User Experience Working Group

November 19, 2025

Participants

- John Keane
- Chris Coffin
- Steve M Christey
- Matthew Coles
- Sarah Felson

Agenda

- CWE Completeness Efforts
- Open Discussion

Meeting Summary

- **CWE Completeness Efforts**
  Steve Christey outlined standardizing, prioritizing, and requiring top-level elements found within CWEs can increase their completeness, ensuring the CWE Program provides the most accurate and quality information to its consumers.

Action Items

- **Meeting Topics:** UEWG Members should let Chris Coffin know if there are any specific topics that they would like covered in the future.
- **Usage Metrics:** Chris Coffin to consider Usage Metrics as a topic of discussion for future meetings.
- **Meeting Slides:** Chris Coffin to collaborate with a third party to ensure past meeting slides are uploaded to GitHub.
- **Future Meeting Date:** UEWG to decide if the next meeting should be pushed to January 2026.
- **CAPEC Inquiry:** Matthew Coles to reach out to Alec Summers regarding the current status of CAPEC and its ownership.

Meeting Notes

CWE Completeness Efforts (Steve M. Christey)

- **Completion:** In the context of the CWE Program, completion refers to the CWE corpus obtaining entries for all weakness-related concepts. A complete CWE entry should include, where feasible and relevant, “high-priority” top-level fields, “preferred” elements, sub-elements, and CWE sets. Additionally, using elements such as maintenance notes and extended descriptions should be minimal.
- **Top-Level Elements:** There are about 25 different elements within the CWE Program. Each element may apply to a different use case, such as mapping or development. Top level elements are fields that have been identified as mandatory for every report.
    - **Related Attack Patterns:** Matthew Coles brought up concerns regarding deprioritizing the “Related Attack Patterns” element as it is important to developers.

Steve responded that the deprioritization is occurring because the CWE Program is no longer actively supporting CAPEC.
    - **Detection Methods:** Detection methods are how a CNA finds instances of weaknesses in codes. Matthew suggested changing the weaknesses name, while acknowledging a name change can cause confusion amongst consumers.
    - **Future Guidelines:** Matthew suggested the CWE Program should distribute guidance that outlines the top-level elements and offers alternatives for elements that are being deprioritized.
- **Quality:** The CWE Program can ensure it provides the most complete information by examining the quality of data fields in new and existing records.
    - **Roadblock:** John Keane warned that there will be certain circumstances where completeness is not achievable. The group agreed and decided that the effort to ensure accuracy and quality of CWE reports is still worth pursuing.
- **Depth:** There are currently 944 active weaknesses within CWE 4.18 that the Program can use to measure completeness of elements. Steve conducted some research and found that of the 944 active weaknesses, only 198 had specified affected language, 231 had affected technology, and 327 CWEs only had 1 demox. The missing information leads to informational gaps that need to be filled.
    - **Collaboration:** Community involvement, specifically from the Python Secure Coding Project, can assist in creating weakness examples, and boost Python support within the CWE Program.
    - **References:** Various CWEs are missing references, such as authors identified, and contain links that are no longer available.
    - **Mitigations:** Mitigations are common practice when working with CWEs, but their effectiveness is unknown. Steve proposed the CWE Program investigate this as most mitigations for CWEs do not fully eliminate a weakness entirely but may still be useful in certain contexts.
    - **AI Use:** Previous trials to determine if AI could generate examples of CWE fields for developers looking to complete the information in their reporting were unsuccessful as the LLM tool was not able to identify the correct CWE. However, if experts review the outputs of the AI generation and continue to build on its models, then it may be more effective in the future. Other AI tools have been explored but their CWE Mappings were also incorrect.
- **Assigning Element Priorities by Use Case:** The CWE Program identified approximately 14 elements that should have 100 percent coverage across all active CWEs and is looking to outline the priority level for each of these elements by use case. For example, the Program could outline that a Developer does not need to prioritize adding the element "Mapping notes" while a Mapper does. To ensure these priority levels are accurate, the CWE Program will conduct outreach to various stakeholders and has already begun collecting and organizing data.
    - **Observed Examples:** Matthew responded to Steve's visual of the data collected regarding elements and their priority levels by use case with a suggestion that the element "Observed Examples" should be medium to low priority for Mappers

because they are useful for comparisons. Steve agreed and mentioned the element "Demonstrative Examples" may also need the same change.
    - **Metrics:** Matthew suggested measuring currency and recency as a means for conducting quality assessments.
- **Completeness Status**: According to collected data, in 2024, 15 of the top 25 CWE fields were almost, if not fully, filled. However, of the most requested and all active Weaknesses, the completion rates were often low.
- **Approach to Prioritization**: There are various methods being considered to evaluate completeness, such as prioritization of a specific task or element, and focusing more on depth than breadth. There will be continued discussion regarding the approach to identifying priority levels for CWE elements, and ensuring quality will be a time priority.

Open Discussion

- **CAPEC:** Matthew Coles mentioned he has found a potential owner for CAPEC and will reach out to Alec Summers to obtain updates regarding its ownership and status.
- **Meeting Notes:** In response to a question, Chris provided the link to the UEWG Meeting Notes, which can be found here on GitHub.