CWE/SANS → si applica in generale alle strutture di calcolo informatico

graduatoria (liste)

alcune voci in comune

OWASP → si applica al web

CWE → é alto in graduatoria, ciò che é diffuso, frequente e ciò che porta un danno (pericoloso)

easy to find, exploit

é facile trovare la vulnerabile, é facile sfruttarla e può avere effetti

CVE

specifici esempi

CWE-416: Use After Free

esempio di debolezza a basso livello

CWE-200: Expose of Sensitive Information to an Unauthorized Actor

→ progettazione di un sistema, non tecnologico

→ Top 5 CWE/SANS

1. Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
2. Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)
3. Buffer Copy without checking Size of Input ('classic Buffer Overflow')
4. Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)

⑤ Missing Authentication for Critical Function

1) SQL Injection

Il problema alla base, sia in questa vulnerabilitá che in molte altre, riguarda il mancato controllo dell'input da parte dell'utente. In questa situazione, l'input dell' utente viene direttamente copiato ed utilizzato in una query SQL al database (comandi come 'DROP table x') o anche piú semplicemente modificare il DB.
La SQL Injection sfrutta tecnologie di Database.
L'impatto e le conseguenze comuni riguardano invece diversi aspetti:

- **Confidentiality**: viene persa la confidenzialitá dei dati sensibili. L'attaccante é in grado di leggere i dati dell'applicazione.
- **Access Control**: l'attaccante puó accedere ad altri account senza conoscere la password.
- **Integrity**: la modifica o cancellazione dei dati

→ Principale soluzione gestire, controllare e pulire l'input prima di inserirlo in una query.

2) OS Command Injection

↳ problema simile al precedente

si sfruttano applicazioni che richiedono input per richiamare funzioni sul sistema operativo dalla web application.

l'app richiede un input per usare un programma

l'applicazione esegue il suo programma sul suo OS. richiede pero' un input

un mancato controllo puó far eseguire all' attaccante il programma che VUOLE!!

→ Impatto → Confidentiality
→ Integrity
→ Availability
→ Non-Repudiant

→ Poiché é l'applicazione di destinazione che esegue direttamente i comandi anziché l'attaccante, é possibile che qualsiasi attività dannosa provenga dall'app o dal proprietario dell'app e venga attribuita ad esso.

3) Buffer Overflow → in C, C++
→ Non controllare la dimensione dell' Input prima di copiarlo in un altro buffer in output può portare a vulnerabilità.
→ copro più memoria di quella disponibile

→ Impatto → Availability → manda in crash!
→ Integry
→ Confidentiality

→ Inserendo codice malevolo dentro il buffer, é possibile eseguire tale codice dallo scope del programma.

4) Cross-site scripting → mancato controllo dell'input
→ XSS

1. Dati non sicuri vengono inseriti in una applicazione web, generalmente tramite una web request
2. La web app genera contenuto non sicuro
3. Non viene impedito inserimento di JS
4. Visita pagina con script infetto

5. Il web browser della vittima esegue lo script che viene generato dal web server

→ 3 tipologie di XSS → Reflected XSS (or Non-Persistent)
→ Stored XSS (or Persistent)
→ DOM-Based XSS

→ Le tecnologie vulnerabili → Web Based app

→ Impatto → Confidentiality
→ Integrity
→ Availability
→ Access Control

→ L'attacco XSS più comune riguarda la divulgazione dei cookie dell'utente, i quali racchiudere informazioni anche private.
→ Sfruttare script sul browser per installare virus
→ Utilizzando i coockie di un altro utente è possibile violare il Controllo degli accessi

5) Missing Authentication for Critical Function
→ Il software non effettua alcune autenticazione per le funzionalità che richiedono l'identità verificata

→ Impatto
→ Access control other
→ assumere privilegi o assumere l'identità di altri

Top 5 OWASP

1. Injection
2. Broken Authentication
3. Cross-site scripting
4. Broken Access Control
5. Security Misconfiguration

1) Injection

- possibilità di iniettare (inviare) dati ostili ad un interprete.
  - SQL Injection dei siti web con PHP e SQL Server
  - DAP, XPath, NoSQL, ORM, OS command, XML...
- Input non controllato!

Impatto

da piccola divulgazione di dati a modifica / cancellazione di essi.

2) Broken Authentication

- accesso ad un account privato da parte dell'attaccante.

bloccare possibilità di ripravare

- mancato filtro su attacchi automatizzati, che prevedano il riempimento automatico dei campi
- mancata prevenzione da attacchi brute force
- autenticazione a singolo fattore

3) Cross-Site Scripting

- sfrutta vulnerabilità del web per eseguire script dinamici

- Reflected XSS → inserimento nel link di un sito vulnerabile di uno script malevolo. La vittima clicca sul link del sito e il browser esegue lo script.
- Persistant / Stored XSS

é la tipologia ad impatto più alto, script memorizzato nel server

- DOM XSS → impatto moderato, il codice viene eseguito direttamente nel framework / JS

4) Broken Access Control

- Verifica che alcuni specifici url generalmente nascosti siano accessibili solo da utenti autorizzati
- L'attaccante, visto come un utente correttamente autenticato accede ad informazioni al di fuori del suo dominio

5) Security Misconfiguration

- configurazione errata dei criteri di sicurezza di un applicazione
- può essere presente ovunque
  - credenziali di default
  - permettono all'attaccante di accedere a dati o a funzionalità non autorizzate, tuttavia in casi più rari