MITRE CWE/CAPEC REST API Specification

1 INTRODUCTION

2 REQUIREMENTS

2.1 DATABASE (DB) STRUCTURE

- Store in JSON format
- Potentially cache data periodically to unload direct db access strains
    - Full complete db may be hosted elsewhere
- Schema of CWE/CAPEC could benefit from unification (unify CWE and CAPEC structure)

Need a picture of the database for vocabulary leveling.

schema version – database version – database target – field – entry

e.g., M001 – 01 – CWE – ID – 1248, or M002 – 03 – CAPEC – ID – 148

- Self-contained JSON access mode
  May or may not have internet access, may not be able to provide server function, so may need whole JSON available locally

    - Library of access code which would mate up with downloaded “local” JSON (stretch goal)
        - Could provide “local” server code with JSON for “internal” (local) access mode
        - Open-sourcing the access code (OpenAPI, plus back-end code (Python))

2.2 VERSIONING

- If/when new db entries come (new field, deleted field, etc.) → new version
- Only two schema (the latest and the one previously available) will be available
    - The “previous” schema database will be retired after XX (time)

Database versioning should encompass new database schema and a sub-version of the database per schema.

A new schema version is created whenever:

1. A new field gets added to the database
2. A field gets removed from the database
3. A field gets renamed in the database

Enumerations are now (for the most part) treated as “data”. No new database version in incremented when the following occur:

1. A new enumeration is added to a field that is constrained to a finite set of values
2. An enumeration is removed from a field that is constrained to a finite set of values
3. An enumeration is renamed in a field that is constrained to a finite set of values

The exception (in CWE) is Related_Weaknesses.Nature which will spawn a new version.

CAPEC also has some structural enumerations which also would be an exception to the “no new version” rules, above. [add entries]

- A new database version is created whenever the database is released with any field entry modified from the previously released version.
- Version of schema and db is embedded in the raw data returned as part of the query response.
- A specific query could return the schema and db versions.
- Notification of schema and db version changes shall be delivered via social media, email lists, and website notifications.
    - Retirement events occur XX (time) after this notification date

2.3 Initial Development Goals

A development avenue shall be made available for new schema and database interaction for client developers.

Query for full database with REST (CWE or CAPEC).

Query one ID in REST and get a full JSON of that ID. [Luke/Alicia proposal to split some types out]

2.4 Optimizations

- ~~ETAG for caching data and reducing latency~~
- Look into filtering requests and whether to support all levels of filtering

2.5 Error Codes

- 200: Success
- 204:
    - No server information available
    - CWEs/CAPECs not found
- 303:
- 4xx: Request timed out
- 429: Too many requests within a given time
- 500: Internal server error
- MITRE fill out list of specified codes, thus far
- 5xx codes should not be returned to the client

2.6 User/System Tracking Metrics

- WAF (web application firewall) could track some aspects depending on WAF source

3 API Syntax

3.1 Specification

Provide spec in OpenAPI format

3.2 Query

Keep “tree” view in path if certain view is required, but default to “all”.

- Query for FULL database with REST (CWE or CAPEC)
- Full list of weaknesses
- Individual IDs
- List of IDs that match a category
- List of IDs that match a view
- List of IDs that contain specific value in a field (e.g., tech name = memory)
- Parent ID of CWE
- List of allowed enumerations within a field
- Meta data of all possible values for CWE field
- Return entry Version and Timestamp of a particular db
- Filter responses (elastic search investigation)
    - Field (!)= XXX
    - Field (not) contains YYY
- List of new CWE entries between version releases (lower priority)
- List of new and modified CWE entries between version releases (lower priority)
- Return “delta doc” in codified syntax (potential)
- List of new CWE entries between release dates (lower priority)
- List of new and modified CWE entries between release dates (lower priority)

3.3 Response

- Do not need to return nested JSON representing tree structure (parentOf, and Relationships (childOf) sufficient) – can return flat structure of weaknesses/categories or IDs
- Unfilled required field returns “null”