COMP3335 Assignment 1

Name: JIANG Guanlin

Student ID: 21093962D

Exercise 1: Database Normalization

Question 1

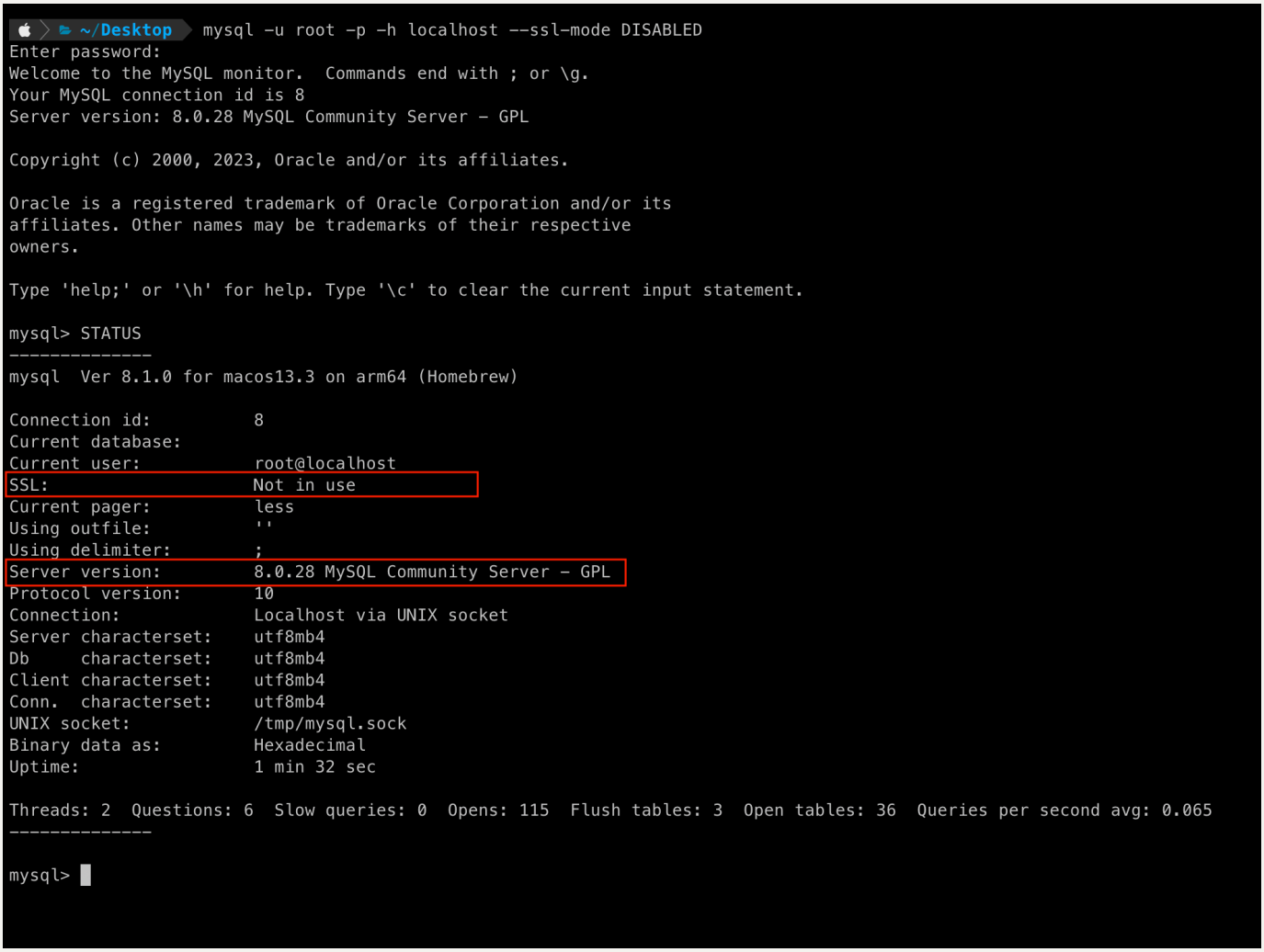
- Partial dependency
    - TxID <- (Qty, TotalPrice, CustomerName, Salesperson)
    - ProductID <- (ProductName, UnitPrice)

Question 3

- Transitive Dependencies
    - CommRate <- Salesperson

Exercise 3: Securing Data-in-motion in MySQL

Question 1



Question 2

The ssl-mode I choose is REQUIRED.

```
~/Desktop mysql -u root -p -h localhost --ssl-mode=REQUIRED
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.28 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

You are enforcing ssl connection via unix socket. Please consider
switching ssl off as it does not make connection via unix socket
any more secure.
mysql> STATUS
--------------
mysql  Ver 8.1.0 for macos13.3 on arm64 (Homebrew)

Connection id:          9
Current database:
Current user:           root@localhost
SSL:                    Cipher in use is TLS_AES_256_GCM_SHA384
Current pager:          less
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.28 MySQL Community Server - GPL
Protocol version:       10
Connection:             Localhost via UNIX socket
Server characterset:    utf8mb4
Db     characterset:    utf8mb4
Client characterset:    utf8mb4
Conn.  characterset:    utf8mb4
UNIX socket:            /tmp/mysql.sock
Binary data as:         Hexadecimal
Uptime:                 1 hour 8 min 32 sec

Threads: 2  Questions: 12  Slow queries: 0  Opens: 115  Flush tables: 3  Open tables: 36  Queries per second avg: 0.002
--------------
```

Question 3

The issuer is: CN = MySQL_Server_8.0.28_Auto_Generated_CA_Certificate Validity

```
~/Desktop openssl x509 -text -in server-cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = MySQL_Server_8.0.28_Auto_Generated_CA_Certificate
        Validity
            Not Before: Aug  8 02:18:42 2023 GMT
            Not After : Aug  5 02:18:42 2033 GMT
        Subject: CN = MySQL_Server_8.0.28_Auto_Generated_Server_Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b7:fc:9e:ff:aa:e8:9c:28:dc:d3:e5:8d:08:12:
                    f1:11:43:32:f6:f0:13:69:fd:e6:9a:6e:36:d7:b5:
                    6e:94:d8:ab:42:33:ef:be:6c:38:8a:59:33:1d:92:
                    db:8b:1d:7c:e1:3a:97:97:f1:63:ce:52:47:f2:73:
                    e3:0d:82:43:dc:bd:ae:af:0a:ee:67:67:2c:b9:e4:
                    11:95:41:d8:58:0d:e4:5c:21:11:97:50:59:73:63:
                    8e:b2:9e:bd:7b:01:87:75:7c:49:dd:bd:ee:e0:6d:
                    eb:15:3a:4d:1c:97:c9:3d:c4:60:e4:0c:27:5f:49:
                    34:76:a0:eb:01:d7:f1:02:f1:74:dc:f5:2f:4b:67:
                    10:18:bc:e9:9b:43:b9:e6:44:db:da:bd:08:85:2e:
```

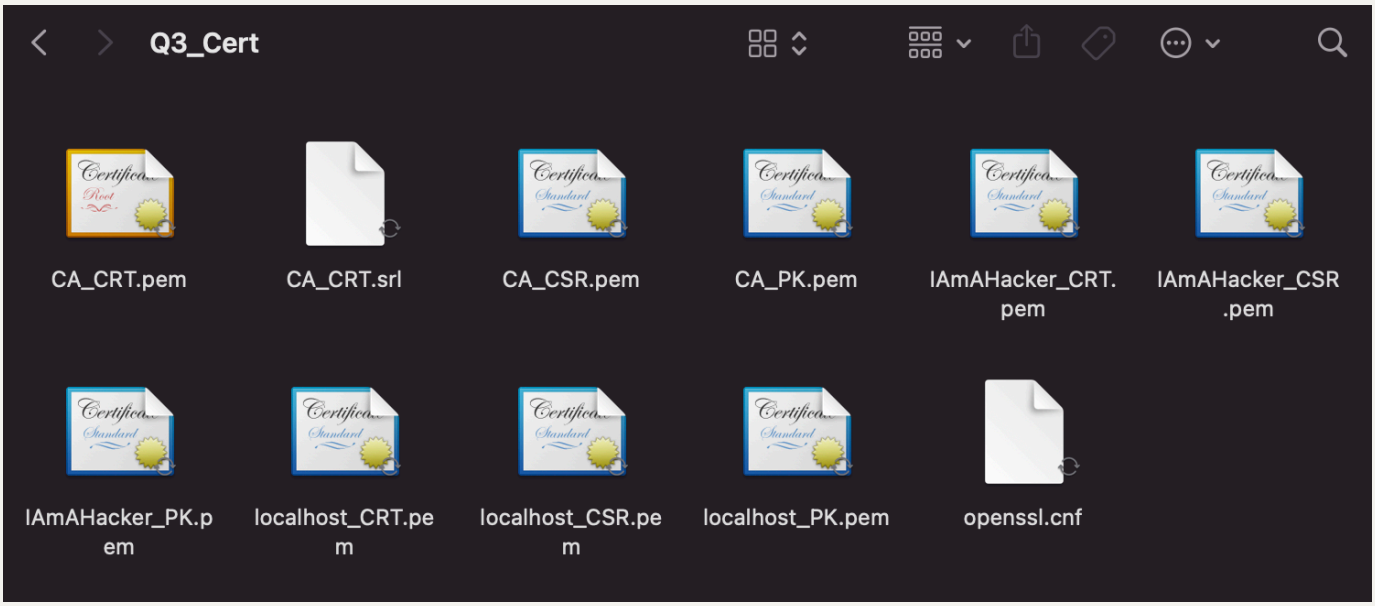
```
                    bb:23:ed:f3:81:e0:b8:ef:8d:e4:dc:24:cd:37:ad:
                    27:8d:a5:ad:7e:04:07:58:c3:0d:98:01:cf:a1:2f:
                    be:6c:48:56:06:1e:01:8d:27:60:c7:db:51:bc:ff:
                    c1:51:4d:f9:6e:05:29:0f:e8:a4:27:5b:e3:bc:6e:
                    9a:ce:cc:f6:a6:94:72:4f:8b:fd:cb:ba:e6:90:31:
                    d3:cf:d0:4e:51:f6:37:25:c2:63:5d:ee:13:2d:0f:
                    74:3b:c9:fe:a0:07:60:32:e6:f4:1c:06:09:98:aa:
                    34:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         76:64:c5:d4:bc:9e:f9:02:c4:1f:a9:6f:dd:2f:bb:17:ee:2e:
         3d:d3:56:7a:b6:1d:5e:f8:1f:d8:15:f0:7c:52:7e:99:62:da:
         03:d7:2c:68:9e:36:91:e6:98:88:79:c0:43:96:74:6b:03:e9:
         ae:0c:bb:a2:d4:98:d7:d8:32:cf:4e:a0:69:df:05:34:6e:8b:
         2e:cc:3f:9c:3b:58:2f:ad:48:7f:8c:94:ec:b3:b9:ee:b9:20:
         a1:73:11:12:01:69:f5:f0:41:61:be:4e:6d:45:29:5c:fa:d8:
         4a:40:36:c9:92:0e:71:d7:55:a1:f3:45:af:05:51:71:bc:b9:
         72:8a:75:87:60:db:38:a8:ca:b2:73:72:1f:e0:20:83:34:e8:
         d6:4f:ca:ce:b3:95:74:61:23:18:bb:f0:0a:ae:c1:b9:3a:e9:
         6b:30:62:8b:33:05:75:9a:8c:fa:f2:47:45:7c:6b:29:81:6e:
         66:ec:04:4b:5f:fc:4b:eb:af:2b:87:7a:e3:7a:05:10:de:b5:
         77:c3:f1:68:5f:04:05:01:49:5c:04:37:e6:d9:49:7f:8e:f2:
         3d:f7:62:d3:6f:91:7a:4b:e1:b7:89:e5:a4:78:ec:0d:ef:b5:
         18:61:ac:25:b0:89:a3:7f:98:36:f8:65:6d:fc:c5:5f:b3:e2:
         8c:20:71:06
-----BEGIN CERTIFICATE-----
MIIDBzCCAe+gAwIBAgIBAjANBgkqhkiG9w0BAQsFADA8MTowOAYDVQQDDDFNeVNR
TF9TZXJ2ZXJfOC4wLjI4X0F1dG9fR2VuZXJhdGVkX0NBX0NlcnRpZmljYXRlMB4X
DTIzMDgwODAyMTg0MloXDTMzMDgwNTAyMTg0MlowQDE+MDwGA1UEAww1TXlTUUxf
U2VydmVyXzguMC4yOF9BdXRvX0dlbmVyYXRlZF9TZXJ2ZXJfQ2VydGlmaWNhdGUw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3/J7/quicKNzT5Y0IEvER
QzL28BNp/eaabjbXtW6U2KtCM+++bDiKWTMdktuLHXzhOpeX8WPOUkfyc+MNgkPc
va6vCu5nZyy55BGVQdhYDeRcIRGXUFlzY46ynr17AYd1fEndve7gbesVOk0cl8k9
xGDkDCdfSTR2oOsB1/EC8XTc9S9LZxAYvOmbQ7nmRNvavQiFLrsj7fOB4LjvjeTc
JM03rSeNpa1+BAdYww2YAc+hL75sSFYGHgGNJ2DH21G8/8FRTfluBSkP6KQnW+O8
bprOzPamlHJPi/3LuuaQMdPP0E5R9jclwmNd7hMtD3Q7yf6gB2Ay5vQcBgmYqjQh
AgMBAAGjEDAOMAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggEBAHZkxdS8
nvkCxB+pb90vuxfuLj3TVnq2HV74H9gV8HxSfpli2gPXLGieNpHmmIh5wEOWdGsD
6a4Mu6LUmNfYMs9OoGnfBTRuiy7MP5w7WC+tSH+MlOyzue65IKFzERIBafXwQWG+
Tm1FKVz62EpANsmSDnHXVaHzRa8FUXG8uXKKdYdg2zioyrJzch/gIIM06NZPys6z
lXRhIxi78Aquwbk66WswYoszBXWajPryR0V8aymBbmbsBEtf/EvrryuHeuN6BRDe
tXfD8WhfBAUBSVwEN+bZSX+O8j33YtNvkXpL4beJ5aR47A3vtRhhrCWwiaN/mDb4
ZW38xV+z4owgcQY=
-----END CERTIFICATE-----
```

Question 4

```
## Own CA
openssl ecparam -out CA_PK.pem -name prime256v1 -genkey

openssl req -new -key CA_PK.pem -out CA_CSR.pem -config openssl.cnf

openssl req -x509 -key CA_PK.pem -in CA_CSR.pem -out CA_CRT.pem -
days 365 -config openssl.cnf
```

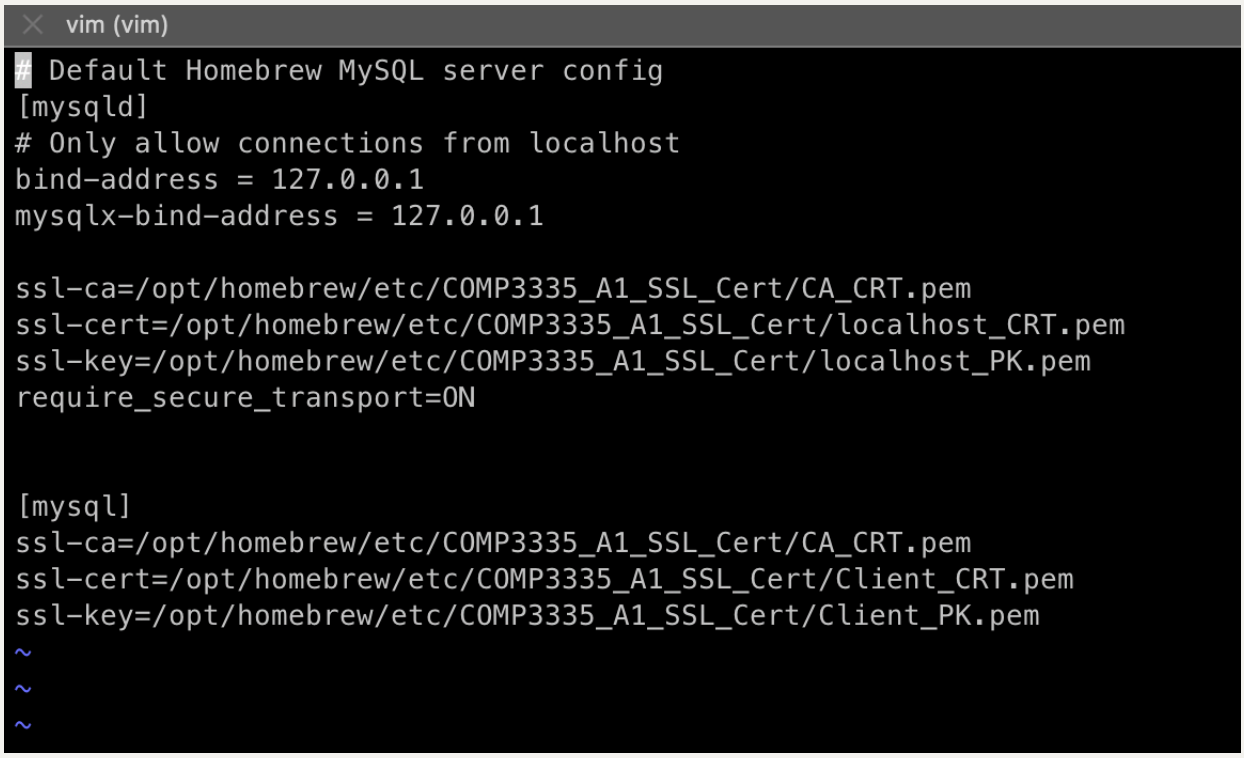
```
## IAmAHacker.com
openssl ecparam -out IAmAHacker_PK.pem -name prime256v1 -genkey

openssl req -new -key IAmAHacker_PK.pem -out IAmAHacker_CSR.pem -
config openssl.cnf

openssl x509 -req -in IAmAHacker_CSR.pem -CA CA_CRT.pem -CAkey
CA_PK.pem -CAcreateserial -out IAmAHacker_CRT.pem -days 365

## LocalHost
openssl ecparam -out localhost_PK.pem -name prime256v1 -genkey

openssl req -new -key localhost_PK.pem -out localhost_CSR.pem -
config openssl.cnf

openssl x509 -req -in localhost_CSR.pem -CA CA_CRT.pem -CAkey
CA_PK.pem -CAcreateserial -out localhost_CRT.pem -days 365
```

```
~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl ecparam -out CA_PK.pem -name prime256v1 -genkey

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl req -new -key CA_PK.pem -out CA_CSR.pem -config openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [HK]:
State or Province Name (full name) [Kowloon]:
Locality Name (eg, city) []:
Organization Name (eg, company) [PolyU]:
Organizational Unit Name (eg, section) [COMP3335]:
Common Name (e.g. server FQDN or YOUR name) []:Guanlin Jiang
Email Address []:

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl req -x509 -key CA_PK.pem -in CA_CSR.pem -out CA_CRT.pem -days 365 -
config openssl.cnf
Warning: No -copy_extensions given; ignoring any extensions in the request

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl ecparam -out IAmAHacker_PK.pem -name prime256v1 -genkey

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl req -new -key IAmAHacker_PK.pem -out IAmAHacker_CSR.pem -config ope
nssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [HK]:
State or Province Name (full name) [Kowloon]:
Locality Name (eg, city) []:
Organization Name (eg, company) [PolyU]:
Organizational Unit Name (eg, section) [COMP3335]:
Common Name (e.g. server FQDN or YOUR name) []:IAmAHacker.com
Email Address []:

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl x509 -req -in IAmAHacker_CSR.pem -CA CA_CRT.pem -CAkey CA_PK.pem -C
Acreateserial -out IAmAHacker_CRT.pem -days 365
Certificate request self-signature ok
subject=C = HK, ST = Kowloon, O = PolyU, OU = COMP3335, CN = IAmAHacker.com

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl ecparam -out localhost_PK.pem -name prime256v1 -genkey

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl req -new -key localhost_PK.pem -out localhost_CSR.pem -config opens
sl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [HK]:
State or Province Name (full name) [Kowloon]:
Locality Name (eg, city) []:
Organization Name (eg, company) [PolyU]:
Organizational Unit Name (eg, section) [COMP3335]:
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert openssl x509 -req -in localhost_CSR.pem -CA CA_CRT.pem -CAkey CA_PK.pem -CA
createserial -out localhost_CRT.pem -days 365
Certificate request self-signature ok
subject=C = HK, ST = Kowloon, O = PolyU, OU = COMP3335, CN = localhost

~/L/Cl/OneDrive-P/HK/3/Sem 1/COMP33/A/A/Q3_Cert                                    ✔ base 14:09:35
```



Question 5

```
## Client
openssl ecparam -out Client_PK.pem -name prime256v1 -genkey

openssl req -new -key Client_PK.pem -out Client_CSR.pem -config
openssl.cnf

openssl x509 -req -in Client_CSR.pem -CA CA_CRT.pem -CAkey
CA_PK.pem -CAcreateserial -out Client_CRT.pem -days 365
```



- Server [my.cnf]

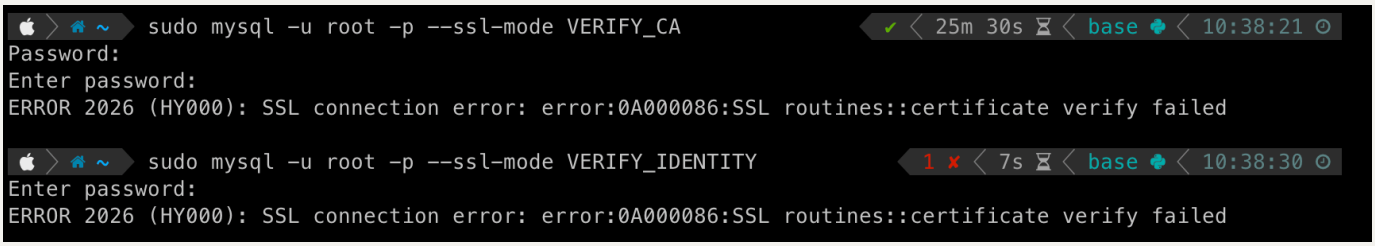
```
ssl-ca=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/CA_CRT.pem
ssl-cert=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/localhost_CRT.pem
ssl-key=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/localhost_PK.pem
require_secure_transport=ON
```

- Client [my.cnf]

```
ssl-ca=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/CA_CRT.pem
ssl-cert=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/Client_CRT.pem
ssl-key=/opt/homebrew/etc/COMP3335_A1_SSL_Cert/Client_PK.pem
```

Question 6

```
sudo mysql -u root -p --ssl-mode VERIFY_CA
sudo mysql -u root -p --ssl-mode VERIFY_IDENTITY
```



- The answer is failed. The reason is I use the self signed SSL Certification, which is not verify by CA, also not trusted, so I can't into MySQL database.