

Użytkownicy, uprawnienia i role

Czas: 2 × 45 min

praca indywidualna

Cel: Nauczenie się tworzenia kont z minimalnymi niezbędnymi uprawnieniami, nadawania i odbierania uprawnień oraz sprawdzania ich działania przez logowanie się na ograniczone konto.

Po zajęciach potrafisz:

- tworzy konta użytkowników z określonym hostem i hasłem
- nadaje i odbiera uprawnienia na poziomie bazy, tabeli i kolumny
- sprawdza uprawnienia poleceniem `SHOW GRANTS` i testem logowania
- tworzy rolę, przypisuje ją użytkownikowi i aktywuje
- zmienia hasło konta root w XAMPP i dostosowuje konfigurację phpMyAdmin

Sprzęt i materiały

- komputer z XAMPP (MariaDB 10.4) lub MySQL 8.4
- baza `sklep` zaimportowana z pliku `sklep.sql` (folder Pliki_do_zadan)

Oprogramowanie

- **XAMPP (Apache + MariaDB + phpMyAdmin)** — phpMyAdmin → zakładka Konta użytkowników apachefriends.org
- **Konsola mysql** — dwa okna: jedno jako root, drugie jako testowany użytkownik
- **Edytor tekstu (VS Code lub Notatnik)** — plik `zad27.sql` oraz edycja `config.inc.php` code.visualstudio.com

Przygotowanie przed zajęciami

- Przypomnij sobie strukturę bazy `sklep` (tabele i kolumny tabeli `pracownicy`).
- Sprawdź, jak otworzyć drugie okno konsoli: w panelu XAMPP przycisk Shell (otwiera się w folderze `C:\xampp`), polecenie `mysql -u nazwa -p`.

Bezpieczeństwo

- Hasła w zadaniu są przykładowe i służą tylko do ćwiczeń — w prawdziwych systemach używaj długich, unikalnych haseł i nie zapisuj ich w sprawozdaniu ani na zrzutach ekranu.
- Krok 5 (hasło root) wykonuj tylko za zgodą nauczyciela. Zapisz nowe hasło na kartce na czas zajęć — bez niego nie zalogujesz się do serwera. Na koniec przywróć stan wyjściowy zgodnie z poleceniem nauczyciela, bo z komputera korzystają inne klasy.
- Nie nadawaj kontom uprawnień `ALL PRIVILEGES ON *.*` ani `WITH GRANT OPTION` — zasada najmniejszych uprawnień.
- Nie usuwaj kont `root`, `pma` ani kont systemowych (np. `mariadb.sys`). Usuwać tylko konta utworzone przez siebie.

Przebieg zadania

1 Konta na serwerze

Konto w MariaDB/MySQL to para nazwa@host. 'jan'@'localhost' i 'jan'@'%' to dwa różne konta.

1. Z1. Jako root wyświetl listę kont (`SELECT user, host FROM mysql.user;`), swoje bieżące konto (`SELECT CURRENT_USER();`) i swoje uprawnienia (`SHOW GRANTS;`). Zapisz, jakie konta root istnieją i z jakich hostów.
2. Z2. Utwórz konto `sprzedawca`, które może logować się tylko z tego komputera, z hasłem `Sprzed#2026`. Nadaj mu prawo odczytu wszystkich tabel bazy `sklep` (poziom bazy). Wyświetl jego uprawnienia poleceniem `SHOW GRANTS FOR`.
3. Z3. W drugim oknie zaloguj się jako `sprzedawca` (`mysql -u sprzedawca -p sklep`). Wykonaj `SELECT COUNT(*) FROM produkty;`, a potem spróbuj zmienić cenę dowolnego produktu. Zapisz numer i treść błędu. Spróbuj też zalogować się z błędnym hasłem i zapisz kod błędu.

2 Uprawnienia na poziomie tabeli i kolumny

1. Z4. Utwórz konto `magazynier@localhost` (hasło `Magaz#2026`), które może tylko odczytywać i zmieniać dane w tabeli `produkty` (`SELECT`, `UPDATE` na jednej tabeli).
2. Z5. Zaloguj się jako `magazynier` i sprawdź: `SHOW TABLES;` (ile tabel widzi?), zmianę stanu magazynowego produktu nr 7 o +5 sztuk, odczyt tabeli `klienci` i usunięcie produktu (`DELETE` z warunkiem na nieistniejący numer, np. 999). Zapisz, co się udało, a co zakończyło się błędem.
3. Z6. Utwórz konto `recepcja@localhost` (hasło `Recep#2026`), które w tabeli `pracownicy` może odczytać tylko kolumny `imie`, `nazwisko` i `stanowisko` (uprawnienie na poziomie kolumn).
4. Z7. Zaloguj się jako `recepcja` i wykonaj kolejno: `SELECT` dozwolonych kolumn, `SELECT * FROM pracownicy;` oraz `SELECT` kolumny `pensja`. Zapisz kody błędów i wyjaśnij, dlaczego `SELECT *` też jest zabroniony.
5. Z8. Rozszerz uprawnienia konta `sprzedawca` o dodawanie wierszy do tabel `zamowienia` i `pozycje_zamowienia` (dwa polecenia `GRANT` na poziomie tabeli). Sprawdź `SHOW GRANTS FOR`.

3 Odbieranie uprawnień i zmiana hasła

1. Z9. Odbierz kontu `magazynier` prawo `UPDATE` do tabeli `produkty`. Sprawdź `SHOW GRANTS FOR`, zaloguj się ponownie i spróbuj zmienić stan produktu — zapisz wynik.
2. Z10. Zmień hasło konta `sprzedawca` na `Nowe#Haslo2026` (`ALTER USER`). Sprawdź logowanie starym i nowym hasłem.

4 Role

Rola to nazwany zestaw uprawnień, który przypisuje się wielu użytkownikom. Rola przypisana użytkownikowi musi być aktywna — inaczej jej uprawnienia nie działają. Składnia roli domyślnej różni się w MariaDB i MySQL.

```
-- aktywacja roli w bieżącej sesji (MariaDB i MySQL):
SET ROLE nazwa_rol;
SELECT CURRENT_ROLE();

-- rola domyślna (aktywna od zalogowania):
SET DEFAULT ROLE nazwa_rol FOR 'uzytkownik'@'localhost'; -- MariaDB (XAMPP)
SET DEFAULT ROLE nazwa_rol TO 'uzytkownik'@'localhost'; -- MySQL 8.4
```

1. Z11. Utwórz rolę `odczyt_sklep` z prawem SELECT do całej bazy `sklep`. Utwórz konto `stazysta@localhost` (hasło `Staz#2026`) i przypisz mu tę rolę.
2. Z12. Zaloguj się jako `stazysta` (bez podawania bazy: `mysql -u stazysta -p`). Sprawdź `SELECT CURRENT_ROLE();` i spróbuj odczytać `SELECT COUNT(*) FROM sklep.klienci;`. Następnie aktywuj rolę poleceniem SET ROLE i powtórz zapytanie. Zapisz oba wyniki.
3. Z13. Jako root ustaw rolę `odczyt_sklep` jako domyślną dla konta `stazysta` (składnia właściwa dla Twojego serwera), zaloguj się ponownie i sprawdź `CURRENT_ROLE()`.

5 Hasło root w XAMPP i porządki

W XAMPP konto root nie ma hasła, a phpMyAdmin loguje się automatycznie danymi zapisanymi w pliku `C:\xampp\phpMyAdmin\config.inc.php`. Wykonaj ten krok tylko za zgodą nauczyciela.

```
/* fragment C:\xampp\phpMyAdmin\config.inc.php */
$config['Servers'][$i]['auth_type'] = 'config';
$config['Servers'][$i]['user'] = 'root';
$config['Servers'][$i]['password'] = '';
```

1. Z14. Ustaw hasło dla konta `root@localhost` (ALTER USER). Odśwież phpMyAdmin i zapisz komunikat błędu. Zrób kopię pliku `config.inc.php`, a następnie zmień w nim `auth_type` z `config` na `cookie` (phpMyAdmin zacznie pytać o login i hasło). Zaloguj się jako root i jako `sprzedawca` — porównaj, co widzi każde konto. Wyjaśnij, dlaczego `cookie` jest bezpieczniejsze niż wpisanie hasła w pliku.
2. Z15. Porządki: usuń konta `sprzedawca`, `magazynier`, `repcja`, `stazysta` i rolę `odczyt_sklep`. Sprawdź listę kont. Jeśli nauczyciel tak zdecyduje, przywróć puste hasło root i oryginalny plik `config.inc.php` z kopii.
3. Zapisz plik `zad27.sql` z poleceniami (bez haseł z kroku 5) i zrzuty ekranu: SHOW GRANTS z Z2, Z6 i Z8, błędy z Z3, Z5, Z7, wynik Z12 przed i po SET ROLE oraz okno logowania phpMyAdmin.

W sprawozdaniu umieść

- ☐ tabela poleceń Z1–Z15 z treścią SQL i wynikiem
- ☐ tabela testów uprawnień: konto, operacja, oczekiwany wynik, faktyczny wynik / kod błędu
- ☐ zrzuty ekranu SHOW GRANTS (Z2, Z6, Z8), błędów (Z3, Z5, Z7) i ról (Z12)
- ☐ opis zmian w `config.inc.php` i porównanie `auth_type` config i cookie
- ☐ plik `zad27.sql`
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różnią się konta `'jan'@'localhost'` i `'jan'@'%'`? Które jest bezpieczniejsze dla aplikacji działającej na tym samym serwerze?

2. Co oznaczają kody błędów 1044, 1045, 1142 i 1143?
3. Na czym polega zasada najmniejszych uprawnień? Podaj przykład z tego zadania.
4. Dlaczego po przypisaniu roli użytkownik nadal mógł nie mieć dostępu do danych i jak to naprawić na stałe?
5. Jakie ryzyko niesie puste hasło root w XAMPP i kiedy jest ono szczególnie groźne?

Kryteria oceny

Kryterium	Punkty
Z1–Z3: konto z uprawnieniami na poziomie bazy i test logowania	3
Z4–Z8: uprawnienia na poziomie tabeli i kolumny z testami	5
Z9–Z10: REVOKE i zmiana hasła	2
Z11–Z13: role (utworzenie, aktywacja, rola domyślna)	3
Z14–Z15: hasło root, config.inc.php, porządki	3
Dokumentacja: tabela testów, zrzuty, plik .sql	2
Odpowiedzi na pytania kontrolne	2
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).