CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, December 20, 2023

Members in Attendance

Faheem Ahmed – CISA
Erin Alexander – CISA
Abhi Balakrishnan – Kroll
Charity Calloway
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew DiVisconte – California Department of Transportation (Caltrans)
Jim Duncan
Farbod Foomany – Security Compass
John Keane
Art Manion – Analygence
Prajesh Mehta – Greater Toronto Airports Authority
Doug Nichols – GE Aerospace
Lisa Olson – Microsoft
Rae Powers – California Department of Transportation (Caltrans)
Gerald Rigdon – Boston Scientific Corporation
Remy Stolworthy – INL
Alec Summers – MITRE
Paul Wortman – Wells Fargo

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - Simplified CWE Terminology and Weakness Visualizations (Member Presentation)
    - Open Discussion
- Reminders and Adjourn

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 Board (Q4-2023 Meeting was Monday Dec 18)
- Please solicit participation from your network (contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- CWE UEWG January Meeting
    - The next regularly scheduled meeting is Wednesday Jan 31

- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org

Simplified CWE Terminology and Weakness Visualizations (Abhi Balakrishnan)

- Two topics: (1) simplified names, (2) diagrams to represent weaknesses in systems.
- Simplified names:
    - An example use of technical jargon – reflected cross scripting – was shown along with corresponding terms that are easier for developers to understand. The corresponding terms came from discussion with staff, and my own understanding/experience.
    - In the industry, we have a tendency to speak our own security language, but with a wider audience, it would help to simplify jargon. Asked a client for their thoughts on the new terms for cross xss, but no feedback yet.
- Diagrams:
    - In the August meeting, the idea came up to use diagrams or graphics to communicate weakness information. I have been doing that for years with pen test reports to simplify things.
    - https://pentest-report-pro-max.web.app/diagrams.html
    - An example diagram was shown of a malicious actor depicting a sequel injection on a login form scenario, and gaining access. It also showed a user being denied access for using invalid credentials. The diagram was created using Excali Draw. Look for ease of updating as the diagram is reviewed by others.
    - Kept on experimenting and came up with an isometric diagram (using ISO flow) that is aesthetically pleasing, but if you have to create your own icons, that can a stopper.
    - Built another high level diagram using SketchWow, created for the CWE Top 25. It uses casual fonts, is not symmetrical, and is slightly rough. These choices were intentional. Creating diagrams that are technically accurate and symmetrical can keep people from contributing.
    - Five rules:
        - Keep it high level (to appeal to a non-technical audience)
        - Target non-technical people
        - Keep it simple (use common language, not jargon, and do not convey too much information in a single diagram, instead break up into pieces)
        - Keep it rough (informal)
        - Accessibility is important (e.g., using colors to convey information can be confusing for visually-impaired people, use patterns instead)
    - Comments:
        - A challenge is finding the right balance between technical accuracy and understanding by a less technical audience.
        - Use diagrams as an entryway to the more detailed text.
        - Links to the diagram slides provided in Chat.
    - Next steps to be discussed off-line, e.g., incorporating diagrams into CWE.

Open Discussion

- Comment: A continuing problem I see is getting people motivated to fix weaknesses versus vulnerabilities. If we could find a way to incorporate cost and expense associated with a weakness into CWE, it might help to make it more influential.
    - Cost/expense can vary depending on the organization and the context.
    - Consider a more qualitative approach.
- FIRST and CVE are co-sponsoring a Vulnerability Conference in Spring 2024 in Raleigh, North Carolina. A link for more information is in Chat. CWE will do a panel discussion around the idea of root cause mapping.
- Regarding the first topic, Simplified CWE Terminology and Weakness Visualizations, I think it would be an interesting exercise to figure out which personas are helped by this kind of work, because I suspect that the target audience for this might not line up exactly with the different personas. A second point is CWE was originally created by experts for experts. This work is another aspect of outreach to other kinds of stakeholders.

Reminders and Adjourn

- Next meeting is January 31 at 12pm EST.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.