User Experience Working Group

March 26, 2025

Participants

- Steve Christey
- Chris Coffin
- Scott Drinkall
- Jim Duncan
- John Keane
- Rich Piazza
- Przemyslaw (Rogue) Roguski
- Suzanna Schmeelk
- Christopher Sundberg

Agenda

- CWE Views Questions & Guidance
- Macro-Usability Changes for CWE 4.17
- Open Discussion

Meeting Summary

- **CWE Views Questions & Guidance:** Chris invited the group to share their thoughts on questions raised by a CWE power user. The discussion aimed to gather insights and suggestions on how to better support users in understanding and representing CWE data accurately.
- **Macro-Usability Changes for CWE 4.17:** Steve provided an overview of the proposed changes, emphasizing the need to make individual CWE entry pages less text-heavy and more user-friendly. He mentioned that the changes would include better organization and visual presentation of information.

Action Items

1. **VulnCon Participation:** Send the invite to the regular meeting to Jim Duncan. (Chris)
2. **CWE Views Customization:** Explore the possibility of allowing users to define their own CWE views for specific custom use cases. (Chris)
3. **CWE Views Simplification:** Consider reducing the number of CWE views and focus on generic ones that cover specific use cases. (Chris)

Meeting Notes

CWE Views Questions & Guidance (Chris Coffin)

- **Background:** Chris shared questions from a CWE power user regarding the role of views and their relationships with CWE hierarchies. The user wants to ensure they are representing CWE correctly and providing appropriate context for their customers.
- **Specific Questions:** The specific questions centered on providing CWE relationships without view context, the structure of CWEs and views, CWE and category relationships, and the depth of relationships.
- **Addressing CWE View Questions:** Steve noted that every relationship is tied to a specific view. For example, if SQL injection is a child of injection, that would be relative to a particular view. Most categories are tied to a single view, although in the past some categories belonged to parts of different views (still recorded as separate relationships).

- **Developer View for Higher-Level Analysis:** Jim pointed out the bias of expecting two parents. The influence is multi-varied and should not be assumed to be constrained. Jim emphasized the importance of ancestry to formulate relationships, group ideas, and help decision-makers. Jim noted that in his experience he preferred the developer view rather than the research view, which tends to lead to counterproductive paths.
- Steve explained that the developer view is incomplete, covering a subset of weaknesses. As it is organized by categories, they may be more understandable to developers but categories may not be specifically about weaknesses. As a limitation, not all CWEs are in the software developer view. Some CWEs that are low level are intentionally omitted.
- Steve noted in the chat that having lots of views can make large numbers of relationships for popular CWEs, which can make it more difficult for new users (see CWE-89 or CWE-79, for example).
- Steve noted in the chat that View-1400 covers all weaknesses and is rather flat, using high-level categories such as "memory safety." There is similarity across categories and similarity to high-level classes in the research field. These categories offer more friendly descriptions to many end users.
- Suzanna noted in the chat that learning more about the general view development is helpful and that she has worked with them in the past.
- Rogue stated that while the software developer view is not complete, categories provide a value for developers.
- Chris mentioned that research view on the homepage is now listed as *all weaknesses*.
- Chris stated that the next steps are to educate about CWE views and how to interpret them.
- Rogue suggested reducing the number of CWE views and focusing on a few generic ones that cover a specific use case. This would allow people to create their own views.
- Chris responded about the value of specific CWE views.

Macro-Usability Changes for CWE 4.17 (Steve Christey)

- **Background:** Chris introduced the topic, which covers proposed macro usability changes discussed by Steve on the last call. These changes aim to address the wall-of-text issue and make CWE entries more digestible and easier to read and interpret.
- **Overview of Proposed Changes:** Steve noted several efforts to improve UX for individual web pages, including reducing the "wall of text" by changing the default from "comprehensive" to include only some elements and changing the color/presentation for presenting different types of entries (deprecated, obsolete, categories, views). To help reduce the confusion or misuse of categories and views for mapping, the presentation of IDs could be minimized.
- **CWE-89 (SQL Injection):** Steve walked through updates including:
    - Clearer demarcations between rows and cells in tables including line shading
    - Removal of the likelihood column (retaining it under 'scope' if present)
    - Emphasis of scoping
    - Table view for Potential Mitigations to create separation between items
    - Cleaned up Relationships section by using ID as the link to reduce eye fatigue
    - Greater vertical separation to Demonstrative Examples

    - Reframing Observed Examples as *selected* to address common misunderstanding that a single CWE points to all affected CVEs
    - Changes to presentation of relationships in Memberships
- **Upcoming CWE Release:** Steve mentioned that some of the proposed changes would be implemented in the upcoming CWE 4.17 release on April 3rd. He noted that while some changes would be quick wins, others might require more time and effort to implement fully.

VulnCon Participation

- The group discussed participation at VulnCon in Raleigh and organizing a brown bag lunch or social event to advocate for CWE. Chris and Rogue confirmed their attendance, while Steve will present remotely.

Other

- John shared a link of the Share IT Act.
- Chris relayed the recent trend of "vibe coding" to use AI to generate code. This could be worth a CWE View. He posted in the chat that vibe coding may bring code snippets back into focus on FOSS scanners and probably call into question what FOSS license the VIBE tool uses.

NEXT MEETING 4/30