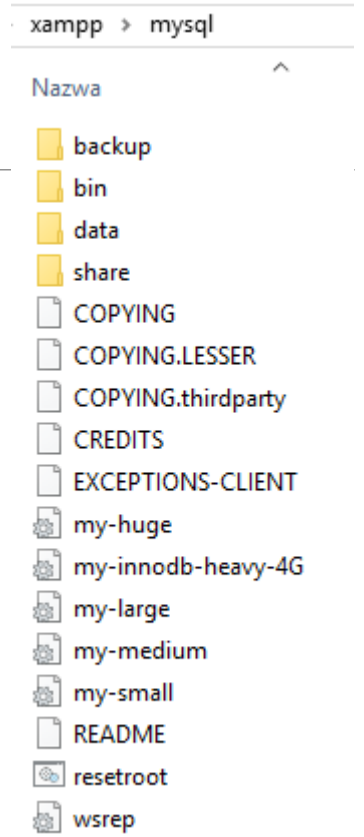
Administrowanie serwerami baz danych

ZADANIA ADMINISTRATORA BAZ DANYCH

Konfigurowanie serwera

Domyślnym folderem instalacyjnym serwera MySQL jest …XAMPP\MySQL\....

Istotne z punktu widzenia administratora mogą być foldery:
bin — serwer MySQL, programy użytkowe;
data — bazy danych, pliki dzienników;
examples — przykładowe programy i skrypty;
include — pliki nagłówkowe;
lib — biblioteki;
scripts — skrypty użytkowe;
share — pliki błędów, zestawy znaków.



Uruchamianie serwera

Uruchamianie i zatrzymanie serwera w systemie Windows można wykonać za pomocą systemowych narzędzi administracyjnych przez zatrzymanie lub uruchomienie usługi.

Można go również uruchomić lub zatrzymać, wpisując w wierszu poleceń jedną z poniższych komend:
NET START mysql, NET STOP mysql

Logowanie do programu (z wiersza poleceń)**:**
mysql –u root –h localhost –p

- parametr **-u** określa konto, na które chcemy się zalogować;
- parametr **-h** określa komputer, na którym pracuje serwer baz danych;
- parametr **-p** określa uwierzytelnienie za pomocą hasła.

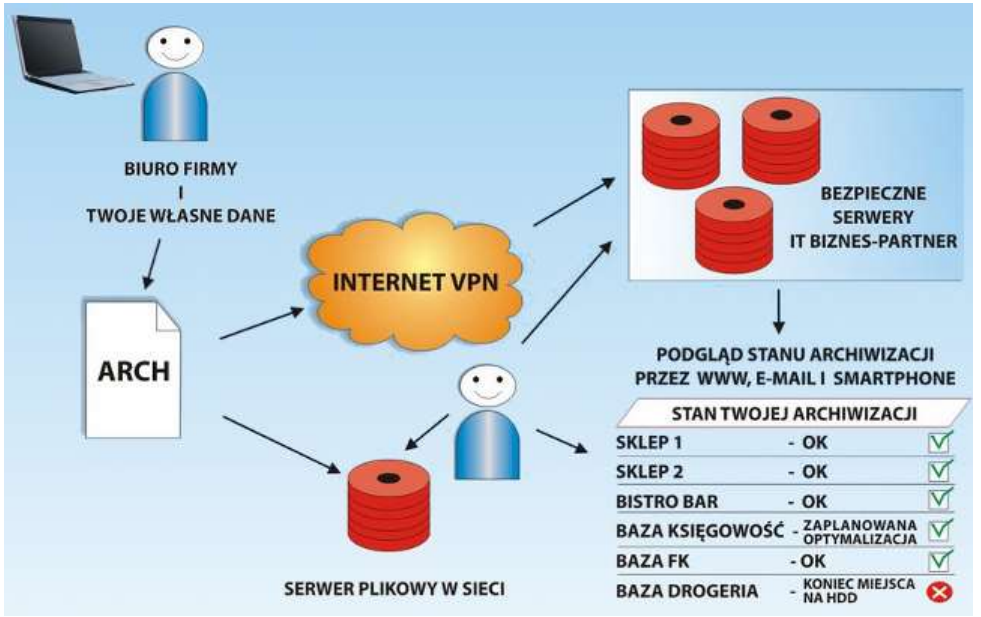
W wyniku wykonania podanego wyżej polecenia zostaniemy zalogowani do serwera jako użytkownik **root**.

Zadania administratora baz danych

Podstawowym celem działań administratora baz danych powinno być zapewnienie niezawodności i bezawaryjnego działania systemu. Wiąże się to z zarządzaniem dostępem użytkowników do baz danych, zabezpieczeniem przed częściową lub całkowitą utratą danych oraz monitorowaniem pracy serwera baz danych.

Bezpieczeństwo danych to:

- uwierzytelnienie użytkownika,
- autoryzacja użytkownika,
- zarządzanie dostępem do baz danych,
- replikacja bazy danych,
- tworzenie kopii zapasowych.



Administrowanie bazami danych na poziomie użytkownika

Administrowanie bazami danych na poziomie użytkownika to:

- dodawanie nowego konta z różnymi uprawnieniami,
- usuwanie konta,
- wprowadzanie ograniczeń i nadawanie przywilejów dla konta,
- zarządzanie bazą danych przez definiowanie ról,
- dołączanie lub odłączanie baz danych,
- zakładanie baz danych,
- konserwacja i aktualizacja baz danych,
- monitorowanie bieżącego działania baz danych.

Uwierzytelnianie użytkownika

Domyślnie tylko administratorzy komputera mają pełny dostęp do serwera SQL.

Uwierzytelnianie to jednoznaczna weryfikacja tożsamości danego użytkownika np. za pomocą hasła czy bardziej zaawansowanych metod takich jak dowód z wiedzą zerową.

Aby połączyć się z serwerem, użytkownik musi potwierdzić swoją tożsamość, podając login i hasłoczyli przejść przez proces uwierzytelnienia użytkownika.

Podczas uwierzytelniania wykorzystuje się trzy czynniki:

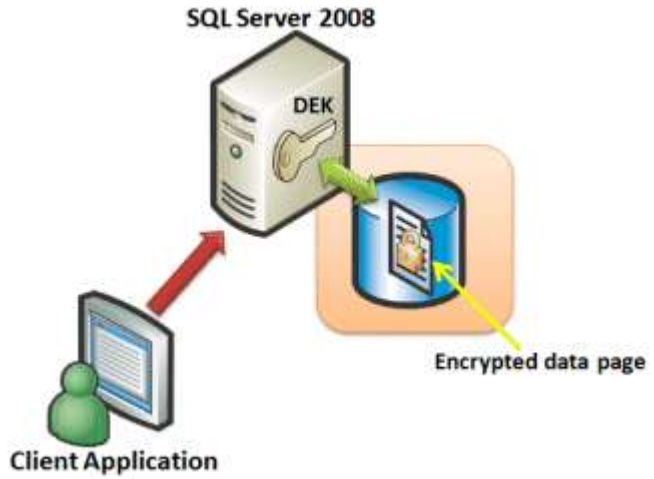
- wiedza – coś co wiesz – hasło, odpowiedź na ustalone pytanie;
- posiadanie – coś co masz – sprawdza się czy użytkownik jest w posiadaniu wybranego przedmiotu np. tokena generującego kody jednorazowe, klucza;
- obecność – zwykle stosowane są metody biometryczne takie jak rozpoznawanie odcisku palca, tęczówki oka, głosu, układu naczyń krwionośnych.

Autoryzacja

Autoryzacja polega na sprawdzaniu, czy dana operacja dla danego użytkownika jest dozwolona. Autoryzacja ma miejsce po pomyślnym uwierzytelnieniu.

Jeżeli użytkownik zalogowany do bazy danych próbuje wykonać jakąkolwiek operację (na przykład odczytanie lub modyfikowanie danych), serwer sprawdza, czy ma on wystarczające uprawnienia do wykonania tej operacji.

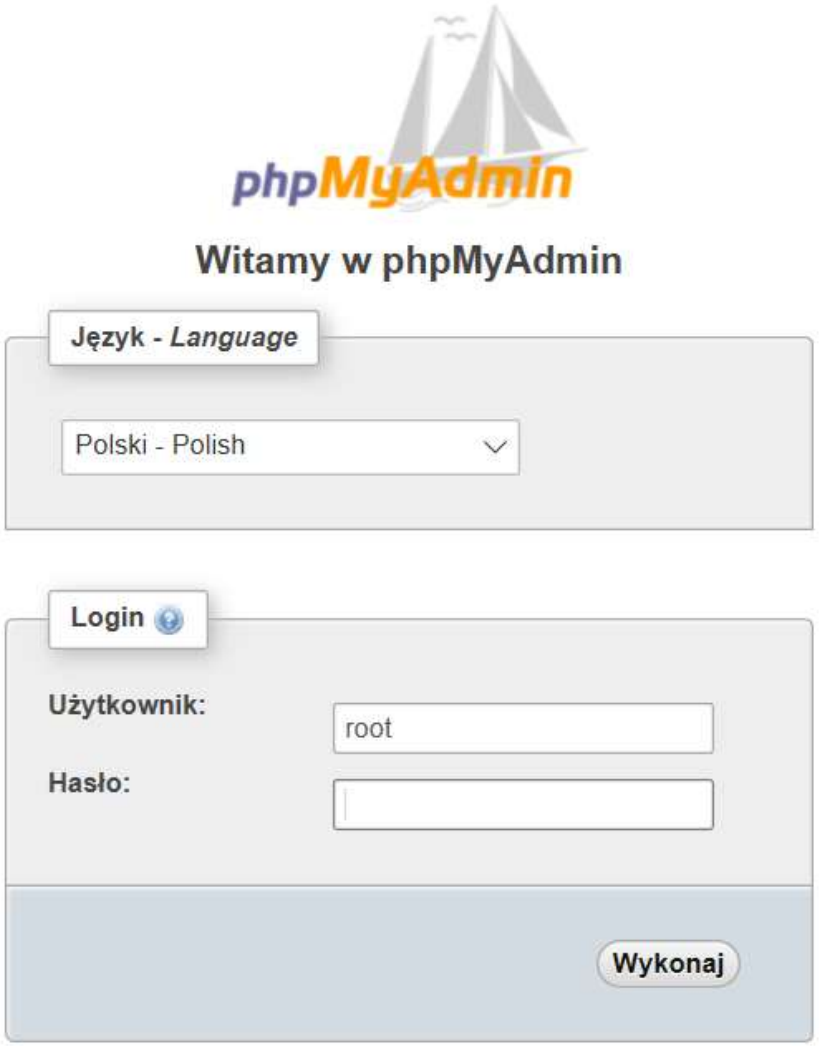
Jeżeli użytkownik nie ma wymaganych uprawnień, nastąpi przerwanie wykonywania operacji, ten proces nazywany jest autoryzacją.



Konta użytkowników

Podczas instalowania serwera MySQL tworzone jest wbudowane konto root. Ma ono pełne uprawnienia i w codziennej pracy nie powinno być używane nawet przez administratora.
Korzystając z konta root, wyłączamy cały mechanizm autoryzacji i obniżamy poziom bezpieczeństwa serwera.

Założenie konta użytkownika i nadanie użytkownikowi minimalnych uprawnień potrzebnych do wykonywania jego pracy powinno być podstawową zasadą bezpieczeństwa podczas korzystania z serwera baz danych.



Tryby uwierzytelniania

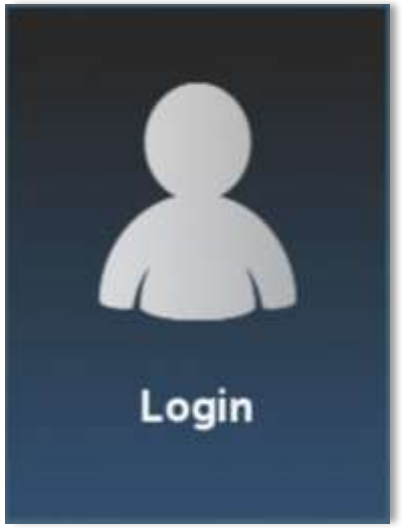
Serwer MySQL powinien być uruchamiany z konta zwykłego użytkownika, specjalnie w tym celu utworzonego, z minimalnymi prawami, które są potrzebne do pracy. Aby serwer uruchamiał się z tego konta, w pliku my.ini należy dodać wpis:

```
[mysqld]
user=mysql
```

W serwerze MySQL konta użytkownika związane są z nazwą komputera, z którego użytkownik korzysta.

Jeżeli użytkownik łączy się z serwerem z wielu komputerów, to dla każdego z nich możliwe jest ustawienie innego hasła i innych praw dostępu.

Tworzenie konta użytkownika



- Istnieje kilka sposobów definiowania użytkowników i ich uprawnień w MySQL
- Najbardziej popularne to użycie polecenia **CREATE USER** lub **GRANT**

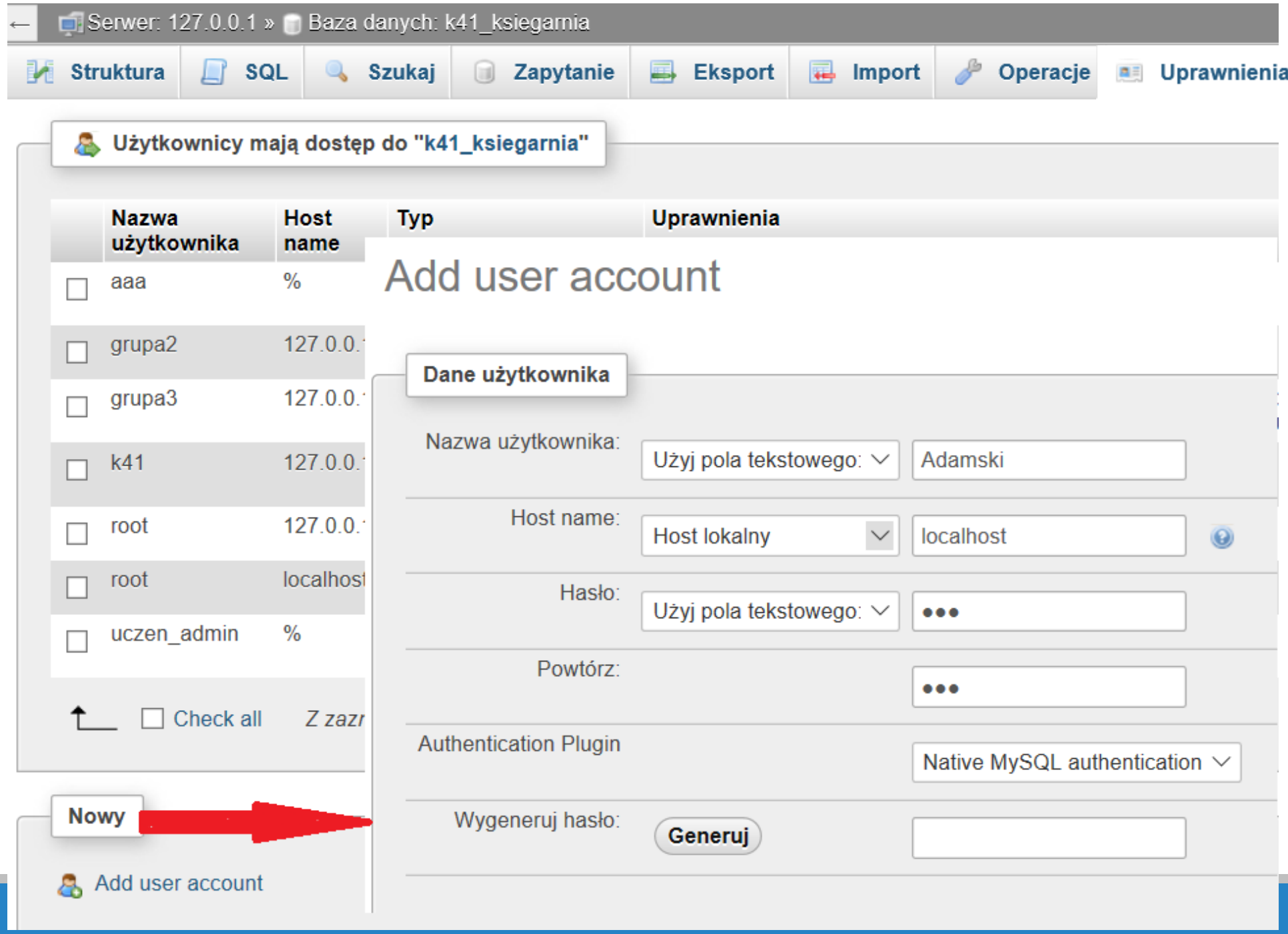
Utworzenie użytkownika przez realizację polecenia CREATE USER.

Przykład: CREATE USER adam IDENTYFIED BY ’haslo’;
CREATE USER adam IDENTYFIED BY PASSWORD ’tajne_haslo’;

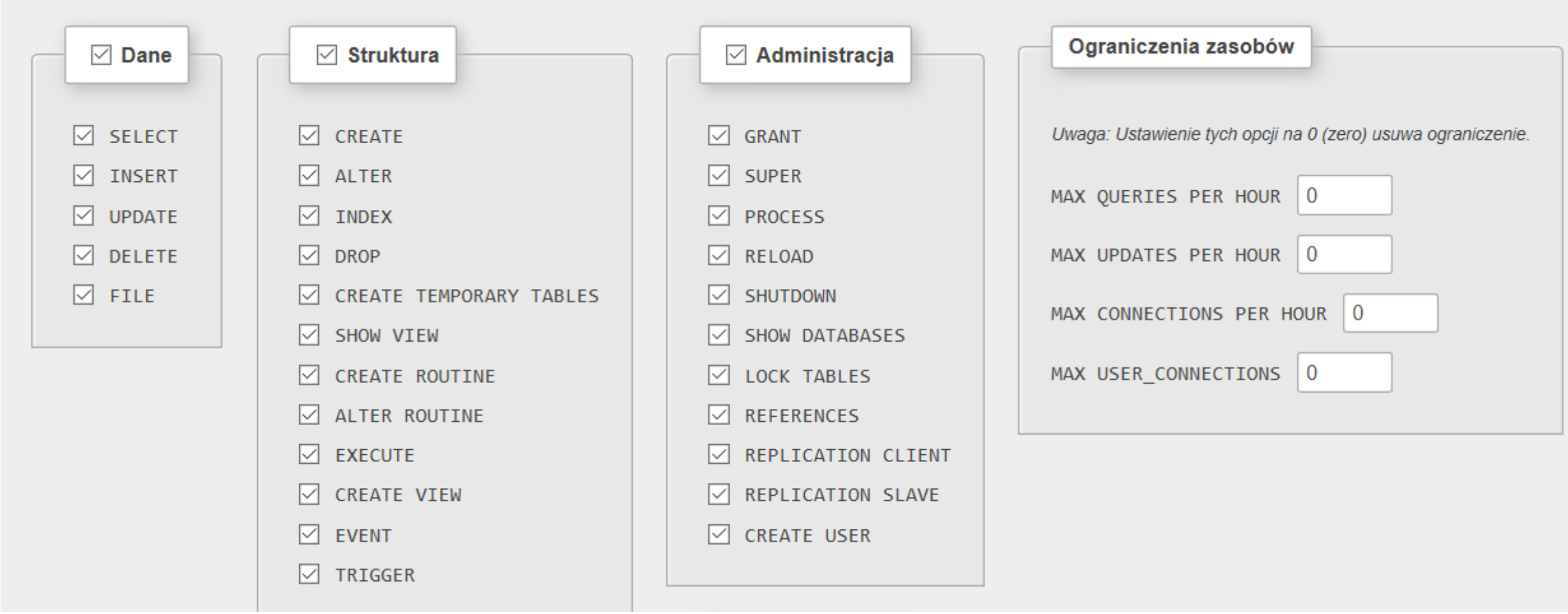
W wyniku wykonania polecenia w tabeli mysql.user zostanie utworzony wpis oznaczający, że użytkownik adam może korzystać z dowolnego komputera do połączenia się z serwerem.

- Maksymalna długość nazwy użytkownika wynosi 16 znaków i nie może zawierać znaków spacji
- Wielkość znaków jest rozróżniana
- Nazwa hosta określa komputer z którego użytkownik próbuje się połączyć
  - *localhost*- użytkownik może się podłączyć tylko z tego komputera na którym działa MySQL
  - *%* - można korzystać z dowolnego hosta
  - *adres IP* np. 192.168.0.1
  - *nazwa hosta* np. mojkomputer.pl
- Hasło nie posiada ograniczenia długości , wielkość znaków jest rozróżniana
- Nieuwzględnienie klauzuli IDENTIFIED BY powoduje , że użytkownik nie musi podawać hasła

Dodawanie nowego użytkownika poprzez interfejs graficzny:



Nadawanie uprawnień poprzez interfejs graficzny:



Przykład:

```
CREATE USER 'Adamski'@'localhost' IDENTIFIED VIA mysql_native_password USING '***';GRANT ALL PRIVILEGES ON *.* TO 'Adamski'@'localhost' REQUIRE NONE WITH GRANT OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0;GRANT ALL PRIVILEGES ON `k41_ksiegarnia`.* TO 'Adamski'@'localhost';
```

Usuwanie użytkownika i zmiana hasła użytkownika

Aby usunąć użytkownika, należy użyć polecenia DROP USER.

Przykład: DROP USER 'Adamski'@'localhost'

Nazwę bieżącego użytkownika można uzyskać po wpisaniu polecenia:

```
SELECT CURRENT_USER ( )
```

Zmianę hasła bieżącego użytkownika uzyskamy po wpisaniu polecenia:

```
SET PASSWORD = PASSWORD('HASŁO');
```

Zmiana hasła dla innego konta wymaga odpowiednich uprawnień i ma postać:

```
SET PASSWORD FOR adam = PASSWORD('haslo_adama');
```

Prawa dostępu do serwera

Podczas pracy z serwerem MySQL należy przestrzegać zasad bezpieczeństwa.

- Trzeba pamiętać o ustawieniu hasła dla konta administratora oraz konta anonimowego (User="").
- Jeżeli po wpisaniu polecenia mysql -u root nie pojawi się komunikat z prośbą o podanie hasła, to znaczy, że hasło nie zostało ustawione.
- Nie należy pracować na koncie root.
- Nie należy definiować dostępu do bazy mysql innym użytkownikom poza administratorem.
- Użytkownikom należy nadawać jak najmniejsze uprawnienia — tylko te, które są konieczne.
- Nie należy nadawać praw dostępu do wszystkich baz danych, a jedynie do wybranych.

Prawa dostępu serwera MySQL

Prawa dostępu serwera MySQL mogą być nadawane użytkownikom na poziomie:

- całego serwera,
- bazy danych np. CREATE, ALTER, DROP,
- obiektów bazy danych np. SELECT, INSERT, UPDATE, DELETE

Informacje na temat praw dostępu do serwera MySQL są przechowywane w tabelach słownikowych bazy danych mysql.

Są to tabele: host, db, user, tables_priv, columns_priv i procs_priv.

- user przechowuje informacje o prawach dostępu użytkownika niezależnie od bazy danych
- db przechowuje informacje o prawach dostępu użytkownika w zależności od bazy danych
- host przechowuje informacje w kontekście komputera, z którego łączy się użytkownik.

Pozostałe tabele przechowują informacje szczegółowe dotyczące praw dostępu do tabel, kolumn itp.

Lista dostępnych tabel

Po zalogowaniu się do bazy mysql można wyświetlić listę dostępnych tabel.

Przykład:

```
Use mysql;
SHOW TABLES;
SELECT Host, User FROM user WHERE = ”adam”;
```

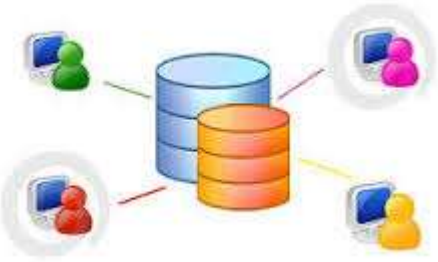
Użyte w przykładzie polecenie SELECT pozwoli wyświetlić prawa dostępu użytkownika adam.

W serwerze MySQL prawa są dziedziczone. Oznacza to, że prawa nadane do obiektu znajdującego się wyżej w hierarchii są domyślnie dziedziczone przez obiekty znajdujące się niżej.

Jednak prawa mogą być nadawane i odbierane na dowolnym poziomic.

Tables_in_mysql
column_stats
columns_priv
db
event
func
general_log
gtid_slave_pos
help_category
help_keyword
help_relation
help_topic
host
index_stats
innodb_index_stats
innodb_table_stats
ndb_binlog_index
plugin
proc
procs_priv
proxies_priv
roles_mapping
servers
slave_master_info
slave_relay_log_info
slave_worker_info
slow_log
table_stats
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user

Uprawnienia – nadawanie praw



Prawa są nadawane użytkownikom instrukcją GRANT.

Składnia polecenia ma postać:
GRANT *[prawo]* ON *baza_danych.** TO *'[użytkownik]'&'[host]'* IDENTIFIED BY *'[HASŁO]';*

Prawa mogą być nadawane na różnych poziomach.

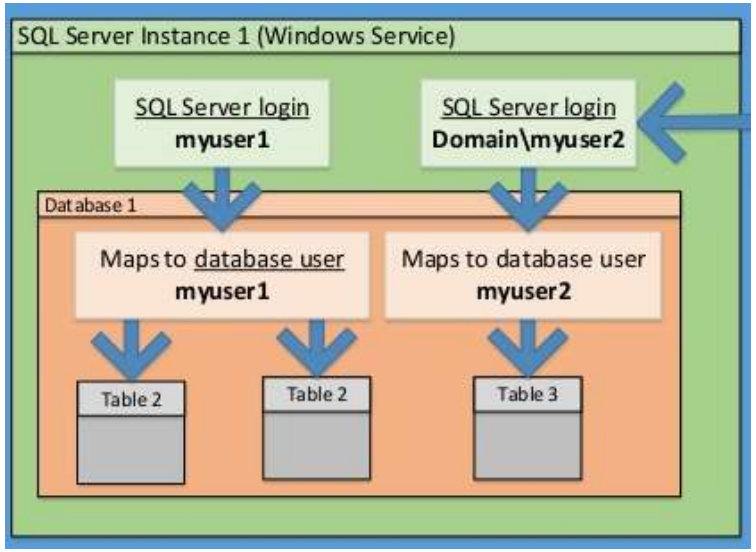
- Prawa nadawane globalnie:
  GRANT UPDATE ON *.* TO Marcin;
- Prawa nadawane na poziomie domyślnej bazy danych:
  GRANT UPDATE ON ksiegarnia_internetowa.* TO Marcin;
- Prawa nadawane na poziomie obiektów bazy danych (na przykład do wybranej tabeli);
  GRANT INSERT ON ksiegarnia_internetowa. ksiazki TO Marcin;
- Prawa nadawane na poziomie wybranych kolumn tabeli:
  GRANT UPDATE (ksiazki . tytul) , INSERT ON ksiegarnia_internetowa. ksiazki TO Marcin;

Polecenie GRANT

GRANT lista_praw_dostępu ON nazwa_tabeli TO nazwa_użytkownika IDENTIFIED BY ’haslo’

Pole „lista_praw_dostępu” może zawierać jedno, lub kilka z poniższych uprawnień:

- SELECT– odczytanie danych z tabeli
- INSERT – wstawianie danych do tabeli
- UPDATE – modyfikowanie danych w tabeli
- DELETE – usunięcie danych z tabeli
- REFERENCE – odwoływanie się do innych tabel
- CREATE – tworzenie nowych tabel i baz danych
- DROP – usuwanie tabel oraz baz danych
- ALL – wszystkie dostępne uprawnienia



USAGE- nie nadaje żadnych uprawnień. Powoduje zarejestrowanie użytkownika i pozwala mu na zalogowanie się, lecz jakiekolwiek czynności są dla niego niedostępne. Odpowiednie przywileje są w takiej sytuacji nadawane później.

Klauzule polecenia GRANT

Polecenie GRANT może zawierać dodatkowe klauzule:

- MAX_QUERIES_PER_HOUR — ogranicza liczbę zapytań;
- MAX_UPDATES_PER_HOUR — ogranicza liczbę zmian wprowadzanych do bazy;
- MAX _ CONNECTIONS_PER_HOUR— ogranicza liczbę logowań użytkownika wciągu godziny;
  MAX_USER_CONNECTIONS — ogranicza liczbę jednoczesnych połączeń uzyskiwanych z jednego konta.

Przykład:

GRANT USAGE ON *.* TO Marcin WITH MAX_QUERIES_PER_HOUR 1;

Prawo USAGE oznacza ,że użytkownikowi nie zostały nadane żadne prawa

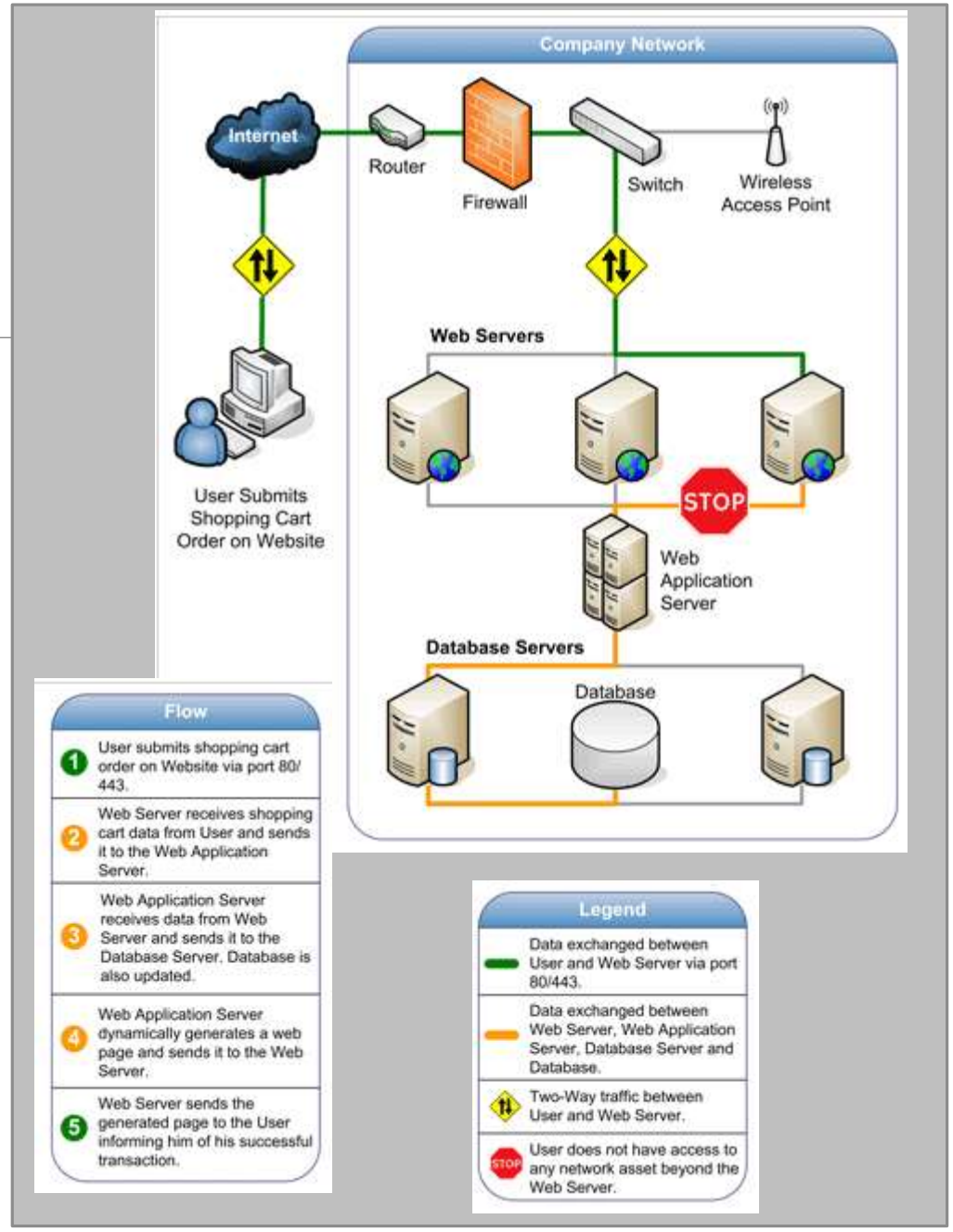
Odbieranie praw

Instrukcją **REVOKE** można usunąć wcześniej nadane prawa.

Przykład

```
REVOKE UPDATE ON ksiegarnia_internetowa FROM Marcin;
```

W podanym przykładzie użytkownikowi Marcin zostały odebrane uprawnienia do modyfikowania danych w tabeli Ksiazki.



Role administracyjne

Aby ułatwić przypisywanie uprawnień użytkownikom, w MySQL została wprowadzona koncepcja ról administracyjnych. Za pomocą ról można w szybki sposób przyznawać użytkownikowi zestaw uprawnień potrzebnych do pracy na serwerze. Użytkownikowi można nadać jedną rolę lub kilka ról.

Dostępne role

- **DBA** — wszystkie uprawnienia.
- **MaintenanceAdmin** — uprawnienia do utrzymania serwera.
- **ProcessAdmin** — uprawnienia do monitorowania i zatrzymywania procesów użytkownika.
- **UserAdmin** — uprawnienia do tworzenia użytkowników i ustawiania haseł.
- **SecurityAdmin** — uprawnienia do zarządzania kontami oraz nadawania i odbierania uprawnień serwera.
- **MonitorAdmin** — uprawnienia do monitorowania serwera.
- **DBManager** — uprawnienia do zarządzania bazami danych.
- **DBDesigner** — uprawnienia do tworzenia i modyfikowania schematów baz danych.
- **ReplicationAdmin** — uprawnienia do tworzenia replikacji i zarządzania nią.
- **BackupAdmin** — uprawnienia do tworzenia kopii zapasowych baz danych.

Uprawnienia administratorów

Uprawnienie	Opis
CRETE TEMPORARY TABLES	Pozwala administratorowi używać słowo kluczowe TEMPORARY w instrukcji CREATE TABLE
FILE	Pozwala wczytywać dane z plików do tabel i odwrotnie
LOCK TABLES	Pozwala jawnie używać instrukcji LOCK TABLES
PROCESS	Pozwala śledzić procesy wykonywane przez serwer i je przerywać
RELOAD	Pozwala powtórnie załadować tabele zwierające informacje na temat praw dostępu oraz na odświeżenie przywilejów, listy nazw łączących się komputerów, dziennika zdarzeń i tabel
REPLICATION CLIENT	Pozwala używać instrukcję SHOW STATUS na nadawcach i odbiorcach replikacji
REPLICATION SLAVE	Pozwala serwerom będącym odbiorcami replikacji łączyć się z serwerem nadawcą.
SHOW DATABASES	Pozwala odczytywać listę wszystkich baz danych przy użyciu instrukcji SHOW DATABASES. Użytkownicy, którzy nie mają tego uprawnienia, mogą zobaczyć tylko bazy, do których przydzielono im dostęp
SHUTDOWN	Pozwala zakończyć pracę serwera MySQL
SUPER	Pozwala zabijać wątki, należące do dowolnego użytkownika

Ustawianie okna logowania do MySQL

1. Za pomocą Notepad++(lub Notatnika), otwieramy plik xampp\phpMyAdmin\config.inc.php.

```
/* Authentication type and info */
$cfg['Servers'][$i]['auth_type'] = 'config';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'admin123';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['AllowNoPassword'] = true;
$cfg['Lang'] = '';
```

2. Wpisz hasło admin123 w wierszu kodu PHP - $cfg['Servers'][$i]['password'] = 'admin123';
   a następnie zapisz zmiany:
3. Nie otwierając żadnej z baz (dla pewności kliknij napis phpMyAdmin), wpisz w zakładce SQL polecenie:
   SET PASSWORD FOR 'root'@'localhost'= PASSWORD('admin123');,
   a następnie kliknij Wykonaj. Fakt ustanowienia hasła powinien pokazać phpMyAdmin

4. Ponownie za pomocą Notepad++, otwórz plik xampp\phpMyAdmin\config.inc.php, wpisz zamiast config – cookie.Od tej pory uruchomienie panelu administracyjnego będzie wymagało wpisanie użytkownika root oraz hasła admin123.

Otwarcie panelu administracyjnego wymaga hasła