MI-SP-SP-4 (MI-BPR.16)

Bezpečnost databází. Útoky typu SQL Injection a obrana proti nim.

- veškerý vstup musí být prověřen
- pokud dodržujeme běh za nejmenších oprávnění, můžeme problémům částečně předejít
  - → ne ale úplně (information disclosure - SELECT)
  - ji běžně sanitizovat vstupy

- mysql_query a mysqli::query umožňují pouze jeden query, pořád se ale dají obejít

```
DELETE FROM x WHERE jmeno = '|' OR '1' = '1|';
```

! – o nedávat větší oprávnění než třeba
  - o důsledná kontrola vstupů – pozor hlavně na apostrofy
    - mysql_real_escape_string – PHP funkce pro escapování stringu
  - o používání placeholderů (prepared statements)
    - na místech parametrů placeholdery, které se přepíší skutečnou DB systému
    - mysql_real_escape_string není potřeba

  + získáváme lepší efektivitu u opakovaně vykonávaných query

  - data v placeholdech může nakonec i databázový systém (DB procedury)
    [QUOTENAME – bezpečné escapování]

Specializované nástroje

SQL firewall – detekce pokusů o injection
- může vyžadovat seznam povolených struktur

Nástroje testování zranitelnosti
- [sqlmap]