PROTEGGERSI DAGLI ATTACCHI SQLi

Aggiornare il software di gestione del database. Non esiste un software privo di bug. I criminali informatici possono sfruttare queste vulnerabilità con una SQLi. Per proteggersi è necessario applicare le ultime patch di sicurezza al software di gestione del database.

Applicare il principio del privilegio minimo. Fare in modo che ogni account abbia solo accesso sufficiente per svolgere il proprio lavoro e nient'altro. Ad esempio, un account web che necessita solo dell'accesso in lettura a un determinato database non dovrebbe avere la capacità di scrivere, modificare o cambiare i dati in alcun modo.

Assumere sviluppatori competenti ed esperti. Gli attacchi SQLi derivano spesso da una codifica superficiale. È meglio far sapere in anticipo agli sviluppatori di software cosa ci si aspetta per quanto riguarda la sicurezza.

Visitare OWASP. L'Open Web Application Security Project, abbreviato OWASP, è l'autorità principale sulle applicazioni web e ha molte letture aggiuntive su come prevenire le SQL injection.

UNA STORIA MODERNA

Gli attacchi SQL injection non devono essere sottovalutati, è stato il metodo alla base della gigantesca violazione TalkTalk del 2015, che ha portato al furto di oltre 150.000 informazioni personali dei clienti e a una multa di 400.000 sterline per l'azienda.

Nel 2012, un gruppo ha anche utilizzato attacchi SQL injection per rubare 450.000 dati di login degli utenti Yahoo, in una delle numerose violazioni che avrebbero colpito la società web negli anni successivi.

Secondo un recente rapporto della società di sicurezza web Akamai, gli attacchi SQL injection hanno rappresentato oltre il 65% degli attacchi basati sul web tra novembre 2017 e marzo 2019, con gli Stati Uniti e il Regno Unito in cima alle classifiche come i paesi più frequentemente bersagliati.

CHI È A RISCHIO DI UN ATTACCO SQLi E COSA PUÒ ACCADERE ALLE VITTIME?

Per essere a rischio di subire un attacco SQLi, basta che un'organizzazione abbia due semplici prerequisiti: avere un sito web e far interagire quel sito web con un database SQL.

Gli effetti di una SQL injection ben riuscita possono includere:

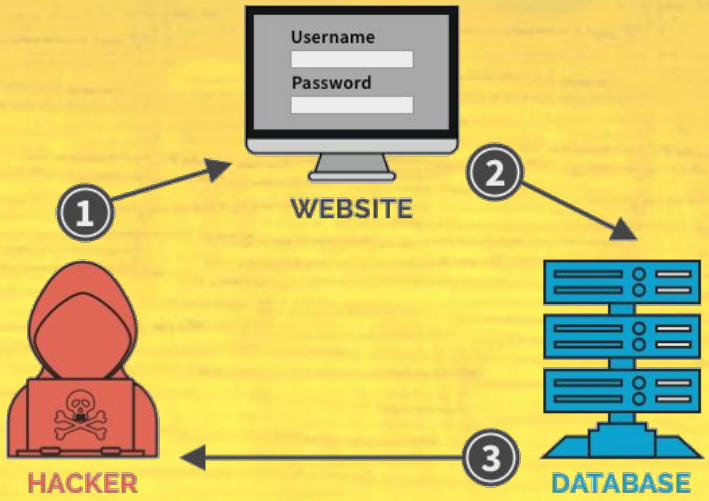
- clonazione (completa o parziale) dell'intero database a favore dell'attaccante;
- un utente malintenzionato che falsifica le credenziali di accesso, si spaccia per un utente lecito o addirittura aggira completamente l'autenticazione;
- modifica del database (aggiunta, rimozione o modifica di particolari dati);
- esecuzione di comandi del sistema operativo che consentono a un utente malintenzionato di accedere ad altre risorse sulla rete che ospita il database SQL;
- mettere offline l'applicazione web di destinazione.

Questi risultati diretti di un attacco SQLi di successo sono di per sé problemi abbastanza grandi, ma non sono l'unica cosa da considerare: c'è anche una ricaduta a lungo termine. Vendita di dati riservati, perdita di clienti, costi di ripristino, erosione della fiducia e altro ancora possono essere il risultato di un attacco SQLi riuscito.

RIFERIMENTI

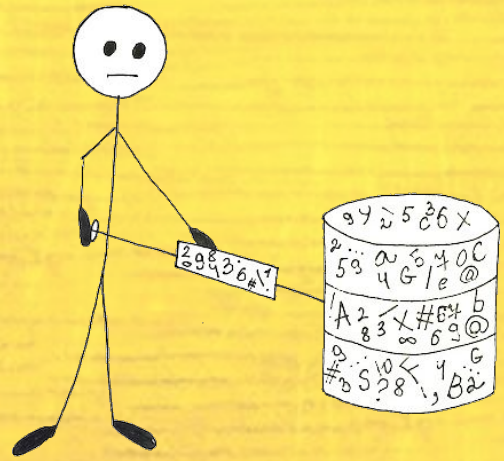
➢ http://www.c3t.it/projects/awareness/articoli&brochure/sql_inj/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)



SQL INJECTION

Scopri cos'è un attacco del tipo SQL Injection e preparati a prevenirlo.



Poche cose terrorizzano i professionisti della sicurezza IT (*Information technology*) - e le organizzazioni che proteggono - quanto il **furto di dati**. In un solo momento, i dati privati di un'azienda, dei clienti, gli ID dei dipendenti e una miriade di altri tipi di dati riservati possono essere prelevati dai server interni. Ancora un momento, e quei dati saranno disponibili per la vendita al miglior offerente.

Uno dei metodi più comuni per rubare dati sensibili è la **SQL injection (SQLi)**, che prende di mira le vulnerabilità di sicurezza nelle applicazioni web per iniettare un'istruzione SQL dannosa nel database che archivia le informazioni.

I database SQL archiviano informazioni critiche e, nonostante ciò, **molti siti web rimangono vulnerabili agli attacchi SQLi** che rimangono il rischio più critico per la sicurezza delle applicazioni web.

Un attacco SQLi funziona, almeno in superficie, in modo molto semplice: un utente malintenzionato **immette un'istruzione SQL dannosa in un campo compilabile** di una pagina web (come ad esempio nelle caselle di testo per inserire username e password nelle pagine di login); questa istruzione sfrutta una vulnerabilità nell'implementazione dell'applicazione web.

In caso di esito positivo, l'istruzione "iniettata" potrebbe eseguire il salvataggio dell'intero contenuto di un database o comunque selezionare particolari dati sensibili.

Un'iniezione SQL può anche fornire l'accesso come amministratore a un database, consentendo al criminale di eliminare o modificare i dati.

Peggio ancora, un attacco SQLi potrebbe persino fornire l'accesso al sistema operativo della macchina che lo ospita, il che consentirebbe all'autore dell'attacco di accedere ad altre risorse di rete.

Che cos'è un'istruzione SQL? → SQL sta per *Structured Query Language* ed è un linguaggio di programmazione standardizzato per la gestione dei database. Ogni volta che si usufruisce di un servizio web è molto probabile che (direttamente o indirettamente) si abbia a che fare con un database. In questi casi, il linguaggio SQL è usato per interrogare la base di dati mediante l'utilizzo di istruzioni denominate **query**.

Si pensi ad un database come una grossa tabella che memorizza informazioni di vario genere. Es. tabella di persone:

Persone

ID	Nome	Cognome	Età
0	Mario	Rossi	18
1	Luca	Verdi	24
2	Marco	Neri	21
:	:	:	:

Un esempio di istruzione SQL per "interrogare" il database ed ottenere le informazioni richieste potrebbe essere la seguente.

```
SELECT Nome, Cognome FROM Persone WHERE Età >= 20 AND Età < 25
```

Il risultato di tale istruzione è l'estrapolazione dalla base di dati dei campi "Nome" e "Cognome" di tutti quei **record** (righe della tabella) in cui il campo "Età" è compreso tra 20 (incluso) e 25 (escluso).

Quando un utente, tramite un sito web, deve accedere alle informazioni di un database, il linguaggio SQL viene utilizzato dall'applicazione web per accedere e presentare tali dati all'utente.

"Un criminale informatico può manipolare le query del database in modo tale che una richiesta di informazioni su un paio di calzini restituisca il numero della carta di credito per uno sfortunato cliente."