CWE/CAPEC User Experience Working Group (UEWG)

Overview

Alec Summers, CWE/CAPEC Program
Agenda

- Welcome!

- CWE/CAPEC User Experience Working Group
  - Goals, Intent, and Overview

- Program Overview
Welcome!

- Why are we here?
  - Action as a response to community feedback (e.g., “wall of text”, complicated and inconsistent taxonomies, inconsistent definitions, poor “look and feel”, difficult to apply

- Idea:
  - Start a UEWG comprised of volunteer community stakeholders

- Goal:
  - Identifying areas where CWE/CAPEC content, rules, guidelines, and best practices must improve to better support stakeholder persona use cases, and work collaboratively to fix them
UEWG: What to Expect (1 of 2)

- Active discussion and collaborative engagement
- Minimal time commitment outside of meetings
- Ongoing membership expansion and activity
- Potential for establishment of sub-groups for specific discussion and activity
- Moderate Secretariat Services:
  - capturing general discussion and tracking of action items
UEWG: What to Expect

- **Schedule:**
  - Bi-Weekly / Monthly Meetings
  - 12:00 – 1:00 PM EST
    - Microsoft Teams

- Periodic reporting of activities to CWE/CAPEC Board

- **Contact:** [cwe@mitre.org](mailto:cwe@mitre.org) & [capec@mitre.org](mailto:capec@mitre.org)

- **Questions?**
GET AHEAD OF BOOM!

Weaknesses

The root cause of a vulnerability

Vulnerabilities

Specific instances of a weakness type that are demonstrably exploitable

Attack Patterns

How the weakness could be exploited

CVE/CWE/CAPEC Program(s) Overview
Differentiating CAPEC and MITRE ATT&CK

- MITRE manages both CAPEC and ATT&CK, although both are community-based programs.

- Both curate cyber-attack knowledge, but from *different points of view*
  - CAPEC details how an adversary can exploit a weakness, (e.g., a CWE)
  - ATT&CK is more oriented towards understanding known attack techniques “from the wild” to detect/prevent adversary actions.

- CAPEC aimed at “getting ahead of boom” – avoiding the weaknesses in the first place before they can be exploited.

- MITRE provides a partial mapping between the entries in each corpus.

- The mapping is partial because many ATT&CK techniques are not related to a weakness, just malicious use of a common application or utility.
PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

CAPEC@MITRE.ORG