CWEISANS -D si applica in generale alle strutture di calcolo informatico

graduatoria (liste)

A alcune vaci in comune

OWASP -D si applica al web

CWE -D é alto in graduatoria, ció che é diffuso, frequente e ció che parta un danno (pericoloso) é facile trovore la easy to find, vulnevabile, é facile exploit struttarla e puó avere effetti specifici esempi CWE -416: Use After Free 3) esempio di delcolezza a basso livello CWE-200: Expose of Sensitive Information to an Unauthorized Actor

~D progettazione di un sistema, non tecnologico

### -D 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 Authorication for Critical Function

# 1) SQL Injection

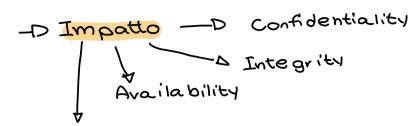
Il problema alla base, sia in questa vulne rabilità che in molte altre, riguarda il mancato controllo dell'input da parte dell'utente. In questa situazione, l'input dell' utente viene divettamente copiato ed utilizzato in una query SQL al database (comandicome 'DROP table x') o anche più samplicemente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

- · Confidentiality: viene persa la confidentialita dei dati sensibili. L'attaccante é in grado di leggere i dati dell'applicazione.
- · Access Control: l'attacconte puó accedere ad altri account serza conoscere la possivard.
- · Integrity: la modifica o concellazione dei dati
- -D Principale soluzione gestive, controllare e pulire l'input prima di inserirlo in una query.

### 2) OS Command Injection

I problema simile al precedente si stuttano applicazioni che richiedono input l'apo vichiede per vichiamave funcioni sul sistema operativo a input per usare un dalla web application. programma

1, obblicasione essone !! w moncato 11 programma - controllo puó a suo programma sul suo OS. one VUOLE!! 4 for ese quive all' vichiede pero un input attaccate



Non-Repudient

- D Poiché é l'applicazione di destinazione che esegue divettamente i comandi anziché l'attaccante, e possibile che qualsiasi attività danno sa provenga dall'app che qualsiasi attività danno sa provenga dall'app o dal proprietario dell'app e venga attribuita ad esso.
- 3) Buffer Overflow —D in C, C++

  D Non controllare la dimensione dell'

  D Non controllare la dimensione dell'

  Input prima di copiarb in un altro

  Copro più memoria

  D Non controllare la dimensione dell'

  Input prima di copiarb in un altro

  di quella disponibile buffer in output può portare a

  winerabilità.

-D Impatto
D Availability -D manda in crash!

Integry

Confidentiality

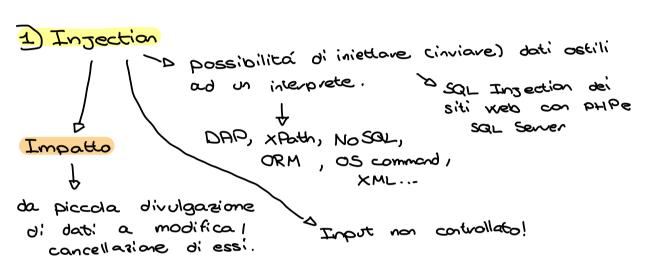
- -D Inserado codice malevolo datro il buffer, é possibile eseguire tale cooice dallo scape del programma.
- 4) Cross-site scripting \_p mancato controllo dell'input
- 1. Dati non sicuri vengono inseriti in una applicazione web, general mente tramite una web request
- 2. La vvelo app genera contenuto non sicuro
- 3. Non viene impedito inserimento di JS
- 4. Visita pagna con script infetto

5. Il web browser della vittima esegue lo script one vitione generato dal web server
-D 3 tipologie oi xSS —D Reflected XSS (or Non-Persistent)  Stored XSS (or Persistent)  DOM - Based XSS
-D Le tecnologie wherabili -D Web Based app
Tintegrity  Availability  Access  Control  DL'attacco XSS più comune riguarda la divulgazione dei racchivolere informazioni anche cookie dell'utente, i quali racchivolere informazioni anche private.  Sfruttare script  Sfruttare script  Sfruttare script  Sil browser per  violare il Controllo degli installare vivus  accessi
5) Missing Authentication for Critical Function DII software non effective
alcune autenticazione per le  alcune autenticazione per le funzionalita one vioniedono  D'Access control l'identita verificata  other de assumere privilegi o assumere l'identita

ai altri

#### -D TOP S OWASP

- 1 Injection
- a Broken Authentication
- 3 Cross-site scripting
- 4) Broken Access Control
- 5 Security Misconfiguration



### a) Broken Authentication

D accesso ad un accent privato da parte dell'attaccente.

bloccare

possibilità

- mancato filtro su attacani automatiszati, che

prevedano il viempimento automatico dei compi

- mancata prevenzione de attacani brute force.

- autenticazione a singolo fortone

#### 3) Cross-Site Scripting

Desfruta vulnerabilità del meb per eseguire script dinamici

- Reflected XSS

Dinserimento nel link oi un sito vulnerabile

- Persistent/Stored

La vittima clicca sul link del sito

El prom ser esegue lo script:

e la tipologia ad impatto più alto, script

menorizzato nel server

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

# 4) Broken Access Control

Verifica one alcuni nascosti siano accessibili suo dominio Solo da utenti autovizzati

L'attaccente, visto come un utente correttomente autenticato accede Specifici url generalmente ad informazioni al difuori del

5) Security Misconfiguration

credenziali di default

D configurazione ervata dei criteri
di sicurezza di un applicazione
può essere
presente orunque

D permettono all'attacconte di accedene a dati o a funcionalité non autorizzate, tuttavia in casi più vavi