CWE User Experience Working Group Meeting

December 20, 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**
  - Simplified CWE Terminology and Weakness Visualizations (Member Presentation)
  - Open Discussion
- **Reminders and Adjourn**

UEWG: Purpose

- **Mission:** Identifying areas where CWE 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 participations from your contacts**
  - Contact: cwe@mitre.org & capec@mitre.org

Housekeeping

- **CWE UEWG January Meeting**
  - The next regularly scheduled meeting is Wed 1/31

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

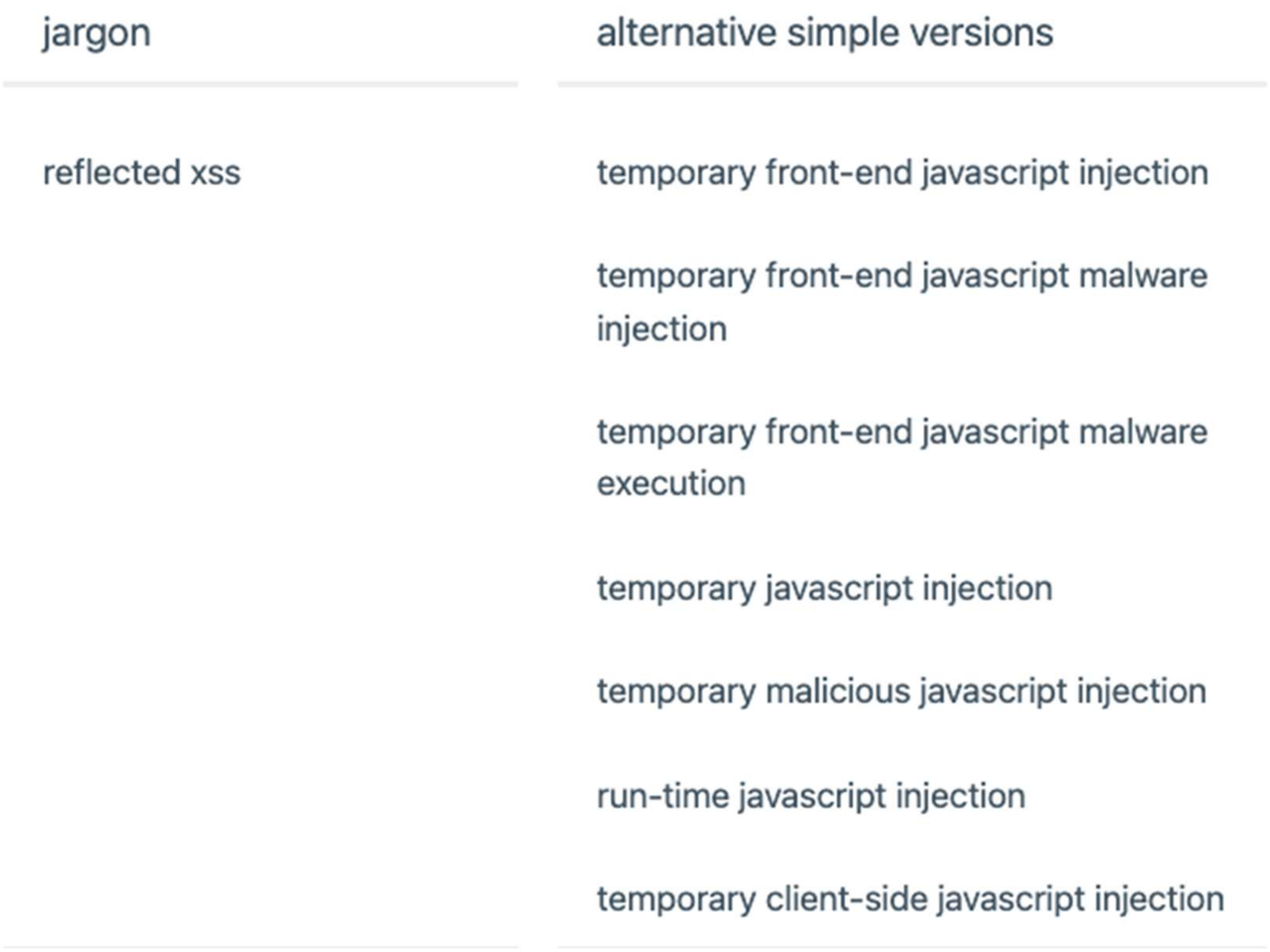
Topic 1

Simplified CWE Terminology and Weakness Visualizations

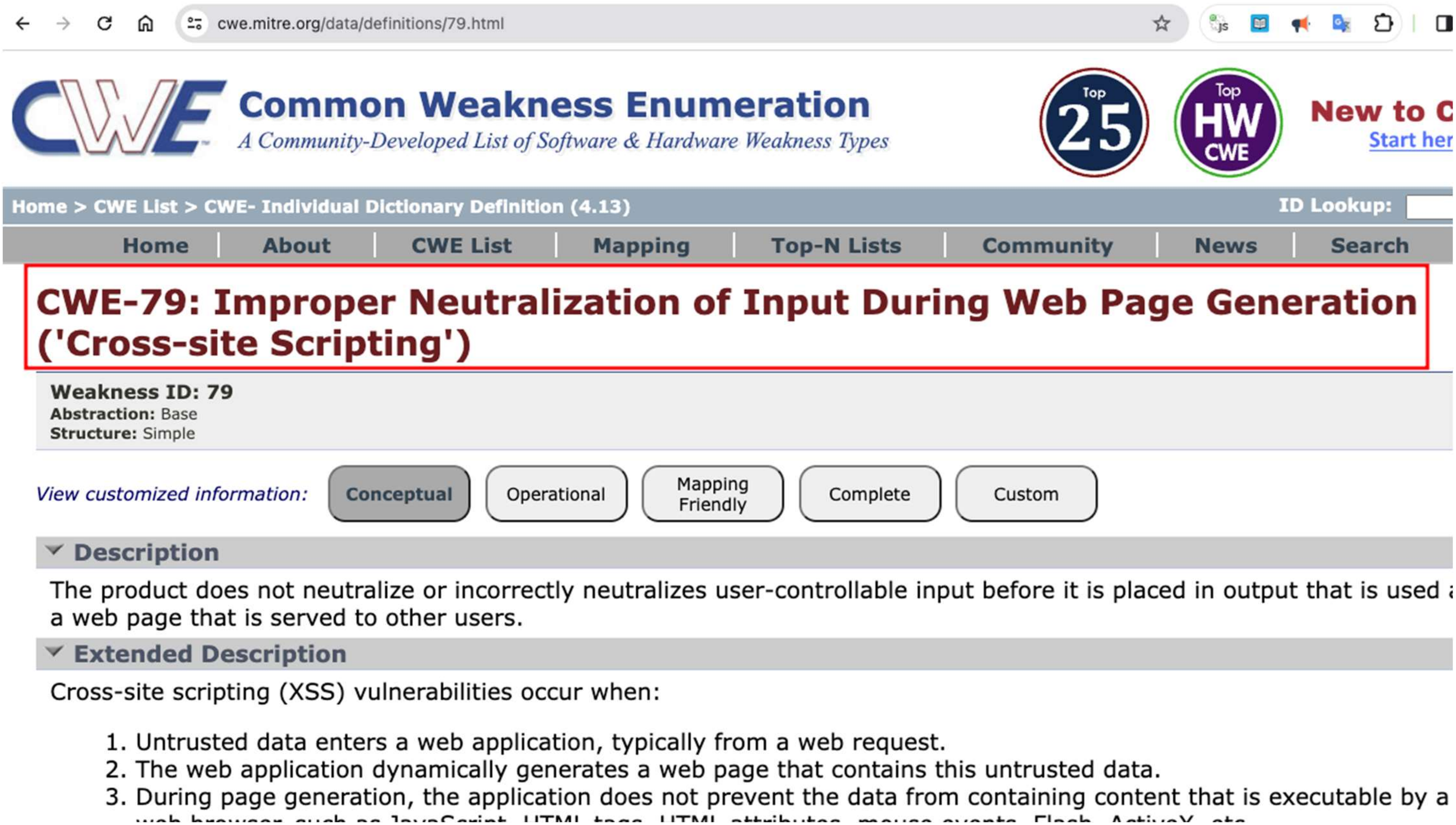
UEWG Member – Abhi M Balakrishnan

Simplified names and diagrams

Abhi Balakrishnan



jargon	alternative simple versions
reflected xss	temporary front-end javascript injection
	temporary front-end javascript malware injection
	temporary front-end javascript malware execution
	temporary javascript injection
	temporary malicious javascript injection
	run-time javascript injection
	temporary client-side javascript injection


cwe.mitre.org/data/definitions/79.html
CWE
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Top 25
Top HW CWE
New to C
Start her
Home > CWE List > CWE- Individual Dictionary Definition (4.13)
ID Lookup:
Home
About
CWE List
Mapping
Top-N Lists
Community
News
Search

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Weakness ID: 79
Abstraction: Base
Structure: Simple

View customized information:
Conceptual
Operational
Mapping Friendly
Complete
Custom

Description

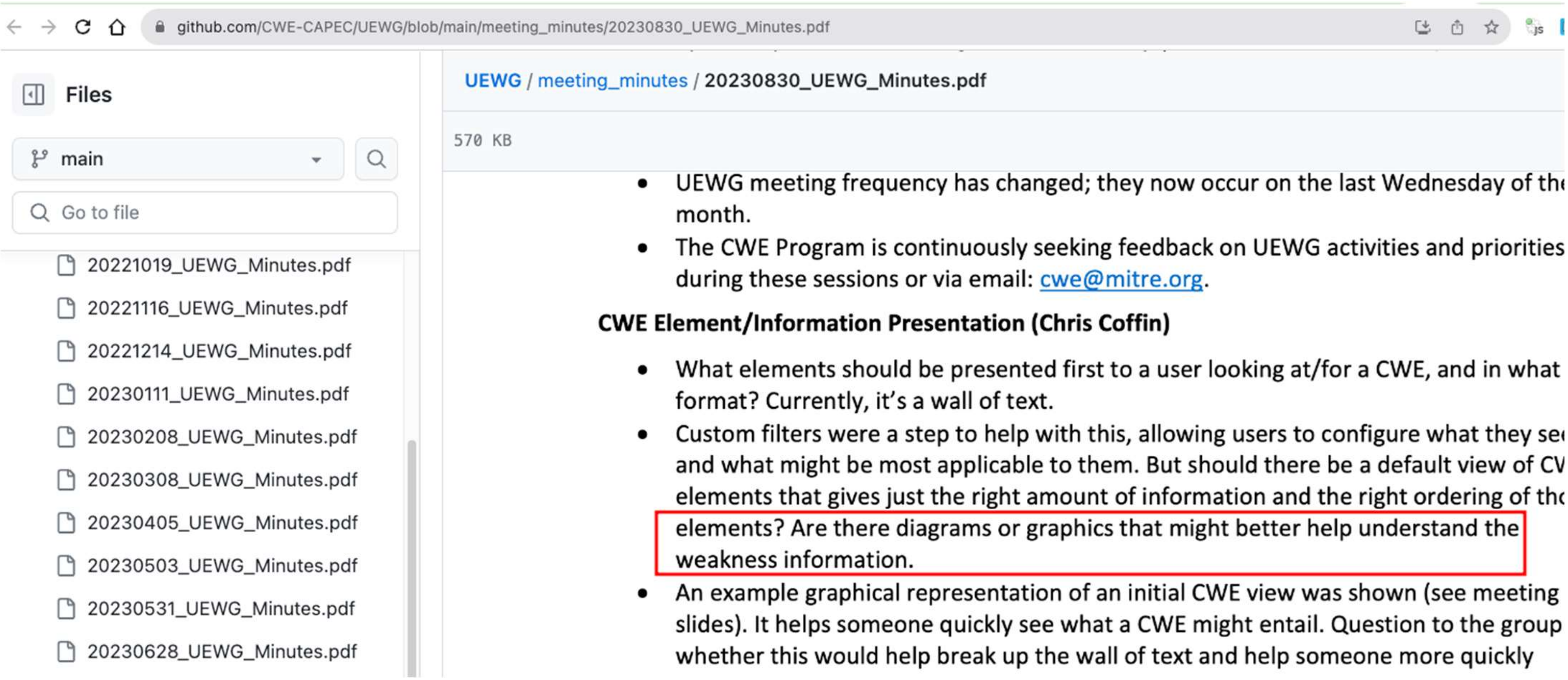
The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used a
a web page that is served to other users.

Extended Description

Cross-site scripting (XSS) vulnerabilities occur when:

1. Untrusted data enters a web application, typically from a web request.
2. The web application dynamically generates a web page that contains this untrusted data.
3. During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX, etc.

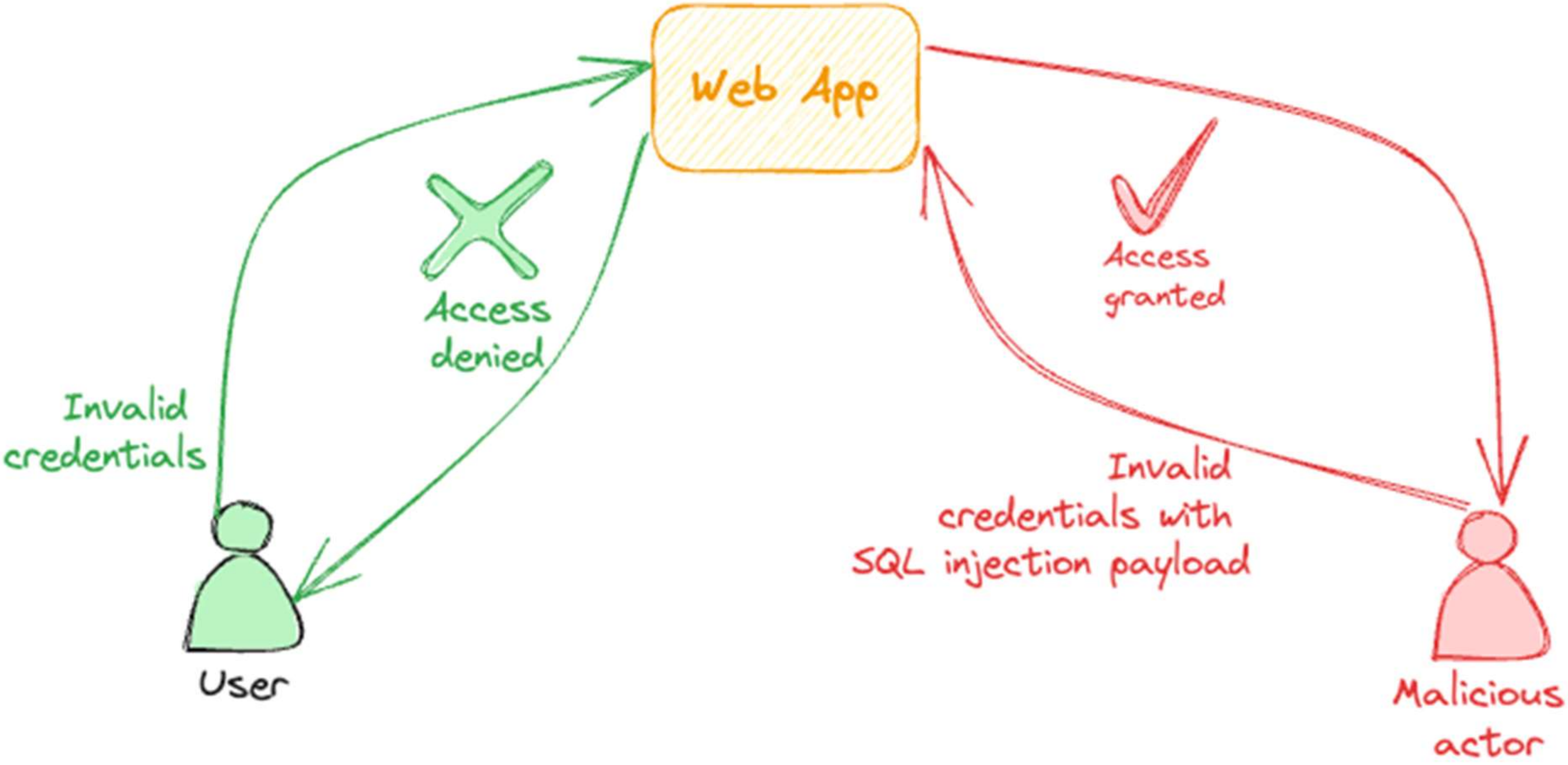
Diagrams

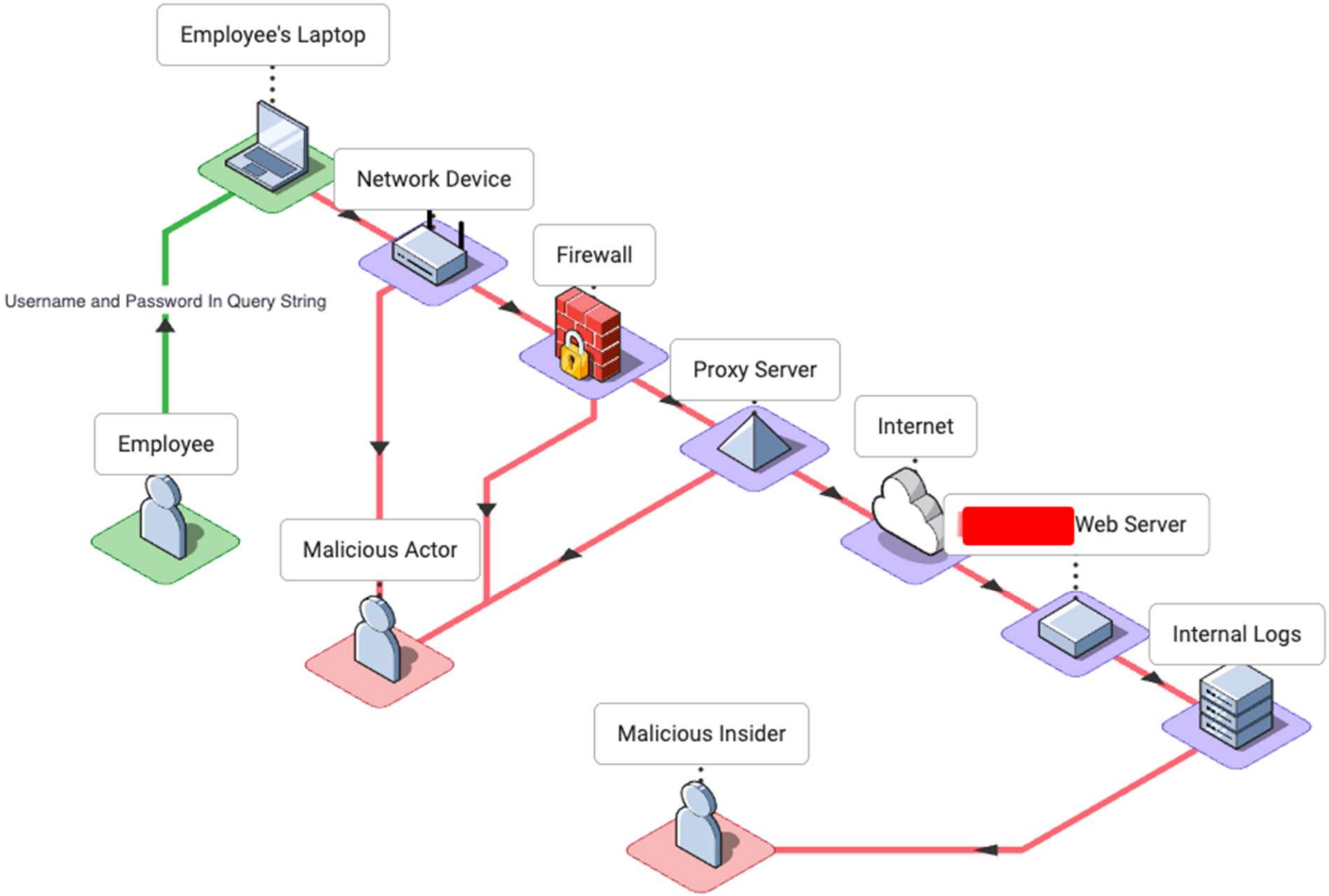

github.com/CWE-CAPEC/UEWG/blob/main/meeting_minutes/20230830_UEWG_Minutes.pdf
Files
main
Go to file
20221019_UEWG_Minutes.pdf
20221116_UEWG_Minutes.pdf
20221214_UEWG_Minutes.pdf
20230111_UEWG_Minutes.pdf
20230208_UEWG_Minutes.pdf
20230308_UEWG_Minutes.pdf
20230405_UEWG_Minutes.pdf
20230503_UEWG_Minutes.pdf
20230531_UEWG_Minutes.pdf
20230628_UEWG_Minutes.pdf
UEWG / meeting_minutes / 20230830_UEWG_Minutes.pdf
570 KB

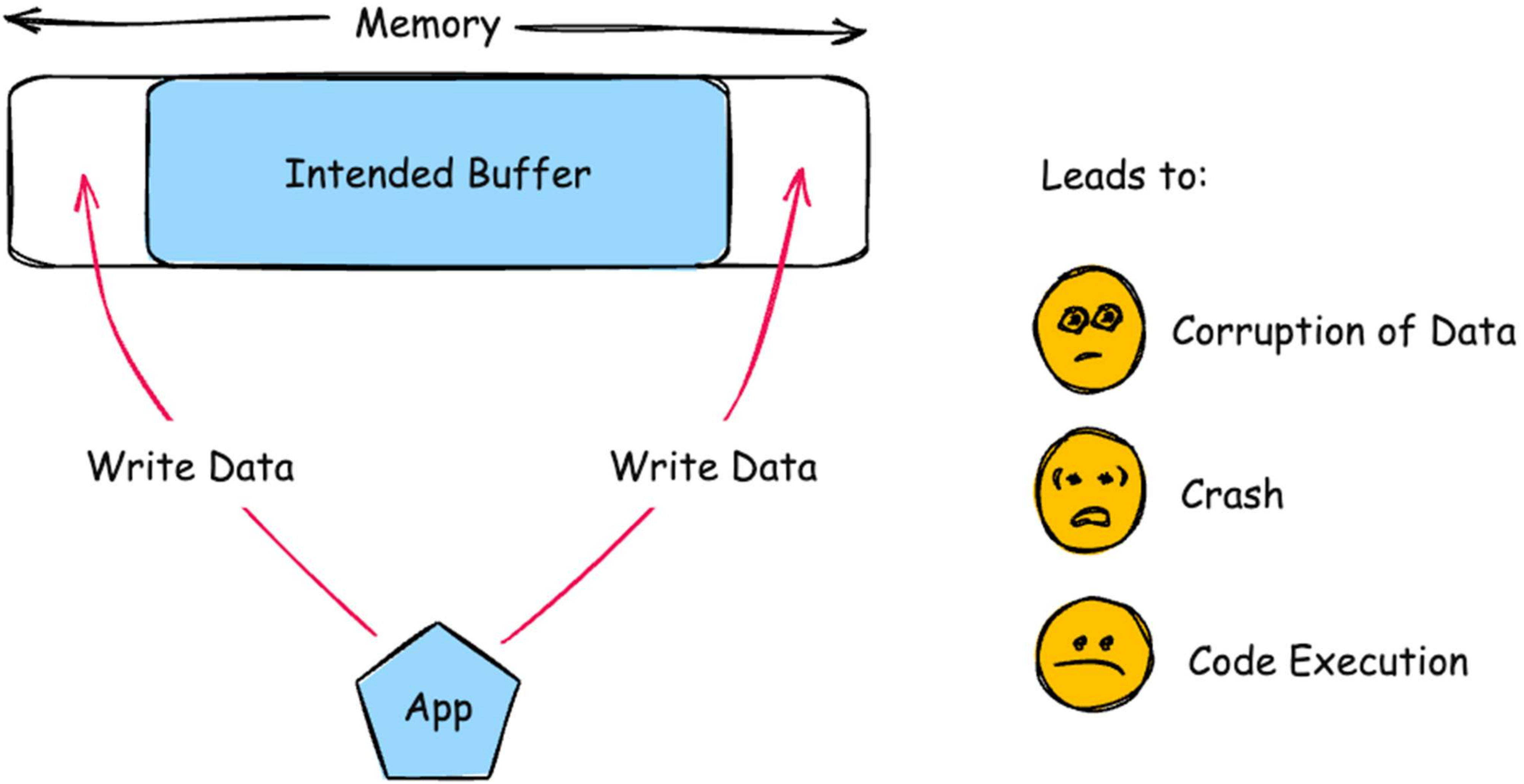
- UEWG meeting frequency has changed; they now occur on the last Wednesday of th month.
- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org.

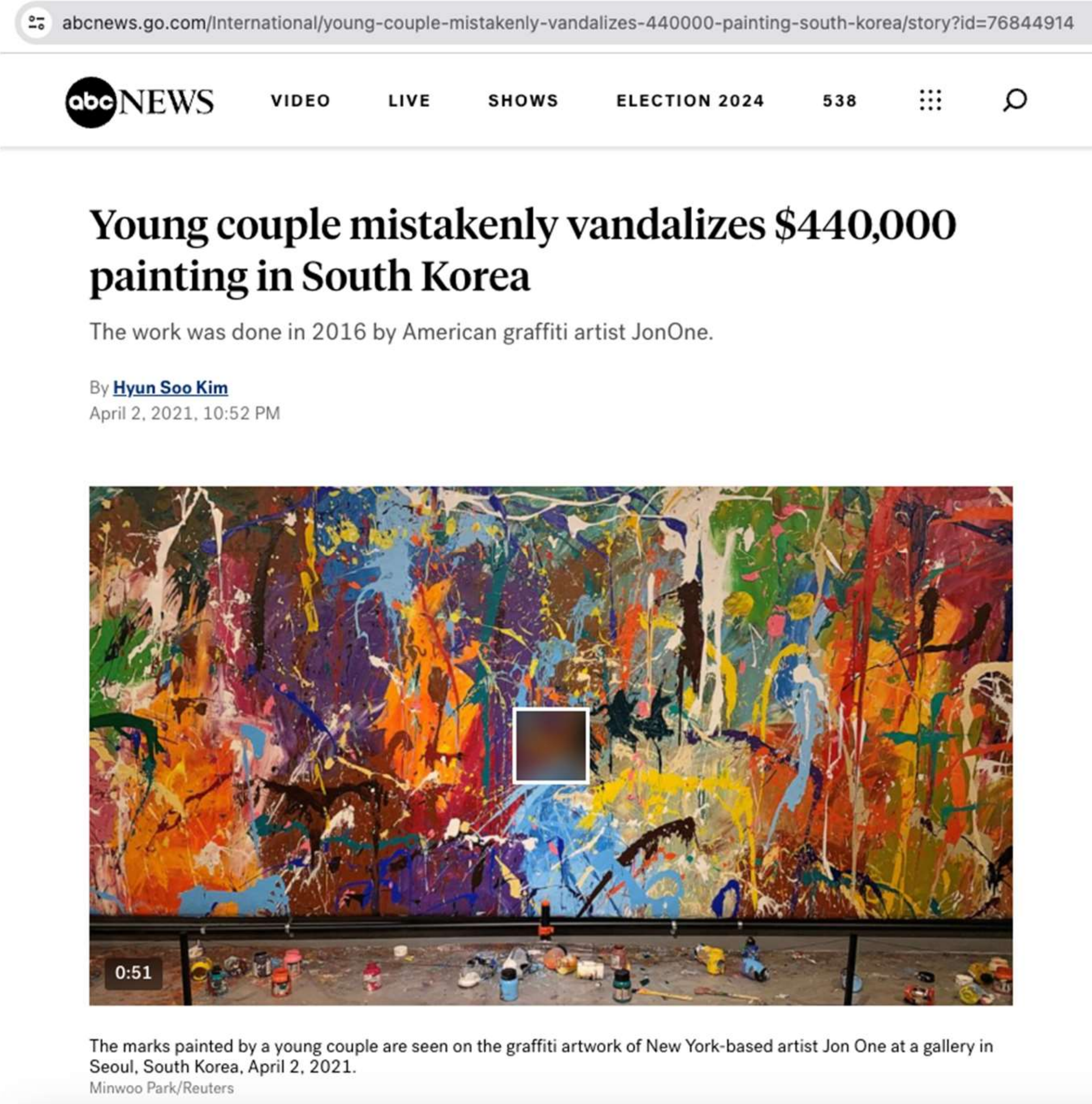
CWE Element/Information Presentation (Chris Coffin)

- What elements should be presented first to a user looking at/for a CWE, and in what format? Currently, it's a wall of text.
- Custom filters were a step to help with this, allowing users to configure what they se and what might be most applicable to them. But should there be a default view of CV elements that gives just the right amount of information and the right ordering of th elements? Are there diagrams or graphics that might better help understand the weakness information.
- An example graphical representation of an initial CWE view was shown (see meeting slides). It helps someone quickly see what a CWE might entail. Question to the group whether this would help break up the wall of text and help someone more quickly


Web App
Invalid credentials
Access denied
User
Access granted
Invalid credentials with SQL injection payload
Malicious actor


Employee's Laptop
Network Device
Firewall
Username and Password In Query String
Proxy Server
Internet
Employee
[redacted] Web Server
Malicious Actor
Internal Logs
Malicious Insider


Memory
Intended Buffer
Write Data
Write Data
App
Leads to:
Corruption of Data
Crash
Code Execution


abcnews.go.com/International/young-couple-mistakenly-vandalizes-440000-painting-south-korea/story?id=76844914
abc NEWS
VIDEO
LIVE
SHOWS
ELECTION 2024
538
0:51

Young couple mistakenly vandalizes $440,000 painting in South Korea

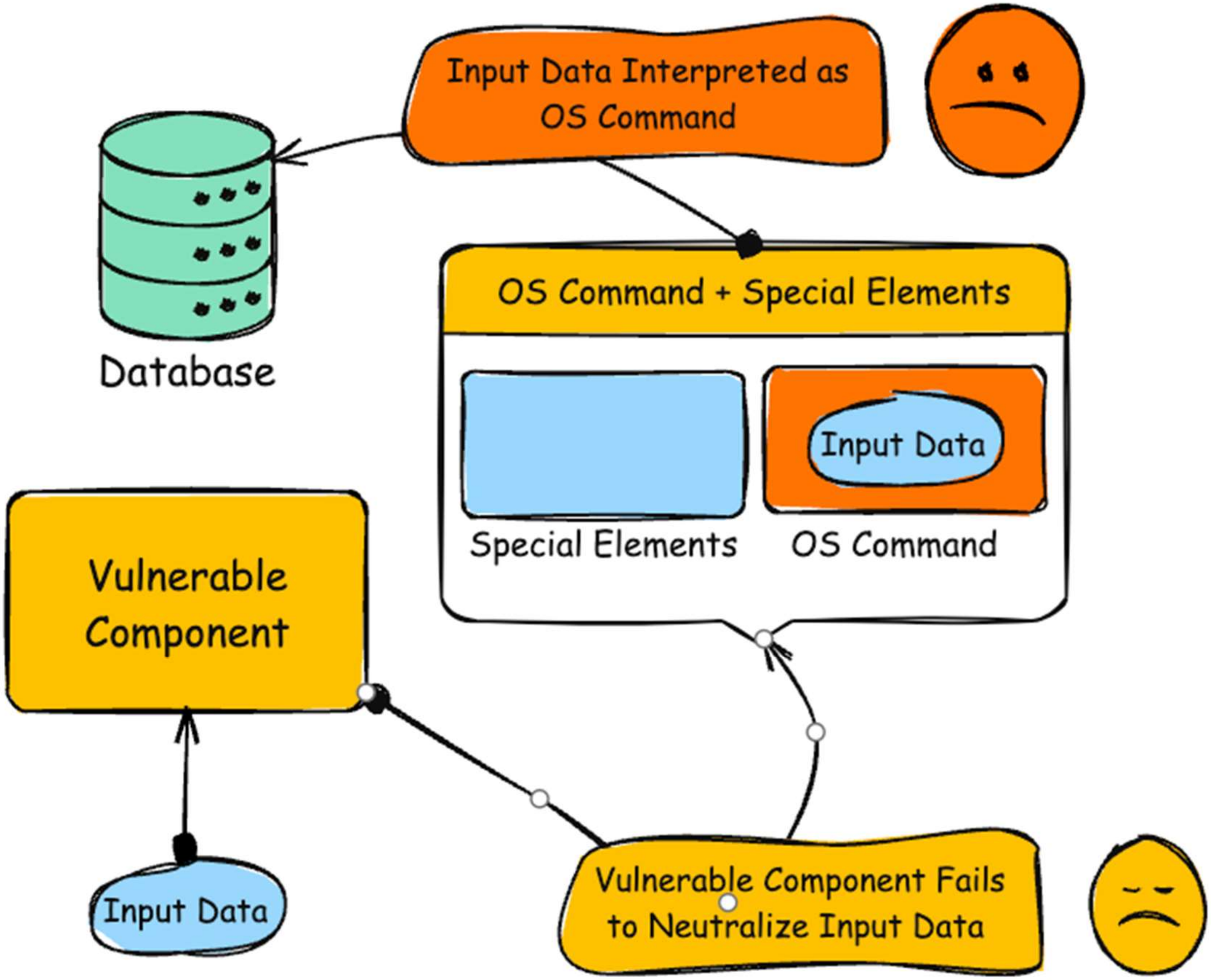
The work was done in 2016 by American graffiti artist JonOne.

By Hyun Soo Kim
April 2, 2021, 10:52 PM

The marks painted by a young couple are seen on the graffiti artwork of New York-based artist Jon One at a gallery in Seoul, South Korea, April 2, 2021.
Minwoo Park/Reuters

Five Rules

- **Keep it high level**
- **Target non-technical people**
- **Keep it simple**
- **Keep it rough**
- **Accessibility is important**


Input Data Interpreted as OS Command
Database
OS Command + Special Elements
Special Elements
Input Data
OS Command
Vulnerable Component
Input Data
Vulnerable Component Fails to Neutralize Input Data

Topic 2

Open Discussion

Chris Coffin

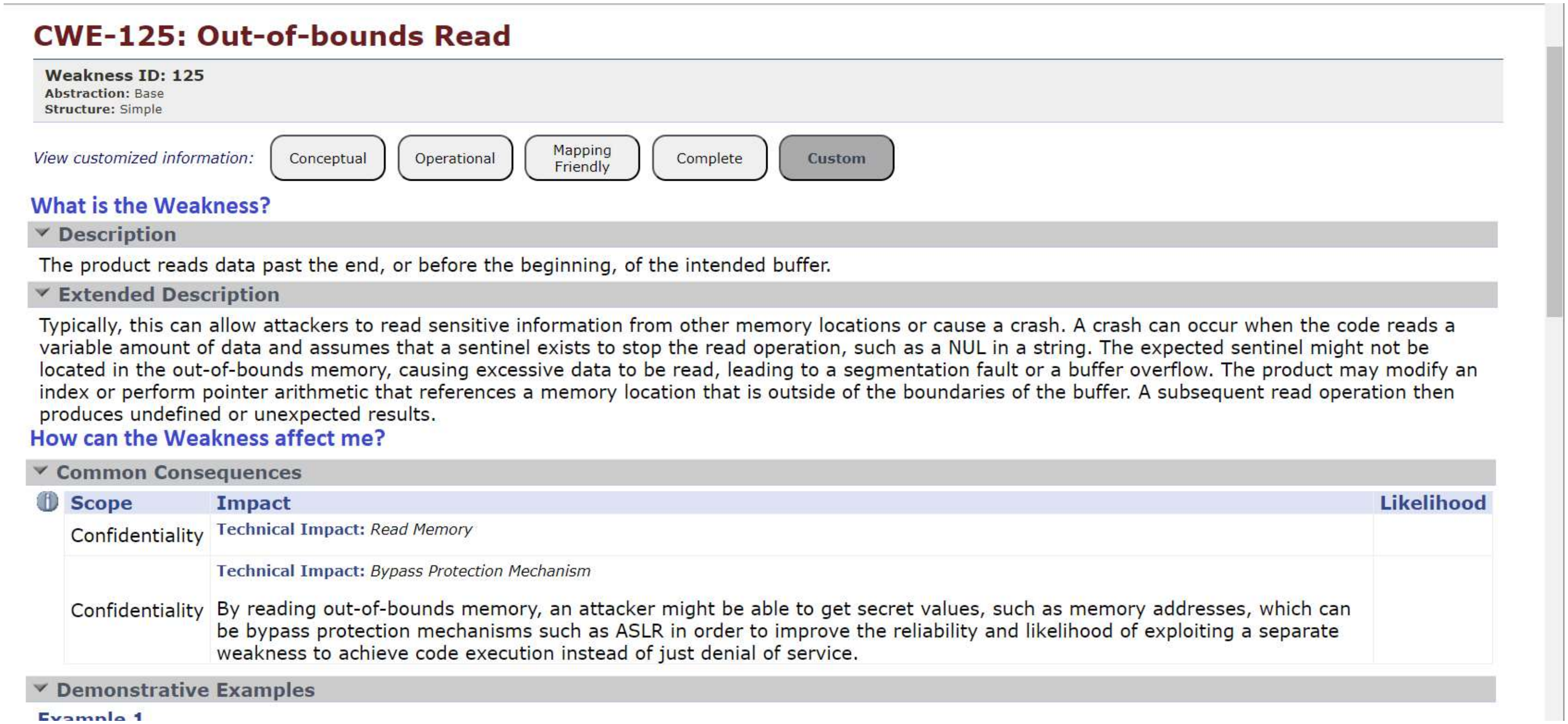
Next Meeting – January 31 @ 12pm

PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS

CWE@MITRE.ORG

Backups

CWE Element/Information Presentation – Mockup for New CWE Users



CWE-125: Out-of-bounds Read

Weakness ID: 125
Abstraction: Base
Structure: Simple

View customized information:

What is the Weakness?

Description

The product reads data past the end, or before the beginning, of the intended buffer.

Extended Description

Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. A crash can occur when the code reads a variable amount of data and assumes that a sentinel exists to stop the read operation, such as a NUL in a string. The expected sentinel might not be located in the out-of-bounds memory, causing excessive data to be read, leading to a segmentation fault or a buffer overflow. The product may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent read operation then produces undefined or unexpected results.

How can the Weakness affect me?

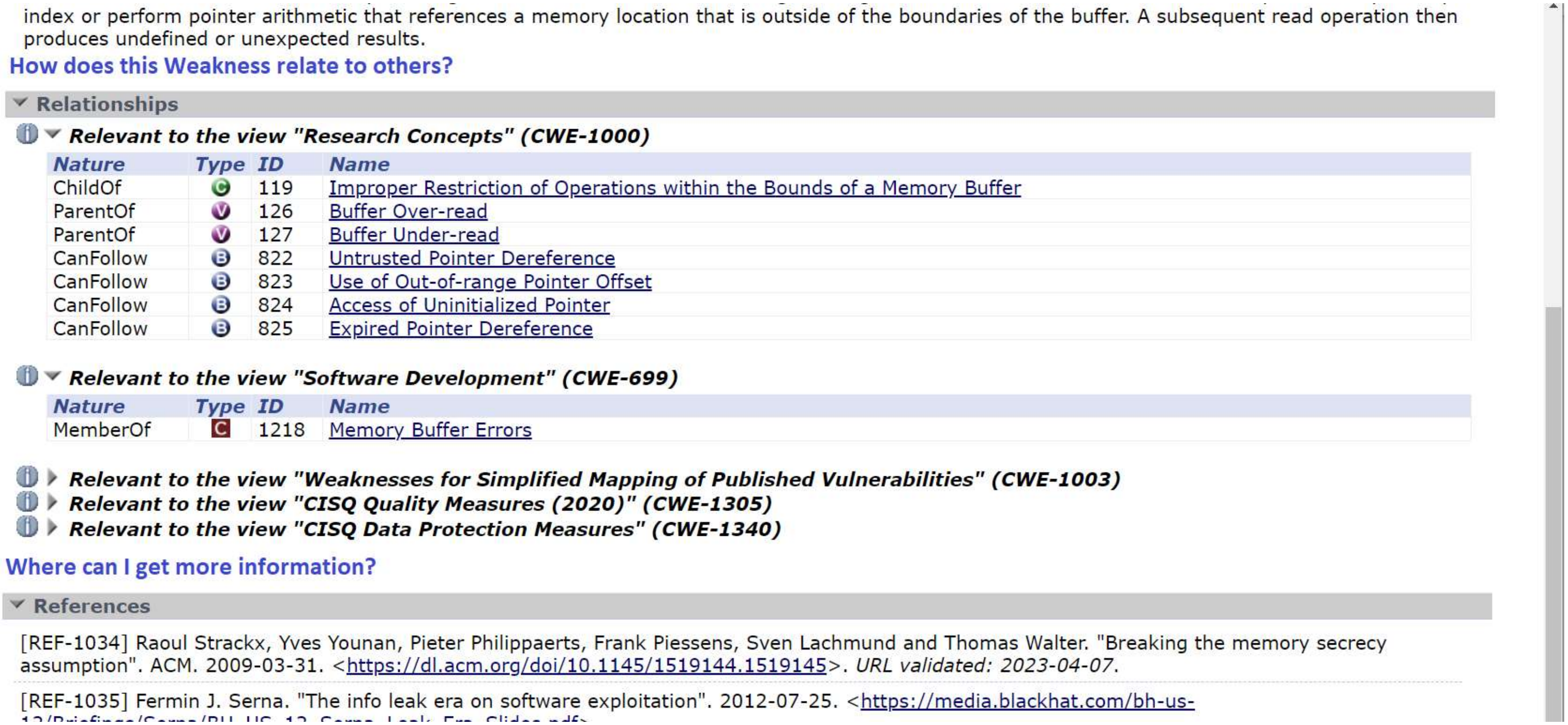
Common Consequences

Scope	Impact	Likelihood
Confidentiality	**Technical Impact:** *Read Memory*	
Confidentiality	**Technical Impact:** *Bypass Protection Mechanism* By reading out-of-bounds memory, an attacker might be able to get secret values, such as memory addresses, which can be bypass protection mechanisms such as ASLR in order to improve the reliability and likelihood of exploiting a separate weakness to achieve code execution instead of just denial of service.	

Demonstrative Examples

Example 1

CWE Element/Information Presentation – Mockup for New CWE Users



index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent read operation then produces undefined or unexpected results.

How does this Weakness relate to others?

▼ Relationships

ⓘ ▼ *Relevant to the view "Research Concepts" (CWE-1000)*

Nature	*Type*	*ID*	*Name*
ChildOf	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer
ParentOf	V	126	Buffer Over-read
ParentOf	V	127	Buffer Under-read
CanFollow	B	822	Untrusted Pointer Dereference
CanFollow	B	823	Use of Out-of-range Pointer Offset
CanFollow	B	824	Access of Uninitialized Pointer
CanFollow	B	825	Expired Pointer Dereference

ⓘ ▼ *Relevant to the view "Software Development" (CWE-699)*

Nature	*Type*	*ID*	*Name*
MemberOf	C	1218	Memory Buffer Errors

ⓘ ▶ *Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)*

ⓘ ▶ *Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)*

ⓘ ▶ *Relevant to the view "CISQ Data Protection Measures" (CWE-1340)*

Where can I get more information?

▼ References

[REF-1034] Raoul Strackx, Yves Younan, Pieter Philippaerts, Frank Piessens, Sven Lachmund and Thomas Walter. "Breaking the memory secrecy assumption". ACM. 2009-03-31. <https://dl.acm.org/doi/10.1145/1519144.1519145>. *URL validated: 2023-04-07.*

[REF-1035] Fermin J. Serna. "The info leak era on software exploitation". 2012-07-25. <https://media.blackhat.com/bh-us-12/Briefings/Serna/BH_US_12_Serna_Leak_Era_Slides.pdf>

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

Grouping CWEs

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a

- **CWE entries are currently “grouped” in different ways to provide useful subsets of the CWE corpus for different purposes:**
  - Views: a subset of CWE entries that provides a way of examining CWE content. The two main view structures are Slices (flat lists) and Graphs (containing relationships between entries), examples include:
    - CWE-1194: Hardware Design
    - CWE-699: Software Development
    - CWE-1400: Comprehensive Categorization for Software Assurance Trends
    - CWE-1003: Weaknesses for Simplified Mapping of Published Vulnerabilities (NVD)
  - Categories: a CWE entry that contains a set of other entries that share a common characteristic. A category is not a weakness, but rather a structural item that helps users find weaknesses that share the stated common characteristic.
    - CWE-1199: General Circuit and Logic Design Concerns
  - ~ Overall Hierarchy
    - CWE-1000: Research Concepts contains all CWE entries in one hierarchical structure

Grouping CWEs, cont.

- What groupings are most useful to new or casual CWE users? Experienced users?

- How can groupings be better presented/discovered/identified to the user?

- Should new users be guided to groupings of CWEs for learning about CWE? (e.g., links in user stories)

- Are there additional groupings that we are missing? Too many?

CSV Single Colon Separators Within Column Data

- **A double colon is used to separate csv fields/columns data, while a single colon is used to separate multi-value data within fields/columns**
- **The Observed Examples field contains Reference and link data that includes a url in some cases (colon within "http://…")**
- **Should a note be added to the download data that warns the user of this, or should we look into an alternative separator?**
- **Example taken from CWE - CWE-41: Improper Resolution of Path Equivalence (4.12) (mitre.org)**
  - ::REFERENCE:CVE-2000-1114:DESCRIPTION:Source code disclosure using trailing dot:LINK:https://www.cve.org/CVERecord?id=CVE-2000-1114::REFERENCE:CVE-2002-1986:DESCRIPTION:Source code disclosure using trailing

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

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)