

CWE/CAPEC User Experience Working Group Meeting Notes

April 24, 2024

Members in Attendance

- Chris Coffin
- Matthew Coles
- Alec Summers
- Christopher Sundberg
- Abhi Balakrishnan
- Faheem Ahmed
- John Keane
- Remy Stolworthy
- Lisa Olson
- Farbod Foomany
- Rae Powers
- David Maxwell
- Andrea Schweiger
- Erin Alexander
- Steve Christey Coley
- Matthew DiVisconte
- Rich Piazza
- Przemyslaw (Rogue) Roguski
- Kyle Rudnitski
- Paul Wortman

Agenda

- Purpose
- Housekeeping
- Primary topics
 - Prioritizing corpus user experience modifications
 - Open discussion
- Reminders and Adjourn

Purpose

- Mission: identifying areas where CWE content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them.
- Periodic reporting of activities to CWE Board
 - Next quarterly board meeting TBD Q2-2024
- Please solicit participation from your contacts

Meeting Key Points

- Prioritizing user experience modifications, including simplifying language, ensuring completeness, adding visualizations, and organizing weaknesses at both macro and micro levels.
- Discussed the potential benefits of visualizations for different CWE personas.

Housekeeping

- CWE UEWG May Meeting
 - The next regularly meeting is Wednesday 5/29.
- The CWE program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email.

Meeting Notes

Prioritizing Corpus User Experience Modifications

- **Prioritizing User Experience Improvements**
 - UEWG was established in response to negative feedback related to CWE's usability.
 - This group has accomplished much in response (e.g., submission guidelines, mapping guidance, "New to CWE?" launch, weakness filtering)
 - We must now begin to address usability and understandability in further ways throughout the corpus structure and down to individual weakness language.
 - CWE entry clean-up (across the entire corpus)
 - Understandability: revising all entries for simpler language; remove redundancy
 - Simplifying descriptions/extended descriptions to leverage other elements appropriately
 - Completeness: ensuring all entries have basic required elements populated
 - Visualizations: adding to entries to explain topics visually (leverage Abhi's Top25 examples and build from there)
- **Usability: Macro- and Micro-Level**
 - Macro – How to organize weaknesses at a structural, site-wide level?
 - Organizing views and site wide navigation
 - Micro – How to define a weakness understandably/accurately?
 - Remove redundant and unnecessary information and better leverage the schema
- An example of CWE entries were displayed; one depicted how the CWE currently looks like and the other depicted the updates made (CWE-89: SQL Injection).
- **Overall Prioritization**
 - The group needs to ask themselves at what level should we begin our focus?
 - Macro (CWE organization and navigation) vs. Micro-level (weakness understandability)
 - Micro could include CWE record: understandability, completeness, and visualizations.
- **A Possible Path Forward**

- Discuss a single CWE and how we could improve usability by...
 - Merging the description and extended descriptions
 - Removing redundant information
 - Moving information that belongs in other parts of the schema
 - Removing vulnerability specific information
- We could walk through one example in the meeting.
- Open discussion on if anyone would be interested in trying this exercise with another CWE on their own and then presenting their results in the next meeting.
- **Open Discussion**
 - The participants had an open discussion on the following topics:
 - CWE persona for technical manager?

Action Item: Develop user persona for technical manager