Security Professional,

The MITRE Corporation maintains the Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) databases. A new effort is underway to ease the interface between security SW and HW architects, EDA tool developers, verification engineers concerned about mitigating security risks in their products; and the databases themselves. A new RESTful API will be designed.

You are invited to join this effort and become a member of the Working Group performing the work to:

1) Craft the RESTful API syntax and semantics which users will send to the CWE and CAPEC database web services;
2) Determine which content and syntax the databases will use to deliver content back to the users;
3) Determine if there are structures or content missing from these databases which would complete a link between this content and that required for tools and standards (such as the Accellera SA-EDI standard); and
4) List any structure or content missing from these databases that would help with further automation (such as versioning, etc.).

This effort will require your attendance at virtual meetings, once a week, likely through the end of 2022. At the end of this process, the Working Group will provide development and design support, and deliver a document and any other collateral that can be used by MITRE to craft the required infrastructure to support the RESTful API.

Please reply to a.cron@ieee.org if you are interested in actively participating in this effort.

Best regards,

Adam Cron, Synopsys

Chair, CWE/CAPEC REST API Working Group