CWE/CAPEC User Experience Working Group Meeting

July 26, 2023

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
  - New to CWE Examples
  - User Stories Updates
  - Open Discussion
- **Reminders and Adjourn**

UEWG: Purpose

- **Mission:** Identifying areas where CWE/CAPEC 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/CAPEC Board**
  - (next quarterly Board meeting TBD Q3-2023)
- **Please solicit participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

- **CWE UEWG Meeting frequency**
  - Meetings have been changed and are now set to occur on the last Wednesday of the month
- **We are working to identify further UEWG opportunities and priorities for FY23**

Topic 1

New to CWE Examples

Chris Coffin

New to CWE Examples

- Received feedback on the New to CWE page that more examples of CWEs should be provided. Specifically, what are the details of the CWE and what relationships does it have with other CWEs
- The current New to CWE page focuses on the design-level CWE-798 - Use of Hard-coded Credentials
- Examples should be high quality and easy to understand
- Top 25 list has some good candidates

New to CWE – Example CWEs

- **Proposed Examples:**
  - CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection’)
    - Maybe highlight parent relationship with CWE-79 XSS (both are children of CWE-74 Injection)
  - CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal’)
    - Language-independent
  - CWE-787 - Out-of-bounds Write
    - Top of the list and well understood in community
  - CWE-287 - Improper Authentication
    - Design-level weakness
    - Gives us a chance to describe “Improper” (used as a catch-all term to cover security behaviors that are either "Missing" or "Insufficient/Incorrect)

Topic 2

User Stories Updates

Chris Coffin

User Stories Updates

- **No recent updates to existing user stories**
- **Still have a few previously identified personas that do not yet have a user story**
  - **Security Researcher/Analyst** - Those who look for ways to attack a product by finding weaknesses using manual and/or automated techniques, then reporting the findings to the vendor and/or the general public.
  - **Educator** - Teachers, professors, consultants, or certification programs that educate developers and system designers about how to design more secure products, develop more secure code, define defensive measures, and/or how to find vulnerabilities.
- **The user story consists of**
  - User description (Who?)
  - Story (What?)
  - Benefit (Why?)

Topic 3

Open Discussion

Chris Coffin

Miscellaneous Topics

- **Other thoughts or topics?**

Next Meeting – August 30 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

Backups

CWE User Pain Points

- **Pain point topics that the group is aware of or would like to discuss**
- **For those on the call, what were your biggest questions or concerns when beginning to use CWE?**
- **Are there common questions that CWE users have that are not covered in the current FAQ?**
- **Other potential opportunities:**
  - Features we could expand or improve to make CWE consumption easier?
  - Maybe engage the community in one or more ways to solicit this kind of feedback (see topic #3)
- **Other thoughts?**

Community Engagement Strategy

- **Develop a strategy for engaging the CWE user community for feedback**
- **What are the best methods to query the community on topics such as the pain points covered in topic #2**
- **What communication methods should be employed?**
  - E.g., polls, emails, web, social media
- **Should we target specific user types?**
- **Other thoughts?**

CWE Video Tips Series

- **Current video ideas:**
  - How to search CWE for a weakness
  - How to display only the information that you need with presentation filters
  - What is a weakness (vs a vulnerability)
  - How are weaknesses organized
  - What is a category (how is it different than a pillar)
  - What are views
  - How and why to use the research view
  - Use cases for CWE (could user stories be used?)
  - How do I submit an idea for a new weakness
  - How can I improve the quality of existing weaknesses

New to CWE – Future Content

- **The New to CWE content audience is different from what has been catered to previously**
- **The audience is the casual or new user to CWE or even the manager who makes security funding decisions**
- **The team has previously drafted material for the New to CWE audience that covers the CWE hierarchy**
  - Not yet released material
  - Do members agree that this topic should be covered for New to CWE?
- **Are there other topics that UEWG members feel strongly about or believe should be covered given the intended audience?**
- **Should there be a close coupling of the topics covered here with the CWE Video Tips series?**

CWE Naming and Vulnerability Mapping

- **Being thinking about solutions for common and well-known issues surrounding use of CWE names and how to more easily map vulnerabilities to CWEs**
- **Current CWE structure is difficult to understand and use**
- **Community needs better root cause information for vulnerabilities**
- **Does CWE naming need a change or update to support easier mapping?**
  - Remove CWE names for Views and/or Categories?
  - New naming that embeds a structure (e.g., CWE-1234-1)

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).