

CWE/CAPEC User Experience Working Group Meeting

January 11, 2023



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
 - User Story Development
 - Discussion: User pain points with CWE/CAPEC
 - Discussion: User community engagement strategy
- **Reminders and Adjourn**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

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 Q1-2023)
- **Please solicit participations from your contacts**
 - Contact: cwe@mitre.org & capec@mitre.org



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Housekeeping

- **We are working to identify further UEWG opportunities and priorities for FY23**
 - Open discussions today, Topics #2 and #3
 - As always, any feedback can be sent to cwe@mitre.org, capec@mitre.org, or tweet @cwecapec



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](https://www.dhs.gov/) (DHS) [Cybersecurity and Infrastructure Security Agency](https://www.cisa.gov/) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](https://www.mitre.org/). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Topic 1

User Story Development

Przemyslaw 'Rogue' Roguski, Red Hat



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE / CAPEC user stories

Created by Przemysław Roguski (aka Rogue) from Red Hat

WHY we need user stories?

First of all let's ask: What we as a UEWG want to improve?

Users can use CWE data to better understand how weaknesses lead to vulnerabilities. CWE data can be used to proactively identify how existing weakness in the software or hardware can lead to new vulnerabilities and exploits. Better knowledge of product weaknesses will improve the general security posture of the product. The CWE data is key information in the shift left security initiative.

The only problem is that **CWE users MUST KNOW** and **UNDERSTAND** what they can **ACHIEVE** by using CWE/CAPEC data.

WHAT we want to achieve by creating user stories?

Defining User Personas is not enough, because users don't know which persona they are and what they can do with weaknesses data.

We should help users to identify themselves with specific user personas or groups and show them how to use CWE data in real user stories. People can learn much faster what value is in the CWE / CAPEC data.

HOW do we want to present user stories?

A user story has three unique elements.

We will need a good, clear to everyone template.

Something like:

- Business Problem
Understating the business problem.
- Level of responsibility
The tasks the user is responsible for and cares about
- Outcome
The results achieved by using CWE/CAPEC data.

Example user story - Security Architects

- Business Problem (Context):
Security Architects are responsible for a secure design of application/hardware. They must take into consideration the whole product purpose, future deployment and usage, and make sure that all aspects of it are well designed and protected from the security point of view. The purpose of all this work is a very deep risk assessment process to ensure that the final product is secure. Using the CWE data can help significantly in the Security Architects work to better understand the nature of the weaknesses and at the end help to take the final decision about the remediation steps.

Example user story - Security Architects

- Level of responsibility (Story):
Security Architect is going to review a new SaaS solution. During the risk assessment process it is necessary to verify findings from various security scanners (SAST and DAST) and threat modeling tools. The detected weaknesses can be verified with the CWE available data to better understand the nature of the weaknesses. User can see example usage of the particular weakness and possible mitigation steps. It is also possible to see correlation to other similar weaknesses from the specific weakness category that can help to avoid potential other issues and as a consequence vulnerabilities in the future. Security Architect can use the “Operational” view of the CWE data to see useful technical information about this specific weakness. For example if the CWE-23 Relative Path Traversal is reviewed, the Security Architect might recognize that this weakness is also mapped to the OWASP Broken Access Control risk, which is the top 1 of the web application security risks and take necessary steps for deeper verification.

Example user story - Security Architects

- Outcome:

All information available in the CWE program can help to perform more detailed risk assessment and provide more robust and less vulnerable final product. Using the CWE data can show the correlation between weaknesses and historical CVEs cause by the specific weakness. It can also help to proactively identify other similar weaknesses from the same type of weakness category that will improve the overall security posture of the reviewed service/application/hardware.

Topic 2

Discussion: User pain points with CWE/CAPEC

Open Discussion



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

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?



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Topic 3

Discussion: User community engagement strategy

Open Discussion



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

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 and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Next Meeting – February 8 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

CAPEC@MITRE.ORG



@cwecapec



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).
Copyright © 1999–2023, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.