CWE/CAPEC User Experience Working Group Meeting

June 28, 2023

Agenda

This meeting is being recorded :-)

- **Purpose**
- **Housekeeping**
- **Primary topics**
  - CWE Views
  - CWE Tips and Tricks
- **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

CWE Views

Chris Coffin

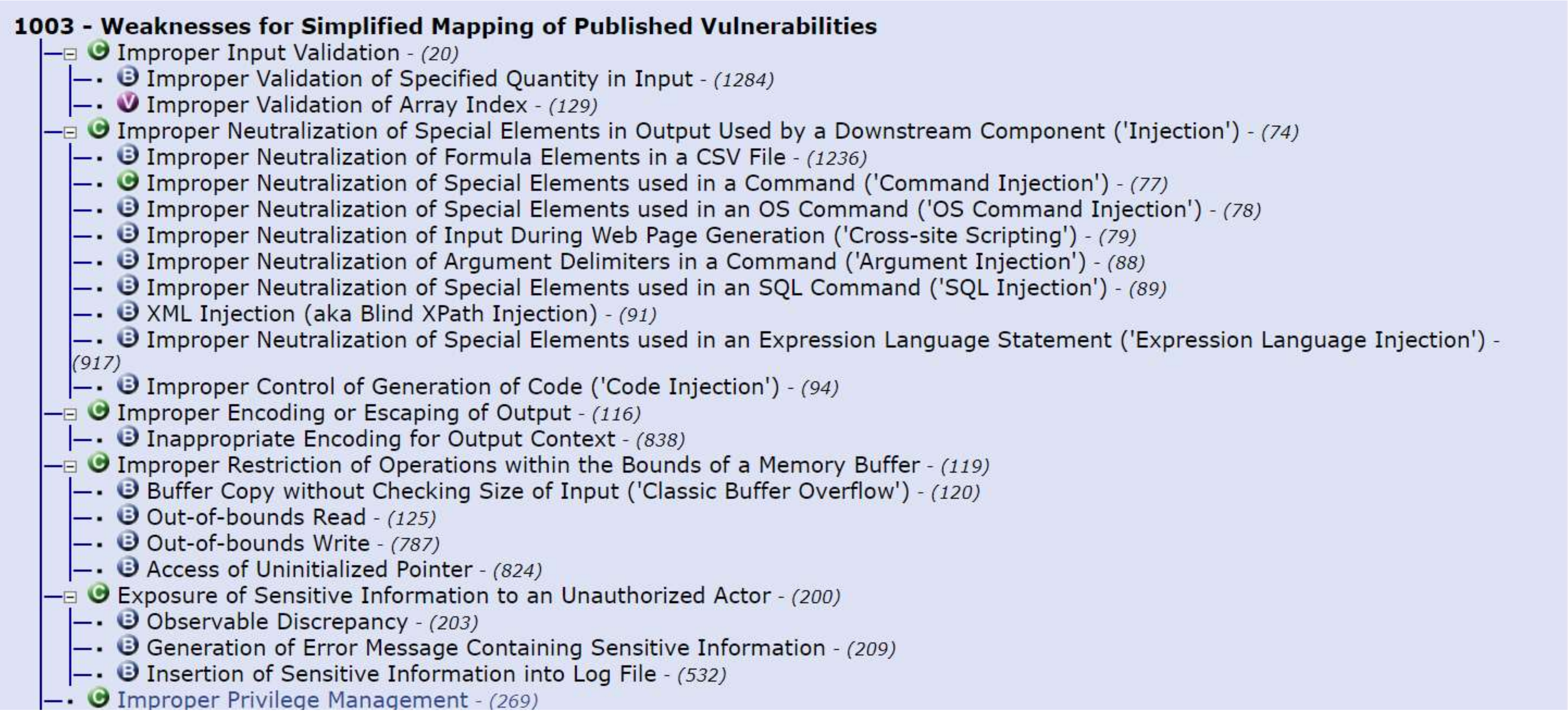
CWE Views

- **What are CWE Views?**
  - "assigned to predefined perspectives with which one might look at the weaknesses in CWE…"
  - Views can help make perusing the CWE list more manageable and exploring the tree to seek out potential CWE(s) based on their name more reasonable
  - Views can also help to narrow down the CWE list to CWEs that are specific to a certain audience (software developer or security researcher), specific technologies (software or hardware, specific programming languages), predefined lists (top 25 CWEs), etc.
  - Views can either be hierarchical or flat
    - View previously highlighted attempt to use only two levels of abstraction for simplicity and ease of use
    - Top 25 CWE Views are flat with no hierarchy
  - Views can contain some or all CWEs depending on the view purpose and intended use

CWE Views (continued)

- **Examples:**
  - **CWE-1003** “Weaknesses for Simplified Mapping of Published Vulnerabilities” – This view provides a subset of CWEs that cover the most commonly-used CWEs that are mapped by CVEs. As of CWE 4.11, it includes 130 different CWEs, mostly at the Class and Base level abstractions. Additionally, this view is meant to be easily digestible by novice users. Has only two levels of abstraction. Used by NIST NVD to perform CVE -> CWE mappings.
  - **CWE-1000** “Research Concepts” - This view captures all weaknesses in CWE. It has a deep tree structure, beginning with 10 high-level Pillars. It might be especially useful when you are looking for unusual weaknesses, as you could perform a top-down search.
  - **CWE-699** “Software Development” - This view captures a subset of weaknesses intended for software developers (399 of 933 as of CWE 4.11). By design, this view is only 2 levels deep. The top level has categories of developer-friendly concepts (but don’t map to these categories – they are only to help you navigate to the appropriate entry). The second level contains Base level weaknesses.

CWE Views (continued)



1003 - Weaknesses for Simplified Mapping of Published Vulnerabilities

- ⊟ C Improper Input Validation - *(20)*
  - B Improper Validation of Specified Quantity in Input - *(1284)*
  - V Improper Validation of Array Index - *(129)*
- ⊟ C Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') - *(74)*
  - B Improper Neutralization of Formula Elements in a CSV File - *(1236)*
  - C Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*
  - B Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
  - B Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
  - B Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') - *(88)*
  - B Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
  - B XML Injection (aka Blind XPath Injection) - *(91)*
  - B Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') - *(917)*
  - B Improper Control of Generation of Code ('Code Injection') - *(94)*
- ⊟ C Improper Encoding or Escaping of Output - *(116)*
  - B Inappropriate Encoding for Output Context - *(838)*
- ⊟ C Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
  - B Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') - *(120)*
  - B Out-of-bounds Read - *(125)*
  - B Out-of-bounds Write - *(787)*
  - B Access of Uninitialized Pointer - *(824)*
- ⊟ C Exposure of Sensitive Information to an Unauthorized Actor - *(200)*
  - B Observable Discrepancy - *(203)*
  - B Generation of Error Message Containing Sensitive Information - *(209)*
  - B Insertion of Sensitive Information into Log File - *(532)*
- C Improper Privilege Management - *(269)*

CWE Views (continued)

- **View types and examples**

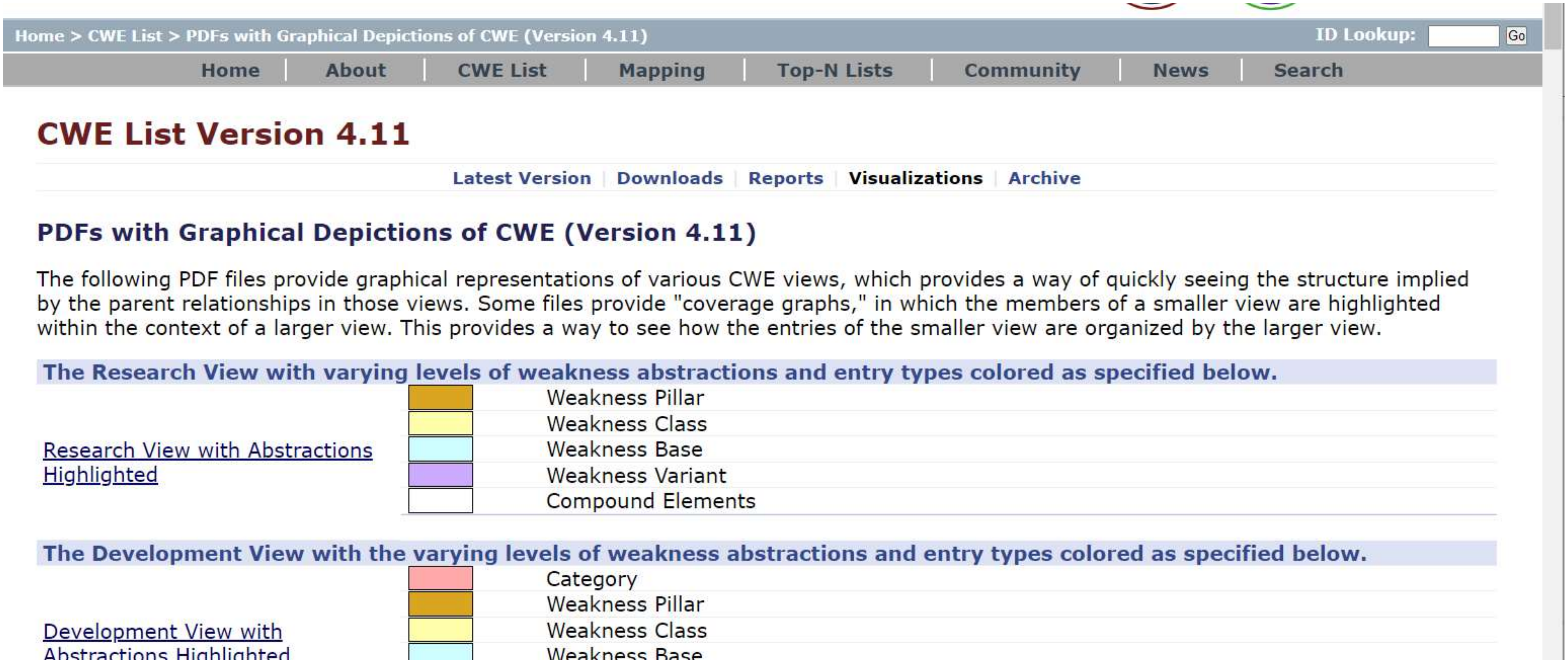
Common Views	External Mappings	Helpful Views
Software Development	CWE Top 25 (2022)	Software Written in C
Hardware Design	Most Important Hardware Weaknesses List (2021)	Weaknesses in Mobile Applications
Research Concepts	OWASP Top Ten (2021)	CWE Simplified Mapping
		Introduced During Design
		Introduced During Implementation

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

CWE Views (continued)

- **How many Views exist today?**
  - 48 total views in CWE 4.11
  - Though some of the 48 are obsolete (previous years CWE Top 25 and OWASP Top Ten)
- **Where are Views located on the CWE web site?**
  - CWE web site -> CWE List menu -> Latest Version
  - Select “by Other Criteria” button in the CWE List Quick Access left side pane
  - https://cwe.mitre.org/data/index.html
- **CWE Visualizations**
  - CWE web site -> CWE List menu -> Visualizations
  - https://cwe.mitre.org/data/pdfs.html
  - PDF files that provide graphical representations of various CWE views, which provides a way of quickly seeing the structure implied by the parent relationships in those views

CWE Views (continued)



Home > CWE List > PDFs with Graphical Depictions of CWE (Version 4.11)

ID Lookup: Go
Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE List Version 4.11

Latest Version | Downloads | Reports | Visualizations | Archive

PDFs with Graphical Depictions of CWE (Version 4.11)

The following PDF files provide graphical representations of various CWE views, which provides a way of quickly seeing the structure implied by the parent relationships in those views. Some files provide "coverage graphs," in which the members of a smaller view are highlighted within the context of a larger view. This provides a way to see how the entries of the smaller view are organized by the larger view.

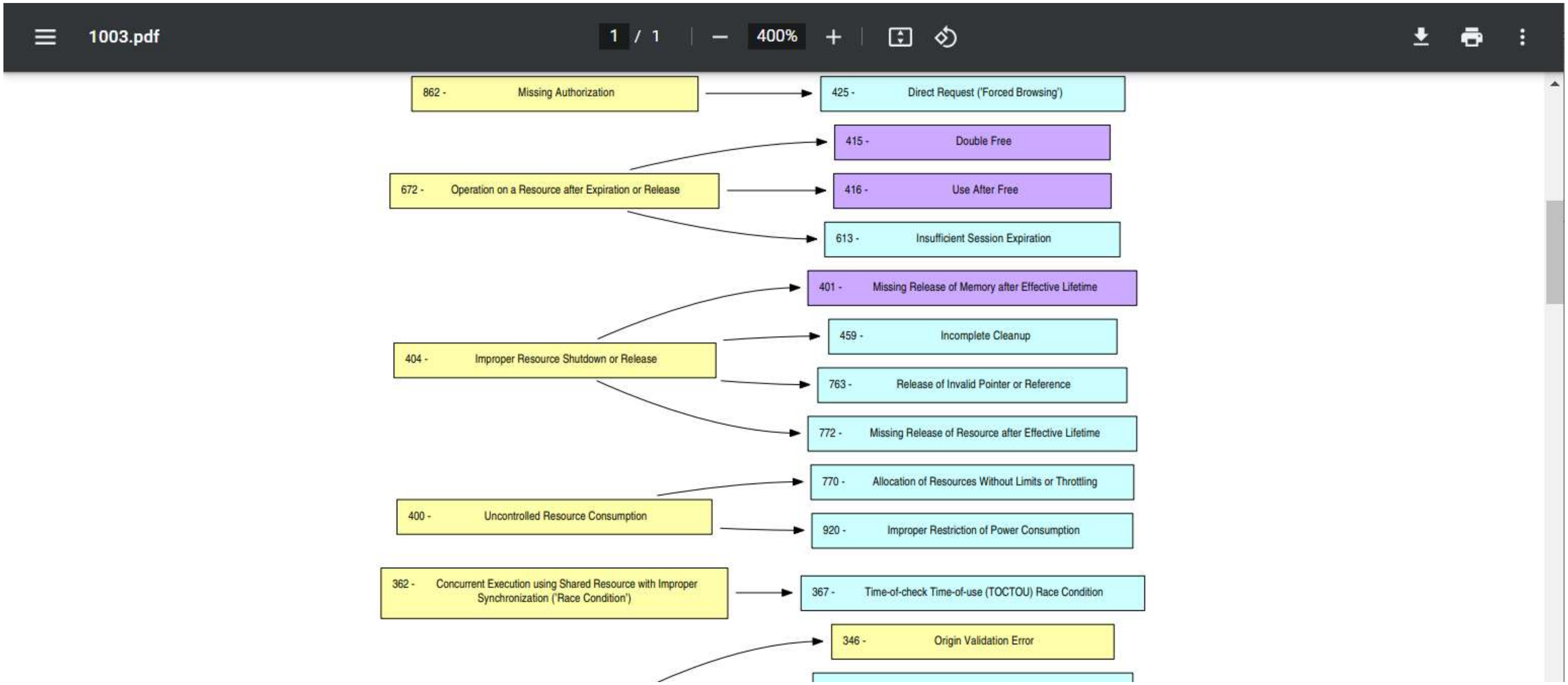
The Research View with varying levels of weakness abstractions and entry types colored as specified below.

Research View with Abstractions Highlighted	🟧	Weakness Pillar
	🟨	Weakness Class
	🟦	Weakness Base
	🟪	Weakness Variant
	⬜	Compound Elements

The Development View with the varying levels of weakness abstractions and entry types colored as specified below.

Development View with Abstractions Highlighted	🟥	Category
	🟧	Weakness Pillar
	🟨	Weakness Class
	🟦	Weakness Base

CWE Views (continued)



862 - Missing Authorization

425 - Direct Request ('Forced Browsing')

415 - Double Free

672 - Operation on a Resource after Expiration or Release

416 - Use After Free

613 - Insufficient Session Expiration

401 - Missing Release of Memory after Effective Lifetime

459 - Incomplete Cleanup

404 - Improper Resource Shutdown or Release

763 - Release of Invalid Pointer or Reference

772 - Missing Release of Resource after Effective Lifetime

770 - Allocation of Resources Without Limits or Throttling

400 - Uncontrolled Resource Consumption

920 - Improper Restriction of Power Consumption

362 - Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

367 - Time-of-check Time-of-use (TOCTOU) Race Condition

346 - Origin Validation Error

CWE Views (continued)

- **Questions and Thoughts**
  - Are there other important points to include when describing views?
    - A New to CWE page or CWE tips video may be created in the future
  - Should Views have their own CWE ID or something else?
    - Seems unlikely that there will be a need to map to a view
    - Does a view need identification outside of its title?
  - Are there other useful views that could be created or are needed?
  - ?

Topic 2

CWE Tips and Tricks

Jim Duncan

CWE Tips and Tricks

- Jim would like to share some knowledge and past experiences with CWE
- The slides are from a previous FIRST conference he presented

Next Meeting – July 26 @ 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)