# Uživatele

## Databázová bezpečnost teorie

### Rozlišení práv

*Co není povoleno, je zakázáno*

* Přiřadit mu práva pro celý server
* Přiřadit mu práva pro jednu nebo více databází (z mnoha existujících)
* Přiřadit mu práva pro jednu nebo více tabulek v databázi (z mnoha existujících)
* Přiřadit mu práva pro jeden sloupec v tabulce
* Přiřadit mu práva vytvářet a používat **pohledy** (jen MySQL 5.x)
* Přiřadit mu práva vytvářet, měnit nebo spouštět uložené **procedury** (jen MySQL 5.x)
* Prohlížet (používat SELECT)
* Vkládat (používat INSERT)
* Upravovat (používat UPDATE)
* Odstraňovat (používat DELETE)
* …

Zvláštní práva:

* Měnit práva uživatelů
* Nastavovat systém

## Tabulky nad databázi MySQL

* **user**
* **db**
* **host**
* **func**
* **columns\_priv**
* **tables\_priv**

### tabulka user

V databázi mysql v tabulce **user** jsou uložena oprávnění pro uživatele, která platí na **úrovni celé databáze**, proto dávejte pozor, co zde komu dovolíte.

* **host** - IP adresa, nebo název počítače, odkud se uživatel může připojit, pokud je vám to jedno, použijte znak **%** jako zástupný symbol pro cokoliv.
* **User** - Jméno uživatele.
* **Password** - Heslo zahashované funkcí PASSWORD().
* Následující položky můžou nabývat hodnot **Y** a **N**, jako výchozí hodnota je nastaveno **N**.
* **Select\_priv** - Vypisování řádků z tabulky.
* **Insert\_priv** - Vkládání řádků do tabulky.
* **Update\_priv** - Update řádků v tabulce.
* **Delete\_priv** - Odstraňování řádků z tabulky.
* **Create\_priv**- Vytváření databází a tabulek.
* **Drop\_priv**- Mazání databází a tabulek.
* **Reload\_priv**- Znovunačtení tabulky přístupových oprávnění.
* **Shutdown\_priv**- Vypínaní serveru.
* **Process\_priv**- Prohlížení informací o vláknech serveru
* **File\_priv**- Přístup k souborům na serveru, číst můžete jen soubory čitelné všemi a vytvářet jen nové soubory tzn. že nemůžete přepsat existující soubor.
* **Grant\_priv**- Udělovaní oprávnění jiným účtům.
* **References\_priv**- Rezervováno pro budoucí použití.
* **Index\_priv**- Vytváření/odstraňování indexů.
* **Alter\_priv**- Změny struktury tabulky.
* **Show\_db\_priv**- Zobrazovat informace o databázích *(SHOW DATABASES)*
* **Super\_priv**- Superuživatelské operace, práce s vlákny apd...
* **Create\_tmp\_table\_priv**- Vytváření dočasných tabulek
* **Execute\_priv**- Spouštění uživatelských procedur *(zatím se nepoužívá, kdyžtak mě opravte ;-)*
* **Lock\_tables\_priv** - Povolí nastavení zámku proti čtení/zápisu.
* **Pár dalších** (dle verze) - další položky, ale ty se nevztahují k přímo k přístupovým právům.

### Tabulka DB

Zde jsou uložena oprávnění k jednotlivým databázím.

### Tabulka tables\_priv

Práva pro jednotlivé tabulky.

### Tabulka columns\_priv

Práva pro jednotlivé sloupce tabulek.

## Různá oprávnění

Zzde je malý výpis oprávnění, která můžete použít

* **ADMINISTRATORSKA**
  + ALL PRIVILEGES- jak jsme předvedli výše – MySQL uživatel má přístup do všech databází  (kromě systémových databází)
  + GRANT OPTION- povolí uživateli přiřazovat, nebo odstraňovat oprávnění
* UŽIVATELSKÁ
  + CREATE TEMPORARY TABLES – Vytvářet dočasné tabulky
  + FILE - Práce se soubory na serveru
  + LOCK TABLES - Povoluje explicitní použití příkazu LOCK TABLES
  + PROCESS - Získávání informací o vláknech.
  + RELOAD - Znovunačítání přístupových oprávnění apd.
  + SHOW DATABASES - Povoluje prohlížet si všechny databáze.
  + SHUTDOWN - Ukončovat práci serveru
  + SUPER – Ukončovat vlákna

Právo Vztahuje se na Popis

SELECT tabulky, sloupce Povoluje vybírat záznamy z tabulek.

INSERT tabulky, sloupce Povoluje vkládat nové řádky do tabulky.

UPDATE tabulky, sloupce Povoluje obnovovat hodnoty záznamů v tabulkách.

DELETE Tabulky Povoluje odstraňovat záznamy (řádky) z tabulek.

INDEX Tabulky Povoluje vytvářet a odstraňovat indexy z tabulek.

ALTER Tabulky Povoluje měnit strukturu stávajících tabulek

(přejmenovávat nebo přidávat sloupce, měnit datové typy sloupců).

CREATE databáze, tabulky Povoluje vytvářet nové databáze a tabulky.

DROP databáze, tabulky Povoluje odstranit databáze a tabulky.

## Prohlídnout uživatelé a práva

### Uživatelé

### Oprávnění GRANT

show grants;

## Vytvořit uživatele

Co měnit a neměnit

### Uživatel pod local host

CREATE USER

## Přiřadit práva GRANT

### GRANT syntaxe

GRANT práva [sloupce]

ON položka\_kde

TO uživatel [IDENTIFIED BY 'heslo' ]

[REQUIRE volby\_ssl]

[WITH [GRANT OPTION | volby\_omezení] ]

**Pro připomenutí:**

* **ALL** - Může všechno.
* **ALTER** - Měnit strukturu tabulky.
* **CREATE** - Vytvářet tabulky a databáze.
* **DELETE** - Mazat záznamy z tabulek.
* **DROP** - Mazat tabulky a databáze.
* **FILE** - Práce se soubory na serveru.
* **INDEX** - Vytvářet a odstraňovat indexy.
* **INSERT** - Vkládat řádky do tabulek.
* **PROCESS** - Získávání informací o vláknech.
* **REFERENCES** - Nepoužívá se.
* **RELOAD** - Znovunačítání přístupových oprávnění apd.
* **SELECT**- Vybírat záznamy z tabulek.
* **SHUTDOWN** - Ukončovat práci serveru.
* **UPDATE**- Aktualizování řádků v tabulce.
* **USAGE**- Nemá žádná oprávnění.

### Přidat jim práva –prakticky

GRANT ALL PRIVILEGES ON jmeno\_databaze.\* TO 'uzivatel'@'localhost'

## Změnit práva uživatele

Nejrychlejší smazat a vytvořit znova

ALTER USER

## Smazat uživatele

DROP USER ‘uživatel’@‘localhost’;

## Obnovení

FLUSH PRIVILEGES;