HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

An Toàn Ứng Dụng Web Và CSDL

Bài Lab 3

Họ Tên: Trần Quốc Trượng

MSSV: N18DCAT100

Lớp: D18CQAT02-N

TP.HCM - 2021

a) Viết script tạo Database có tên QLSV.

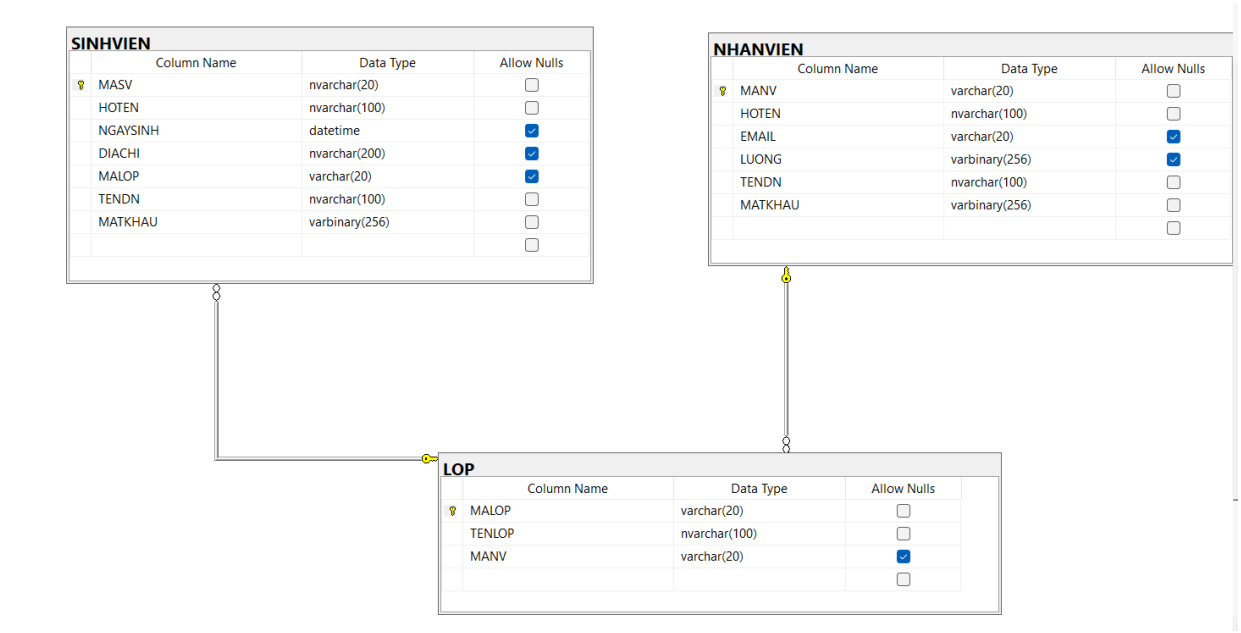
```
/*------------------------------------------------------------
MASV: N18DCAT100
HO TEN: TRẦN QUỐC TRƯỢNG
LAB: 03
NGAY: 9/8/2021
------------------------------------------------------------*/

CREATE DATABASE QLSV
```

b) Viết script tạo mới các Table SINHVIEN, NHANVIEN, LOP

```
/*------------------------------------------------------------
MASV: N18DCAT100
HO TEN: TRẦN QUỐC TRƯỢNG
LAB: 03
NGAY: 9/8/2021
------------------------------------------------------------*/
CREATE TABLE SINHVIEN (
    MASV NVARCHAR(20) PRIMARY KEY,
    HOTEN NVARCHAR(100) NOT NULL,
    NGAYSINH DATETIME,
    DIACHI NVARCHAR(200),
    MALOP VARCHAR(20),
    TENDN NVARCHAR(100) NOT NULL,
    MATKHAU VARBINARY(256) NOT NULL
)
```

```
CREATE TABLE NHANVIEN (
    MAVN VARCHAR(20) PRIMARY KEY,
    HOTEN NVARCHAR(100) NOT NULL,
    EMAIL VARCHAR(20),
    LUONG VARBINARY(256),
    TENDN NVARCHAR(100) NOT NULL,
    MATKHAU VARBINARY(256) NOT NULL
)
```

```
CREATE TABLE LOP (
    MALOP VARCHAR(20) PRIMARY KEY,
    TENLOP NVARCHAR(100) NOT NULL,
    MANV VARCHAR(20)
)
```



c) Viết các Stored procedure sau

i) Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng MD5

```
/*-------------------------------------------------------
MASV: N18DCAT100
HO TEN: TRẦN QUỐC TRƯỢNG
LAB: 03
NGAY: 9/8/2021
-------------------------------------------------------*/
--i
CREATE PROC SP_INS_SINHVIEN @MASV NVARCHAR(20), @HOTEN NVARCHAR(100), @NGAYSINH DATETIME ,
                            @DIACHI NVARCHAR(200), @MALOP VARCHAR(20), @TENDN NVARCHAR(100),
                            @MATKHAU NVARCHAR(50)
AS
    INSERT INTO SINHVIEN
    VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, HASHBYTES('MD5', @MATKHAU))

GO

EXEC SP_INS_SINHVIEN 'SV01', 'NGUYEN VAN A', '1990-1-1', '280 AN DUONG VUONG', 'CNTT-K35', 'NVA', '123456'

SELECT * FROM SINHVIEN
```

121 %

Results | Messages

	MASV	HOTEN	NGAYSINH	DIACHI	MALOP	TENDN	MATKHAU
1	SV01	NGUYEN VAN A	1990-01-01 00:00:00.000	280 AN DUONG VUONG	CNTT-K35	NVA	0xCE0BFD15059B68D67688884D7A3D3E8C

ii) Stored dùng để thêm mới dữ liệu (Insert) vào table NHANVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng SHA1 và thuộc tính LUONG sẽ được mã hóa sử dụng thuật toán AES 256, với khóa mã hóa là mã số của sinh viên thực hiện bài Lab này

- Bước 1: Tạo khóa

```
CREATE SYMMETRIC KEY myKey_AES_256
WITH KEY_SOURCE = 'N18DCAT100',
ALGORITHM = AES_256
ENCRYPTION BY PASSWORD = '123456'
GO
```

- Bước 2: Tạo Stored procedure

```
CREATE PROC SP_INS_NHANVIEN @MAVN VARCHAR(20), @HOTEN NVARCHAR(100), @EMAIL VARCHAR(20), @LUONG INT,
                            @TENDN NVARCHAR(100), @MATKHAU NVARCHAR(100)
AS
    OPEN SYMMETRIC KEY myKey_AES_256 DECRYPTION BY PASSWORD = '123456'

    INSERT INTO NHANVIEN VALUES
    (@MAVN, @HOTEN, @EMAIL, ENCRYPTBYKEY(Key_GUID('myKey_AES_256'), CONVERT(NVARCHAR, @LUONG)),
    @TENDN, HASHBYTES('SHA1', @MATKHAU))

    CLOSE SYMMETRIC KEY myKey_AES_256
GO
```

- Bước 3: Kiểm tra kết quả

```
EXEC SP_INS_NHANVIEN 'NV01', 'NGUYEN VAN A', 'NVA@', 3000000, 'NVA', 'abcd12'

SELECT * FROM NHANVIEN
```

121 %

Results | Messages

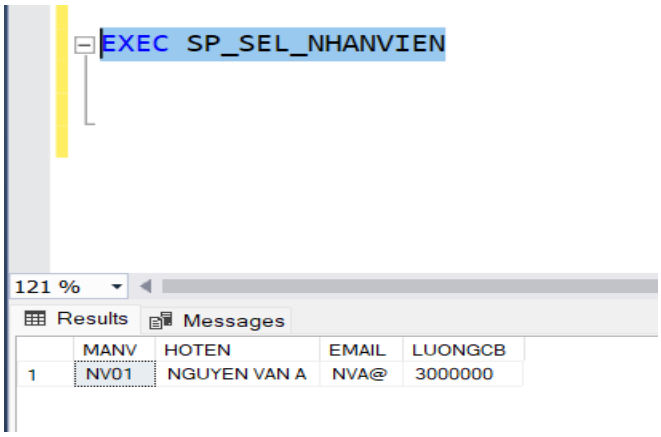
	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU
1	NV01	NGUYEN VAN A	NVA@	0x00506CD979B20944A9A640635EEBD20E020000008103E8...	NVA	0x2F3309423FD7FC1100241B801FE95659465701C1

iii) Stored dùng để truy vấn dữ liệu nhân viên (NHANVIEN)

- Bước 1: Tạo Proc

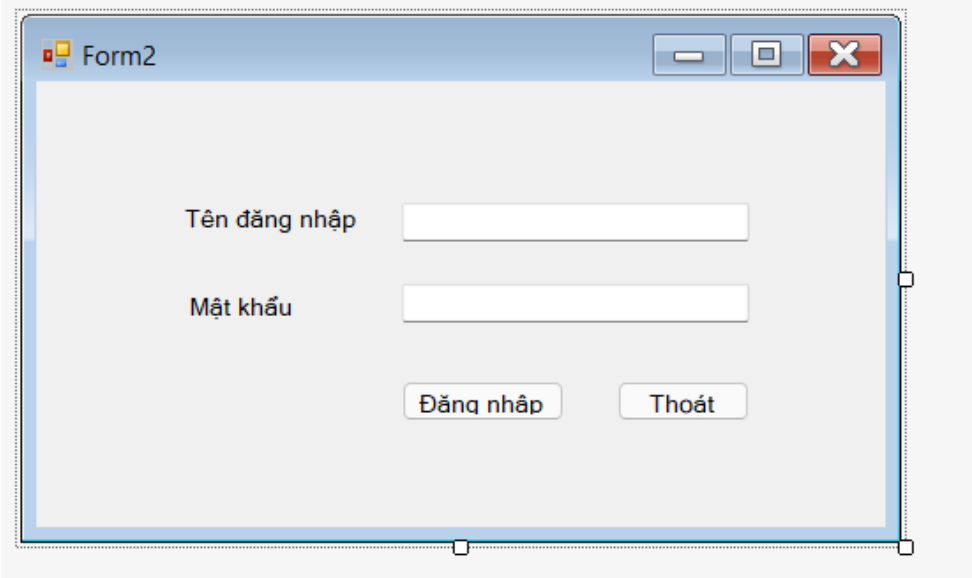
```
CREATE PROC SP_SEL_NHANVIEN
AS
    OPEN SYMMETRIC KEY myKey_AES_256 DECRYPTION BY PASSWORD = '123456'

    SELECT MANV, HOTEN, EMAIL, CONVERT(NVARCHAR, DECRYPTBYKEY(LUONG)) AS LUONGCB
    FROM NHANVIEN

    CLOSE SYMMETRIC KEY myKey_AES_256
GO
```

- Bước 2: Kiểm tra kết quả



d) Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#), cho phép nhập vào tên đăng nhập và mật khẩu

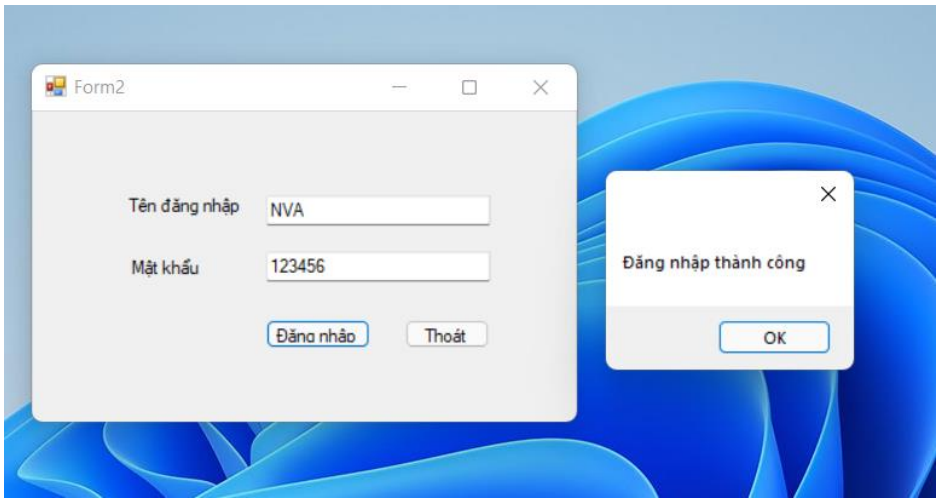
- Bước 1: Tạo form đăng nhập



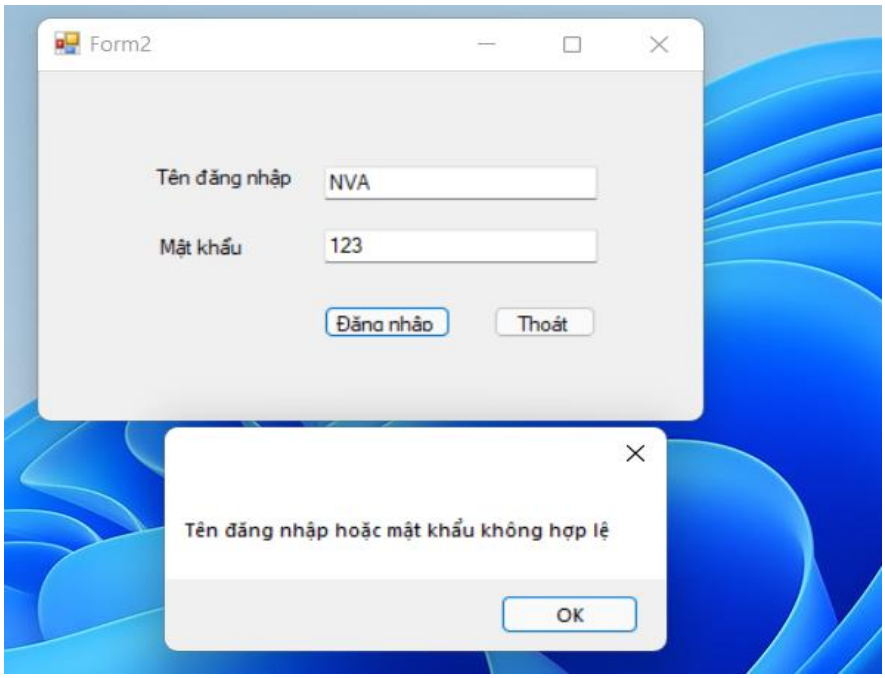
- Bước 2: Viết mã C# kết nối csdl đăng nhập

```
if(sqlCon.State ==  ConnectionState.Closed)
{

    string username = textBox_dangNhap.Text;
    string passwd = textBox_Password.Text;

    string sql = $@"select * from SINHVIEN where TENDN = '{username}' AND MATKHAU = hashbytes('MD5', convert(nvarchar, '{passwd}'))";
    Console.WriteLine(sql);
    sqlCon.Open();
    SqlCommand cmd = new SqlCommand(sql, sqlCon);
    SqlDataReader read = cmd.ExecuteReader();


    if(read.Read() == true)
    {
        MessageBox.Show("Đăng nhập thành công");
    }else
    {
        MessageBox.Show("Tên đăng nhập hoặc mật khẩu không hợp lệ");
    }

    sqlCon.Close();
```

- Bước 3: Chạy và kiểm tra kết quả



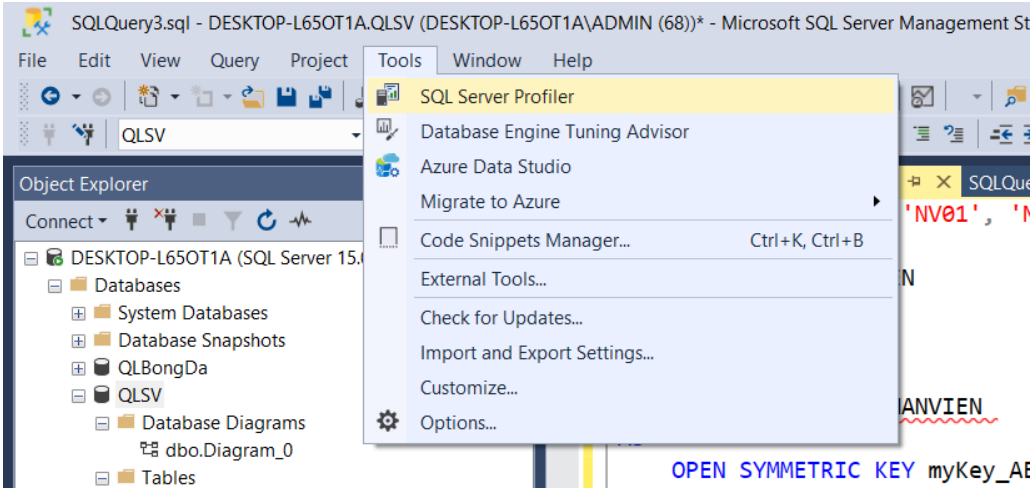
Hình 1. Tên đăng nhập và mật khẩu tồn tại trong table SINHVIEN



Hình 2. Tên đăng nhập và mật khẩu không tồn tại trong table SINHVIEN

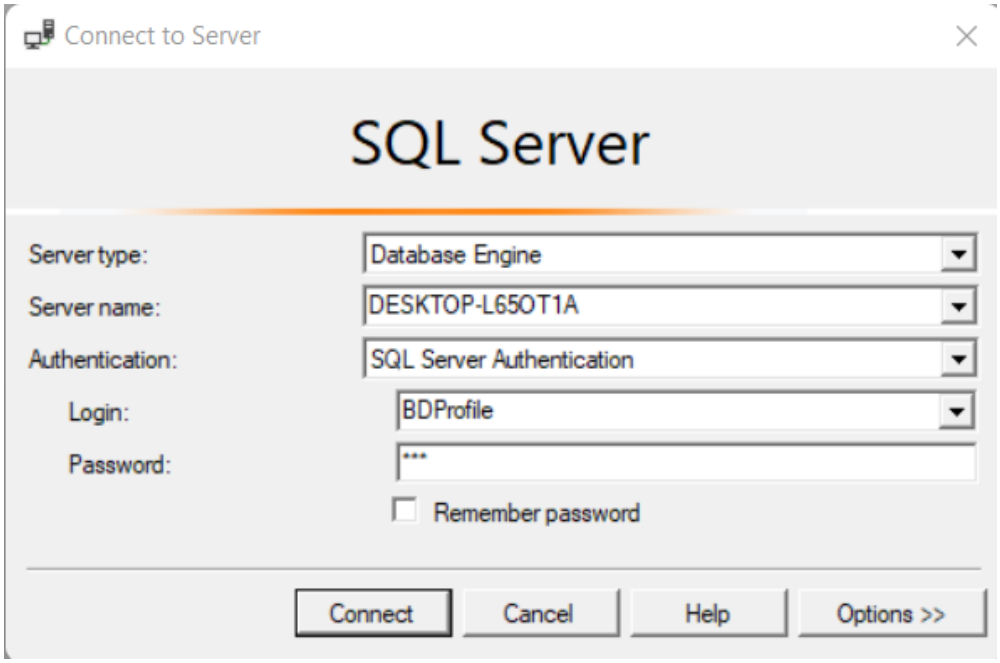
e) Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập từ màn hình quản lý đăng nhập trên, nhận xét.

i) Mở màn hình quản lý đăng nhập

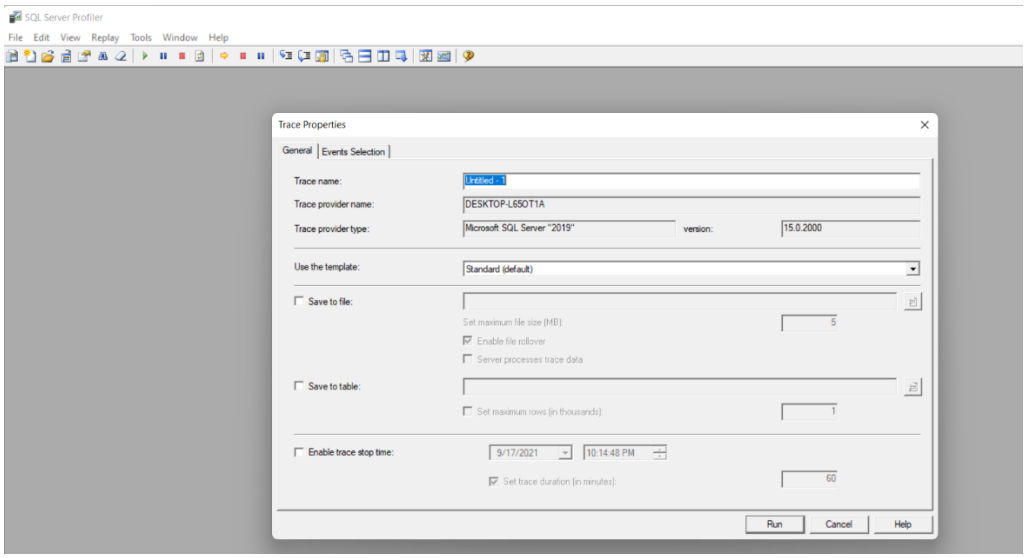


Hình 3. Tools > SQL Server Profiler

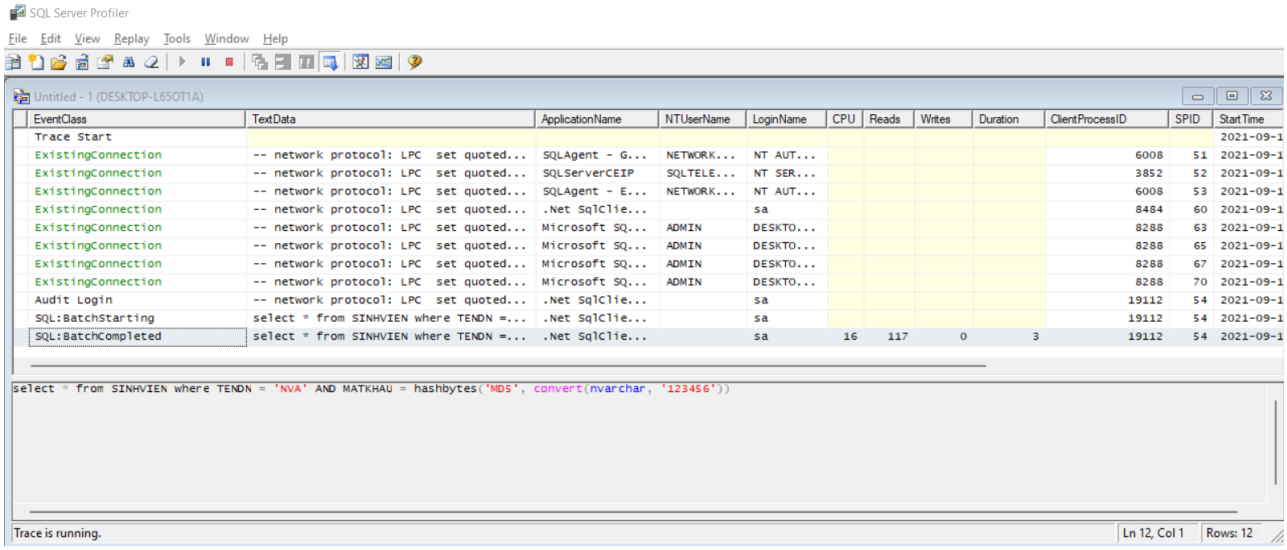
ii) Nhập tên đăng nhập và mật khẩu



iii) Nhấn nút đăng nhập



iv) Chuyển sang màn hình SQL Profile, xem kết quả và viết nhận xét.



Hình 4. Mật khẩu chưa được mã hóa phía client