SQL injection

L’injection SQL è una tecnica di attacco informatico che sfrutta lacune nella gestione dei dati in un’applicazione che interagisce con un database. Gli attaccanti cercano di inserire comandi SQL malevoli nella query per ottenere o modificare dati non autorizzati nel database. Questa è una delle vulnerabilità più comuni e pericolose nelle applicazioni web.

Uno degli attacchi SQL più comuni è l’attacco di tipo SQL injection, basato su UNION.

Con questo tipo di attacco, l’obbiettivo principale è estrarre dati sensibili dal database sfruttando una query SQL vulnerabile.

Esempio

Un’applicazione web che permette agli utenti di cercare prodotti all’interno di un negozio online.

Quando l’utente cerca un prodotto, l’applicazione potrebbe utilizzare una query SQL per recuperare i dati nel database.

Esempio di attacco SQL Injection basato su UNION

Supponiamo che un attaccante voglia estrarre dati dalla tabella ‘users’ all’interno dello stesso database.

Un input malevolo potrebbe essere : https://example.com/search?query=apple' UNION SELECT username, password FROM users—

In questo caso l’attaccante ha aggiunto ‘ UNION SELECT username, password FROM

users - - ‘ alla query di ricerca. Ecco come funziona:

1) L’apostrofo singolo (‘) chiude la stringa della query originale
2) ‘UNION’ consente di unire i risultati di un’altra query alla query principale
3) ‘SELECT username, password FROM users’, potrebbe includere nomi utenti e password dell’applicazione
4) ‘- -‘ è un commento SQL che serve a commentare il resto della query originale

Se l’applicazione è vulnerabile all’SQL injection, l’attaccante otterrà i risultati della query ‘SELECT username, password FROM users‘, che potrebbero includere nomi utenti e password dell'applicazione.

Prevenzione dell'SQL injection:

Per prevenire l'SQL injection bisogna eseguire buone pratiche di sicurezza:

1) Utilizzare librerie o freamwork che consentono di passare i parametri in modo sicuro, evitando la concatenazione diretta delle query
2) Validare e filtrare rigorosamente i dati di ingresso, assicurandosi che soddisfino i criteri previsti
3) Evitare di visualizzare errori SQL dettagliati agli utenti, poiché possono essere sfruttati dagli attaccanti per comprendere la struttura del database
4) Assicurarsi che gli utenti o le applicazioni abbiano solo le autorizzazioni necessarie per accedere ai dati
5) Implementare un sistema di monitoraggio e registrazione delle

attività nel database per rilevare possibili tentativi di attacco.

L’SQl Injection è una minaccia significativa per la sicurezza delle applicazioni web, per questo è fondamentale proteggere le applicazioni implementando pratiche di sviluppo sicure e utilizzando strumenti che aiutino a prevenire questo tipo di attacco.