CWE REST API Working Group Meeting – May 12, 2022

1) Call to order
2) Agenda approval
3) Minutes approval
4) Regular order
   - Note – 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
   - DB/tool chain – deferred to later meeting
      - Rajat compare Swagger and GraphQL
         - Swagger query: need to know the attributes prior to query
            - All information for a single CWE
         - GraphQL filters through the query/response
            - Can filter down to one field of 1 CWE
            - Can get "related" CWEs more easily
            - SQL-like queries
            - Does not support the caching, but Apollo Client or urql can be used
            - For rate-limiting situations, time-outs, responses, and other limits can be set on the MITRE side
            - GraphQL Shield might help with some specific limit issues
            - https://graphql.org/code/ has some utilities
         - Could also shift post-processing of query from MITRE to client
         - May be able to form a query that is problematic for the server
            - Due amount of return data for the query, for example (limits kick in, etc.)
      - Steve CC. and Rich deliver database nomenclature (vocabulary, glossary, taxonomy)
         - Need to unify the terminology between CWE and CAPEC databases
         - "Property" is a generic term for a "part" of an object
      - Note – Swagger (API Documentation & Design Tools for Teams | Swagger)
      - Note – GraphQL and GraphQL Playground (https://graphql.org/)
      - Note – JSON (schema example: https://github.com/oasis-open/cti-stix2-json-schemas)
5) Action item review
      - Examples of schema changes
      - CWE/CAPEC entry with "overlay" of terminology for database items/properties
      - Principals – security
      - 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?
6) Adjourn