University of Essex

Online

Launching into Cyber Security

Week 9 Seminar

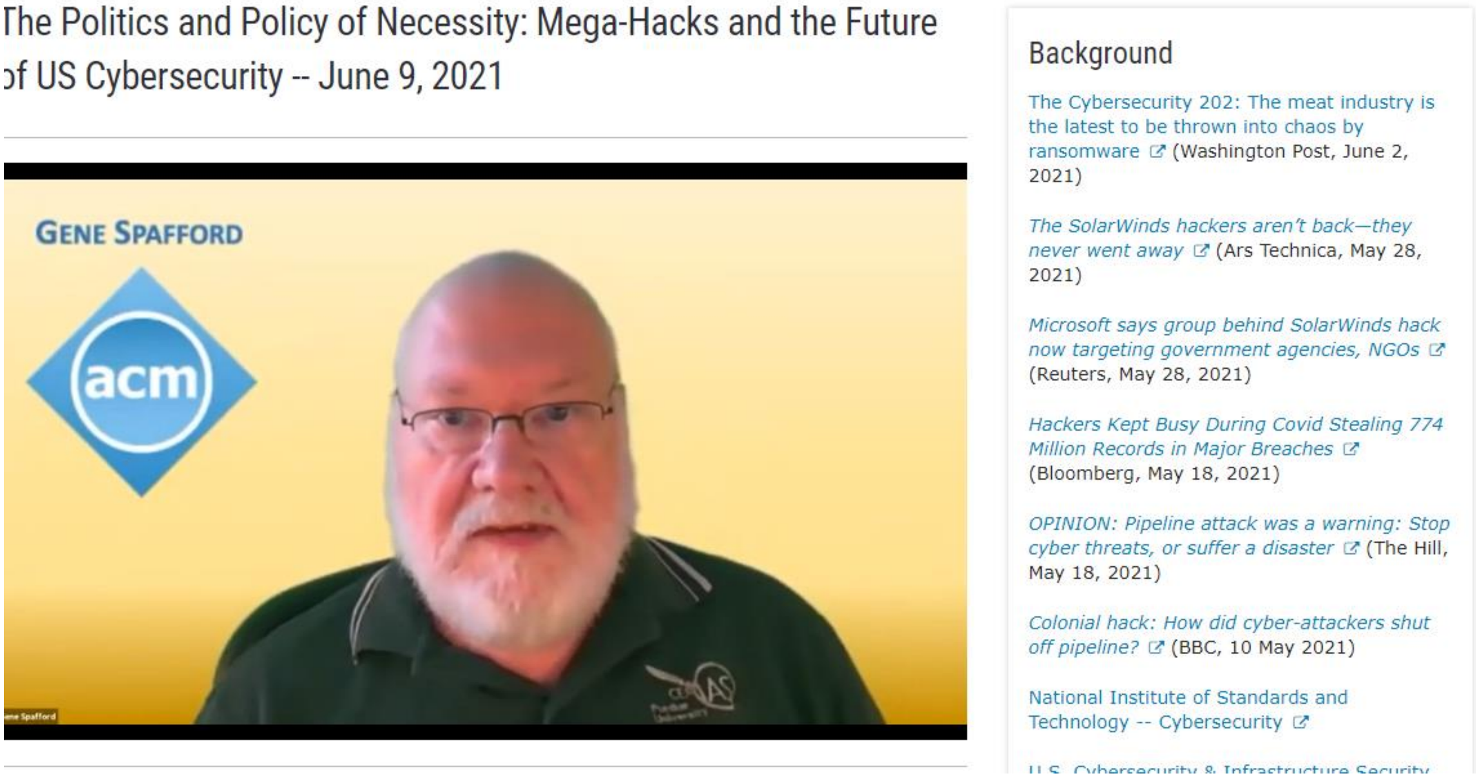
Sammy Danso, PhD

Announcement

- Individual essay
- ACM Webinar and articles on ransomware

Announcement

ACM Webinar by US Technology Policy Committee and articles on ransomware: https://www.acm.org/public-policy/ustpc/hottopics/future-of-us-cybersecurity



The Politics and Policy of Necessity: Mega-Hacks and the Future of US Cybersecurity -- June 9, 2021

Background

The Cybersecurity 202: The meat industry is the latest to be thrown into chaos by ransomware (Washington Post, June 2, 2021)

The SolarWinds hackers aren't back—they never went away (Ars Technica, May 28, 2021)

Microsoft says group behind SolarWinds hack now targeting government agencies, NGOs (Reuters, May 28, 2021)

Hackers Kept Busy During Covid Stealing 774 Million Records in Major Breaches (Bloomberg, May 18, 2021)

OPINION: Pipeline attack was a warning: Stop cyber threats, or suffer a disaster (The Hill, May 18, 2021)

Colonial hack: How did cyber-attackers shut off pipeline? (BBC, 10 May 2021)

National Institute of Standards and Technology -- Cybersecurity

U.S. Cybersecurity & Infrastructure Security

This week’s task

- Implementation of security measures such as access controls and privileges.
- Integration of Python and MySQL.
- Manipulating and updating MySQL database using Python scripts.
- Securing password and implementation of authentications with Python

MySQL : security measures

Access control and account management:

- MySQL enables the creation of account to permit users to connect to server to access data.
- Access control is key to be able to connect to a database.
- User account is assigned to authenticate credentials.
- Identity is determined by **host** from which you connect and the **username** you specify.
- MySQL privilege system authenticates a user and associates user to the privileges set on the database.
- System grants privileges according to your identity and what you want to do.

MySQL : security measures

Accounts username and passwords:

- There is no connection between operating system user login and account names used by MySQL.

- Accounts are stored in a table called ***user*** in MySQL system database

- Passwords stored in the ***user*** table are encrypted using plugin specific algorithms.

- MySQL installation process populates ***grant*** tables with an initial root account.

MySQL : security measures

Privileges provided by MySQL:

- Privileges granted to MySQL account determines the operations performed by the account

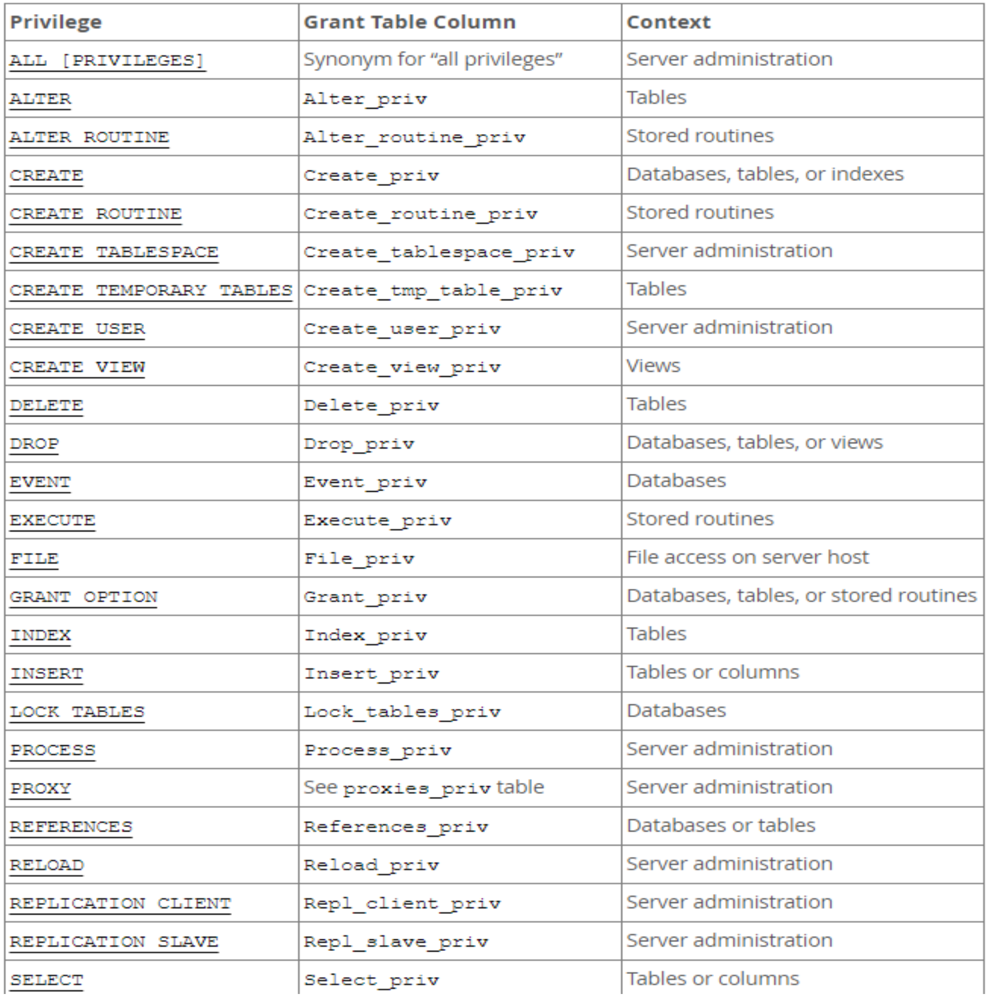
- Administrative – enable users to manage operations of MySQL server

- Administrative privileges are global – not specific to a particular database

- Database privileges are specific to databases and the objects within it

- Privileges for databases

MySQL : security measures



Privilege	Grant Table Column	Context
ALL [PRIVILEGES]	Synonym for "all privileges"	Server administration
ALTER	Alter_priv	Tables
ALTER ROUTINE	Alter_routine_priv	Stored routines
CREATE	Create_priv	Databases, tables, or indexes
CREATE ROUTINE	Create_routine_priv	Stored routines
CREATE TABLESPACE	Create_tablespace_priv	Server administration
CREATE TEMPORARY TABLES	Create_tmp_table_priv	Tables
CREATE USER	Create_user_priv	Server administration
CREATE VIEW	Create_view_priv	Views
DELETE	Delete_priv	Tables
DROP	Drop_priv	Databases, tables, or views
EVENT	Event_priv	Databases
EXECUTE	Execute_priv	Stored routines
FILE	File_priv	File access on server host
GRANT OPTION	Grant_priv	Databases, tables, or stored routines
INDEX	Index_priv	Tables
INSERT	Insert_priv	Tables or columns
LOCK TABLES	Lock_tables_priv	Databases
PROCESS	Process_priv	Server administration
PROXY	See proxies_priv table	Server administration
REFERENCES	References_priv	Databases or tables
RELOAD	Reload_priv	Server administration
REPLICATION CLIENT	Repl_client_priv	Server administration
REPLICATION SLAVE	Repl_slave_priv	Server administration
SELECT	Select_priv	Tables or columns

Details: https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/privileges-provided.html#privileges-provided-summary

MySQL : security measures

Privilege granting guidelines

•FILE can be abused to read into a database table any files that the MySQL server can read on the server host.

•The table can then be accessed using SELECT to transfer its contents to the client host.

•GRANT OPTION enables users to give their privileges to other users.

•Two users that have different privileges and with the GRANT OPTION privilege are able to combine privileges.

•ALTER may be used to subvert the privilege system by renaming tables.

•SHUTDOWN can be abused to deny service to other users entirely by terminating the server.

•PROCESS can be used to view the plain text of currently executing statements, including statements that set or change passwords.

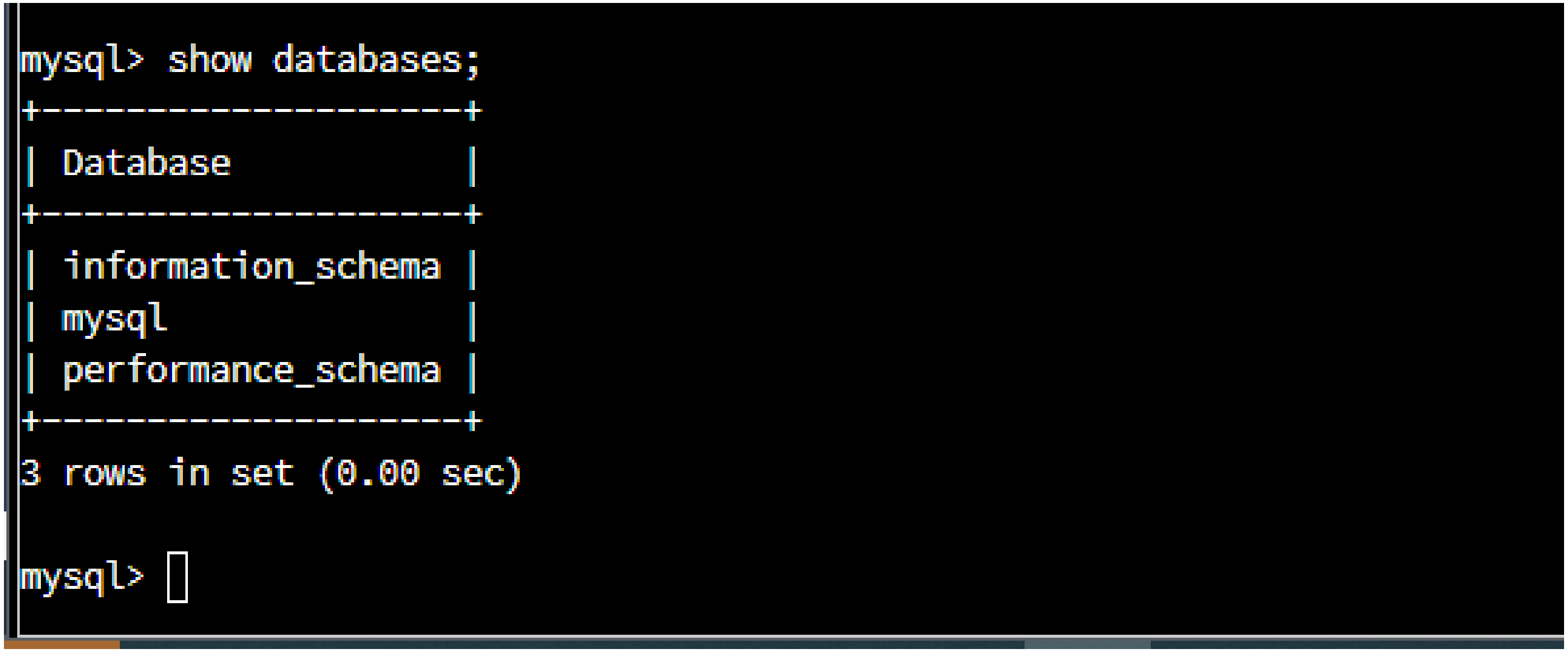
•SUPER can be used to terminate other sessions or change how the server operates.

MySQL : security measures

The Grant tables:

- `user`: user accounts, global privileges, and other non-privilege columns.
- `db`: database-level privileges.
- `tables_priv`: table-level privileges.
- `columns_priv`: column-level privileges.
- `procs_priv`: stored procedure and function privileges.
- `proxies_priv`: proxy-user privileges.

MySQL : security measures

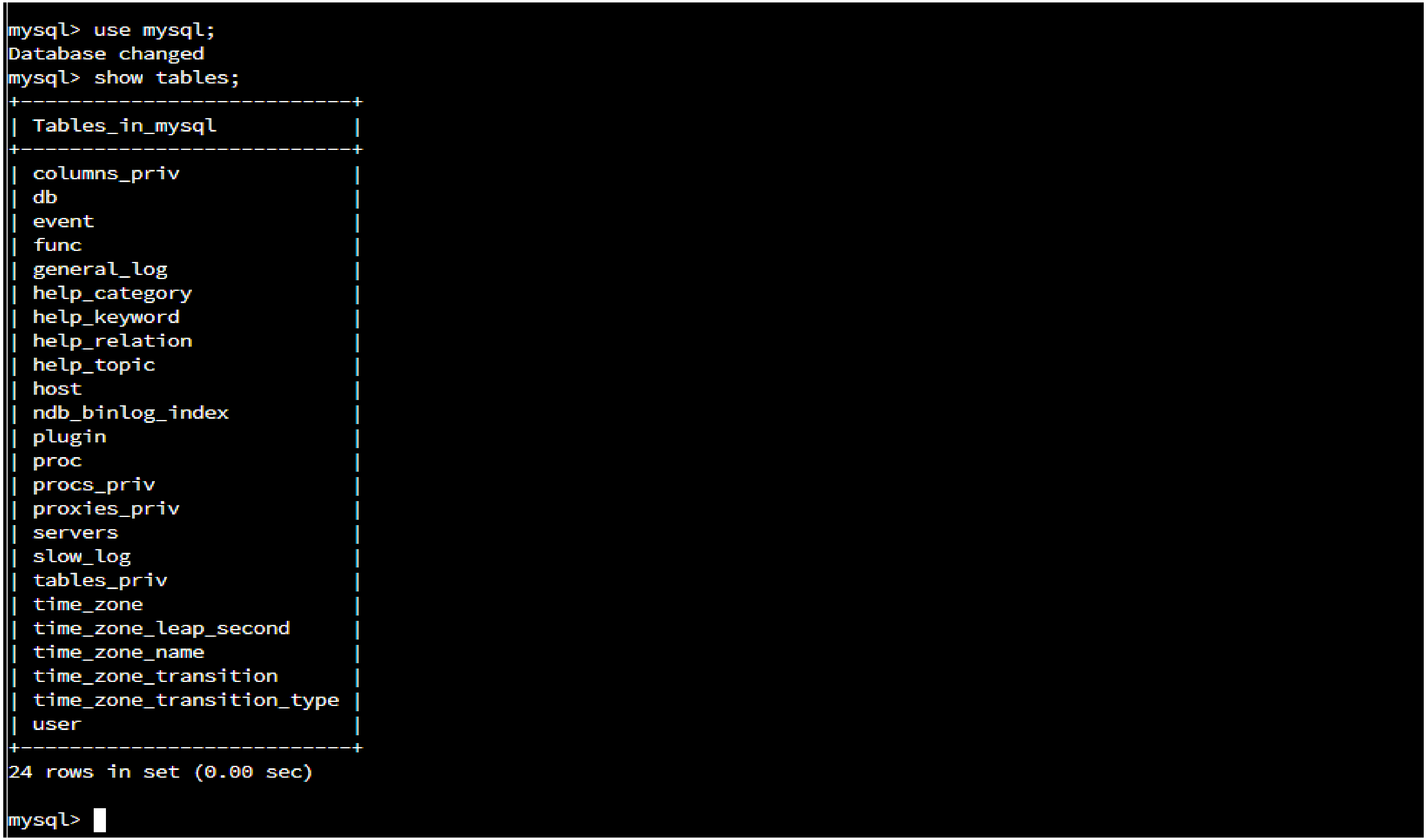


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql> 
```

University of Essex

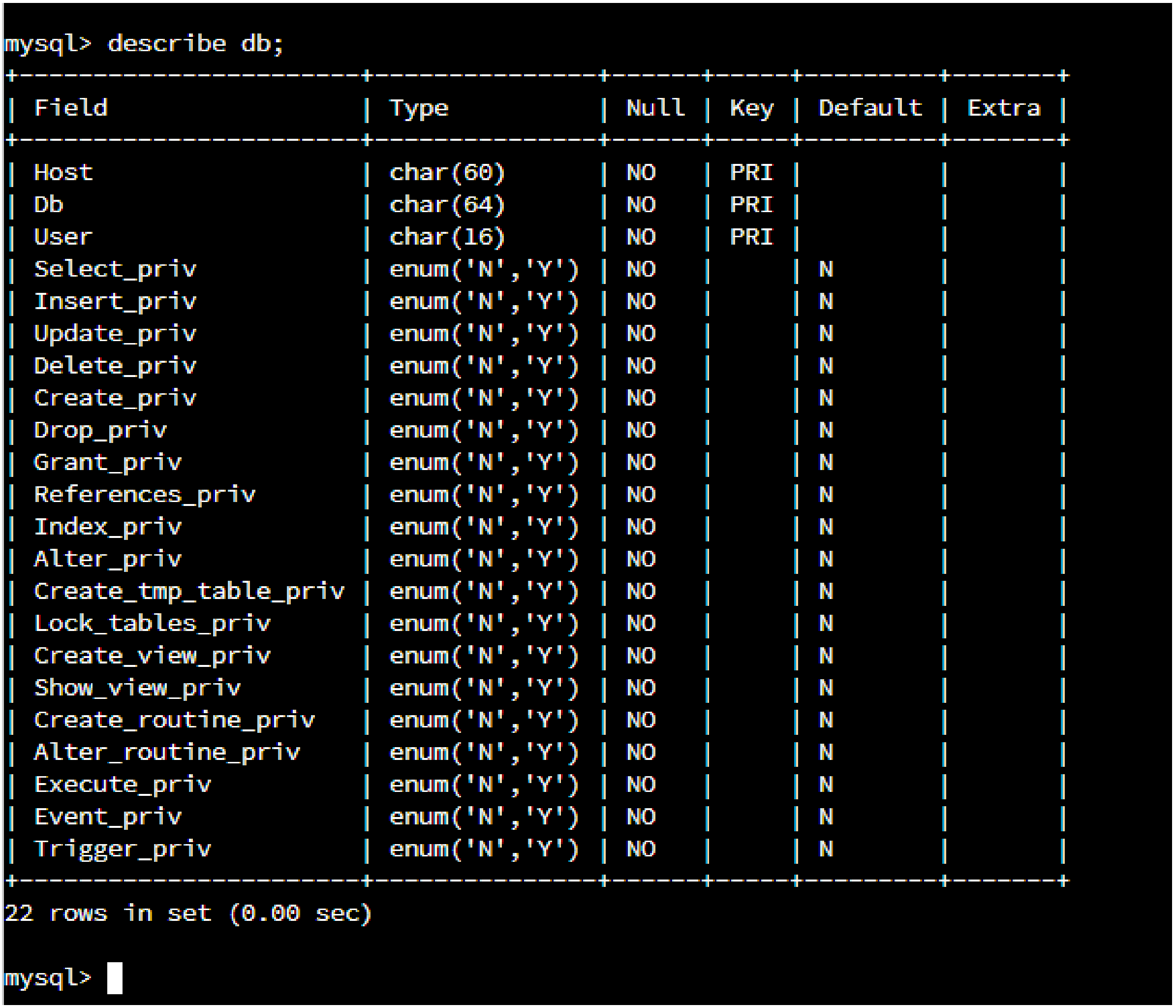
Online

MySQL : security measures



```
mysql> use mysql;
Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| servers                   |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
24 rows in set (0.00 sec)

mysql> 
```

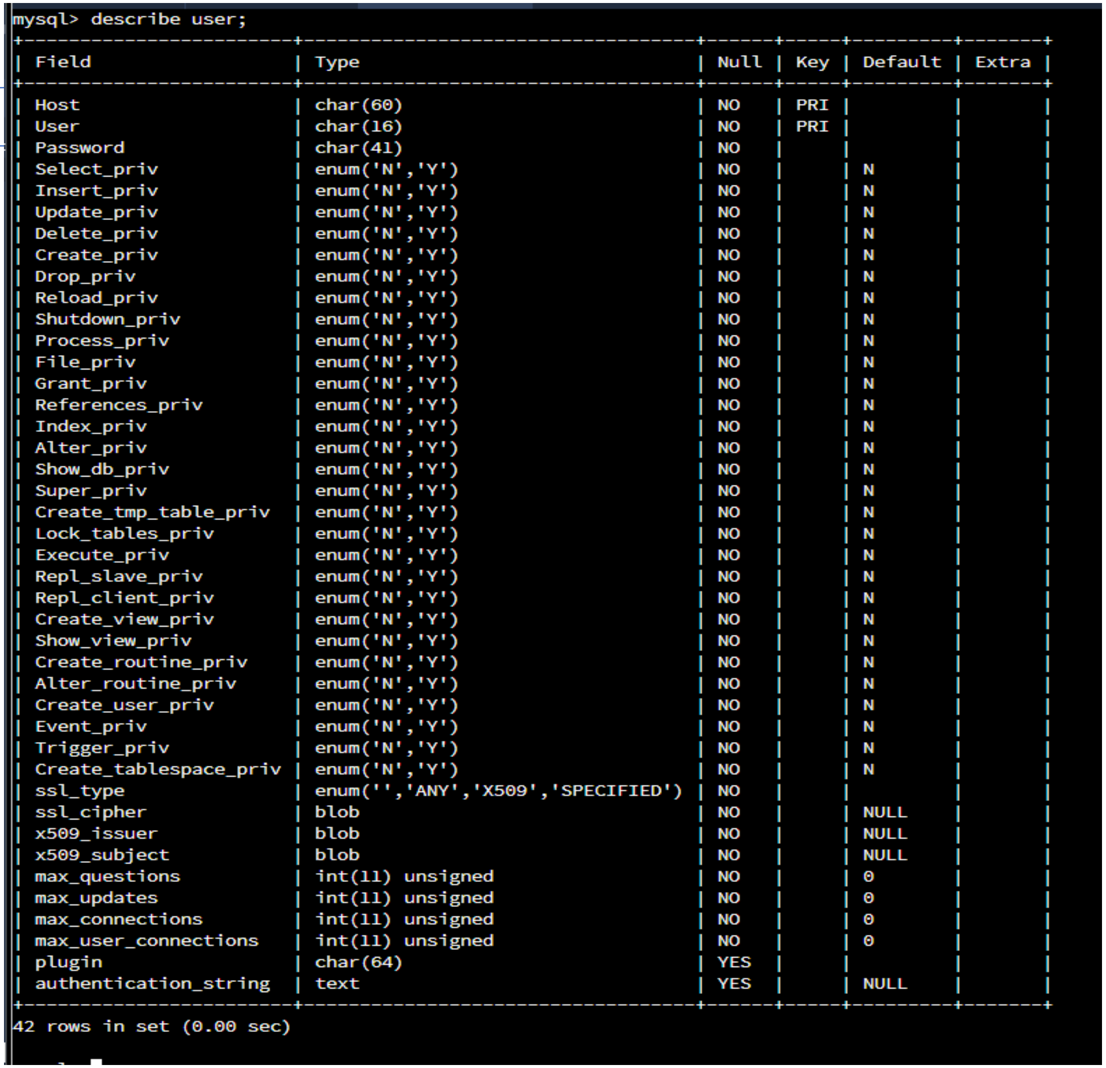
MySQL : security measures



```
mysql> describe db;
+-----------------------+---------------+------+-----+---------+-------+
| Field                 | Type          | Null | Key | Default | Extra |
+-----------------------+---------------+------+-----+---------+-------+
| Host                  | char(60)      | NO   | PRI |         |       |
| Db                    | char(64)      | NO   | PRI |         |       |
| User                  | char(16)      | NO   | PRI |         |       |
| Select_priv           | enum('N','Y') | NO   |     | N       |       |
| Insert_priv           | enum('N','Y') | NO   |     | N       |       |
| Update_priv           | enum('N','Y') | NO   |     | N       |       |
| Delete_priv           | enum('N','Y') | NO   |     | N       |       |
| Create_priv           | enum('N','Y') | NO   |     | N       |       |
| Drop_priv             | enum('N','Y') | NO   |     | N       |       |
| Grant_priv            | enum('N','Y') | NO   |     | N       |       |
| References_priv       | enum('N','Y') | NO   |     | N       |       |
| Index_priv            | enum('N','Y') | NO   |     | N       |       |
| Alter_priv            | enum('N','Y') | NO   |     | N       |       |
| Create_tmp_table_priv | enum('N','Y') | NO   |     | N       |       |
| Lock_tables_priv      | enum('N','Y') | NO   |     | N       |       |
| Create_view_priv      | enum('N','Y') | NO   |     | N       |       |
| Show_view_priv        | enum('N','Y') | NO   |     | N       |       |
| Create_routine_priv   | enum('N','Y') | NO   |     | N       |       |
| Alter_routine_priv    | enum('N','Y') | NO   |     | N       |       |
| Execute_priv          | enum('N','Y') | NO   |     | N       |       |
| Event_priv            | enum('N','Y') | NO   |     | N       |       |
| Trigger_priv          | enum('N','Y') | NO   |     | N       |       |
+-----------------------+---------------+------+-----+---------+-------+
22 rows in set (0.00 sec)

mysql>
```

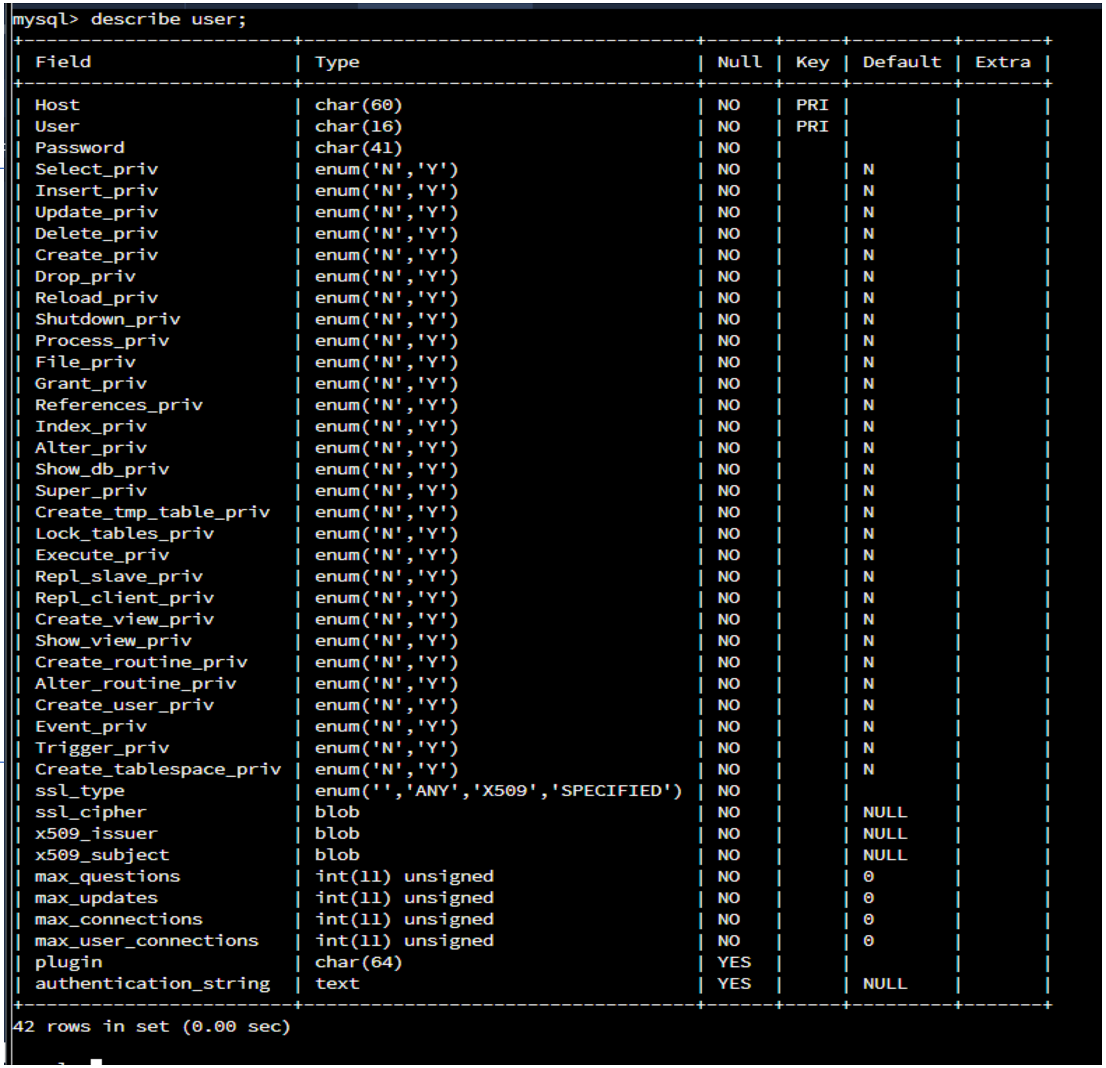
MySQL : security measures

Scope columns



```
mysql> describe user;
+------------------------+-----------------------------------+------+-----+---------+-------+
| Field                  | Type                              | Null | Key | Default | Extra |
+------------------------+-----------------------------------+------+-----+---------+-------+
| Host                   | char(60)                          | NO   | PRI |         |       |
| User                   | char(16)                          | NO   | PRI |         |       |
| Password               | char(41)                          | NO   |     |         |       |
| Select_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Insert_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Update_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Delete_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Create_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Drop_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Reload_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Shutdown_priv          | enum('N','Y')                     | NO   |     | N       |       |
| Process_priv           | enum('N','Y')                     | NO   |     | N       |       |
| File_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Grant_priv             | enum('N','Y')                     | NO   |     | N       |       |
| References_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Index_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Alter_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Show_db_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Super_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Create_tmp_table_priv  | enum('N','Y')                     | NO   |     | N       |       |
| Lock_tables_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Execute_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Repl_slave_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Repl_client_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Create_view_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Show_view_priv         | enum('N','Y')                     | NO   |     | N       |       |
| Create_routine_priv    | enum('N','Y')                     | NO   |     | N       |       |
| Alter_routine_priv     | enum('N','Y')                     | NO   |     | N       |       |
| Create_user_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Event_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Trigger_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Create_tablespace_priv | enum('N','Y')                     | NO   |     | N       |       |
| ssl_type               | enum('','ANY','X509','SPECIFIED') | NO   |     |         |       |
| ssl_cipher             | blob                              | NO   |     | NULL    |       |
| x509_issuer            | blob                              | NO   |     | NULL    |       |
| x509_subject           | blob                              | NO   |     | NULL    |       |
| max_questions          | int(11) unsigned                  | NO   |     | 0       |       |
| max_updates            | int(11) unsigned                  | NO   |     | 0       |       |
| max_connections        | int(11) unsigned                  | NO   |     | 0       |       |
| max_user_connections   | int(11) unsigned                  | NO   |     | 0       |       |
| plugin                 | char(64)                          | YES  |     |         |       |
| authentication_string  | text                              | YES  |     | NULL    |       |
+------------------------+-----------------------------------+------+-----+---------+-------+
42 rows in set (0.00 sec)
```

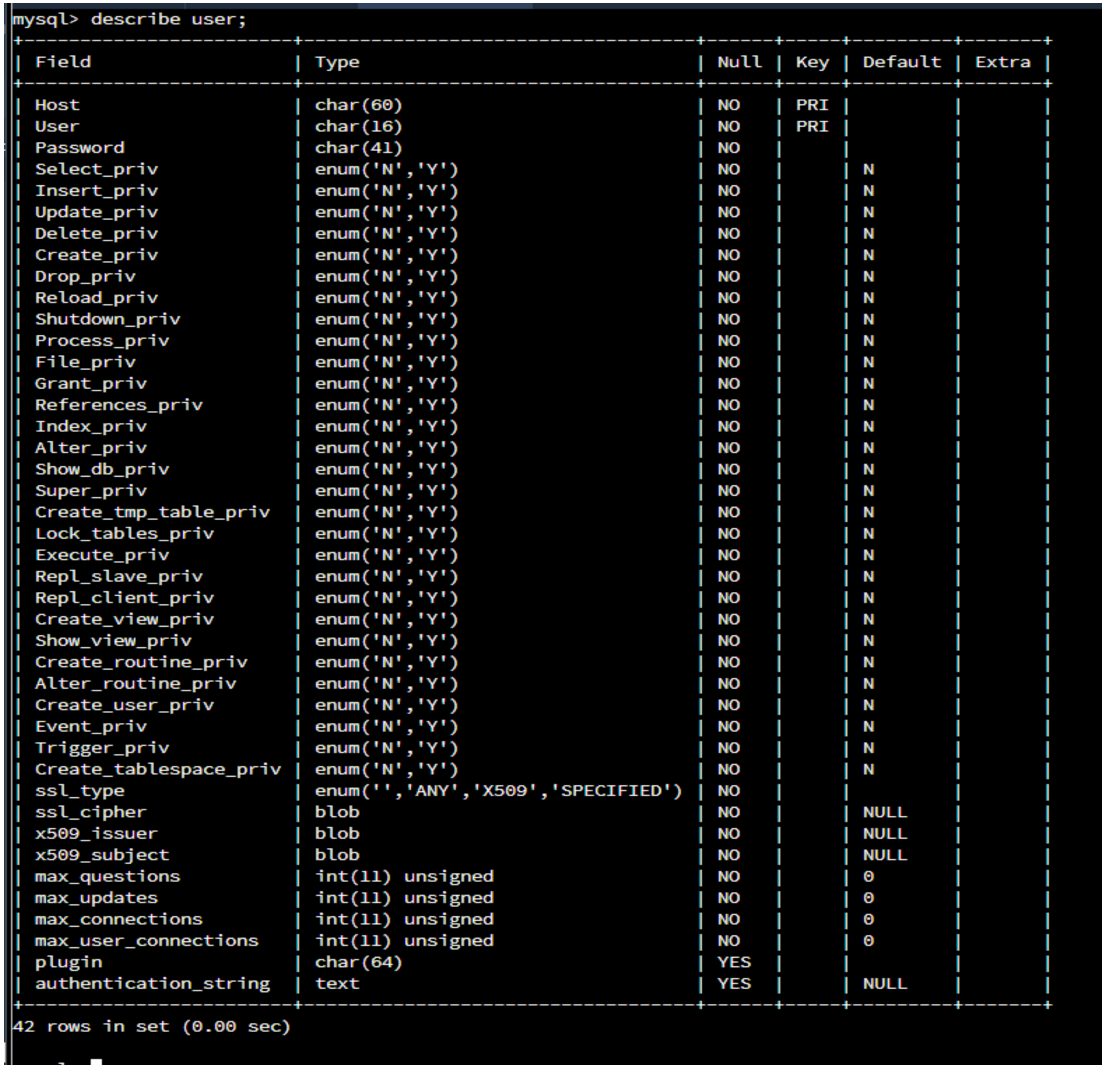
MySQL : security measures



```
mysql> describe user;
+------------------------+-----------------------------------+------+-----+---------+-------+
| Field                  | Type                              | Null | Key | Default | Extra |
+------------------------+-----------------------------------+------+-----+---------+-------+
| Host                   | char(60)                          | NO   | PRI |         |       |
| User                   | char(16)                          | NO   | PRI |         |       |
| Password               | char(41)                          | NO   |     |         |       |
| Select_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Insert_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Update_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Delete_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Create_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Drop_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Reload_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Shutdown_priv          | enum('N','Y')                     | NO   |     | N       |       |
| Process_priv           | enum('N','Y')                     | NO   |     | N       |       |
| File_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Grant_priv             | enum('N','Y')                     | NO   |     | N       |       |
| References_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Index_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Alter_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Show_db_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Super_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Create_tmp_table_priv  | enum('N','Y')                     | NO   |     | N       |       |
| Lock_tables_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Execute_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Repl_slave_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Repl_client_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Create_view_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Show_view_priv         | enum('N','Y')                     | NO   |     | N       |       |
| Create_routine_priv    | enum('N','Y')                     | NO   |     | N       |       |
| Alter_routine_priv     | enum('N','Y')                     | NO   |     | N       |       |
| Create_user_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Event_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Trigger_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Create_tablespace_priv | enum('N','Y')                     | NO   |     | N       |       |
| ssl_type               | enum('','ANY','X509','SPECIFIED') | NO   |     |         |       |
| ssl_cipher             | blob                              | NO   |     | NULL    |       |
| x509_issuer            | blob                              | NO   |     | NULL    |       |
| x509_subject           | blob                              | NO   |     | NULL    |       |
| max_questions          | int(11) unsigned                  | NO   |     | 0       |       |
| max_updates            | int(11) unsigned                  | NO   |     | 0       |       |
| max_connections        | int(11) unsigned                  | NO   |     | 0       |       |
| max_user_connections   | int(11) unsigned                  | NO   |     | 0       |       |
| plugin                 | char(64)                          | YES  |     |         |       |
| authentication_string  | text                              | YES  |     | NULL    |       |
+------------------------+-----------------------------------+------+-----+---------+-------+
42 rows in set (0.00 sec)
```

Privilege columns

MySQL : security measures



```
mysql> describe user;
+------------------------+-----------------------------------+------+-----+---------+-------+
| Field                  | Type                              | Null | Key | Default | Extra |
+------------------------+-----------------------------------+------+-----+---------+-------+
| Host                   | char(60)                          | NO   | PRI |         |       |
| User                   | char(16)                          | NO   | PRI |         |       |
| Password               | char(41)                          | NO   |     |         |       |
| Select_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Insert_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Update_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Delete_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Create_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Drop_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Reload_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Shutdown_priv          | enum('N','Y')                     | NO   |     | N       |       |
| Process_priv           | enum('N','Y')                     | NO   |     | N       |       |
| File_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Grant_priv             | enum('N','Y')                     | NO   |     | N       |       |
| References_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Index_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Alter_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Show_db_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Super_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Create_tmp_table_priv  | enum('N','Y')                     | NO   |     | N       |       |
| Lock_tables_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Execute_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Repl_slave_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Repl_client_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Create_view_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Show_view_priv         | enum('N','Y')                     | NO   |     | N       |       |
| Create_routine_priv    | enum('N','Y')                     | NO   |     | N       |       |
| Alter_routine_priv     | enum('N','Y')                     | NO   |     | N       |       |
| Create_user_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Event_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Trigger_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Create_tablespace_priv | enum('N','Y')                     | NO   |     | N       |       |
| ssl_type               | enum('','ANY','X509','SPECIFIED') | NO   |     |         |       |
| ssl_cipher             | blob                              | NO   |     | NULL    |       |
| x509_issuer            | blob                              | NO   |     | NULL    |       |
| x509_subject           | blob                              | NO   |     | NULL    |       |
| max_questions          | int(11) unsigned                  | NO   |     | 0       |       |
| max_updates            | int(11) unsigned                  | NO   |     | 0       |       |
| max_connections        | int(11) unsigned                  | NO   |     | 0       |       |
| max_user_connections   | int(11) unsigned                  | NO   |     | 0       |       |
| plugin                 | char(64)                          | YES  |     |         |       |
| authentication_string  | text                              | YES  |     | NULL    |       |
+------------------------+-----------------------------------+------+-----+---------+-------+

42 rows in set (0.00 sec)
```

Security columns

MySQL : security measures

How to specify account names:

- Syntax: CREATE USER '***user_name***'@'***host_name***'.
- Note: 'me'@'localhost' **not** 'me@localhost'
- The **`user`** table contains one row for each account
- The **User** and **Host** columns store the username and host name
- Hostname part of the account can have:
  - computer or device name
  - IP address
  - Wildcards: % or _ e.g '198.51.100.%'

MySQL : security measures

How to specify account names – hostname examples

- `198.0.0.0/255.0.0.0`: Any host on the 198 class A network

- `198.51.100.0/255.255.0.0`: Any host on the 198.51 class B network

- `198.51.100.0/255.255.255.0`: Any host on the 198.51.100 class C network

- `198.51.100.1`: Only the host with this specific IP address

Network classification basics

•**Class A** network has subnet mask **255.0.0.0** with first octet range 0 - 127.

✓ E.g IP **124.52.36.11.** First octet is 124 (between 1 and 126).

•**Class B** network has subnet mask **255.255.0.0** with first octet range 128 - 191.

✓ E.g **129.16.52.63.** First octet is 129 (between 128 and 191)

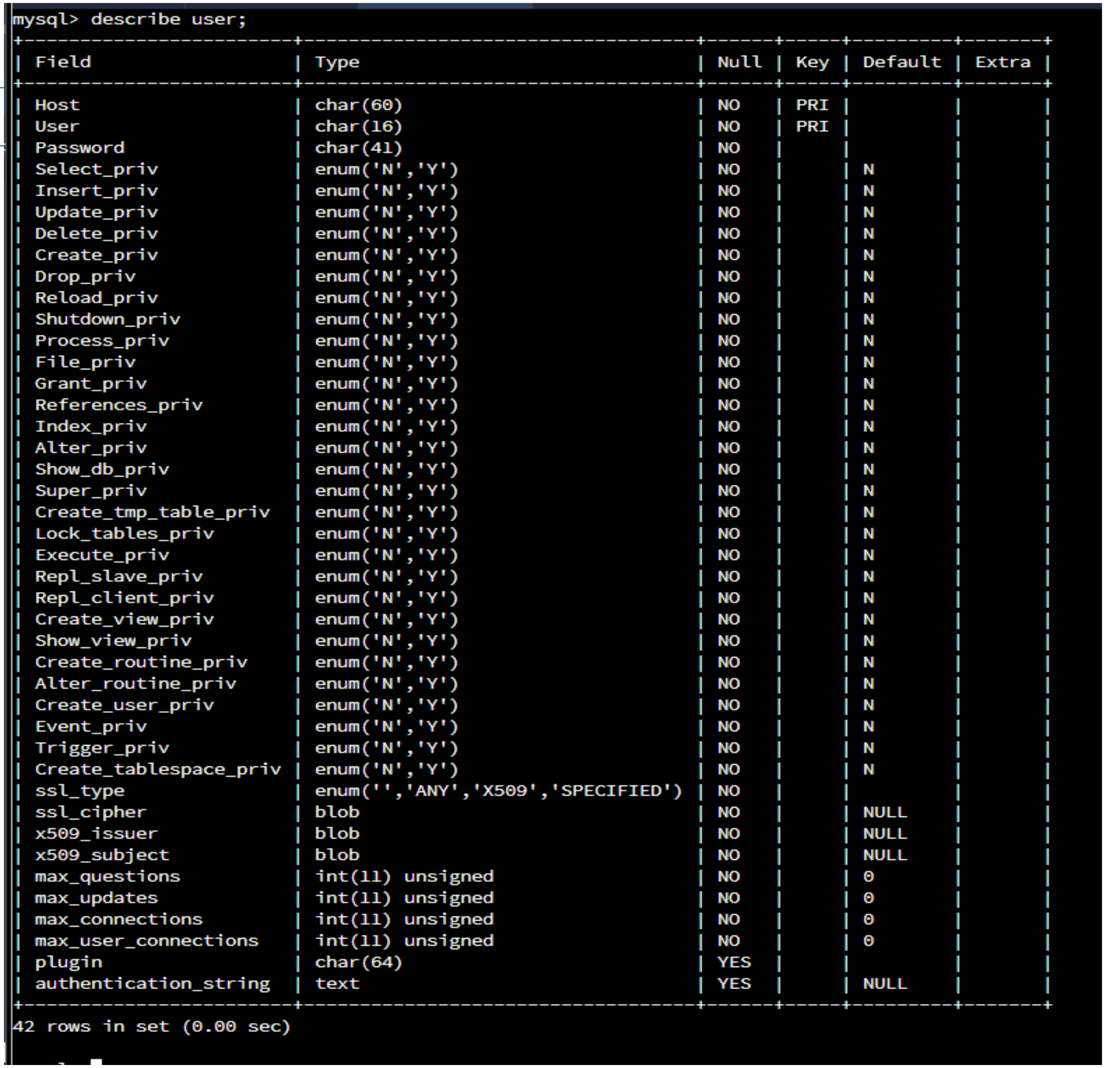
•**Class C** network has subnet mask **255.255.255.0** with first octet range 192-223.

✓ E.g **192.168.123.132**. First octet is 192 (between 192 and 223)

Adapted from: https://www.vskills.in/certification/tutorial/a-b-and-c-classes-of-networks/

MySQL : security measures

Scope columns



```
mysql> describe user;
+------------------------+-----------------------------------+------+-----+---------+-------+
| Field                  | Type                              | Null | Key | Default | Extra |
+------------------------+-----------------------------------+------+-----+---------+-------+
| Host                   | char(60)                          | NO   | PRI |         |       |
| User                   | char(16)                          | NO   | PRI |         |       |
| Password               | char(41)                          | NO   |     |         |       |
| Select_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Insert_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Update_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Delete_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Create_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Drop_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Reload_priv            | enum('N','Y')                     | NO   |     | N       |       |
| Shutdown_priv          | enum('N','Y')                     | NO   |     | N       |       |
| Process_priv           | enum('N','Y')                     | NO   |     | N       |       |
| File_priv              | enum('N','Y')                     | NO   |     | N       |       |
| Grant_priv             | enum('N','Y')                     | NO   |     | N       |       |
| References_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Index_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Alter_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Show_db_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Super_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Create_tmp_table_priv  | enum('N','Y')                     | NO   |     | N       |       |
| Lock_tables_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Execute_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Repl_slave_priv        | enum('N','Y')                     | NO   |     | N       |       |
| Repl_client_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Create_view_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Show_view_priv         | enum('N','Y')                     | NO   |     | N       |       |
| Create_routine_priv    | enum('N','Y')                     | NO   |     | N       |       |
| Alter_routine_priv     | enum('N','Y')                     | NO   |     | N       |       |
| Create_user_priv       | enum('N','Y')                     | NO   |     | N       |       |
| Event_priv             | enum('N','Y')                     | NO   |     | N       |       |
| Trigger_priv           | enum('N','Y')                     | NO   |     | N       |       |
| Create_tablespace_priv | enum('N','Y')                     | NO   |     | N       |       |
| ssl_type               | enum('','ANY','X509','SPECIFIED') | NO   |     |         |       |
| ssl_cipher             | blob                              | NO   |     | NULL    |       |
| x509_issuer            | blob                              | NO   |     | NULL    |       |
| x509_subject           | blob                              | NO   |     | NULL    |       |
| max_questions          | int(11) unsigned                  | NO   |     | 0       |       |
| max_updates            | int(11) unsigned                  | NO   |     | 0       |       |
| max_connections        | int(11) unsigned                  | NO   |     | 0       |       |
| max_user_connections   | int(11) unsigned                  | NO   |     | 0       |       |
| plugin                 | char(64)                          | YES  |     |         |       |
| authentication_string  | text                              | YES  |     | NULL    |       |
+------------------------+-----------------------------------+------+-----+---------+-------+
42 rows in set (0.00 sec)
```

MySQL : security measures

Example:

```
CREATE USER 'david'@'198.51.100.0/255.255.255.0';
```

MySQL : security measures

The root account

- All privileges

- Access to the root

```
mysql -u root -p
Enter password: (enter root password here)
```

MySQL : security measures

Assigning password to accounts:

```
CREATE USER ‘jsmith'@'localhost' IDENTIFIED BY 'password’;
```

Changing password:

```
ALTER USER ‘jsmith'@'localhost' IDENTIFIED BY 'password';
```

MySQL : security measures

Encrypted connections:

- Server-side
- Client-side
- Mandatory

MySQL : security measures

Server-side encrypted connections:

➢ Update system variables in my.cnf file with these lines

[mysqld]

- ssl_ca=ca.pem ##path name for the CA certificate file
- ssl_cert=server-cert.pem ## the path name for the **public** key certificate file
- ssl_key=server-key.pem ## the path name for the server **private** key file

MySQL : security measures

Client-side encrypted connections:

- Client programs attempt to establish an encrypted connection if the server supports encrypted connections by default

```
mysql --ssl-mode=PREFERRED

mysql --ssl-mode=REQUIRED
```

MySQL : security measures

Mandatory encrypted connections:

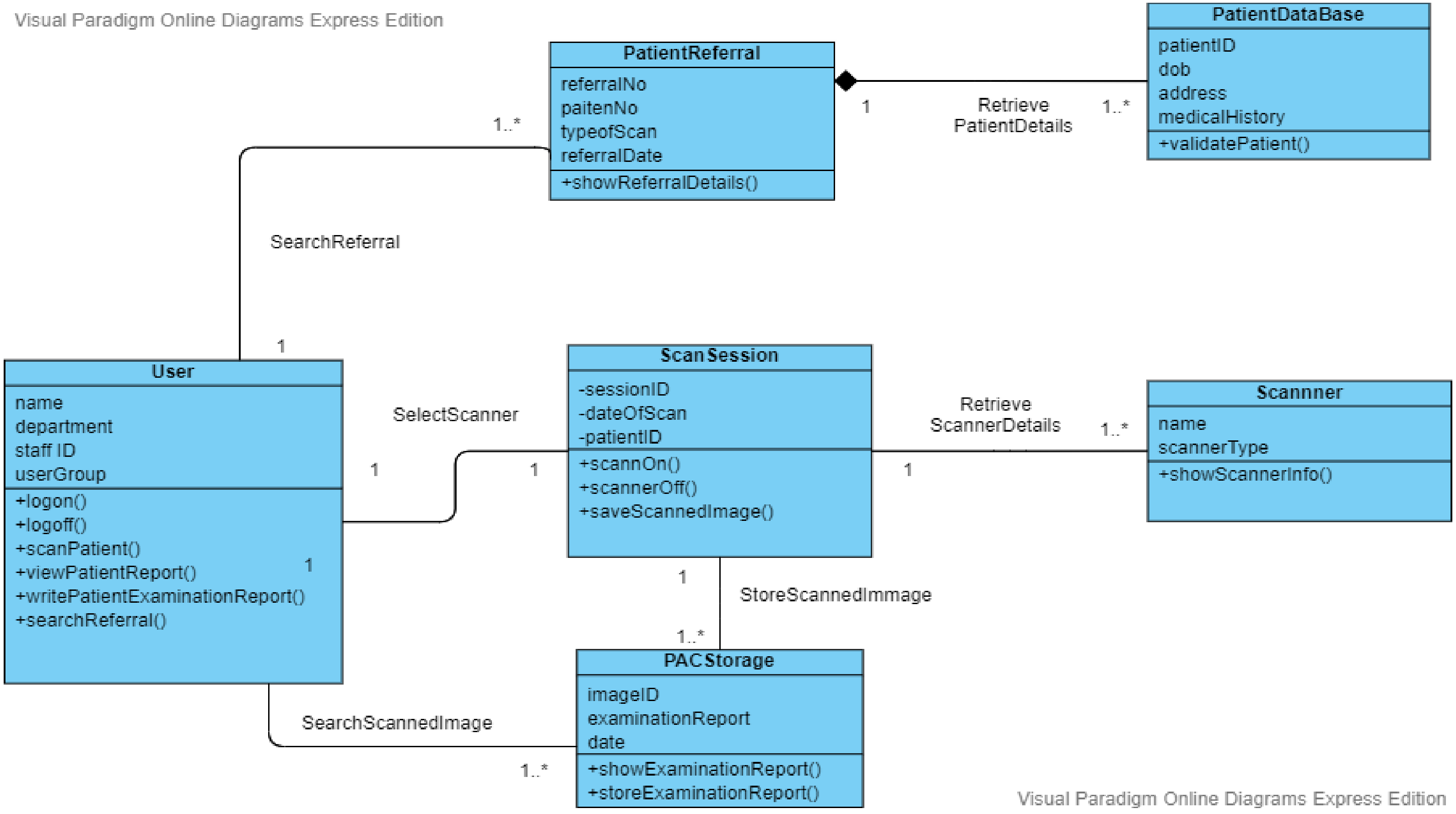
Update system variables in my.cnf file with these lines

[mysqld]

- ssl_ca=ca.pem ##path name of the CA certificate file
- ssl_cert=server-cert.pem ## the path name for the public key certificate file
- ssl_key=server-key.pem ## the path name of the server private key file

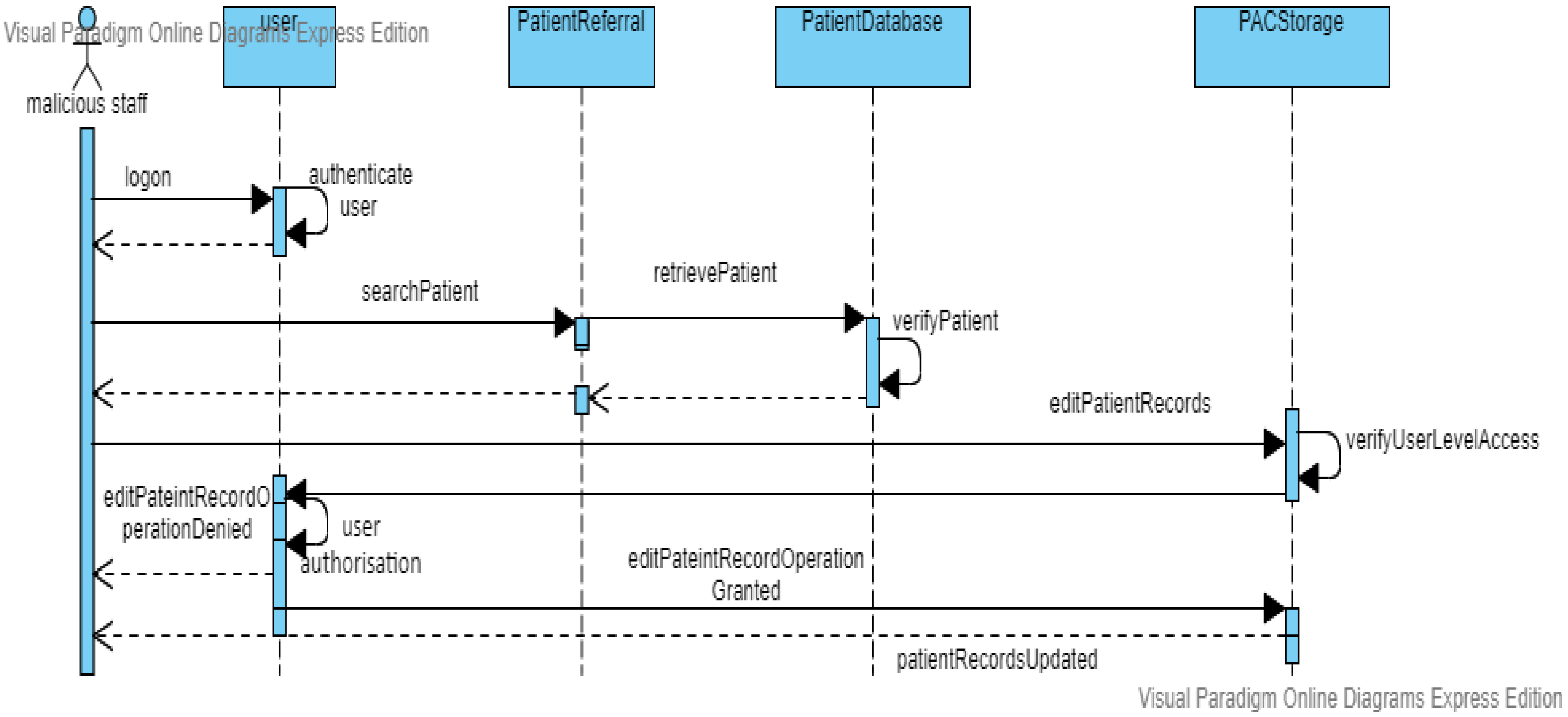
- require_secure_transport=ON ## specifies client is required to use encrypted connection

Application to PACs

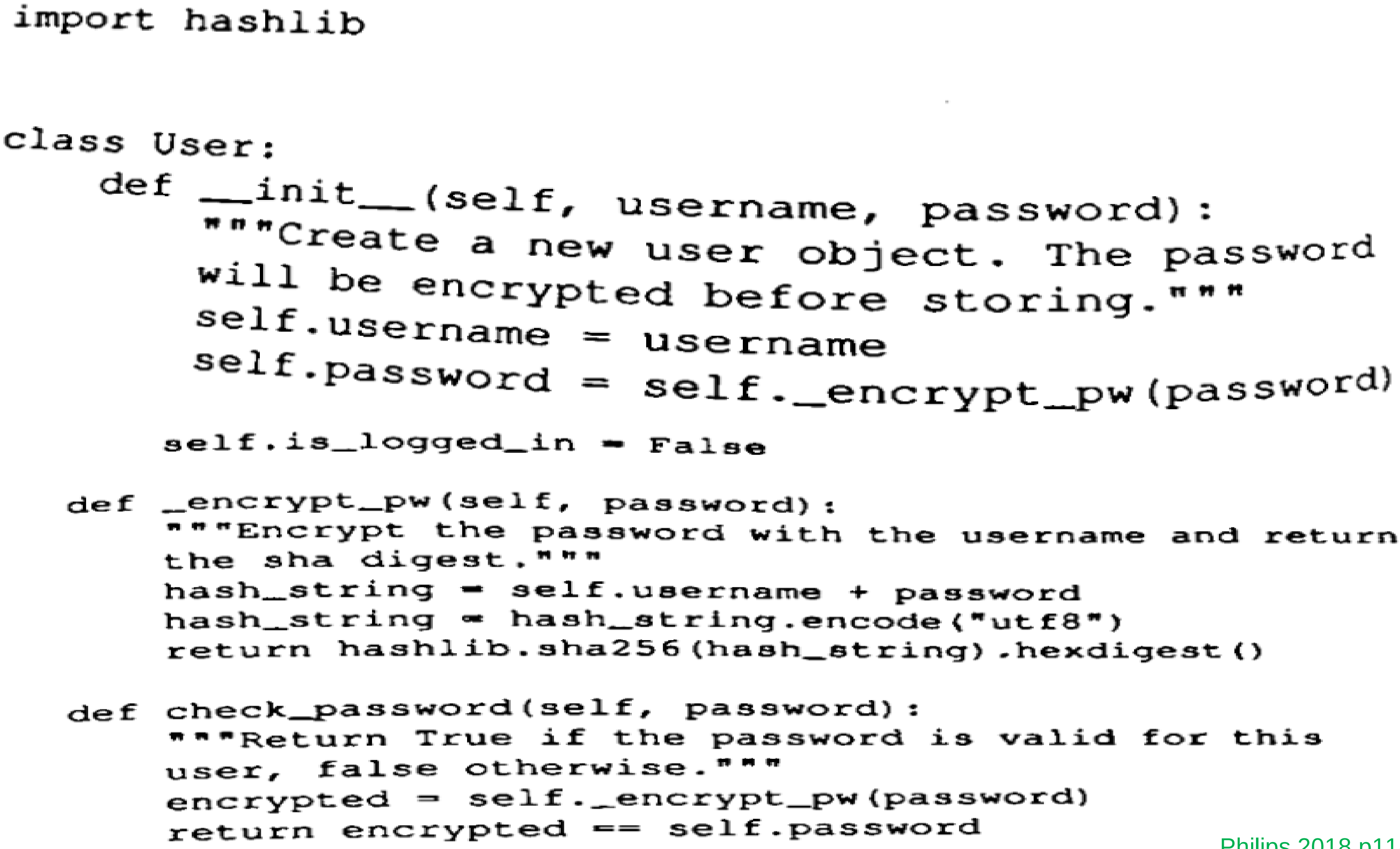


University of Essex
Online

Application to PACs



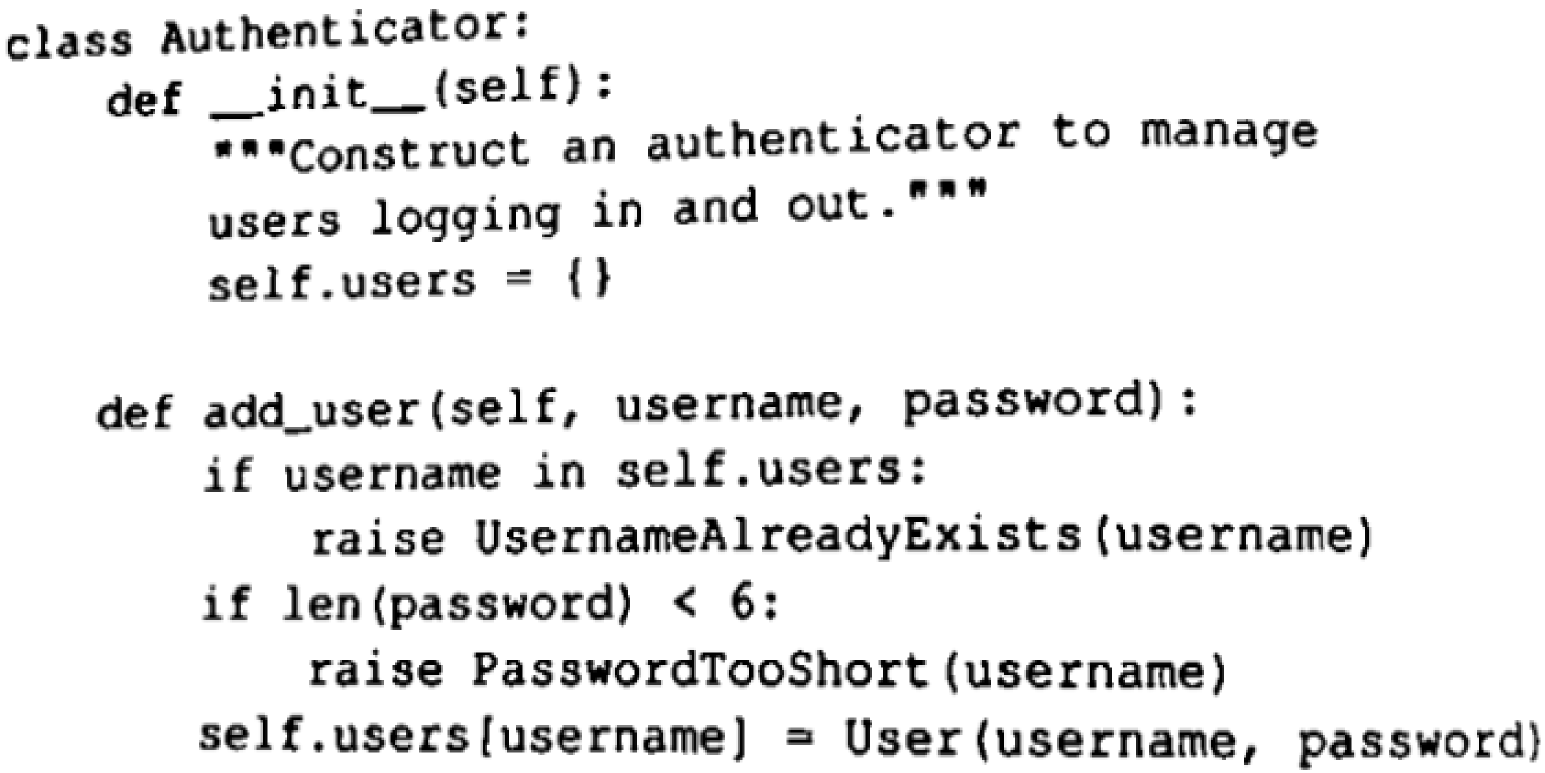
Python: security measures



```
import hashlib


class User:
    def __init__(self, username, password):
        """Create a new user object. The password
        will be encrypted before storing."""
        self.username = username
        self.password = self._encrypt_pw(password)

        self.is_logged_in = False

    def _encrypt_pw(self, password):
        """Encrypt the password with the username and return
        the sha digest."""
        hash_string = self.username + password
        hash_string = hash_string.encode("utf8")
        return hashlib.sha256(hash_string).hexdigest()

    def check_password(self, password):
        """Return True if the password is valid for this
        user, false otherwise."""
        encrypted = self._encrypt_pw(password)
        return encrypted == self.password
```

Philips,2018.p118-119

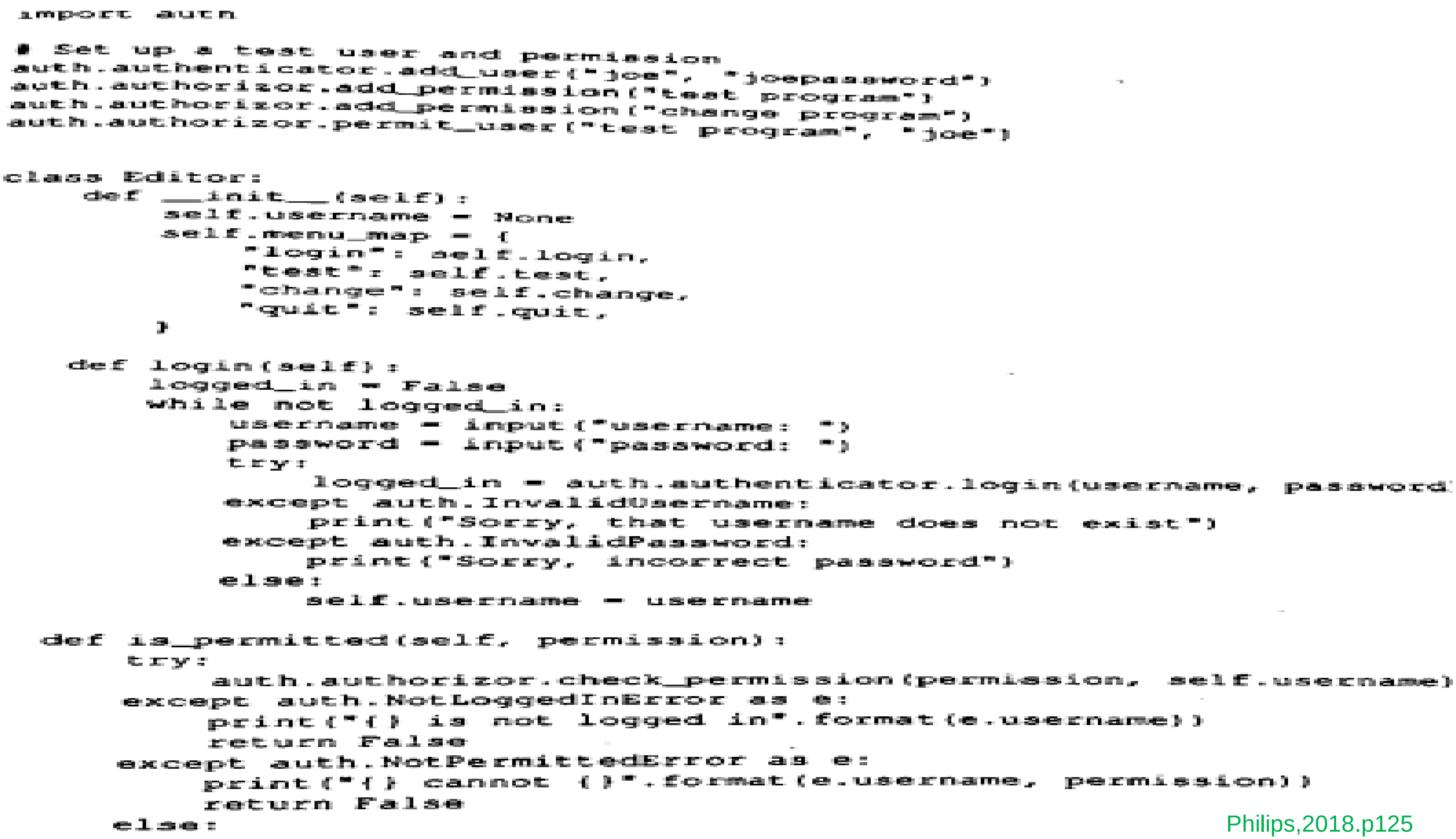
Python: security measures



```
class Authenticator:
    def __init__(self):
        """Construct an authenticator to manage
        users logging in and out."""
        self.users = {}

    def add_user(self, username, password):
        if username in self.users:
            raise UsernameAlreadyExists(username)
        if len(password) < 6:
            raise PasswordTooShort(username)
        self.users[username] = User(username, password)
```

Philips,2018.p118-119

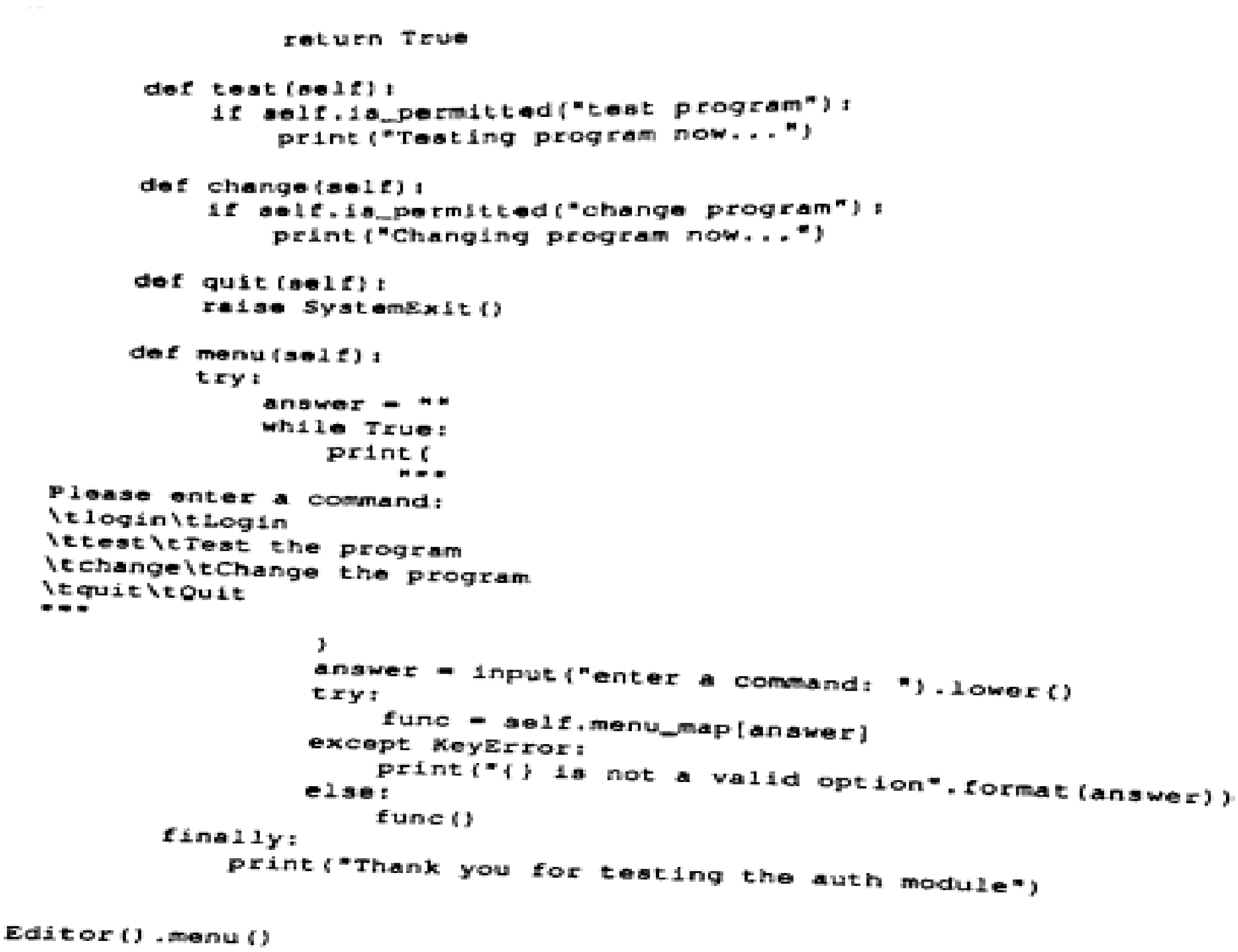
Python: security measures



```
import auth

# Set up a test user and permission
auth.authenticator.add_user("joe", "joepassword")
auth.authorizor.add_permission("test program")
auth.authorizor.add_permission("change program")
auth.authorizor.permit_user("test program", "joe")

class Editor:
        def __init__(self):
                self.username = None
                self.menu_map = {
                        "login": self.login,
                        "test": self.test,
                        "change": self.change,
                        "quit": self.quit,
                }

        def login(self):
                logged_in = False
                while not logged_in:
                        username = input("username: ")
                        password = input("password: ")
                        try:
                                logged_in = auth.authenticator.login(username, password
                        except auth.InvalidUsername:
                                print("Sorry, that username does not exist")
                        except auth.InvalidPassword:
                                print("Sorry, incorrect password")
                        else:
                                self.username = username

        def is_permitted(self, permission):
                try:
                        auth.authorizor.check_permission(permission, self.username)
                except auth.NotLoggedInError as e:
                        print("{} is not logged in".format(e.username))
                        return False
                except auth.NotPermittedError as e:
                        print("{} cannot {}".format(e.username, permission))
                        return False
                else:
```

Philips,2018.p125

Python: security measures



```
            return True

    def test(self):
        if self.is_permitted("test program"):
            print("Testing program now...")

    def change(self):
        if self.is_permitted("change program"):
            print("Changing program now...")

    def quit(self):
        raise SystemExit()

    def menu(self):
        try:
            answer = ""
            while True:
                print(
                    """
Please enter a command:
\tlogin\tLogin
\ttest\tTest the program
\tchange\tChange the program
\tquit\tQuit
"""
                )
                answer = input("enter a command: ").lower()
                try:
                    func = self.menu_map[answer]
                except KeyError:
                    print("{} is not a valid option".format(answer))
                else:
                    func()
        finally:
            print("Thank you for testing the auth module")

Editor().menu()
```

Philips,2018.p126

Questions

Any other questions ?