Centro de
Investigación en
Computación

MITRE CWE

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. CWE
3. CWE Top 25
4. Casos de analisis

Introducción

Conceptos básicos

Introducción

Definiciones

Objetivo de la lista

Knowing the weaknesses that result in vulnerabilities means software developers, hardware designers, and security architects can eliminate them before deployment, when it is much easier and cheaper to do so.

Fuente

https://cwe.mitre.org/about/index.html

CWE

Definiciones

CWE

Intro

Flaw: defecto, imperfección.

Common Weakness Enumeration

- It is a community-developed **list** of software and hardware weakness types that have security ramifications. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
- Definiciones en el sitio:
  - Weaknesses are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack.
  - Weakness is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.

CWE

Intro

Características

- The CWE List is updated three to four times per year.
- Before being published on the CWE website, weaknesses are developed in the CWE Content Development Repository (CDR) on GitHub.com.
- Another useful feature is the external mappings of CWE content to related resources including:
  - The annual CWE Top 25.
  - OWASP Top Ten.
  - Seven Pernicious Kingdoms.
  - Software Fault Pattern Clusters.
  - SEI CERT Coding Standards for C, Java, and Perl.
- The CWE List is:
  - Searchable and may be viewed or downloaded in its entirety.
  - There is also a the CWE REST API to make CWE content available to community applications and websites in a more convenient way.
  - https://github.com/CWE-CAPEC/REST-API-wg/blob/main/Quick%20Start.md

CWE

Intro

Referencias

- Fuentes oficiales
  - Web: https://cwe.mitre.org/
  - Documento: https://cwe.mitre.org/data/published/cwe_latest.pdf
- Otras fuentes
  - https://www.youtube.com/watch?v=GJNaEpv3Ok0&t 2:33min Eng

CWE

Intro

Cifras

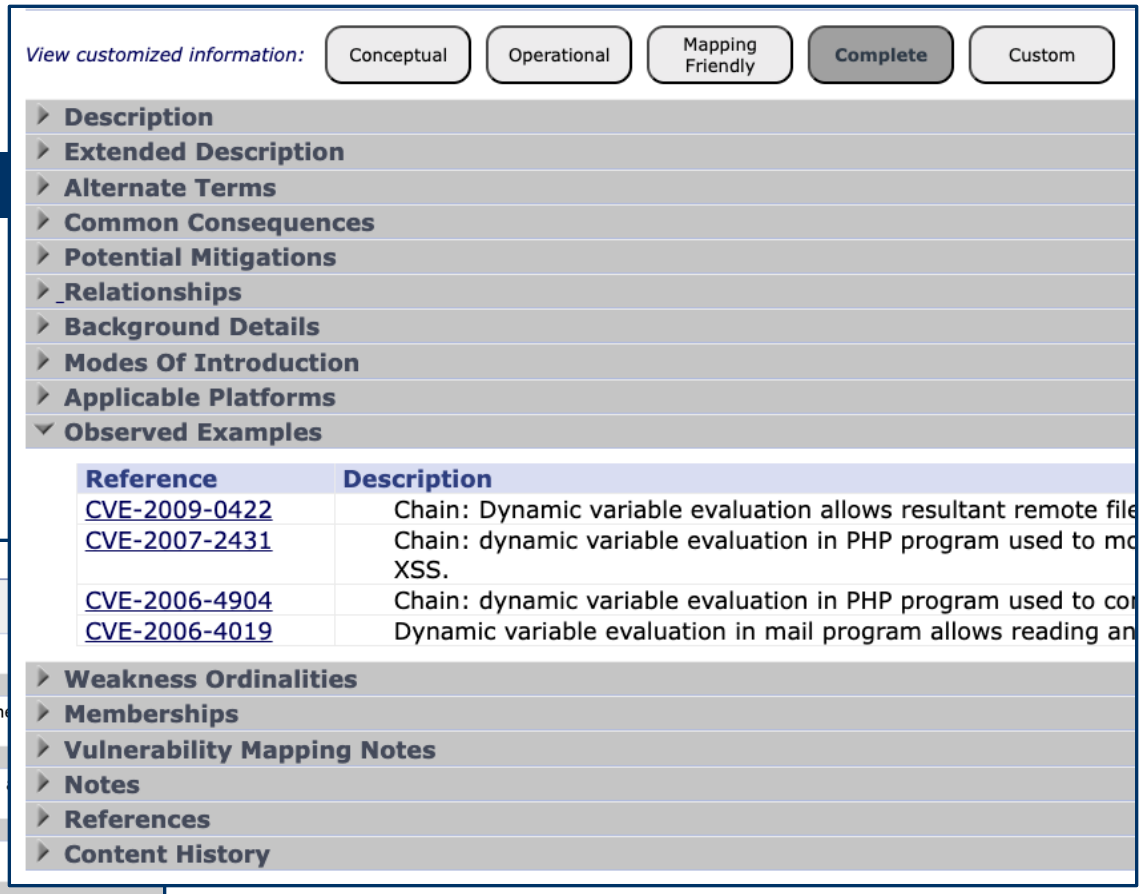
- Estructura
  - Prefijo CWE + Número
  - El número está en el rango [5, 1427] 10/feb/2025
- Registros
  - 31,770 10/feb/2025.
- Última versión
  - Número: 4.16
  - Fecha: 2024-11-19
  - PDF: 2,812 páginas.

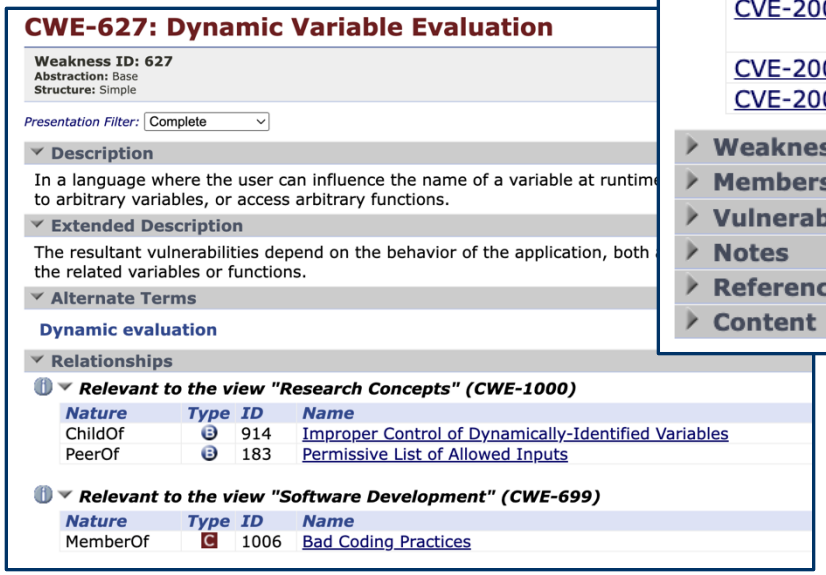
CWE

Intro

CWE registros

Cada uno puede tener hasta 16 elementos que lo describen:





CWE

Intro

https://cwe.mitre.org/documents/glossary/index.html

CWE contains over 900 weaknesses which range from abstract and conceptual to precise and technology specific. A precise weakness will have a “parent” weakness that is more abstract, which may also have “parent” weaknesses, and so on.

Weakness are **grouped** in two ways:

- Categories. They represent a common characteristic used to group related things.
- Abstractions. There are four types of weakness abstractions:
  1. Pillar
  2. Class
  3. Base
  4. Variant

CWE

Intro

Mistake^{noun}. It is an action (decision) that is unintentional or deviates from what was expected.

Una persona toma malas decisions.

Error^{noun}. It is a deviation from accuracy or correctness.

Una computadora produce errores.

Wrong^{adjective}, fault^{noun}, blunder^{noun}.

- Pillar

  It is a type of weakness that describes a mistake, but does not imply anything specific about where such a mistake is made or the type of resource that is affected.

- Class

  A weakness that is described in a very abstract fashion, typically independent of any specific language or technology. More specific than a Pillar Weakness, but more general than a Base Weakness.

- Base

  A weakness that is described in an abstract fashion, but with sufficient details to infer specific methods for detection and prevention. More general than a Variant weakness, but more specific than a Class Weakness.

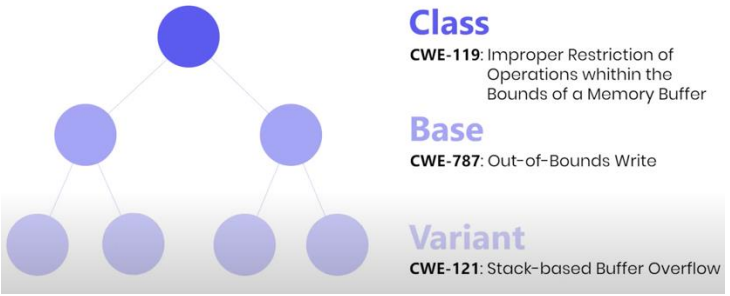
- Variant

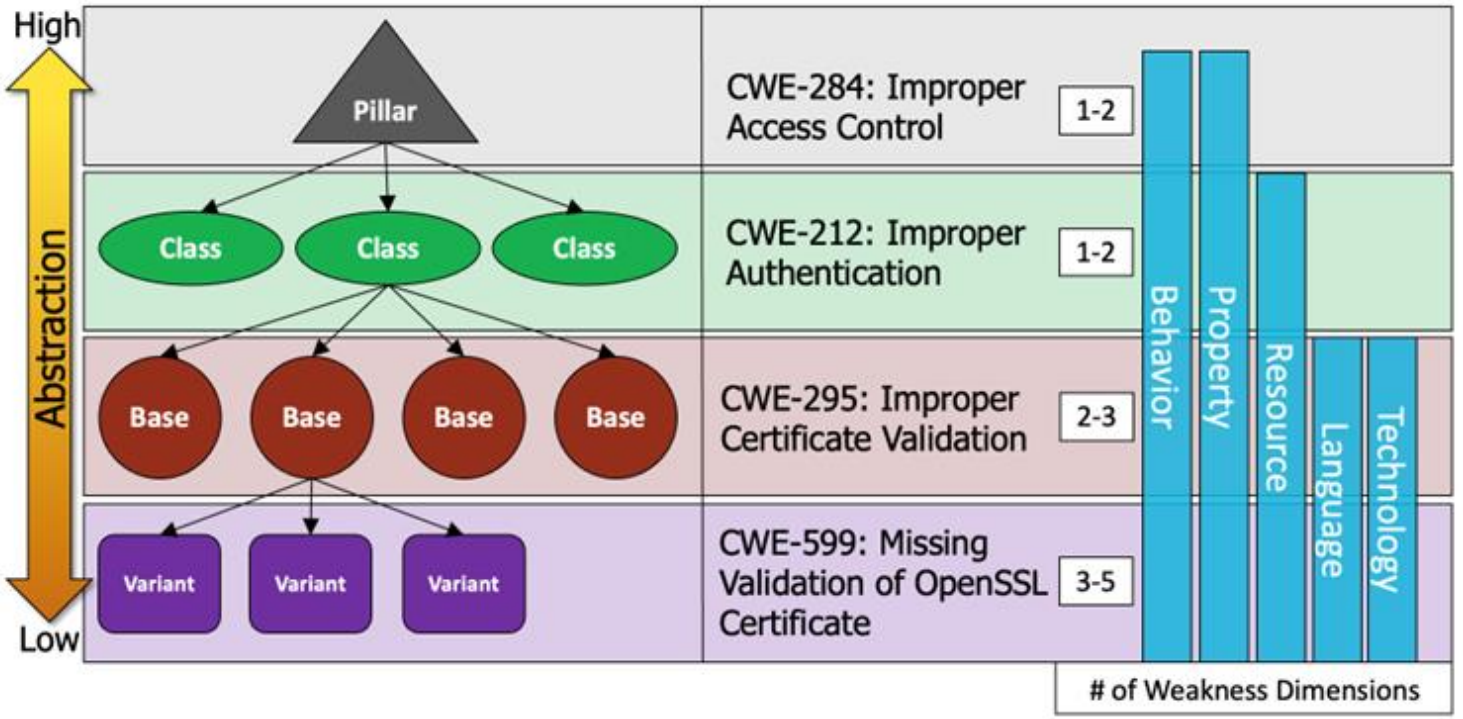
  A weakness that is linked to a certain type of product, typically involving a specific language or technology. More specific than a Base weakness.

Abstractions describe issues in terms of dimensions: behavior, property, technology, language, and resource. They range from 1 or 2 (pillar) to 3 or 5 (variants).

CWE

Intro


Class
CWE-119: Improper Restriction of Operations whithin the Bounds of a Memory Buffer
Base
CWE-787: Out-of-Bounds Write
Variant
CWE-121: Stack-based Buffer Overflow


High
Abstraction
Low
Pillar
Class
Class
Class
Base
Base
Base
Base
Variant
Variant
Variant
CWE-284: Improper Access Control
1-2
CWE-212: Improper Authentication
1-2
CWE-295: Improper Certificate Validation
2-3
CWE-599: Missing Validation of OpenSSL Certificate
3-5
Behavior
Property
Resource
Language
Technology
# of Weakness Dimensions

CWE

Intro

Root cause mapping

It is the identification of the underlying cause(s) of a vulnerability. This is best done by Correlating:

- CVE Records
- Bugs
- Vulnerability tickets

with CWE entries. Today, this is not done accurately at scale by the vulnerability management ecosystem.

CWE

Intro

Ejemplos de CWE

- CWE 5-9, 245,246: J2EE.
- CWE 11-13: ASP.NET.
- CWE 102-110: Struts.
- CWE 23-35, 36-40: Path Traversal: Relative y Absolute
- CWE 41-58: Improper Resolution of Path Equivalence.
- CWE 76-97: Improper Neutralization of XXX.
- CWE 166-178, 228-241: : Improper Handling of XXX.
- CWE 312-97: Cleartext Storage of XXX.
- CWE 1284-58: Improper Validation of XXX.
- Otros terminos: Exposure of, Untrusted, Unprotected, Uncontrolled, etc.

CWE Top 25 Most Dangerous Software Weaknesses

Año 2024

Que porcentaje abarcan?

CWE Top 25 sw

Lista

Año 2024

Improper = 10

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2023
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	56.92	3	+1
2	CWE-787	Out-of-bounds Write	45.20	18	-1
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	35.88	4	0
4	CWE-352	Cross-Site Request Forgery (CSRF)	19.57	0	+5
5	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12.74	4	+3
6	CWE-125	Out-of-bounds Read	11.42	3	+1
7	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.30	5	-2
8	CWE-416	Use After Free	10.19	5	-4
9	CWE-862	Missing Authorization	10.11	0	+2
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.03	0	0
11	CWE-94	Improper Control of Generation of Code ('Code Injection')	7.13	7	+12
12	CWE-20	Improper Input Validation	6.78	1	-6
13	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	6.74	4	+3
14	CWE-287	Improper Authentication	5.94	4	-1
15	CWE-269	Improper Privilege Management	5.22	0	+7
16	CWE-502	Deserialization of Untrusted Data	5.07	5	-1
17	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	5.07	0	+13
18	CWE-863	Incorrect Authorization	4.05	2	+6
19	CWE-918	Server-Side Request Forgery (SSRF)	4.05	2	0
20	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	3.69	2	-3
21	CWE-476	NULL Pointer Dereference	3.58	0	-9
22	CWE-798	Use of Hard-coded Credentials	3.46	2	-4
23	CWE-190	Integer Overflow or Wraparound	3.37	3	-9
24	CWE-400	Uncontrolled Resource Consumption	3.23	0	+13
25	CWE-306	Missing Authentication for Critical Function	2.73	5	-5

CWE Most Important Hardware Weaknesses

Año 2021

Que porcentaje abarcan?

CWE Most important Hw

Lista

Año 2021

CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

Improper = 7 de 12

Casos de Análisis

Revisión detallada

Casos de Análisis

Top 25, #1

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

- URL
  - https://cwe.mitre.org/data/definitions/79.html
- There are three main kinds of XSS:

  'XSS' is commonly used to avoid confusion with Cascading Style Sheets (CSS).
  - Type 1: Reflected XSS (or Non-Persistent)
  - Type 2: Stored XSS (or Persistent)
  - Type 0: DOM-Based XSS

Standars

CWE CATEGORY: Bad Coding Practices

Category ID: 1006

Summary

Weaknesses in this category are related to coding practices that are deemed un
present in the application. These weaknesses do not directly introduce a vulnera
or maintained. If a program is complex, difficult to maintain, not portable, or sh
weaknesses are buried in the code.

Membership

Nature	Type	ID	Name
MemberOf	V	699	Software Developr
HasMember	B	478	Missing Default Ca
HasMember	B	487	Reliance on Packag
HasMember	B	489	Active Debug Code
HasMember	V	546	Suspicious Comme
HasMember	V	547	Use of Hard-coded
HasMember	B	561	Dead Code

CWE-627: Dynamic Variable Evaluation

Weakness ID: 627
Abstraction: Base
Structure: Simple

Presentation Filter: Complete

Description

In a language where the user can influence the name of a variable at runtime, if the variable na
to arbitrary variables, or access arbitrary functions.

Extended Description

The resultant vulnerabilities depend on the behavior of the application, both at the crossover po
the related variables or functions.

Alternate Terms

Dynamic evaluation

Relationships

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

Nature	Type	ID	Name
ChildOf	B	914	Improper Control of Dynamically-Identified Variables
PeerOf	B	183	Permissive List of Allowed Inputs

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

Nature	Type	ID	Name
MemberOf	C	1006	Bad Coding Practices

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652