

**ĐẠI HỌC QUỐC GIA
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**

**Bảo mật cơ sở dữ liệu
CSC15002_20CNTThuc**



LAB 03

Giảng viên giảng dạy:

Trần Ngọc Bảo

Nguyễn Thị Hường

Ngô Đình Hy

Nguyễn Đình Thúc

Sinh viên:

Lê Võ Huỳnh Thanh – 20127072

Lớp: 20CNTThuc

Mục Lục

c) Viết các Stored procedure sau.....	3
i) Stored dùng để thêm mới dữ liệu (Insert) vào table SINHVIEN, trong đó thuộc tính MATKHAU được mã hóa (HASH) sử dụng MD5.....	3
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.....	3
iii) Stored dùng để truy vấn dữ liệu nhân viên (NHANVIEN).....	3
d) Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#), cho phép nhập vào tên đăng nhập và mật khẩu (giả sử tên đăng nhập của sinh viên và nhân viên là duy nhất, nghĩa là tên đăng nhập của tất cả các sinh viên và tất cả nhân viên là khác nhau).....	4
Hình 1: Mở màn hình quản lý đăng nhập trong Visual Studio	4
Hình 2: Nhập tên đăng nhập (NVA) và mật khẩu (123456) (bấm vào nút Đăng Nhập thì đăng nhập thành công).....	5
Hình 3: Nhập tên đăng nhập (NVA) và mật khẩu (1234567) (bấm vào nút Đăng nhập thì đăng nhập thất bại)	6
e) Sử dụng công cụ SQL Profile để theo dõi thao tác đăng nhập từ màn hình quản lý đăng nhập trên, nhận xét.....	6
Nhận xét:	7

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.

```

CREATE TABLE LOP
(
    MALOP VARCHAR(20),
    TENLOP VARCHAR(100) NOT NULL,
    MAHV VARCHAR(20)
    CONSTRAINT PK_LOP
    PRIMARY KEY(MALOP)
)

--C. CẤU LẬP TẠO SToredProcedure
-- I. Insert vào table SINHVIEN, hash MATKHAU bằng MD5
IF OBJECT_ID('SP_INS_SINHVIEN') IS NOT NULL
    DROP PROC SP_INS_SINHVIEN
GO

CREATE PROCEDURE SP_INS_SINHVIEN (@HUSV VARCHAR(20), @HOTEN VARCHAR(100), @NgaySinh DATETIME,
    @Diachi VARCHAR(200), @MALOP VARCHAR(20), @TenDN VARCHAR(100),
    @MatKHAU VARCHAR(100))
AS
    DECLARE @hash_pass VARBINARY(MAX)
    SET @hash_pass = HASHBYTES('MD5', @MatKHAU)
    INSERT SINHVIEN VALUES(@HUSV, @HOTEN, @NgaySinh, @Diachi, @MALOP, @TenDN, @hash_pass)

EXEC SP_INS_SINHVIEN 'SV01', N'NGUYEN VAN A', '1/1/2000', N'200 AN DUONG VUONG', 'CNTT-K35', N'NVA', '123456'
SELECT * FROM SINHVIEN
GO

-- I. Thiết lập để sử dụng mã hoá đối xứng AES_256
-- TẠO MASTER KEY
IF NOT EXISTS
(
    SELECT * FROM sys.symmetric_keys
    WHERE name = 'PrKey'
)
CREATE SYMMETRIC KEY PrKey WITH ALGORITHM = AES_256 ENCRYPTION BY CERTIFICATE Hycert
GO

--Mã hoá dữ liệu (Lương) sử dụng AES256
OPEN SYMMETRIC KEY PrKey
DECRYPTION BY CERTIFICATE Hycert

-- (ii). Thêm dữ liệu vào bảng NHANVIEN, MATKHAU -> SHA1, LUONG -> AES(256, HSSV)
IF OBJECT_ID('SP_INS_NHANVIEN') IS NOT NULL
    DROP PROC SP_INS_NHANVIEN
GO

CREATE PROCEDURE SP_INS_NHANVIEN (@HNV VARCHAR(20), @HOTEN VARCHAR(100), @email VARCHAR(20),
    @luong INT, @TenDN VARCHAR(100), @MatKHAU VARCHAR(100))
AS
    DECLARE @encrypted_luong VARBINARY(MAX)
    SET @encrypted_luong = (SELECT ENCRYPTBYKEY(KEY_GUID('PrKey'), CONVERT(VARCHAR(MAX), @luong)))
    DECLARE @hash_pass VARBINARY(MAX)
    SET @hash_pass = HASHBYTES('SHA1', @MatKHAU)
    INSERT NHANVIEN VALUES(@HNV, @HOTEN, @email, @encrypted_luong, @TenDN, @hash_pass)

EXEC SP_INS_NHANVIEN 'NV01', N'NGUYEN VAN A', 'NVA@', 3000000, N'NVA', 'abcd12'
SELECT * FROM NHANVIEN
GO

-- (iii). Truy vấn dữ liệu nhân viên
IF OBJECT_ID('SP_SEL_NHANVIEN') IS NOT NULL
    DROP PROCEDURE SP_SEL_NHANVIEN
GO
    
```

- 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.

```

SELECT * FROM sys.symmetric_keys
WHERE name = 'PrKey'
)
CREATE SYMMETRIC KEY PrKey WITH ALGORITHM = AES_256 ENCRYPTION BY CERTIFICATE Hycert
GO

--Mã hoá dữ liệu (Lương) sử dụng AES256
OPEN SYMMETRIC KEY PrKey
DECRYPTION BY CERTIFICATE Hycert

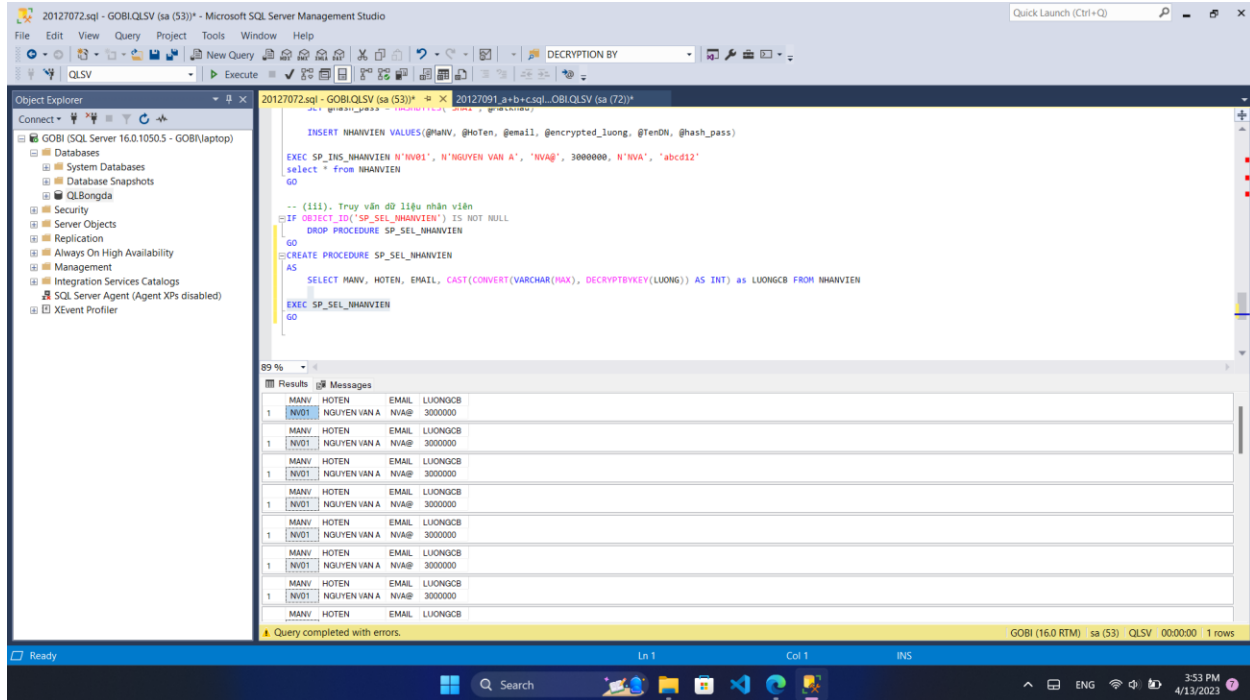
-- (ii). Thêm dữ liệu vào bảng NHANVIEN, MATKHAU -> SHA1, LUONG -> AES(256, HSSV)
IF OBJECT_ID('SP_INS_NHANVIEN') IS NOT NULL
    DROP PROC SP_INS_NHANVIEN
GO

CREATE PROCEDURE SP_INS_NHANVIEN (@HNV VARCHAR(20), @HOTEN VARCHAR(100), @email VARCHAR(20),
    @luong INT, @TenDN VARCHAR(100), @MatKHAU VARCHAR(100))
AS
    DECLARE @encrypted_luong VARBINARY(MAX)
    SET @encrypted_luong = (SELECT ENCRYPTBYKEY(KEY_GUID('PrKey'), CONVERT(VARCHAR(MAX), @luong)))
    DECLARE @hash_pass VARBINARY(MAX)
    SET @hash_pass = HASHBYTES('SHA1', @MatKHAU)
    INSERT NHANVIEN VALUES(@HNV, @HOTEN, @email, @encrypted_luong, @TenDN, @hash_pass)

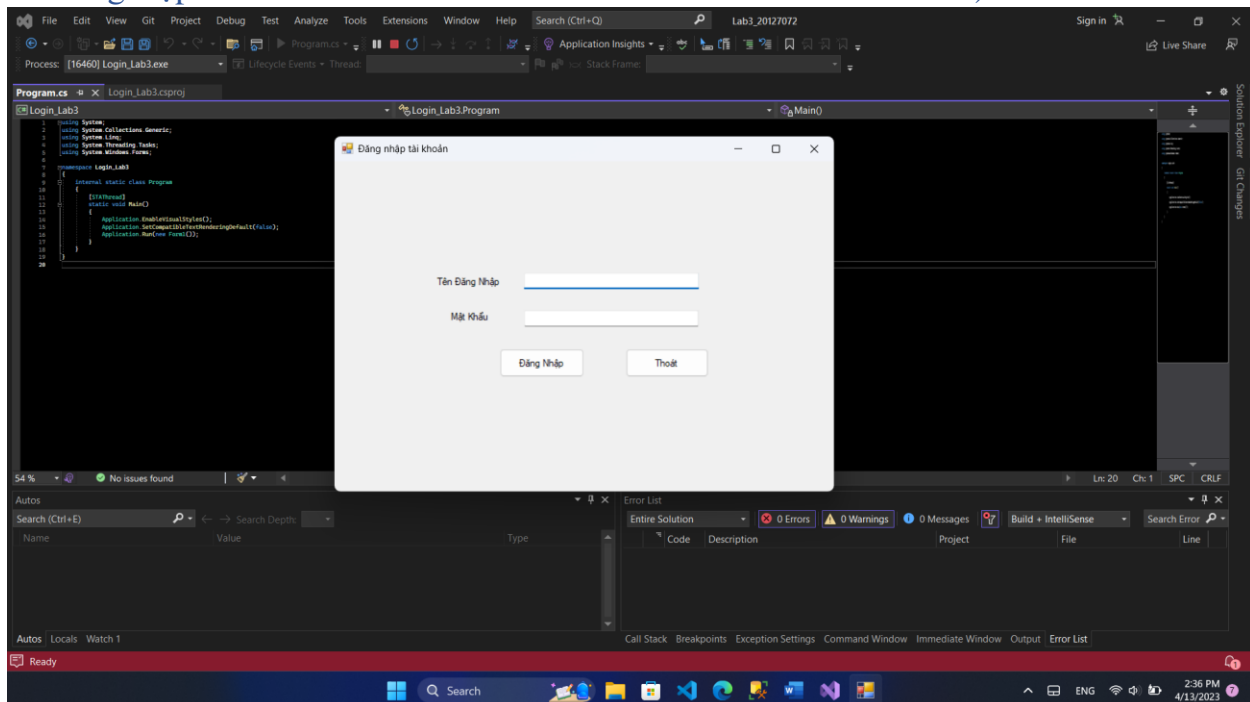
EXEC SP_INS_NHANVIEN 'NV01', N'NGUYEN VAN A', 'NVA@', 3000000, N'NVA', 'abcd12'
SELECT * FROM NHANVIEN
GO

-- (iii). Truy vấn dữ liệu nhân viên
IF OBJECT_ID('SP_SEL_NHANVIEN') IS NOT NULL
    DROP PROCEDURE SP_SEL_NHANVIEN
GO
    
```

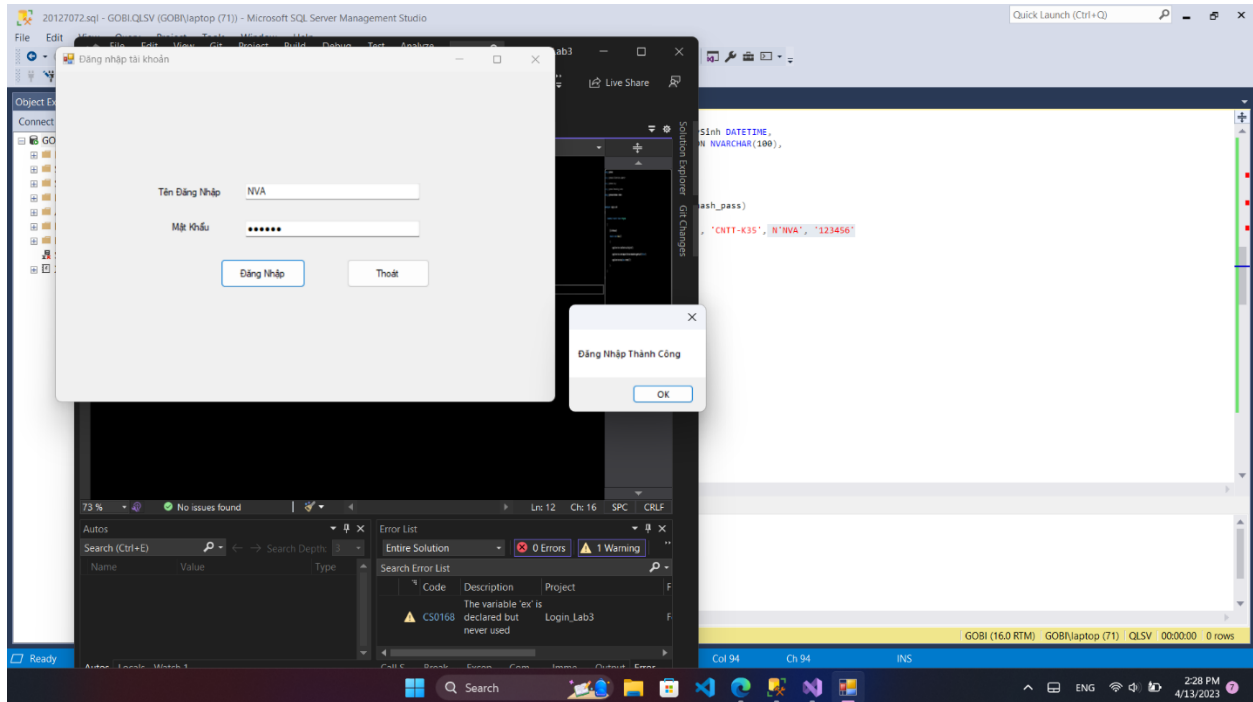
- iii) Stored dùng để truy vấn dữ liệu nhân viên (NHANVIEN)



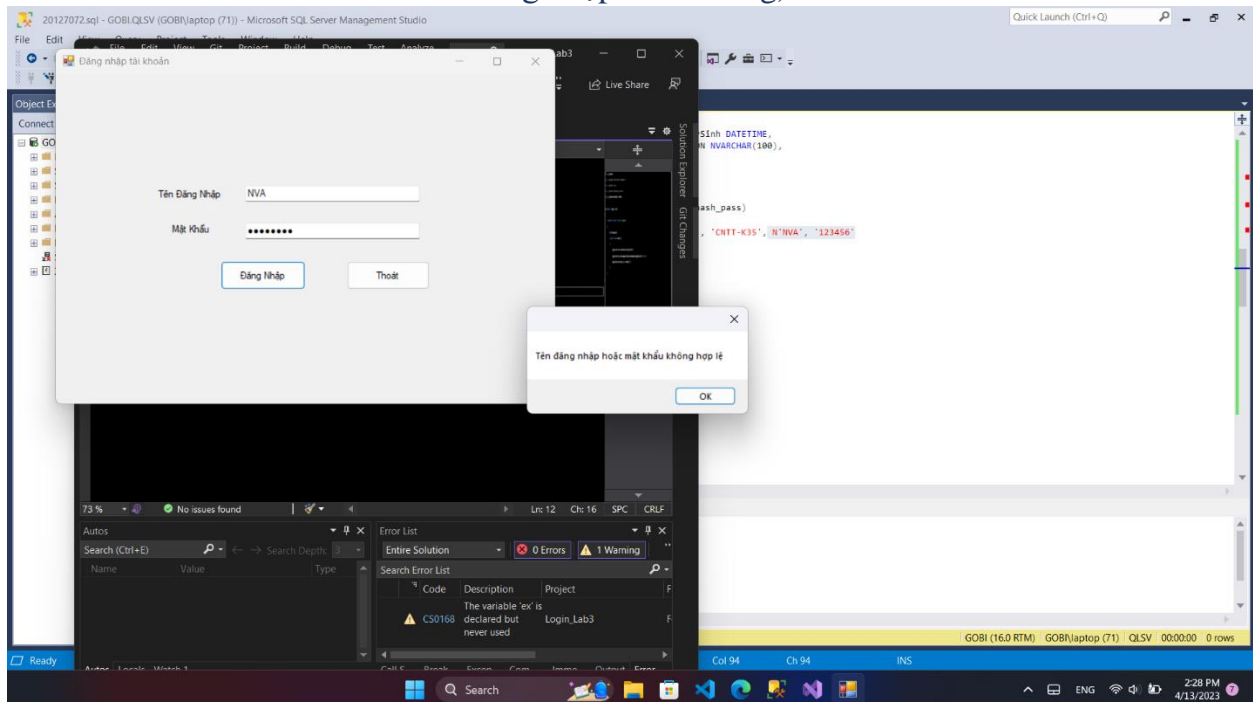
d) Viết màn hình quản lý đăng nhập hệ thống (sử dụng C#), cho phép nhập vào tên đăng nhập và mật khẩu (giả sử tên đăng nhập của sinh viên và nhân viên là duy nhất, nghĩa là tên đăng nhập của tất cả các sinh viên và tất cả nhân viên là khác nhau).



Hình 1: Mở màn hình quản lý đăng nhập trong Visual Studio

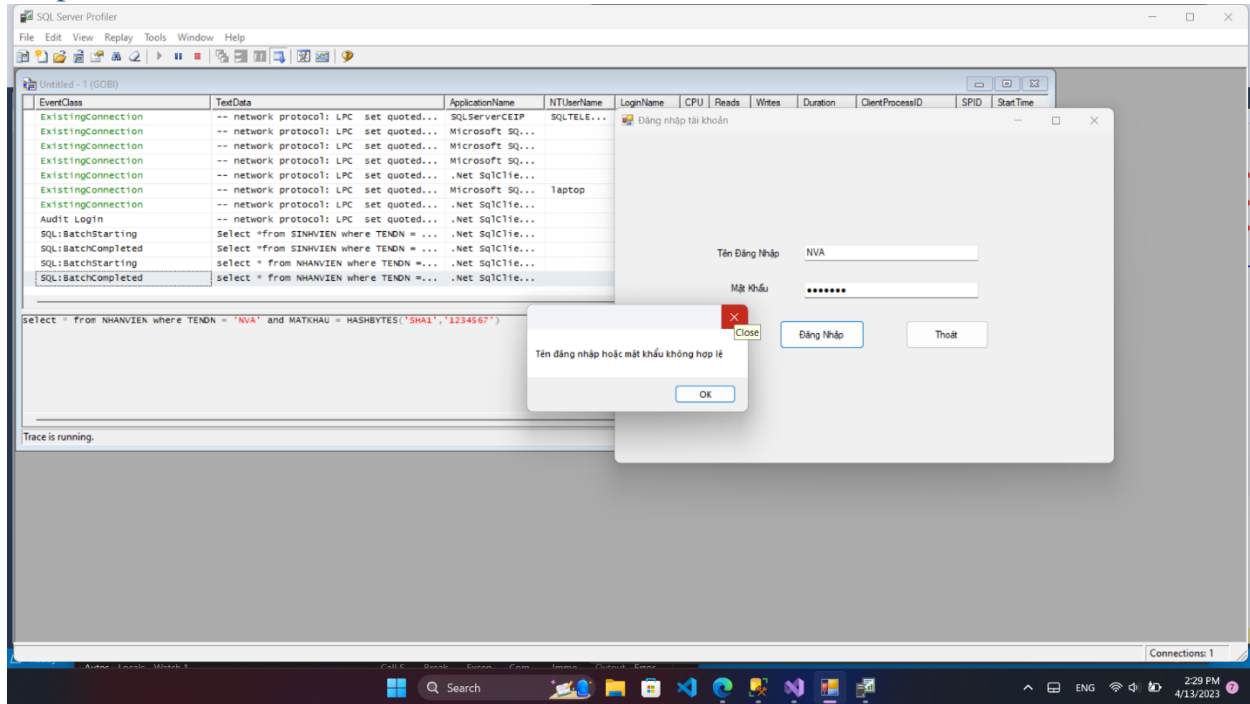


Hình 2: Nhập tên đăng nhập (NVA) và mật khẩu (123456) (bấm vào nút Đăng Nhập thì đăng nhập thành công)

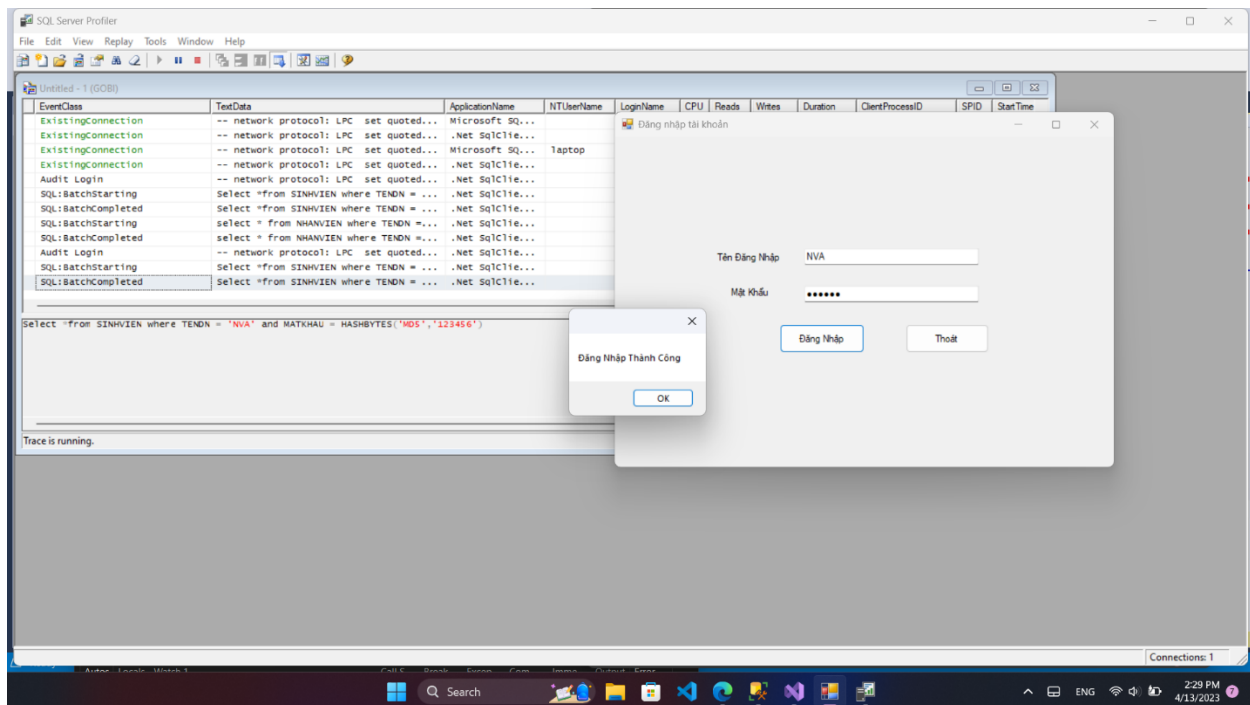


Hình 3: Nhập tên đăng nhập (NVA) và mật khẩu (1234567) (bấm vào nút Đăng nhập thì đăng nhập thất bại)

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



Hình 4: Thông tin đăng nhập không được mã hoá bị lộ trên SQL Profiler



Hình 5: Thông tin đăng nhập không được mã hoá bị lộ trên SQL Profiler

Nhận xét:

Khi bấm nút Đăng nhập, SQL và màn hình quản lý đăng nhập sẽ thiết lập kết nối với nhau thông qua sự kiện Audit Login.

mật khẩu dễ bị đánh cắp do hiện bản rõ trong lúc trao đổi giữa client và server khi truy cập được SQL Server Profiler