Report Rilevamento Attacchi

Utente: Banana

TITOLO: SQL Injection

CATEGORIA: Attacchi alle applicazioni web e ai database

ESITO:

Possibile attacco di tipo 'SQL Injection' rilevato.

DESCRIZIONE:

L’SQL Injection è una tecnica d’attacco che sfrutta vulnerabilità nei campi di input delle applicazioni web per inserire comandi SQL malevoli. Questi comandi vengono poi eseguiti direttamente dal database, permettendo all’attaccante di leggere, modificare o cancellare informazioni riservate. Modalità di esecuzione: L’attaccante identifica un campo non correttamente protetto (ad esempio, un form di login o una barra di ricerca). Inserisce un frammento di codice SQL manipolato (es. OR '1'='1') al posto dell’input previsto. Se il sistema non valida correttamente l’input, il database esegue il comando come se fosse legittimo. In casi più avanzati, l’attaccante può ottenere l’accesso completo al database e ai dati memorizzati. Possibili conseguenze: - Esfiltrazione di dati sensibili (es. dati personali, password, carte di credito). - Cancellazione o alterazione di informazioni nei database. - Possibile compromissione di server e altri sistemi collegati. - Grave danno reputazionale e legale per le aziende colpite.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: - Validare e filtrare ogni input dell’utente in modo rigoroso. - Utilizzare query parametriche o stored procedures, che separano i dati dal codice. - Evitare di mostrare messaggi di errore dettagliati che rivelano la struttura del database. - Eseguire test di sicurezza regolari (penetration test) sulle proprie applicazioni.

Risposte Sì: 3 / 4