weakness type)
       - Might get a schema change asynchronous to the "WGs wishes"
       - Could defer STIX integration to a future date (consult Rich Piazza)
     - TAXII
       - Like the REST API spec for STIX content
       - If STIX is "dropped", so is TAXII
     - Swagger (language: API Documentation & Design Tools for Teams | Swagger) can be used as a design front-end to the API, code, and docs, and supports port to YAML
       - Use this tool for development
       - OpenAPI version – selectable by Swagger
       - Specific URL for Swagger i/f
     - XPATH link to XML
       - Internal infrastructure leveraged to deliver filtered list (for example)
       - Raw data faster access than fully-rendered HTML page
         - https://cwe.mitre.org/data/definitions/1194.html
         - links to https://cwe.mitre.org/custom/view.html?id=1194 by clicking the "Filter View" button above the tree
         -
     - GraphQL and GraphQL Playground (Charles, Ray) (https://graphql.org/)
       - Means to filter returned data
       - Very convenient for forming complex queries
       - Limits requests and data via API
       - Would be interesting to investigate support via MITRE team
       - Helps with the REST API piece by already supporting complex queries OotB
       - GitHub uses GraphQL
       - MITRE server component is required to support
     - JSON (schema example: https://github.com/oasis-open/cti-stix2-json-schemas)
4) Action item review
     - Rajat to compare Swagger and GraphQL for next week
     - Steve CC. and Rich to deliver database nomenclature (vocabulary, glossary) for next week
     - Metrics on API use, yet protect security of users' information
     - Means to restrict use (to avoid DoS issues, etc.) to registered users; API keys/tokens?
     - Principals – security
5) Adjourn