SQL INJECTION

NET. REBELS.

NET. REBELS.

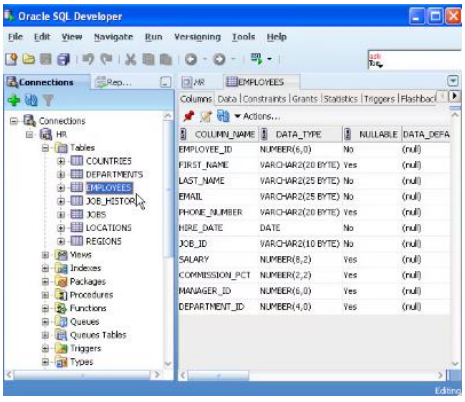
DEFINIZIONE

SQL

SQL (Structured Query Language) è un linguaggio di programmazione specificamente progettato per gestire e manipolare database relazionali. SQL viene utilizzato per eseguire varie operazioni sui dati memorizzati nei database, come ad esempio la creazione, l'aggiornamento, l'eliminazione e il recupero di dati.

Questo linguaggio è diventato lo standard perché fornisce ai programmatori un linguaggio di programmazione flessibile e versatile che offre loro molti modi per personalizzare i sistemi di database.

Ovviamente, i gestori di siti web e app adottano le massime precauzioni di sicurezza nella realizzazione dei codici e delle interfacce di richiesta e query, e anche gli stessi server SQL soddisfano i più elevati standard di sicurezza. Tuttavia, quando si produce il codice sorgente, spesso molto esteso e scritto in un linguaggio di programmazione che generalmente utilizza un testo semplice, è sempre possibile che si verifichino piccoli errori. In genere, queste imprecisioni o errori di script nel codice sorgente non hanno alcun impatto sul funzionamento delle richieste e delle query definite, ma i truffatori informatici possono trovare rapidamente errori nel codice sorgente ed approfittarsene.



NET.
REBELS.

DEFINIZIONE
SLQ INJECTION

Gli attacchi SQL injection sono un tipo di attacco informatico in cui gli hacker mirano a iniettare, o inserire, il proprio codice in un sito web, in un'app o addirittura in un programma. Per cui, quando i criminali informatici trovano piccoli errori di script o imprecisioni nel codice sorgente dei sistemi di database basati su SQL, è come se trovassero una porta aperta perché sono in grado di scoprire vulnerabilità nei programmi, nei siti web e nelle app di aziende, banche o enti governative e di iniettare il proprio codice. Nella maggior parte dei casi, un attacco SQL injection sfrutta una vulnerabilità che può manifestarsi se la connessione tra un'applicazione web e i database è configurata in modo errato.

I codici iniettati in questo punto di connessione possono causare molti danni, come ad esempio bypassare la funzione di accesso e il relativo processo di autenticazione o spiare altri dati. Una volta che gli hacker hanno ottenuto l'accesso a un sistema di database basato su SQL tramite una piccola vulnerabilità, possono anche accedere facilmente ai database in cui sono conservati i dati veramente sensibili. Per fare un esempio, ecco due possibili scenari di come potrebbe iniziare un attacco SQL injection.

NET. REBELS.

PROCEDURE DI ATTACCO

Un attacco SQL injection viene attuato in varie fasi:

Ricognizione:

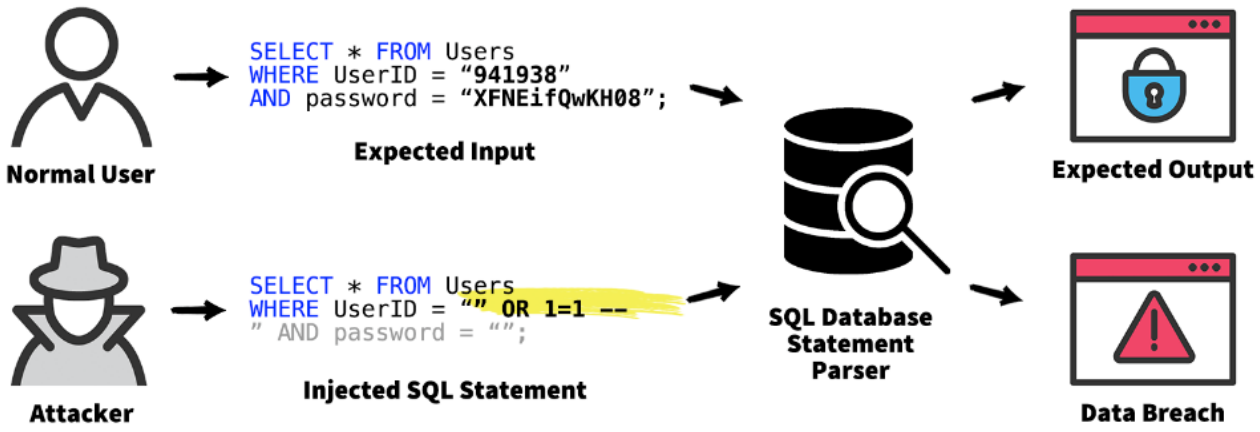
Durante questa prima fase gli aggressori determinano informazioni sui loro obiettivi, punti deboli e vulnerabilità, raccogliendo dati da varie fonti. Conoscere i punti deboli della vittima aiuta gli aggressori a concentrare i propri sforzi per lanciare un attacco efficace più velocemente e con meno sforzo.

Armamento:

Durante questa fase, l'attaccante creerà payload dannosi (malware, script o codice dannoso) progettati per ottenere l'accesso a informazioni sensibili o interrompere le operazioni, puntando a bypassare le misure di sicurezza dell'organizzazione che intendono violare.

Consegna:

Durante le fasi di consegna, gli aggressori possono modificare le funzioni dell'applicazione esistente manipolando l'input dell'utente prima che l'applicazione lato server lo accetti.



Sfruttamento:

Una volta che l'attaccante ha ottenuto l'accesso al sistema di un'azienda, inizierà lo sfruttamento delle risorse. A seconda del tipo di informazioni che hanno ottenuto, possono assumere il controllo di interi database o addirittura di intere reti.

Installazione:

Si verifica dopo che l'attaccante ha consegnato con successo il payload dannoso alla sua destinazione. Durante questa fase, gli aggressori in genere installano backdoor sui sistemi vulnerabili per mantenere l'accesso ed eseguire comandi aggiuntivi senza autorizzazione.

Insabbiamento:

In questa fase, gli aggressori tenteranno probabilmente di coprire le proprie tracce cancellando qualsiasi prova del loro coinvolgimento. Dopo aver completato la loro missione, in genere si disconnetteranno dal punto di accesso remoto e cancelleranno ogni traccia delle loro attività. Gli aggressori possono utilizzare il sistema compromesso come trampolino di lancio per eseguire attacchi DDoS contro altre reti o sistemi o utilizzare il sistema per archiviare dati rubati o ospitare codice dannoso.

NET. REBELS.

COME PREVENIRE
DAGLI ATTACCHI SQL

Per prevenire la SQL Injection, è possibile adottare i seguenti metodi:

- Utilizzare i prepared statements, quando l'infrastruttura lo permette.
- Filtrare ogni singolo input che gli utenti possono inserire.
- Configurare in modo efficace l'user che esegue le query a DB, per limitare eventuali danni.
- Tenere sempre aggiornato il proprio DBMS.
- Tenersi sempre informati sulle nuove tecniche per essere preparati ad affrontare tutti i nuovi attacchi.
- Configurare il proprio sistema dando i giusti privilegi.
- Rispettare le buone norme di programmazione e fare attenta fase di testing.