SQL Injection (SQLi)

SQL Injection je typ kybernetického útoku, který zneužívá nedostatečné ošetření uživatelských vstupů předtím, než jsou použity v SQL dotazu. Místo toho, aby aplikace brala vstup jako prostý text (např. jméno uživatele), interpretuje jej jako součást příkazu pro databázi.

Jak útok probíhá?

Představte si přihlašovací formulář. Aplikace na pozadí vytvoří dotaz typu: `SELECT * FROM uzivatele WHERE jmeno = '$uzivatel' AND heslo = '$heslo';`

Legitimní pokus:

Uživatel zadá jméno `admin` a heslo `mojeheslo123`. Výsledek: Databáze hledá shodu a pokud existuje, uživatele přihlásí.

Útok (Obejití hesla):

Útočník do pole pro jméno zadá: `admin' –` Znaky – v SQL znamenají komentář (vše za nimi je ignorováno).

Výsledný dotaz bude vypadat takto: `SELECT * FROM uzivatele WHERE jmeno = 'admin' – ' AND heslo = '…';`

Databáze nyní vidí pouze příkaz „najdi uživatele admin“ a zbytek dotazu (včetně kontroly hesla) ignoruje. Útočník je přihlášen jako správce bez znalosti hesla.

Hlavní typy SQL Injection

- **In-band (Classic):** Útočník vidí výsledky útoku přímo na webové stránce (např. vypsaná data z jiné tabulky).
- **Inferential (Blind SQLi):** Stránka nezobrazuje data, ale útočník sleduje odpovědi (např. zda se stránka načetla, nebo skončila chybou).
    - **Boolean-based:** Útočník klade otázky typu PRAVDA/NEPRAVDA.
    - **Time-based:** Útočník donutí databázi čekat 10 sekund, pokud je první písmeno hesla 'A'. Pokud stránka tuhne, ví, že trefil správné písmeno.
- **Out-of-band:** Útočník donutí databázi odeslat data na svůj externí server (např. pomocí DNS požadavku).

Důsledky útoku

- **Únik dat:** Masové stahování osobních údajů (e-maily, adresy, hashovaná hesla).
- **Ztráta integrity:** Útočník může změnit ceny v e-shopu, smazat dluhy nebo vytvořit falešné faktury.
- **Úplná ztráta dat:** Pomocí příkazu `DROP TABLE` může útočník smazat celé tabulky.
- **Přístup k OS:** V některých konfiguracích může SQLi vést až k Command Injection na úrovni operačního systému.

Jak se bránit?

Dnešní technologie nabízejí spolehlivé způsoby obrany:

```
1. **Prepared Statements (Parametrizované dotazy):** Nejdůležitější obrana. Data jsou od příkazu oddělena. Databáze předem ví, co je příkaz, a uživatelský vstup bere vždy jen jako text, nikdy jako kód.
2. **Validace vstupu:** Povolení pouze očekávaných formátů (např. pole pro věk musí obsahovat jen čísla).
3. **Princip nejnižších privilegií:** Databázový účet, který používá webová stránka, by neměl mít právo mazat tabulky nebo přistupovat k systémovým tabulkám.
4. **WAF (Web Application Firewall):** Filtr, který dokáže rozpoznat a zablokovat známé vzory SQL útoků dříve, než dorazí k aplikaci.
```

Související pojmy: Command Injection, Databáze, PHP, Kybernetická bezpečnost, WAF, Šifrování.