

BASE DE DADES

CERTIFICAT CLIENT



NOM: *Bixiang Zhu*

CURS: *1r ASIX*

ESCOLA: *InstitutMVM*



ÍNDEX

ÍNDEX	2
CERTIFICAT DIGITAL	3
PREREQUISITS	3
GENERACIÓ DE CLAUS	3
CERTIFICAT CLIENT	4
VERIFICAR CERTIFICACIÓ	4
CREACIÓ USUARI	4
VERIFICACIÓ CERTIFICAT	5
PASAR L'ARXIU EL CLIENT	6
CONNEXIÓ EN REMOT	7
CREACIÓ BASE DE DADES	8
CREACIÓ I INSERTS DE LA TAULA	8
MD5 AMB 8 DIGITS	9
VERIFICACIÓ	10
DESENCRIPTAR LA CONTRASEÑA	10
ALTRES ENCRIPCIÓN I DESENCRIPTACIÓN	10

CERTIFICAT DIGITAL

PREREQUISITS

Crearem una carpeta per guardar les dades amb *mkdir 'nom_carpeta'*:

```
usuari@debian12: ~/certificat
usuari@debian12:~$ mkdir certificat
usuari@debian12:~$ cd certificat
usuari@debian12:~/certificat$ ls
usuari@debian12:~/certificat$
```

GENERACIÓ DE CLAUS

Primer generarem una clau privada i una sollicitud de certificat.

```
usuari@debian12: ~/certificat
usuari@debian12:~/certificat$ openssl req -newkey rsa:2048 -days 365 -nodes -keyout bzhu-key.pem -out bzhu-req.pem
Ignoring -days without -x509; not generating a certificate
.....
-----
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) [AU]:C
String too short, must be at least 2 bytes long
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Catalunya
Locality Name (eg, city) []:Barcelona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MYSQL
Organizational Unit Name (eg, section) []:Community
Common Name (e.g. server FQDN or YOUR name) []:bzhu
Email Address []:bzhu@institutmvm.cat

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:MYSQL
usuari@debian12:~/certificat$ ls
bzhu-key.pem  bzhu-req.pem
usuari@debian12:~/certificat$
```

CERTIFICAT CLIENT

Crearem un certificat pel client de 356 dies

```
usuari@debian12:~/certificat$ sudo openssl x509 -req -in bzhu-req.pem -days 365 -CA /var/lib/mysql/ca.pem  
-CAkey /var/lib/mysql/ca-key.pem -set_serial 01 -out bzhu-cert.pem  
Certificate request self-signature ok  
subject=C = ES, ST = Catalunya, L = Barcelona, O = MYSQL, OU = Community, CN = bzhu, emailAddress = bzhu@i  
nstitutmvm.cat  
usuari@debian12:~/certificat$ ls  
bzhu-cert.pem bzhu-key.pem bzhu-req.pem  
usuari@debian12:~/certificat$
```

VERIFICAR CERTIFICACIÓ

Per verificar l'autenticació del certificat generat utilitzarem la següent comanda 'sudo
openssl verify -CAfile /var/lib/mysql/ca.pem /var/lib/mysql/server-cert.pem bzhu-cert.pem '

```
usuari@debian12:~/certificat$ sudo openssl verify -CAfile /var/lib/mysql/ca.pem /var/lib/mysql/server-cert.pem bzhu-cert.pem  
/var/lib/mysql/server-cert.pem: OK  
bzhu-cert.pem: OK  
usuari@debian12:~/certificat$
```

CREACIÓ USUARI

Crearem un usuari en mysql

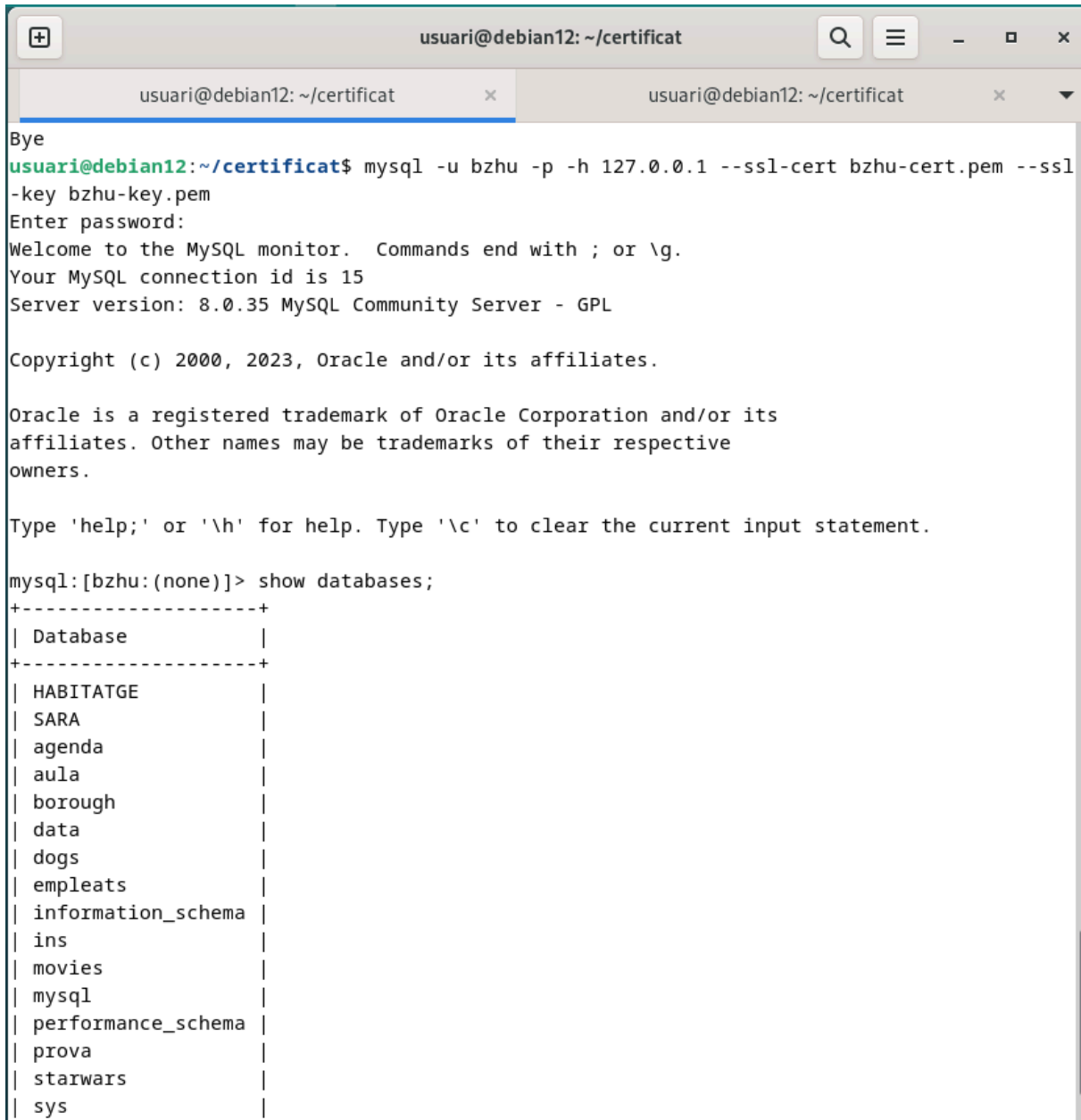
```
usuari@debian12:~/certificat$ mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 13  
Server version: 8.0.35 MySQL Community Server - GPL  
  
Copyright (c) 2000, 2023, Oracle and/or its affiliates.  
  
Oracle is a registered 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.  
  
mysql:[root:(none)]> CREATE USER 'bzhu'@'%' IDENTIFIED BY '1234' REQUIRE SUBJECT '/C=ES/ST  
=Catalunya/L=Barcelona/O=MYSQL/OU=Community/CN=bzhu/emailAddress=bzhu@institutmvm.cat';  
Query OK, 0 rows affected (2,13 sec)  
  
mysql:[root:(none)]> █
```

Ara li donarem permisos l'usuari creat

```
mysql:[root:(none)]> GRANT ALL ON *.* TO 'bzhu'@'%';  
Query OK, 0 rows affected (0,59 sec)  
  
mysql:[root:(none)]> █
```

VERIFICACIÓ CERTIFICAT

Per verificar que funciona la verificació, ens connectarem el servidor:



```
usuari@debian12: ~/certificat
Bye
usuari@debian12:~/certificat$ mysql -u bzhu -p -h 127.0.0.1 --ssl-cert bzhu-cert.pem --ssl-key bzhu-key.pem
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 8.0.35 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.

mysql:[bzhu:(none)]> show databases;
+-----+
| Database |
+-----+
| HABITATGE |
| SARA      |
| agenda    |
| aula      |
| borough   |
| data      |
| dogs      |
| empleats  |
| information_schema |
| ins       |
| movies    |
| mysql     |
| performance_schema |
| prova     |
| starwars  |
| sys       |
```

PASAR L'ARXIU EL CLIENT

Com que ja hem verificat que funciona tot correctament ara passarem el fitxer per el client. Però abans necessitem la seva direcció ip amb un 'ip a':

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:e6:1b:6f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.55/24 brd 192.168.1.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee6:1b6f/64 scope link
        valid_lft forever preferred_lft forever
bixi@bixi:~$
```

Crearem una carpeta en la màquina client

```
bixi@bixi:~$ ls
Descargas  Escritorio  Música      Público      Vídeos
Documentos Imágenes    Plantillas  sortida_slave.txt
bixi@bixi:~$ mkdir certificat
bixi@bixi:~$ cd certificat/
bixi@bixi:~/certificat$ ls
bixi@bixi:~/certificat$
```

després de saber la direcció ip del client utilitzarem la comanda `scp ~/carpeta/arxiu*.pem usuari@ip_client:~/carpeta/` per passar-lo:

```
usuari@debian12:~/certificat$ scp ~/certificat/bzhu*.pem bixi@192.168.1.55:~/certificat/
bixi@192.168.1.55's password:
bzhu-cert.pem          100% 1184      5.1MB/s   00:00
bzhu-key.pem           100% 1704      7.9MB/s   00:00
bzhu-req.pem           100% 1115      6.7MB/s   00:00
usuari@debian12:~/certificat$ ls
bzhu-cert.pem  bzhu-key.pem  bzhu-req.pem
usuari@debian12:~/certificat$
```

Per verificar-lo en el client fem un `ls` per veure els fitxers en la carpeta creada

```
bixi@bixi:~/certificat$ ls
bzhu-cert.pem  bzhu-key.pem  bzhu-req.pem
bixi@bixi:~/certificat$
```

CONNEXIÓ EN REMOT

Ara que ja tenim el fitxers de certificació en la màquina client entrarem el servidor mysql utilitzant el comande `'mysql -u 'usuari' -p -h 'ip_server' --ssl-cert ~/carpeta/arxiu-cert.pem --ssl-key ~/carpeta/arxiu-key.pem'`

```
bixi@bixi: ~/certificat
bixi@bixi: ~/certificat
bixi@bixi:~/certificat$ mysql -u bzhu -p -h 192.168.1.56 --ssl-cert ~/certificat/bzhu-c
ert.pem --ssl-key ~/certificat/bzhu-key.pem
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 8.0.35 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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.

mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| HABITATGE |
| SARA |
| agenda |
| aula |
+-----+
```

CREACIÓ BASE DE DADES

Ara que podem accedir desde remot crearem una base de dades anomenada cypher:

```
bixi@bixi:~/certificat$ mysql -u bzhu -p -h 192.168.1.56 --ssl-cert ~/certificat/bzhu-c
ert.pem --ssl-key ~/certificat/bzhu-key.pem
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 8.0.35 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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.

mysql> create database cypher;
Query OK, 1 row affected (0,25 sec)

mysql> use cypher
Database changed
mysql> █
```

CREACIÓ I INSERTS DE LA TAULA

Com que hem creat una base de dades introduïrem les següents taules:

id_user INT auto_increment

nom_user VARCHAR(20)

password (*)

dataCreacio timestamp default current_timestamp

El password haurà de ser un valor aleatori de 8 digits enters codificat amb la funció md5

Haurem de registrar 5 usuaris i fer un select per veure la codificació dels passwords dels usuaris

Per fer-ho creare un fitxer.sql i introduïre les dades:

```
bixi@bixi:~/Documentos$ touch cypher-insert.sql
bixi@bixi:~/Documentos$ ls
cypher-insert.sql
bixi@bixi:~/Documentos$ gedit cypher-insert.sql
```


MD5 AMB 8 DIGITS

Per el password que haurà de tenir un valor aleatori de 8 digits enters codificat amb la funció md5 he utilitzat el parametre `SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8)`

```
cypher-insert.sql
~/.Documents

1 DROP DATABASE IF EXISTS cypher;
2 CREATE DATABASE IF NOT EXISTS cypher;
3 USE cypher;
4
5 CREATE TABLE users (
6     id_user INT PRIMARY KEY auto_increment,
7     nom_user VARCHAR(20),
8     password VARCHAR(8),
9     dataCreacio TIMESTAMP DEFAULT CURRENT_TIMESTAMP
10 );
11
12 INSERT INTO users(nom_user,password) VALUES
13 ('user1',SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8)),
14 ('user2',SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8)),
15 ('user3',SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8)),
16 ('user4',SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8)),
17 ('user5',SUBSTRING(MD5(FLOOR(RAND()*10000000)),1,8));
```

Fem un source del arxiu.sql

```
mysql> source ~/.Documents/cypher-insert.sql
Query OK, 0 rows affected (0,01 sec)

Query OK, 1 row affected (0,13 sec)

Database changed
Query OK, 0 rows affected (0,68 sec)

Query OK, 5 rows affected (0,28 sec)
Records: 5  Duplicates: 0  Warnings: 0

mysql> show tables;
+-----+
| Tables_in_cypher |
+-----+
| users             |
+-----+
1 row in set (0,00 sec)
```

VERIFICACIÓ

Per verificar que ho hem fet bé el create, insert i el password farem un `select * from users`

```
mysql> select * from users;
+-----+-----+-----+-----+
| id_user | nom_user | password | dataCreacio |
+-----+-----+-----+-----+
|      1 | user1    | b58212a9 | 2024-04-14 21:29:49 |
|      2 | user2    | e5342431 | 2024-04-14 21:29:49 |
|      3 | user3    | b9f80c65 | 2024-04-14 21:29:49 |
|      4 | user4    | 4d6a617a | 2024-04-14 21:29:49 |
|      5 | user5    | f6aa8913 | 2024-04-14 21:29:49 |
+-----+-----+-----+-----+
5 rows in set (0,00 sec)
```

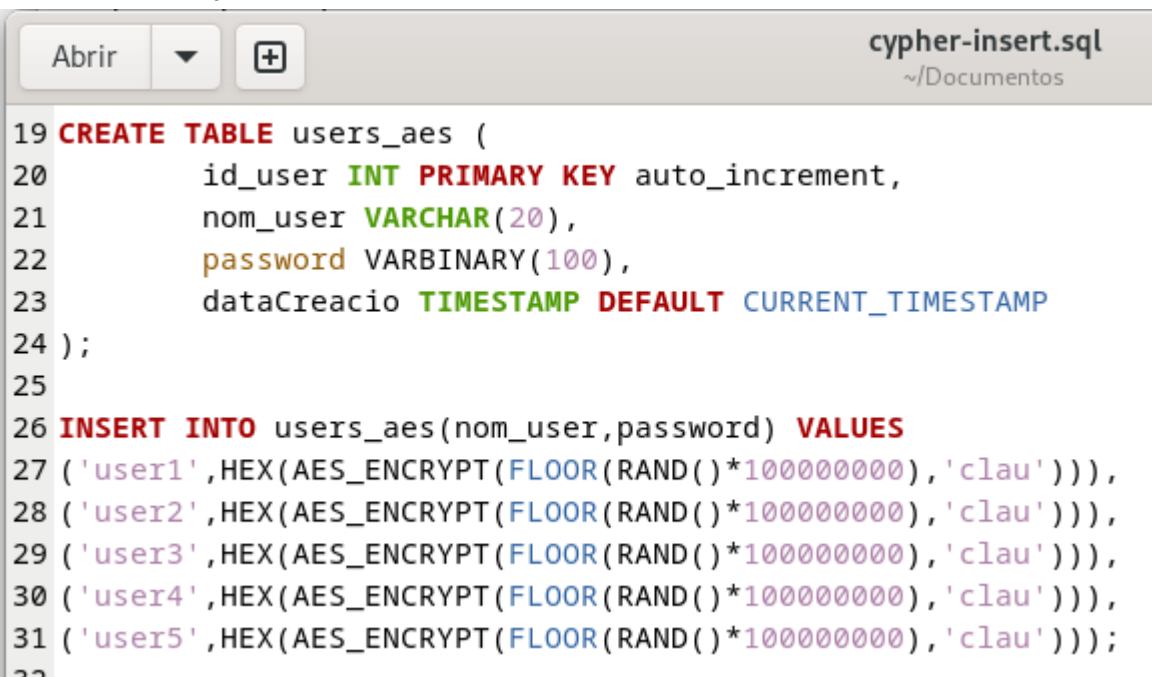
DESENCRIPTAR LA CONTRASEÑA

En principi la manera de "descifrar" un hash MD5 és mitjançant força bruta, és a dir, provar diferents combinacions de valors fins que trobis un que coincideixi amb el hash donat. La funció MD5 és un algorisme unidireccional, el que significa que no es pot desfer per obtenir l'entrada original.

ALTRES ENCRIPCIÓN I DESENCRIPTACION

Com que el md5 no era una solució viable hi ha algunes altres que són bastant populars com AES: Advanced Encryption Standard i SHA: Secure Hash Algorithms.

Utilitzaré el AES ja que és el que més he utilitzat.



```
cypher-insert.sql
~/Documents

19 CREATE TABLE users_aes (
20     id_user INT PRIMARY KEY auto_increment,
21     nom_user VARCHAR(20),
22     password VARBINARY(100),
23     dataCreacio TIMESTAMP DEFAULT CURRENT_TIMESTAMP
24 );
25
26 INSERT INTO users_aes(nom_user,password) VALUES
27 ('user1',HEX(AES_ENCRYPT(FLOOR(RAND()*100000000),'clau'))),
28 ('user2',HEX(AES_ENCRYPT(FLOOR(RAND()*100000000),'clau'))),
29 ('user3',HEX(AES_ENCRYPT(FLOOR(RAND()*100000000),'clau'))),
30 ('user4',HEX(AES_ENCRYPT(FLOOR(RAND()*100000000),'clau'))),
31 ('user5',HEX(AES_ENCRYPT(FLOOR(RAND()*100000000),'clau')));
32
```

```
bixi@bixi: ~/certificat
mysql> select * from users_aes;
+-----+-----+-----+-----+
| id_user | nom_user | password | dataCreacio |
+-----+-----+-----+-----+
| 1 | user1 | 0x3945323538353037423939304542413341314633463243394433324532374544 | 2024-04-15 18:31:25 |
| 2 | user2 | 0x4532453443424334323844373144423744394541433835374142464331303946 | 2024-04-15 18:31:25 |
| 3 | user3 | 0x4139373438463832463831343232304141383532434642463638413233334435 | 2024-04-15 18:31:25 |
| 4 | user4 | 0x3546323339364337463330383145463931453243393832303537463343373633 | 2024-04-15 18:31:25 |
| 5 | user5 | 0x4146334532443943383331424130424239334641353239303043413138334630 | 2024-04-15 18:31:25 |
+-----+-----+-----+-----+
5 rows in set (0,00 sec)

mysql>
```

i per veure la desencryptació farem servir aes_descript:

```
bixi@bixi: ~/certificat
+-----+-----+-----+-----+
| 4 | user4 | 0x3546323339364337463330383145463931453243393832303537463343373633 | 2024-04-15 18:31:25 |
| 5 | user5 | 0x4146334532443943383331424130424239334641353239303043413138334630 | 2024-04-15 18:31:25 |
+-----+-----+-----+-----+
5 rows in set (0,00 sec)

mysql> select nom_user, CAST(AES_DECRYPT(UNHEX(password),'clau')as CHAR) AS password from users_aes;
+-----+-----+
| nom_user | password |
+-----+-----+
| user1 | 38869118 |
| user2 | 29533281 |
| user3 | 31059055 |
| user4 | 66695436 |
| user5 | 40300020 |
+-----+-----+
5 rows in set (0,00 sec)

mysql>
```