CWE REST API Working Group Meeting – December 15, 2022

1) Call to order – recording
2) Agenda approval
3) Minutes approval
4) Regular order
   - Note – email list reflector: cwe-capec-rest-api-working-group-list@mitre.org
   - Note – GitHub: https://github.com/CWE-CAPEC/REST-API-wg
   - Note – CWE data response content: https://cwe.mitre.org/data/xsd/cwe_schema_latest.xsd
   - Note – Swagger: API Documentation & Design Tools for Teams | Swagger
   - Note – GraphQL and GraphQL Playground: https://graphql.org/
   - Note – Specs are here: https://github.com/CWE-CAPEC/REST-API-wg/tree/main/specifications
   - Status (MITRE)
     - Slipping roll-out of initial content
     - OpenAPI doc could be made available (MITRE to check)
       - That spec can drive client library development (REST library)
     - Prototyping server code could be made available for simple testing
       - Someone could use that to create an internal testing sandbox
   - Search process/discussion
     - Access (search) syntax schema versions might change at db release time
     - Enumerations change more frequently (these days)
     - History content (shape) has changed, for example adding proper attributions to content addition
       - https://cwe.mitre.org/data/archive.html - The full list of schema changes can be found in the far right column "Difference Reports" under the "Schema" link. Most things are minor changes (enums) vs major changes (changing datatype/required)
       - "Difference" reports should remain as they are
     - For historic comparisons or searches, let folks save off their own db histories "internally"
       - No need for MITRE to answer a query for "historic minutia"
     - Constrain search fields to "alpha-numeric"
       - Is there reason for adding and allowing special characters in search query?
       - Content search
         - Tags? (https://documentation.softwareag.com/webmethods/compendiums/v10-5/C_API_Management/index.html#page/api-mgmt-comp/co-api_tagging.html)
         - Keywords?
         - Index only the enumerated items? – this seems to handle the main need
         - Questioning whether the entire db is completely searchable…
         - Maybe a "blacklisted" word list (like "the")
         - In terms of special characters in the query, we do have enums such as:
           <xs:enumeration value="ASP.NET"/>
           ...
           <xs:enumeration value="C++"/>
           <xs:enumeration value="C#"/>

        - Since it's Go I thought there are C strings or C++ strings under the hood essentially. I'm not 100% sure what the concern is with special characters when we aren't parsing and forwarding onto a database query.
        - "Code injection" seems to be handled, already, although buffer overflow might still be an issue
        - Elastic search should be considered
    - List of "decisions" doc review
5) Action item review
    - Continue review of list of "decisions" doc review
    - Check GitHub for enhanced views of db content (all)
    - Status update
6) Adjourn