

# CWE/CAPEC User Experience Working Group Meeting

---

**August 24, 2022**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).  
Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Agenda

---

**This meeting is being recorded :-)**

- **Housekeeping**
- **Primary topics**
  - Definitions! (continued...)
    - *Why are we doing this? The questions we asked ourselves...*
    - *Distillation of the many responses we received*
    - *Present newly proposed definitions*
  - Personas and Presentation Filters
- **Reminders and Adjourn**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

## UEWG: Reminders

---

- **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 Sept/Oct)
- **Please solicit participations from your contacts**
  - Contact: [cwe@mitre.org](mailto:cwe@mitre.org) & [capec@mitre.org](mailto:capec@mitre.org)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).  
Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

## Housekeeping

---

- **We are working to identify ongoing opportunities and priorities for FY23**
  - (Underway) Collaborative CWE/CAPEC content development space collaboration space
  - Provide users technical reach back
  - Socialization strategy
  
- **This discussion/action, drive working group activities, etc.**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Topic

## Definitions! (continued...)

### *Harmonizing common terms across CWE/CAPEC*

Alec Summers – CWE/CAPEC Deputy PL

Shadya Maldonado Rosado – UEWG Co-Chair



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).  
Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# CWE / CAPEC Terminology

- **Authoritative sources define terms differently**
  - Vulnerability is defined three different ways between CVE, CWE, and CAPEC ☹
- **Vulnerability, Weakness, and Attack Patterns have multiple definitions across CISA, NIST, ISO Standards, etc.**

Vulnerability			
Source	Definition	Source	Notes
CVE	A flaw in a software, hardware, firmware, or other component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or component	CWE	includes
Vulnerability	A characteristic or specific weakness that enables an attacker to obtain unauthorized access to information or an information system open to exploitation by a given threat or susceptible to a given hazard	CISA	- DHS Risk Lessons - CISA 4109 - NIST SP 800-51 Rev 4
Vulnerability	(CISA Extended Definition) Characteristics of location or security posture or of design, security procedures, internal controls, or the implementation of them that present a threat or hazard to users. Vulnerability regarding degree of vulnerability (qualitative or quantitative) measures of the level of susceptibility to harm when a threat or hazard is realized	CISA	- DHS Risk Lessons - CISA 4109 - NIST SP 800-51 Rev 4
Vulnerability	A vulnerability is a software weakness that can be exploited by an attacker. Bugs and flaws collectively form the basis of most software vulnerabilities	CISA	
Vulnerability	An occurrence of a weakness (or multiple weaknesses) within a product, in which the weakness can be used by a party to cause the product to misbehave, access unauthorized data, prevent proper execution, or perform unwanted actions that were not specifically granted to the party who uses the weakness	CWE	includes
Vulnerability	A vulnerability is a weakness that can be directly used by an adversary (as an exploit) to get a cyber-enabled capability to function in an unintended manner. Typically, this is the violation of reasonable security policy for the cyber-enabled capability resulting in a negative technical impact. Although all vulnerabilities involve a weakness, not all weaknesses are vulnerabilities. Common Vulnerabilities and Exposures (CVE) is a dictionary of common names for publicly known software-related vulnerabilities.	CAPEC	includes
Vulnerability	Weakness is an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source	NIST	Glossary
Vulnerability	A weakness is the design, implementation, operation or internal control of a process that could expose the system to adverse events from threat events	ISACA	Glossary
Vulnerability	A vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats	ISO	27001
Vulnerability	A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the confidentiality of an application	OWASP	includes

Weakness			
Source	Definition	Source	Notes
Point, point, insert point (Maybe insert things you want to say about this)			
Weakness	A type of mistake made during the implementation, design, or other phases of a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities in a range of products made by different vendors	NIST	- NIST SP 800-51 Rev 4
Weakness	Then existing practice, or something by CISOs	CISA	
Weakness	A weakness is an underlying condition or constraint existing in a software system that has the potential for negatively impacting the security of the system	CISA	
Weakness	A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities	CISA	- FY 2014 CISO FISMA Reporting Metrics - JTC1/SC 152 CWE
Weakness	A type of preliminary or final finding, which is an ineffective, or lack of implementation of one or more processes that meet the intent and value of a practice based on verified objective evidence, and applicable across the project(s) and organizational support function or organizational unit or a vehicle. This is defined either by the process itself does not address a CMMI practice requirement, or by the project(s) or organizational support function are not following their process that is compliant with the intent and value of the applicable CMMI practice	ISACA	Glossary
Weakness	A type of condition that, in proper conditions, could contribute to the introduction of vulnerabilities within that product. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a product lifecycle	CWE	includes

Attack Pattern			
Source	Definition	Source	Notes
Attack Pattern	The common approach and strategies related to the exploitation of a known weakness type, usually in cyber-enabled capabilities	as	related from def on CAPEC website
Attack Pattern	Single cycle events or behaviors that may initiate an attack, but are not an attack, resulting in a security violation or a potential security violation	US-CERT	- Oak Ridge National Laboratory - Vulnerabilities Techniques for Computer Network Defense - C. CAPEC Website
Attack Pattern	(US-CERT Extended Definition) For software, descriptions of common methods for exploiting software systems	US-CERT	- Oak Ridge National Laboratory - Vulnerabilities Techniques for Computer Network Defense - CAPEC Website
Attack Pattern	An abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed	ISACA	
Attack Pattern	An attack pattern is a general framework for carrying out a particular type of attack, such as a particular method for exploiting a buffer overflow or an interpretive attack that leverages architectural weaknesses. In this paper, an attack pattern describes the approach used for attack to generate an exploit against software	CISA	Glossary
Attack Pattern	Attack patterns are descriptions of common methods for exploiting software. They derive from the concept of design patterns (Gamma et al.) applied in a destructive rather than constructive context and are generalized from in-depth analysis of specific real-world exploit examples	CISA	
Attack Pattern	An attack pattern is a description of the common methods and approaches employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. Attack patterns differ from the challenges that an adversary may face and how they go about solving it. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generalized from in-depth analysis of specific real-world exploit examples. Common Attack Pattern Enumeration and Classification (CAPEC) provides a formal list of known attack patterns	CAPEC	includes



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security \(DHS\) Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Early Thought Process

---

- ***The questions we asked ourselves...***

- *What problem are we trying to solve?*
- *Are circular definitions problematic or important?*
- *Can we accommodate with the CVE 'vulnerability' definition without changes?*

- **Other thoughts**

- Steve's 'APES' Test (i.e., 'aspirin', physical, extension cord, spelling)



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

## Compilation of Feedback (1 of 2)

---

- **Feedback providers agreed to delete "... in a range of products made by different vendors"**
- **Follow CVE vulnerability definition format/style**
- **Using the term "flaw" may create a circular definition**
- **Leverage the term "condition" instead of "defect"**
- **May or may not be exploitable**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



## Compilation of Feedback (2 of 2)

---

- **Vulnerability = one or more weaknesses + known exploit**
  - vulnerability weakness(es) that can be exploited as part of an attack path
  - weakness Condition that can lead to undesirable behavior
- **A condition that under the right circumstances begins a process or combines with other weaknesses to cause a harm in a product or system**
- **Under the right conditions, could lead to undesirable behavior**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Sample Proposed Definitions

## Original Proposed definition for Weakness:




A type of flaw or defect inserted during a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities in a range of products made by different vendors

- A **condition** that under the right circumstances begins a process or combines with other weaknesses to cause a harm in a product or system
- A condition or mistake made during the implementation, design, or other **phases of a product lifecycle** could contribute to the introduction of exploitable elements
- A type of flaw or defect inserted during a product lifecycle that, **under the right conditions**, could lead to undesirable behavior
- A type of flaw or defect **inserted {or inadvertently developed}** during a product lifecycle that, under the right conditions, could contribute to the introduction of vulnerabilities
- A condition created or introduced during a product lifecycle that, under the right conditions, could lead to undesirable behavior



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

## Definitions: Take Two

Term	Definition	Authority	Authorities Doc
 Vulnerability	A flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components	CVE	website
 Weakness	A condition in a software, firmware, hardware, or service component that, under the right circumstances, could contribute to the introduction of vulnerabilities	n/a	edited from def on CWE website
 Attack Pattern	The common approach and attributes related to the exploitation of a weakness, usually in cyber-enabled capabilities	n/a	edited from def on CAPEC website



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Topic 2

## User Personas and CWE/CAPEC Presentation Filters

*Alec Summers*

*CWE/CAPEC Deputy PL*

**CWE/CAPEC minor releases coming in late Sept / early Oct**



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA).  
Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Personas: Finalizing

- ~~Formally define each user persona~~
- ~~Share with CWE/CAPEC Board~~
- Once finalized, make public on our sites
- Use that as a catalyst for modernizing presentation according to persona needs

- **“Development lifecycle”**

- Those who build, use, and protect infrastructure around information systems

- **Educators:** Teachers, professors, or certification programs that educate developers and system designers how to develop more secure code, design more secure products, and/or how to find vulnerabilities.
- **Technical Writers:** Those who communicate advanced technical concepts as clearly, accurately, and comprehensively as possible to their intended audience (e.g., code analysis tool users or system designers)
- **Tool Developers:** Developers of code scanning products, services, and other types of automated techniques for finding weaknesses and attacking systems, and reporting/educating on findings to users
- **Security Researchers/Analysts:** Those who look for ways to attack a product by finding weaknesses using manual and/or automated techniques, then reporting the findings to the vendor and/or the general public (to include threat modeling, C-SCRM)
- ~~**Incident Response Teams:** Those responsible for preparation and reaction to any security event ??~~



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Adjusting our Presentation Filters

---

- **Better serve our user persona needs**
- **“Two-Types” Proposal by Premyslaw Roguski (Red Hat)**
  1. Theoretical: users who are more focused on the theoretical aspects of the weaknesses
    - Educators (teachers, professors, solution architects who design the systems' requirements)
    - Technical Writers (people responsible for security content, security blogs and articles)
    - Project and Program Managers who need some level of understanding about security and weaknesses
  2. Technical: users who are managing the security issues and need more details about the nature of the weakness and how to prevent this from happening
    - Tool Developers, Security Researchers, Pentesters, Incident Response Analysts



# Proposed Data Elements for Each Group

---

- **Theoretical:**

- Description, Extended Description, Alternate Terms, Common Consequences

- **Technical (operational?):**

- Description, Extended Description, Alternate Terms, Modes of Introduction, Demonstrative Examples, Observed Examples (include recent CVE tracking data\*), Potential Mitigations, Relationships

- **Mapping-Friendly:**


- Description, Extended Description, Alternate Terms, ~~Modes of Introduction, Likelihood of Exploitation~~, Taxonomy Mappings, Memberships, Notes


- **Complete:**

- all



# Discussion: How best to Improve Awareness/Utility?


**Common Weakness Enumeration**  
*A Community-Developed List of Software & Hardware Weakness Types*

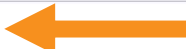


Home > CWE List > CWE- Individual Dictionary Definition (4.8)
ID Lookup:  Go

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

## CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Weakness ID: 120  
Abstraction: Base  
Structure: Simple

Presentation Filter:  

**Description**  
The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.

**Extended Description**  
A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold, or when a program attempts to put data in a memory area outside of the

- Do people know it's there on each entry?
- Where else could we draw attention to it (e.g., landing page, how-to/guidance material?)



## Slide 16

---

**AJS0** Name change:  
presentation filter? "View customized information"  
Alec J Summers, 2022-08-24T16:25:27.388

**AJS1** Instead of drop down menu... present four buttons in one line for each "presentation filter" or whatever new term we called. These buttons could have hover text with definitions  
Alec J Summers, 2022-08-24T16:26:09.594

**Next Meeting – September 21 @ 12pm**

---

**PLEASE CONTACT WITH ANY QUESTIONS OR THOUGHTS**

**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 © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Use Case Scenarios → Content Presentation

- **CAPEC Existing functionality to filter content detail**
  - Basic, High-level, Mapping-friendly, Complete

CWE Content Filter			
BASIC	HIGH-LEVEL	MAPPING	COMPLETE
Description	Description	Description	Description
Applicable_Platforms	View_Audience	View_Audience	View_Audience
Common_Consequences	Alternate_Terms	Alternate_Terms	Alternate_Terms
Likelihood_of_Exploit	Time_of_Introduction	Terminology_Notes	Terminology_Notes
Demonstrative_Examples	Common_Consequences	Relationships	Applicable_Platforms
Potential_Mitigations	Relationships	Relationship_Notes	Modes_of_Introduction
Relationships	Content_History	Theoretical_Notes	Common_Consequences
Content_History		Related_Attack_Patterns	Likelihood_of_Exploit
		Content_History	Enabling_Factors_for_Exploitation
			Detection_Methods

and more...



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

# Use Case Scenarios → Content Presentation

## ■ CAPEC Existing functionality to filter content detail

- Basic, Complete

CAPEC CONTENT	
BASIC	COMPLETE
Description	Description
Relationships	Relationships
Memberships	Memberships
Execution_Flow	Execution_Flow
Prerequisites	Prerequisites
Mitigations	Mitigations
Related_Weaknesses	Likelihood_Of_Attack
	Alternate_Terms
	Typical_Severity
	Skills_Required
	Resources_Required
	Indicators
	Consequences
	Example_Instances
	Related_Weaknesses
	Taxonomy_Mappings
	References
	Notes
	Content_History



CWE and CAPEC are sponsored by [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 1999–2022, [The MITRE Corporation](#). CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.