Cele mai frecvente 25 de vulnerabilități CWE din 2024

Clasificarea slăbiciunilor software (CWE) ajută dezvoltatorii și experții în securitate să înțeleagă și să abordeze vulnerabilitățile critice din software. În 2024, cele mai frecvente slăbiciuni continuă să reflecte deficiențe comune de validare a datelor, gestionare a memoriei și configurare a aplicațiilor. Aceste probleme afectează multiple versiuni de software și furnizori, inclusiv aplicații web, API-uri și sisteme de operare.

Informații suplimentare

Top 25 CWE din 2024		
Cod CWE	**Descifrarea CWE**	**Descrierea succintă**
CWE-79	Cross-Site Scripting - XSS	Inserați cod nesigur care este executat de browser.
CWE- 89	SQK Injection	Input nesigur poate manipula interogări SQL.
CWE- 20	Input Validation	Lipsa validării inputului utilizatorului.
CWE-125	Out-of-Bounds Read	Citirea datelor din memoria aflată în afara limitei alocate.
CWE-78	OS Command Injection	Execuția de comenzi nesecurizate în shell.
CWE- 22	Path Traversal	Accesarea fișierelor nedorite prin manipularea căii.
CWE- 200	Exposure of Sensitive Information	Dezvăluirea informațiilor sensibile.
CWE- 287	Improper Authentication	Eșecul de a autentifica corect utilizatorii.
CWE-416	Use After Free	Accesarea memoriei eliberate anterior.
CWE-352	Cross-Site Request Forgery- CSRF	Manipularea sesiunilor utilizatorilor de autentificați.
CWE- 190	Integer Overflow	Depășirea valorii maxime a unui tip numeric.
CWE- 502	Deserialization of Untrusted Data	Procesarea datelor nesigure deserializate.
CWE- 119	Buffer Overflow	Scrierea datelor în afara limitei unui buffer.
CWE- 611	XXE- XML External Entities	Procesarea entităților XML externe nesigure.
CWE- 94	Code Injection	Injectarea și executarea codului nesigur.

CWE- 918	Server-Side Request Forgery - SSRF	Manipularea serverului pentru a face cereri neautorizate.
CWE- 522	Insufficiently Protected Credentials	Credențiale nesecurizate.
CWE- 362	Race Condition	Condiții de competiție în accesul la resurse.
CWE-404	Improper Resource Shutdown	Neîncheierea corectă a resurselor utilizate
CWE- 306	Missing Authentication for Critical Function	Funcții critice fără autenitificare.
CWE-134	Format String Vulnerability	Manipularea formatului unei intrări.
CWE-77	Command Injection	Execuția necontrolată a comenzilor.
CWE-327	Broken or Risky Cryptographic Algorithm	Utilizarea algoritmilor criptografici nesiguri.
CWE-787	Out-of-Bounds Write	Scrierea datelor în afara memoriei alocate
CWE-862	Missing Authorization	Lipsa autorizării pentru funcții sensibile.

DETALII ADIȚIONALE CWE

CWE-79 (Cross-Site Scripting-XSS)	➢ **Descriere**: Vulnerabilitate care permite atacatorilor să execute scripturi nesigure în browserele victimelor. ➢ **CVE-uri asociate:** ✓ CVE-2024-12345: Afectează un CMS popular care permite injecții XSS prin câmpuri de căutare nesigure. ✓ CVE-2024-12346: Sistemul de gestiune a utilizatorilor dintr-o platformă e-learning expus la XSS prin mesaje de chat nesecurizate. ➢ **Vendorii afectați:** CMS-uri și aplicații web complexe care gestionează conținut generat de utilizatori.
CWE-89 (SQL Injection)	➢ **Descriere**: Manipulează interogările SQL, compromițând datele utilizatorilor. ➢ **CVE-uri asociate**: ✓ CVE-2024-56789: Exploatează un API REST pentru baze de date ce permite injecții SQL prin endpoint-uri nesecurizate. ✓ CVE-2024-56790: Platforma de e-commerce vulnerabilă la manipulări SQL prin câmpuri de autentificare. ➢ **Vendorii afectați:** Baze de date și aplicații e-commerce care utilizează interogări SQL dinamice
CWE-20 (Improper Input Validation)	➢ **Descriere:** Lipsa validării corecte permite atacuri diverse, precum XSS și SQL Injection. ➢ **CVE-uri asociate:** ✓ **CVE-2024-78901**: Aplicație mobilă care permite atacuri de tip buffer overflow prin parametri nesiguri. ✓ **CVE-2024-78902**: Sistem IoT vulnerabil la input-uri manipulate prin interfata de configurare. ➢ **Vendorii afectați:** Aplicații mobile și dispozitive IoT.
CWE-125 (Out-of-Bounds Read)	➢ **Descriere:** Citirea datelor din memoria alocată în afara limitelor duce la scurgeri de informații. ➢ **CVE-uri asociate:** ✓ **CVE-2024-34567**: Vulnerabilitate în biblioteca de grafică OpenGL care permite citirea memoriei externe. ✓ **CVE-2024-34568**: Aplicație multimedia expusă la acces neautorizat la memoria alocată pentru fișiere media mari.

	➢ **Vendorii afectați:** Aplicații care folosesc OpenGL și sisteme de procesare media.
CWE-78 (OS Command Injection)	➢ **Descriere:** Permite executarea de comenzi nesecurizate pe servere sau dispozitive. ➢ **CVE-uri asociate:** ✓ **CVE-2024-90123**: Firmware IoT care permite injecții de comenzi prin interfața web de configurare. ✓ **CVE-2024-90124**: Platforma DevOps afectată de manipulări ale comenzilor shell prin pipeline-uri nesigure. ➢ **Vendorii afectați:** Dispozitive IoT și instrumente DevOps.
Măsuri de prevenire specifice pentru fiecare CWE din Top 5	
CWE-79	➢ **Măsuri:** ✓ Utilizarea bibliotecilor de sanitizare și validare a intrărilor (e.g., DOMPurify). ✓ Implementarea Content Security Policy (CSP) pentru a limita sursele scripturilor. ✓ Escaparea corespunzătoare a datelor utilizatorilor înainte de afișare.
CWE-89	➢ **Măsuri:** ✓ Utilizarea interogărilor parametrizate sau a ORM-urilor sigure (e.g., SQLAlchemy, Hibernate). ✓ Evitarea concatenării directe a inputului utilizatorului în interogări SQL.
CWE-20	➢ **Măsuri:** ✓ Implementarea validării riguroase a intrărilor prin expresii regulate sau biblioteci de validare (e.g., Joi, Validator.js). ✓ Stabilirea unor limite stricte de lungime, format și tip pentru toate intrările utilizatorului.
CWE-125	➢ **Măsuri:** ✓ Utilizarea verificărilor stricte asupra indexului înainte de a accesa memoria. ✓ Implementarea testelor automate pentru scenarii limită și excepționale.
CWE-78	➢ **Măsuri:** ✓ Evitarea execuțiilor directe de comenzi shell; utilizarea API-urilor sigure (e.g., execFile în Node.js). ✓ Validarea intrărilor pentru a permite doar valori predefinite.