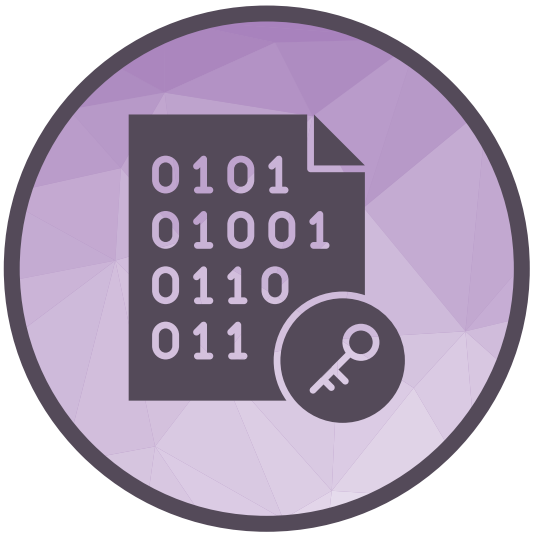
FIT@HCMUS
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG - HCM
KHOA CÔNG NGHỆ THÔNG TIN



LAB 3 - MÃ HÓA DỮ LIỆU SỬ DỤNG CÁC THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

BỘ MÔN: BẢO MẬT CƠ SỞ DỮ LIỆU

Sinh viên thực hiện:
21120396 - Đào Thị Ngọc Giàu
21120419 - Vũ Thành Công
21120446 - Kiên Đinh Mỹ Hạnh

TP. Hồ Chí Minh, tháng 4/2024

Mục lục

I. Các stored procedure (câu c)

1. Stored procedure SP_INS_PUBLIC_NHANVIEN

a. Cài đặt

```
GO
CREATE PROCEDURE SP_INS_PUBLIC_NHANVIEN @MANV VARCHAR(20), @HOTEN NVARCHAR(100),
                                        @EMAIL VARCHAR(20), @LUONG INT,
                                        @TENDN NVARCHAR(100), @MATKHAU VARCHAR(32)


AS
BEGIN
    DECLARE @PUBKEY VARCHAR(20)
    SET @PUBKEY = @MANV

    DECLARE @AKEY NVARCHAR(MAX)
    SET @AKEY = 'CREATE ASYMMETRIC KEY '+@MANV+' WITH ALGORITHM = RSA_2048 ENCRYPTION BY PASSWORD = '''+@MATKHAU+''''
    EXEC(@AKEY)
    INSERT INTO NHANVIEN(MANV, HOTEN, EMAIL, LUONG, TENDN, MATKHAU, PUBKEY)
    VALUES (@MANV, @HOTEN, @EMAIL,
            ENCRYPTBYASYMKEY(ASYMKEY_ID(@PUBKEY), CONVERT(VARBINARY(MAX),@LUONG)),
            @TENDN,CONVERT(VARBINARY, HASHBYTES('SHA1', @MATKHAU)),
            @PUBKEY)
END
```

b. Thực thi

```
EXEC SP_INS_PUBLIC_NHANVIEN 'NV04', N'NGUYEN VAN A', 'NVd@', 3000000, 'NV04', 'abcd12'
```

132 %

Messages

(1 row affected)

```
EXEC SP_INS_PUBLIC_NHANVIEN 'NV04', N'NGUYEN VAN A', 'NVd@', 3000000, 'NV04', 'abcd12'

SELECT* FROM NHANVIEN
```

109 %

Results Messages

	MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	PUBKEY
1	NV04	NGUYEN VAN A	NVd@	0x2645323DF7AD25DA97C60DE5682EFE8E27E0246C4752930...	NV04	0xC35A37F0BCA08AFA583247CC461CAD9C8082A47C	NV04

2. Stored procedure SP_SEL_PUBLIC_NHANVIEN

a. Cài đặt

```
GO
CREATE PROCEDURE SP_SEL_PUBLIC_NHANVIEN @TENDN NVARCHAR(100),@MATKHAU VARCHAR(100)
AS
BEGIN
    SELECT MANV,HOTEN,EMAIL,
            LUONGCB = CONVERT(INT, DECRYPTBYASYMKEY(ASYMKEY_ID(MANV), LUONG, CONVERT(NVARCHAR, @MATKHAU)))
    FROM NHANVIEN
    WHERE CONVERT(NVARCHAR, @TENDN) = TENDN AND MATKHAU = HASHBYTES('SHA1', @MATKHAU)
END
```

b. Thực thi

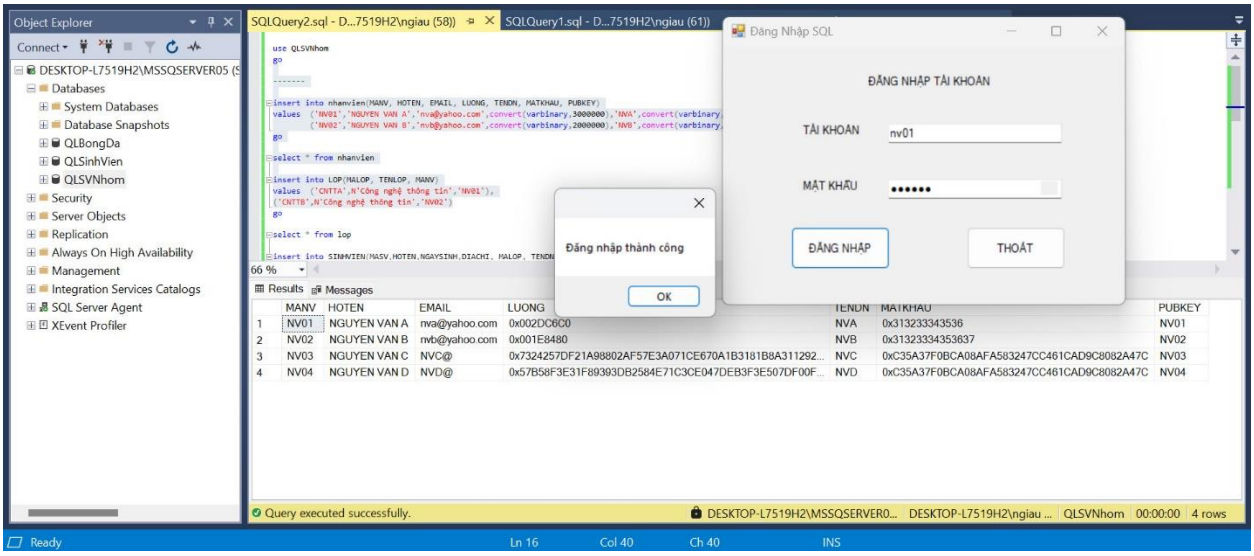
```
123
124  EXEC SP_SEL_PUBLIC_NHANVIEN 'NV04', 'abcd12'
125
```

109 %

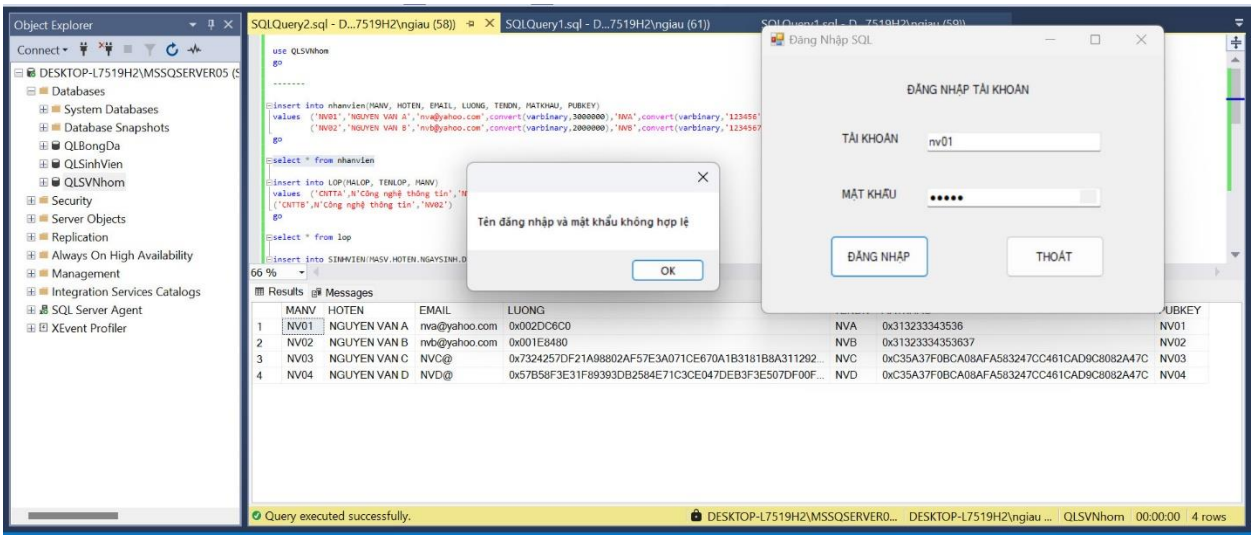
Results | Messages

	MANV	HOTEN	EMAIL	LUONGCB
1	NV04	NGUYEN VAN A	NVd@	3000000

II. Màn hình quản lý đăng nhập

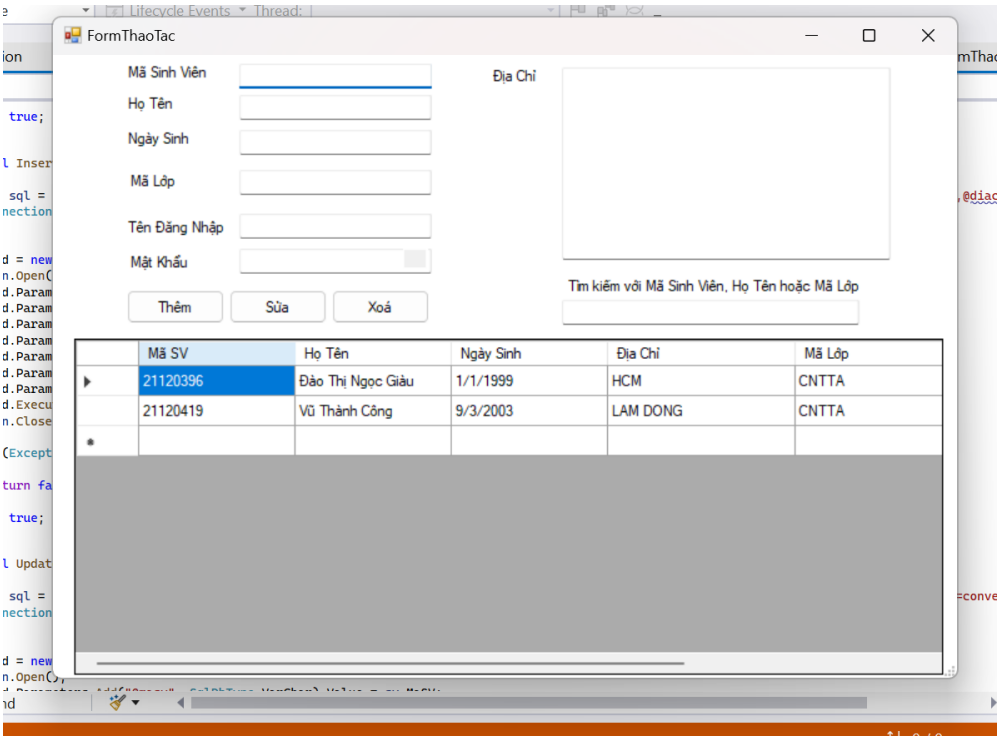


Đăng nhập thành công



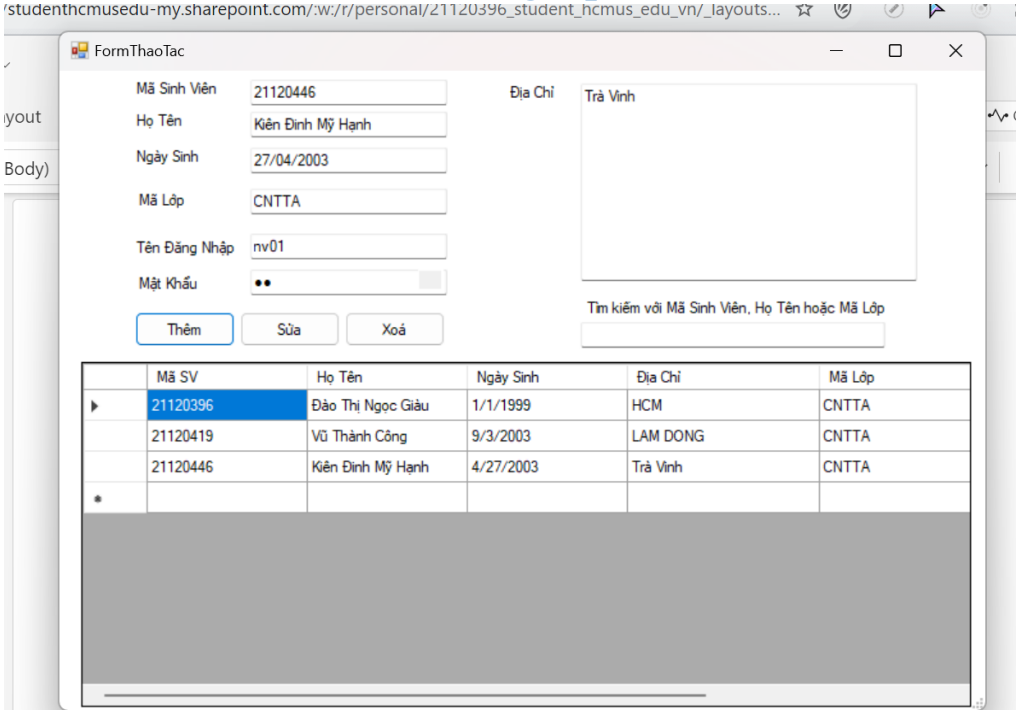
Đăng nhập không thành công

III. Màn hình quản lý lớp học

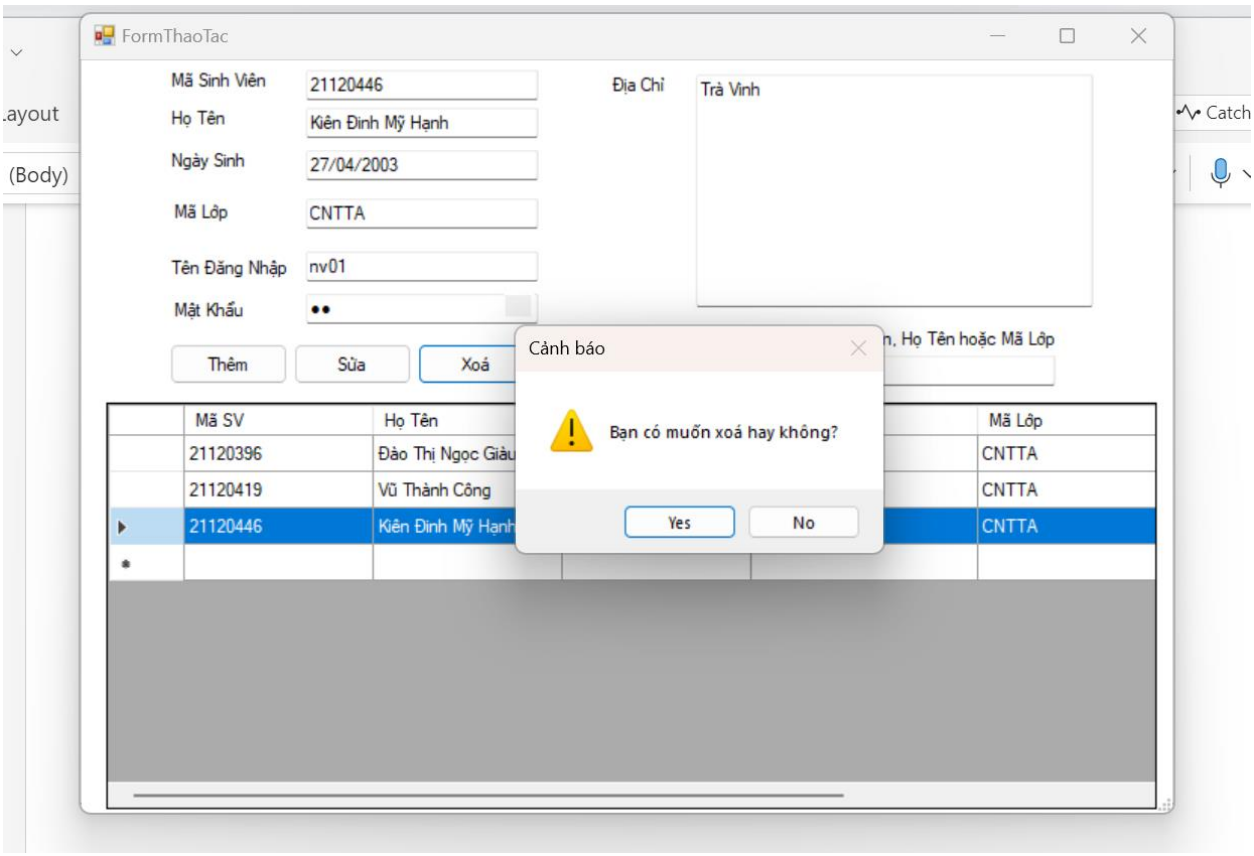


Sau khi đăng nhập, nhân viên chỉ có thể theo dõi những sinh viên thuộc mã lớp do nhân viên quản lý.

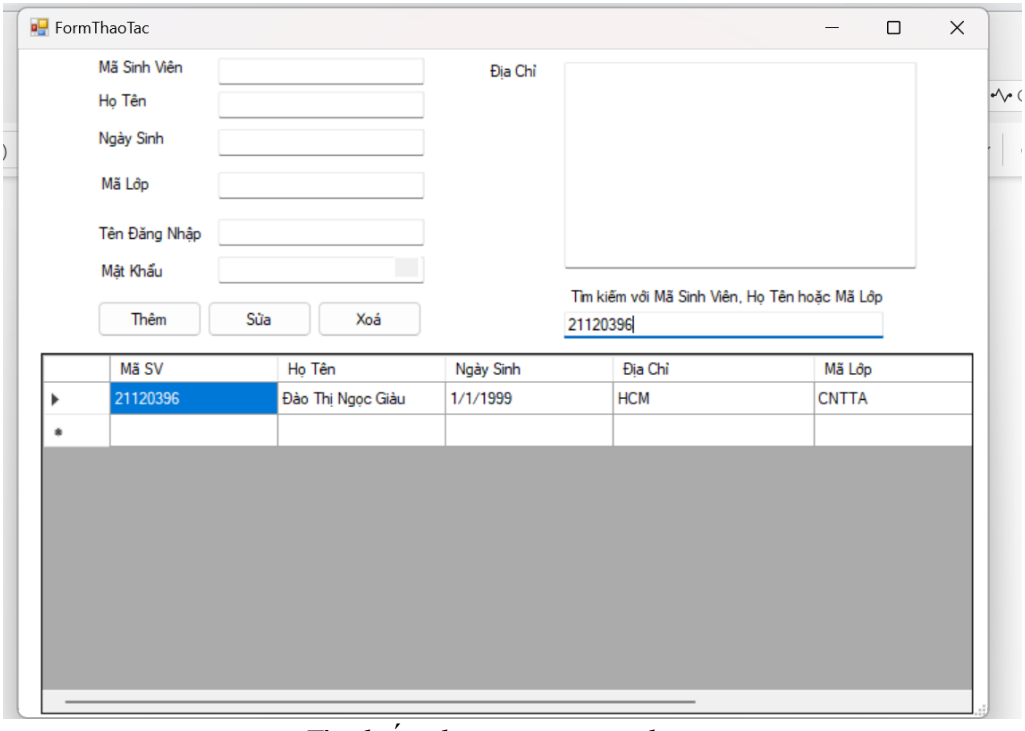
IV. Màn hình sinh viên của từng lớp



Thêm sinh viên



Xóa một sinh viên

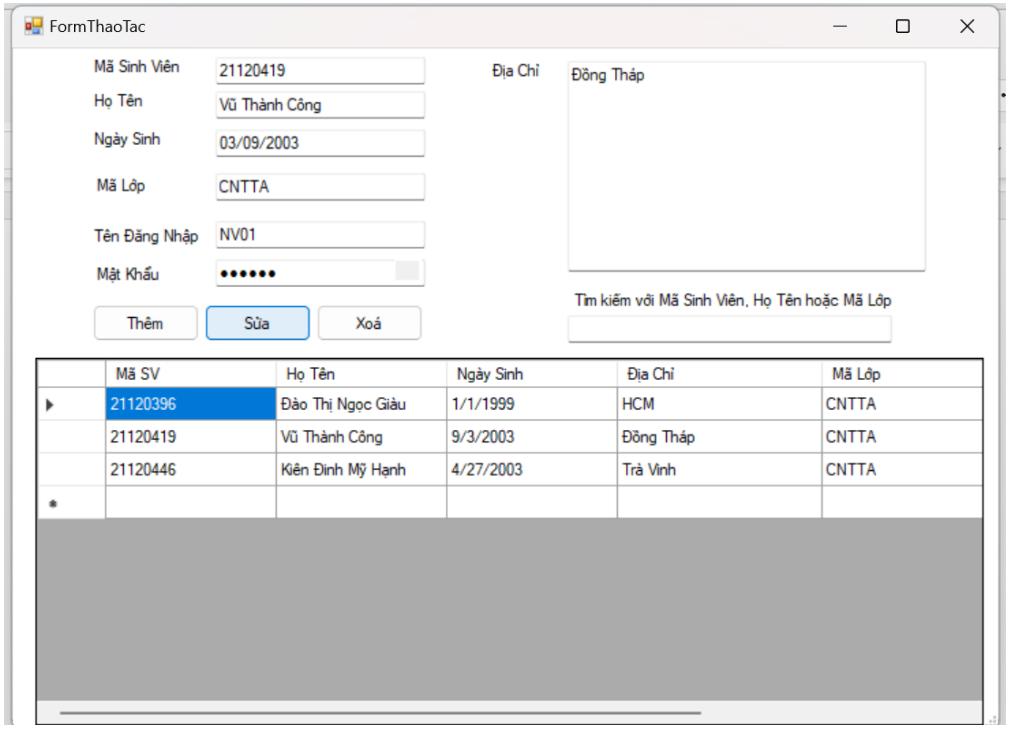


Tìm kiếm thông tin một sinh viên

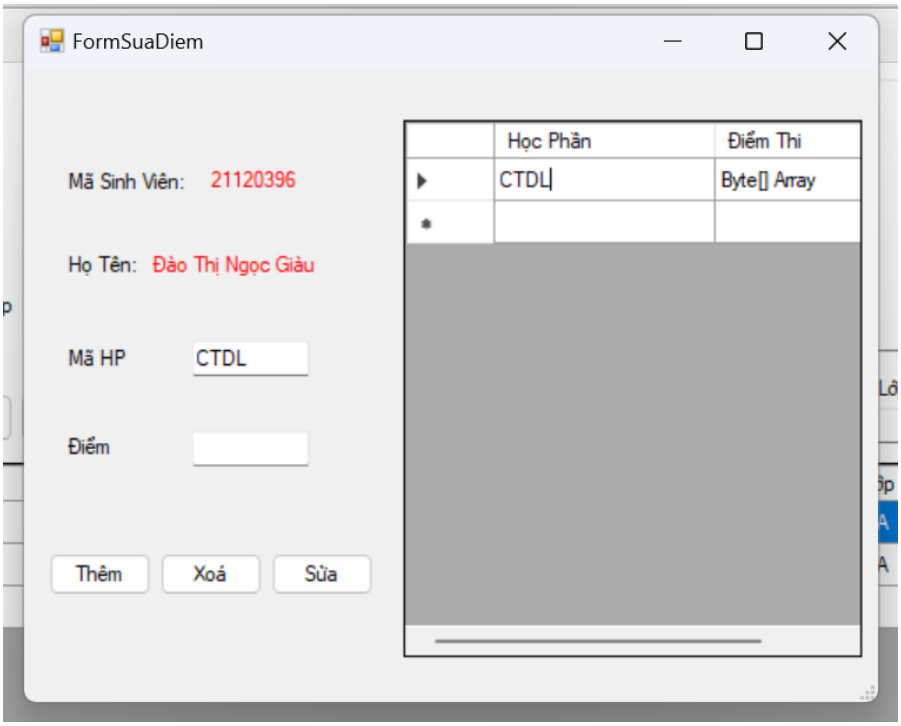
Nhân viên quản lý sinh viên của một lớp có các quyền thêm, xóa, sửa, hoặc tìm kiếm bất kỳ một sinh viên nào.

V. Nhập điểm cho từng sinh viên

Bước 1: Chọn sinh viên cần nhập điểm bằng cách nhấn vào phần sửa.

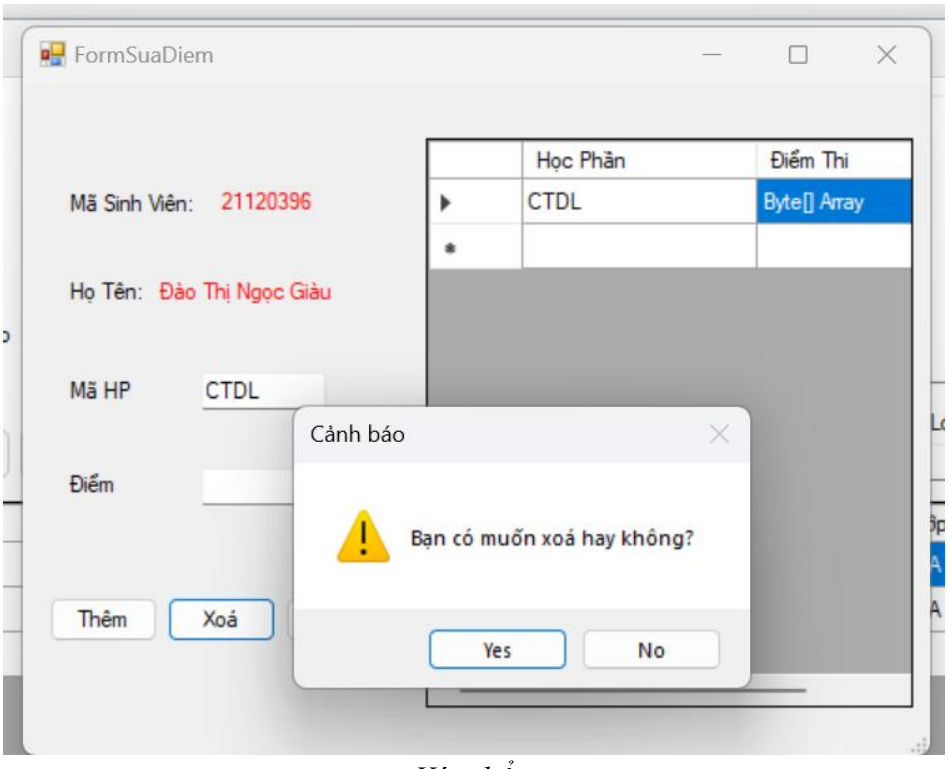


Bước 2: Màn hình giao diện thông tin sinh viên cần nhập điểm sẽ được hiện lên

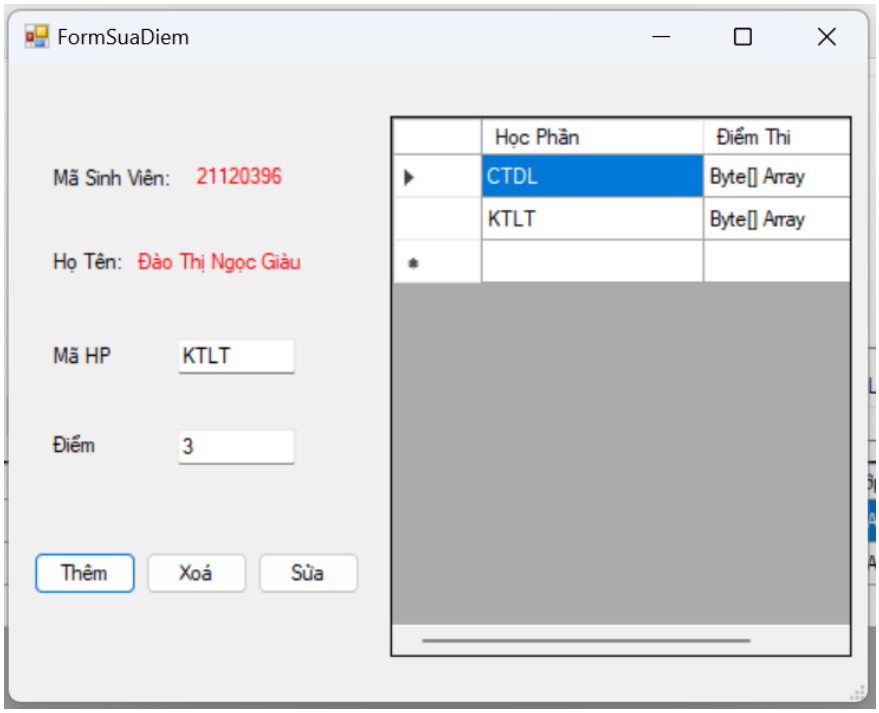


Giao diện nhập điểm

Bước 3: Thao tác với điểm số: Có thể xóa điểm đó đi, hoặc nhập thêm điểm vào



Xóa điểm

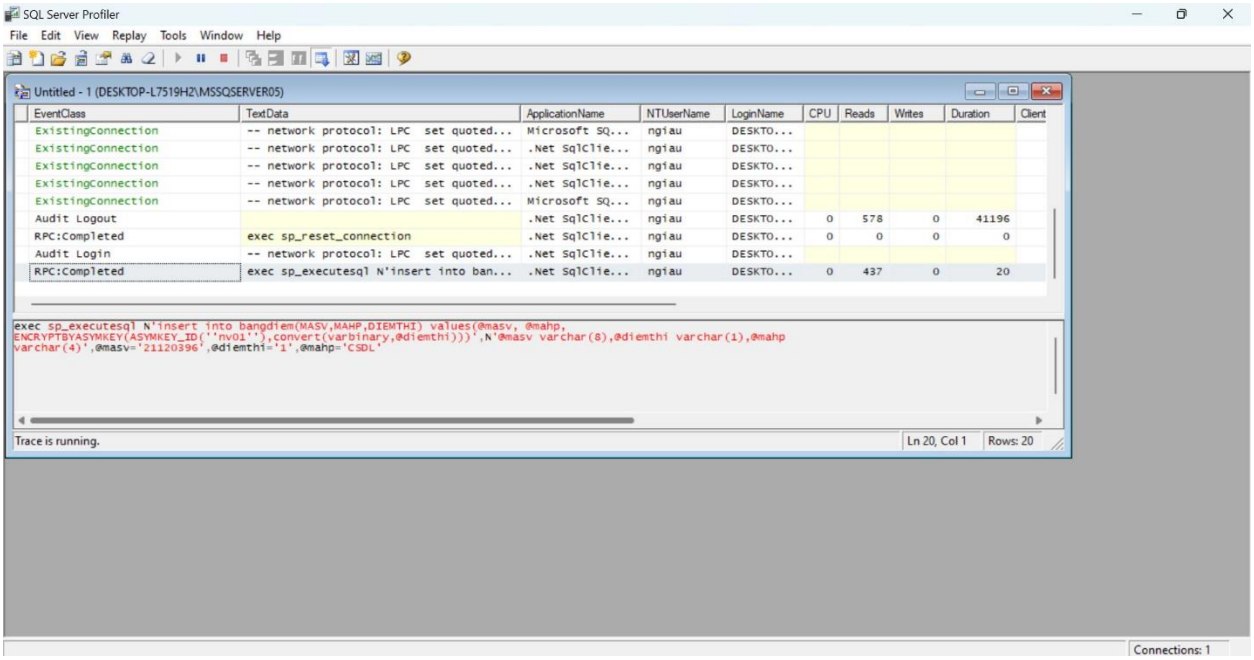


Nhập điểm

Do ngay từ đầu, nhóm em đã xây dựng app theo cách đăng nhập của nhân viên và chỉ có nhân viên có thể đăng nhập. Và đồng thời, nhân viên chỉ có thể nhìn thấy lớp mà mình quản lý, do đó không thể sửa đổi điểm của lớp khác.

VI. Sử dụng SQL Profile theo dõi thao tác màn hình nhập điểm

1. Đăng nhập



2. Nhận xét

- Trong bài này, người dùng SQL Profiler nhận thấy nhân viên chỉ chỉnh sửa được điểm của sinh viên thuộc lớp do nhân viên đó quản lý.
- Người có quyền truy cập tới tool SQL Profiler hoặc nghe trộm liên lạc giữa ứng dụng và Database hoàn toàn có thể biết được mật khẩu người lẫn điểm số đã nhập.
- Do đó, thông tin điểm số sẽ bị lộ