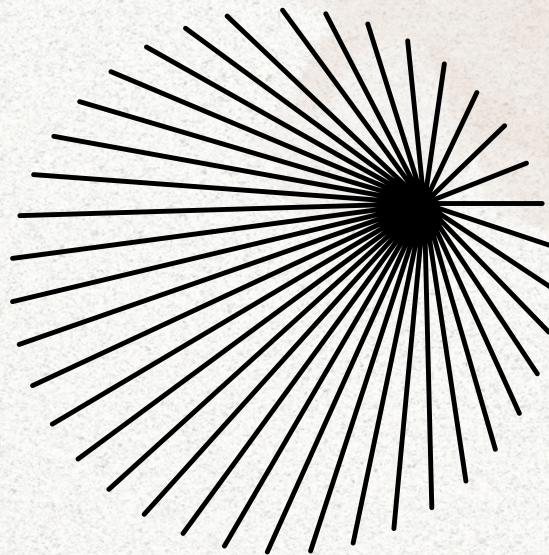




FIT@HCMUS

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



LAB 4 - CÁ NHÂN

BỘ MÔN: BẢO MẬT CƠ SỞ DỮ LIỆU

Sinh viên thực hiện:
21120419 - Vũ Thành Công

TP. Hồ Chí Minh, tháng 5/2024

Mục lục

<i>I. Các stored procedure</i>	2
1. <i>Stored procedure SP_INS_ENCRYPT_SINHVIEN</i>	2
a. <i>Cài đặt</i>	2
b. <i>Thực thi</i>	2
2. <i>Stored procedure SP_INS_ENCRYPT_NHANVIEN.....</i>	2
a. <i>Cài đặt</i>	2
b. <i>Thực thi</i>	2
3. <i>Stored procedure SP_SEL_ENCRYPT_NHANVIEN</i>	2
a. <i>Cài đặt</i>	3
b. <i>Thực thi</i>	3
<i>II. Màn hình quản lý đăng nhập hệ thống</i>	3
1. <i>Màn hình quản lý đăng nhập</i>	3
a. <i>Đăng nhập thành công</i>	3
b. <i>Đăng nhập không thành công</i>	4
2. <i>Theo dõi tác vụ bằng SQL Profile</i>	6
<i>III. Màn hình load danh sách nhân viên</i>	8
1. <i>Màn hình load danh sách</i>	8
a. <i>Màn hình load</i>	8
b. <i>Thao tác thêm nhân viên</i>	9
2. <i>Theo dõi load màn hình danh sách nhân viên bằng SQL Profile</i>	11
3. <i>Theo dõi thêm mới nhân viên bằng SQL Profile</i>	12

I. Các stored procedure

1. Stored procedure SP_INS_ENCRYPT_SINHVIEN

a. Cài đặt

```
--CREATE PROC SP_INS_ENCRYPT_SINHVIEN
(
    @MASV NVARCHAR(20),
    @HOTEN NVARCHAR(100),
    @NGAYSINH DATETIME,
    @DIACHI NVARCHAR(200),
    @MALOP VARCHAR(20),
    @TENDN NVARCHAR(100),
    @MATKHAU VARBINARY(MAX)
)
AS
INSERT INTO SINHVIEN
VALUES (@MASV, @HOTEN, @NGAYSINH, @DIACHI, @MALOP, @TENDN, @MATKHAU)
```

b. Thực thi

```
EXEC SP_INS_ENCRYPT_SINHVIEN '21120419', N'VŨ THÀNH CÔNG', '1/1/2003', N'LÂM ĐỒNG', 'CNTT-K21', '21120419', 0xD6FDC1A6004C3A44DC40EC97A8961FAE;
EXEC SP_INS_ENCRYPT_SINHVIEN '35120001', N'CÔNG THÀNH VŨ', '11/11/2017', N'LONG AN', 'CNTT-K35', '35120001', 0x192A1A8DDDC67D7CFB5EB7AA692FB143;
EXEC SP_INS_ENCRYPT_SINHVIEN '46120030', N'VŨ CÔNG', '12/12/2028', N'DÔNG THÁP', 'CNTT-K46', '46120030', 0x194A5E7DCBEE7955205C8D99C4573090;
-- 21120419 : abcd419
-- 35120001 : abcd001
-- 46120030 : abcd030
```

2. Stored procedure SP_INS_ENCRYPT_NHANVIEN

a. Cài đặt

```
--CREATE PROC SP_INS_ENCRYPT_NHANVIEN
(
    @MANV VARCHAR(20),
    @HOTEN NVARCHAR(100),
    @EMAIL VARCHAR(20),
    @LUONG VARBINARY(MAX),
    @TENDN NVARCHAR(100),
    @MATKHAU VARBINARY(MAX)
)
AS
INSERT INTO NHANVIEN
VALUES (@MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MATKHAU)
```

b. Thực thi

```
EXEC SP_INS_ENCRYPT_NHANVIEN 'NV10', N'Kali Mall', 'kali@mail.com', 0x65CAE6AE21D77088679DDE132FAB0265, N'kali', 0xE4FF1A53D4C61D8727838A0DE0197FBFE030653E;
-- tendn: kali
-- pass: kalixxx
-- luong: 5000
```

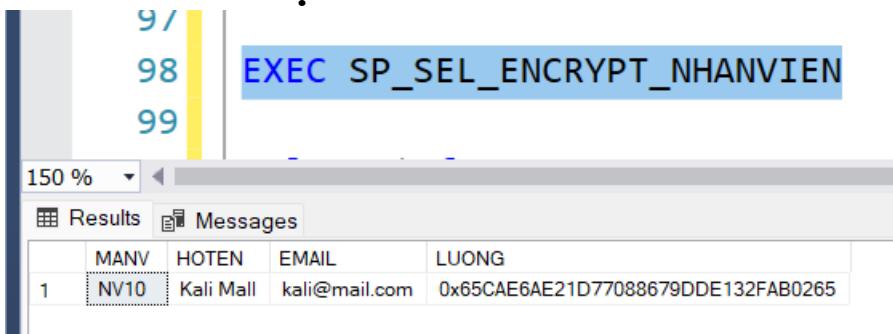
3. Stored procedure SP_SEL_ENCRYPT_NHANVIEN

a. Cài đặt

```

CREATE PROC SP_SEL_ENCRYPT_NHANVIEN
AS
    SELECT MANV, HOTEN, EMAIL, LUONG FROM NHANVIEN

```

b. Thực thi


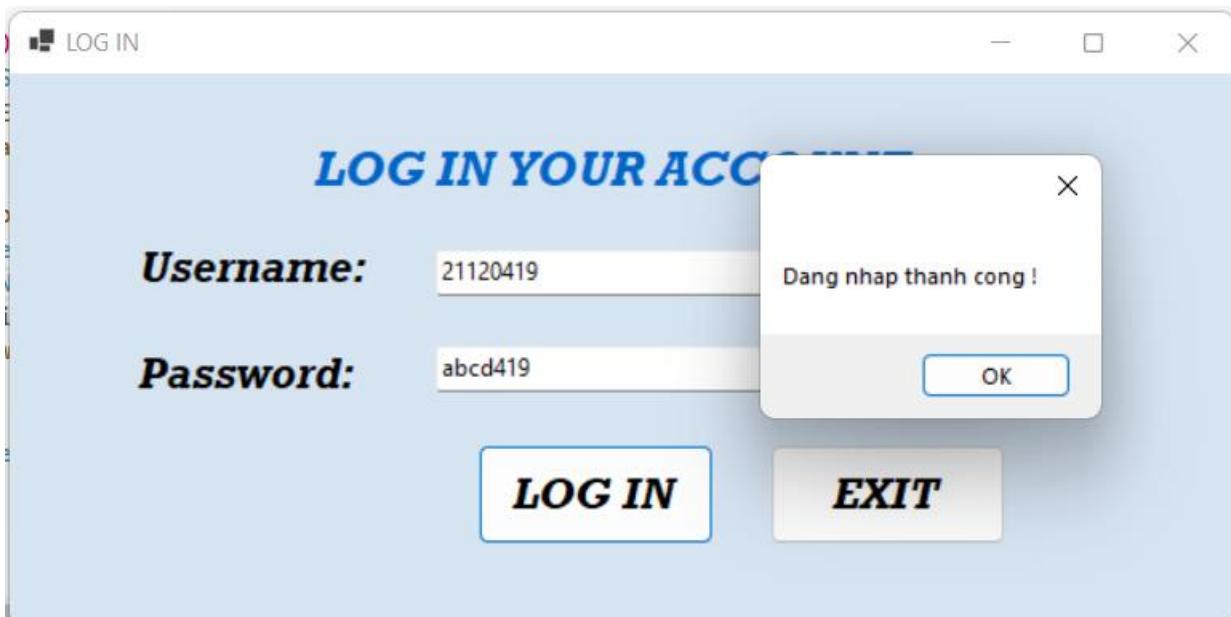
```

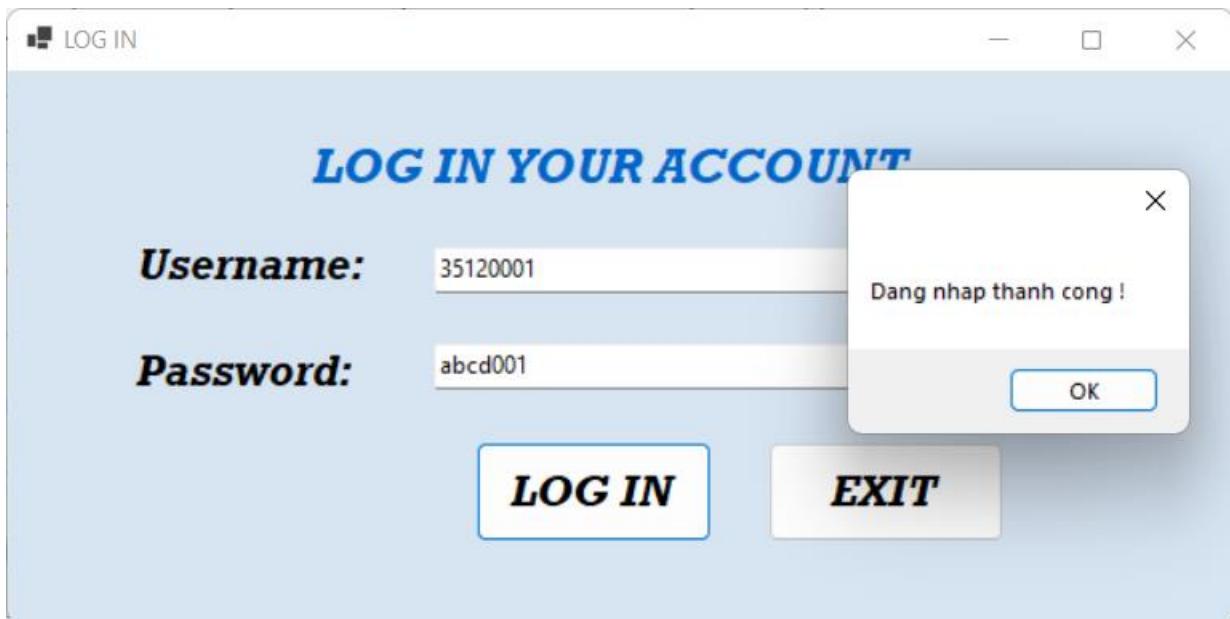
9/
98 EXEC SP_SEL_ENCRYPT_NHANVIEN
99
150 %
Results Messages
MANV HOTEN EMAIL LUONG
1 NV10 Kali Mall kali@mail.com 0x65CAE6AE21D77088679DDE132FAB0265

```

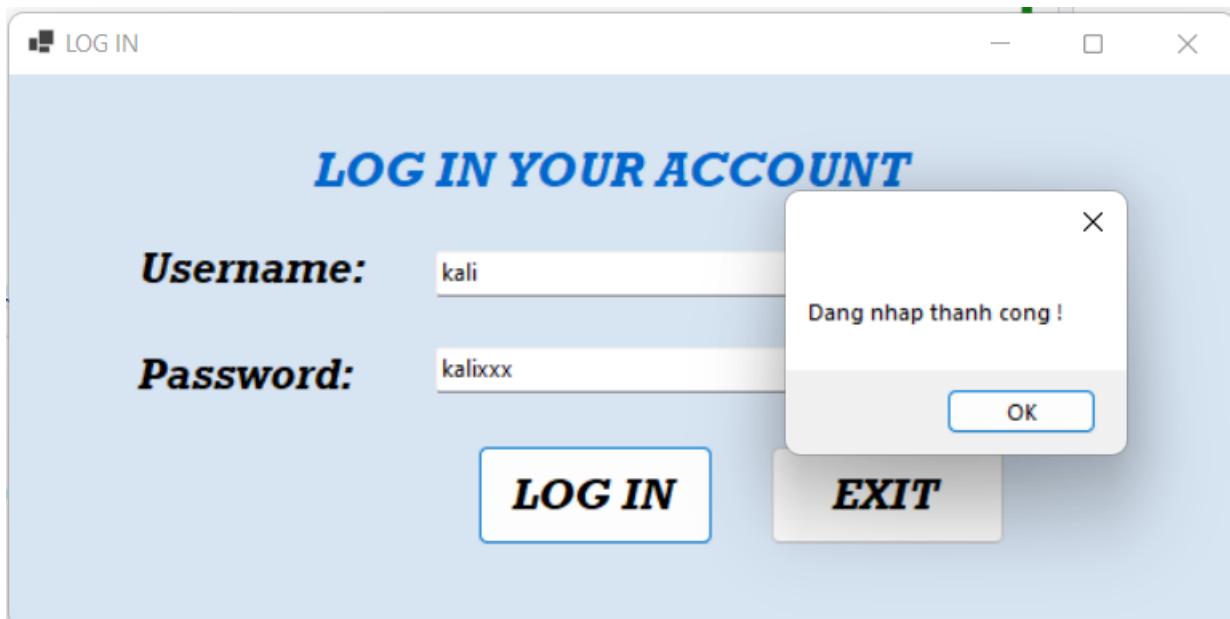
II. Màn hình quản lý đăng nhập hệ thống**1. Màn hình quản lý đăng nhập****a. Đăng nhập thành công**

- Đối với SINH VIÊN



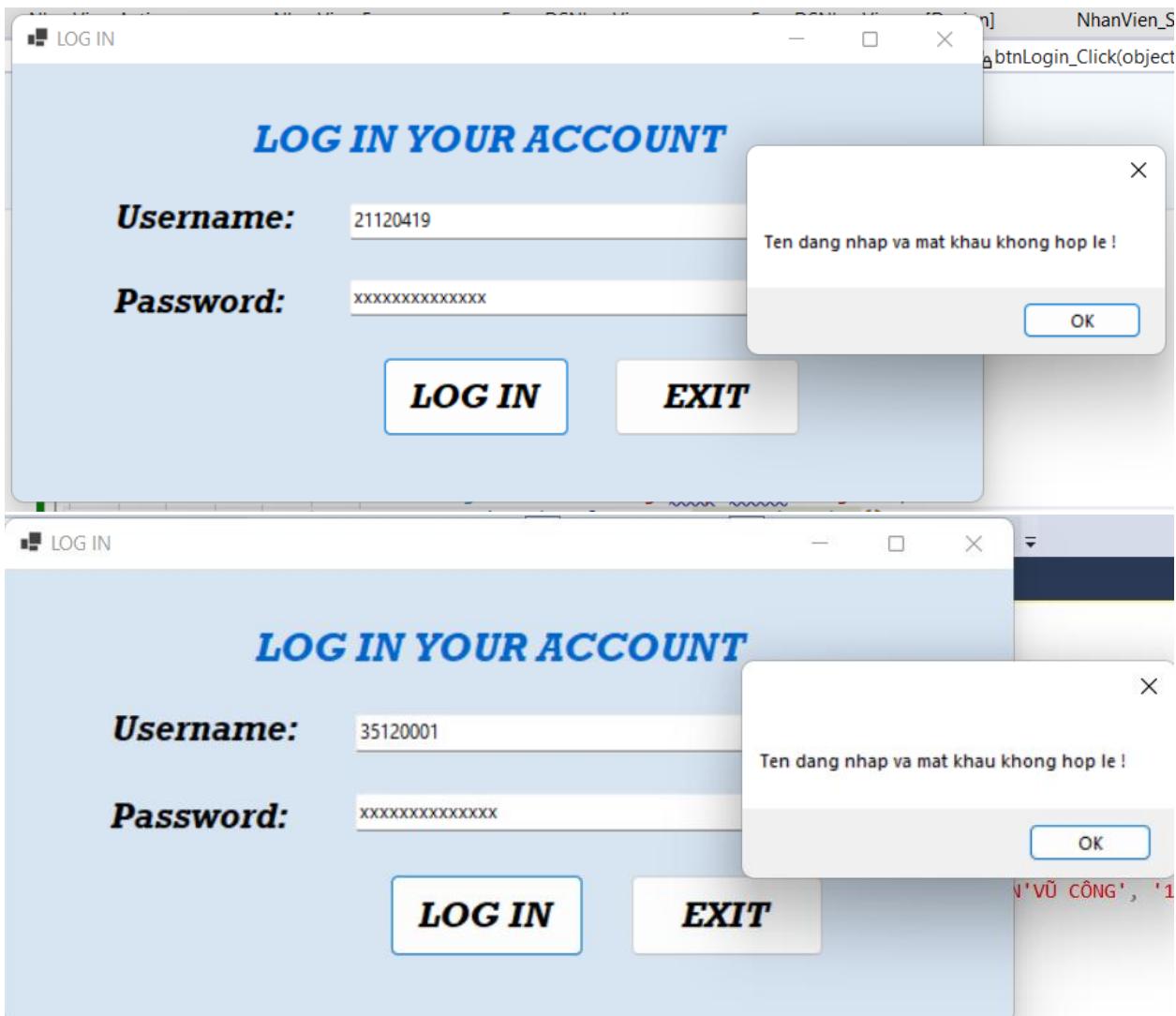


- *Đối với NHÂN VIÊN*

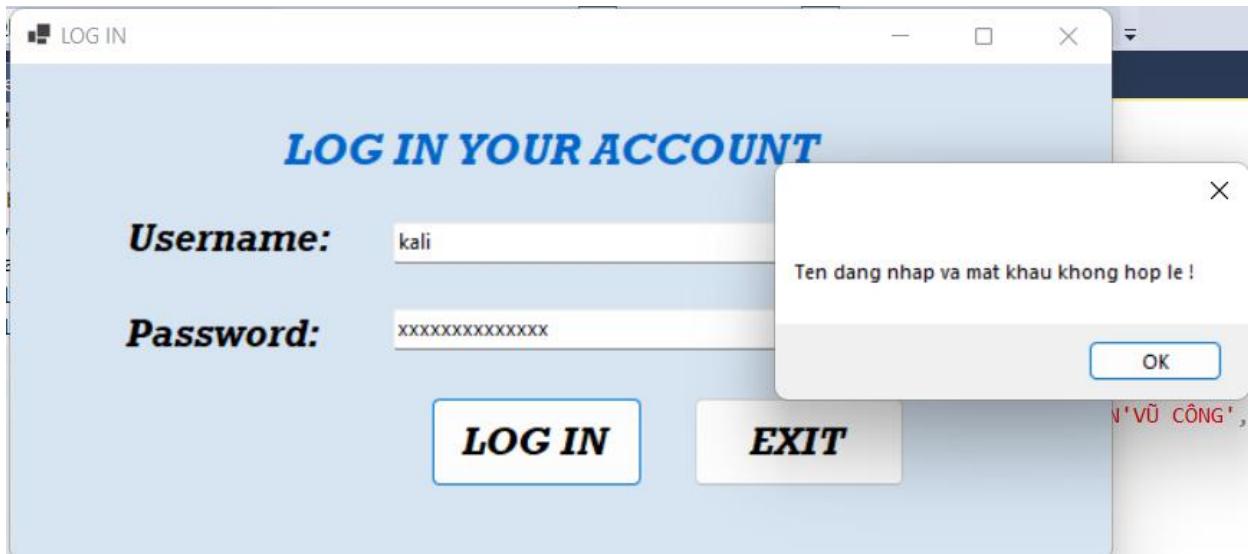


b. Đăng nhập không thành công

- *Đối với SINH VIÊN*



- Đối với NHÂN VIÊN

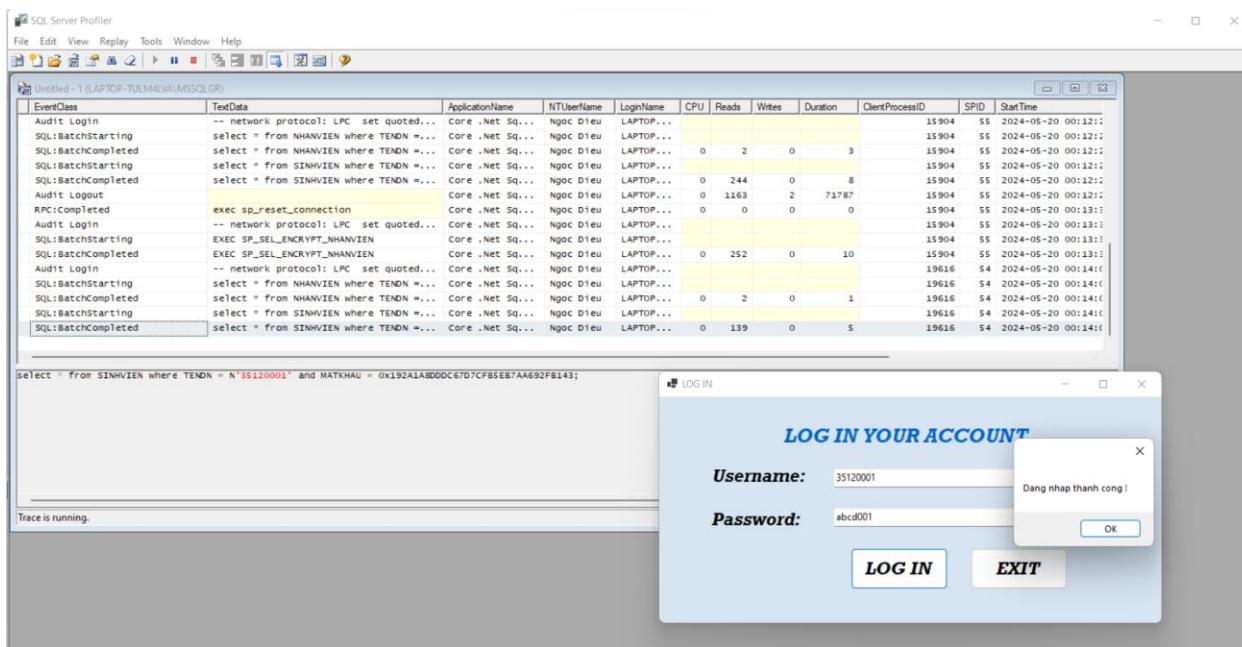


2. Theo dõi tác vụ bằng SQL Profile

- *Đối với SINH VIÊN*

- Đăng nhập:

EventClass	TedData	ApplicationName	NTUserName	LoginName	CPU	Reads	Wites	Duration	ClientProcessID	SPID	StartTime
Audit Login	-- network protocol: LPC set quoted...	SQLServerCEIP	SQLELE...	NT SER...					21984	\$1	2024-01-01 00:00:00.000
SQL:BatchStarting	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLELE...	NT SER...					21984	\$1	2024-01-01 00:00:00.000
SQL:BatchCompleted	SET DEADLOCK_PRIORITY -10	SQLServerCEIP	SQLELE...	NT SER...	0	0	0	0	21984	\$1	2024-01-01 00:00:00.000
SQL:BatchStarting	if not exists (select * from sys.dm...	SQLServerCEIP	SQLELE...	NT SER...					21984	\$1	2024-01-01 00:00:00.000
SQL:BatchCompleted	if not exists (select * from sys.dm...	SQLServerCEIP	SQLELE...	NT SER...	0	20	0	1	21984	\$1	2024-01-01 00:00:00.000
Audit Logout	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	917	2	732570		15904	\$5	2024-01-01 00:00:00.000
RPC:Completed	exec sp_reset_connection	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	0	0	0	15904	\$5	2024-01-01 00:00:00.000
Audit Login	-- network protocol: LPC set quoted...	Core .Net Sq...	Ngoc Dieu	LAPTOP...					15904	\$5	2024-01-01 00:00:00.000
SQL:BatchStarting	select * from NHANVIEN where TENDON =...	Core .Net Sq...	Ngoc Dieu	LAPTOP...					15904	\$5	2024-01-01 00:00:00.000
SQL:BatchCompleted	select * from NHANVIEN where TENDON =...	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	2	0	3	15904	\$5	2024-01-01 00:00:00.000
SQL:BatchStarting	select * from SINHVIEN where TENDON =...	Core .Net Sq...	Ngoc Dieu	LAPTOP...					15904	\$5	2024-01-01 00:00:00.000
SQL:BatchCompleted	select * from SINHVIEN where TENDON =...	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	244	0	8	15904	\$5	2024-01-01 00:00:00.000



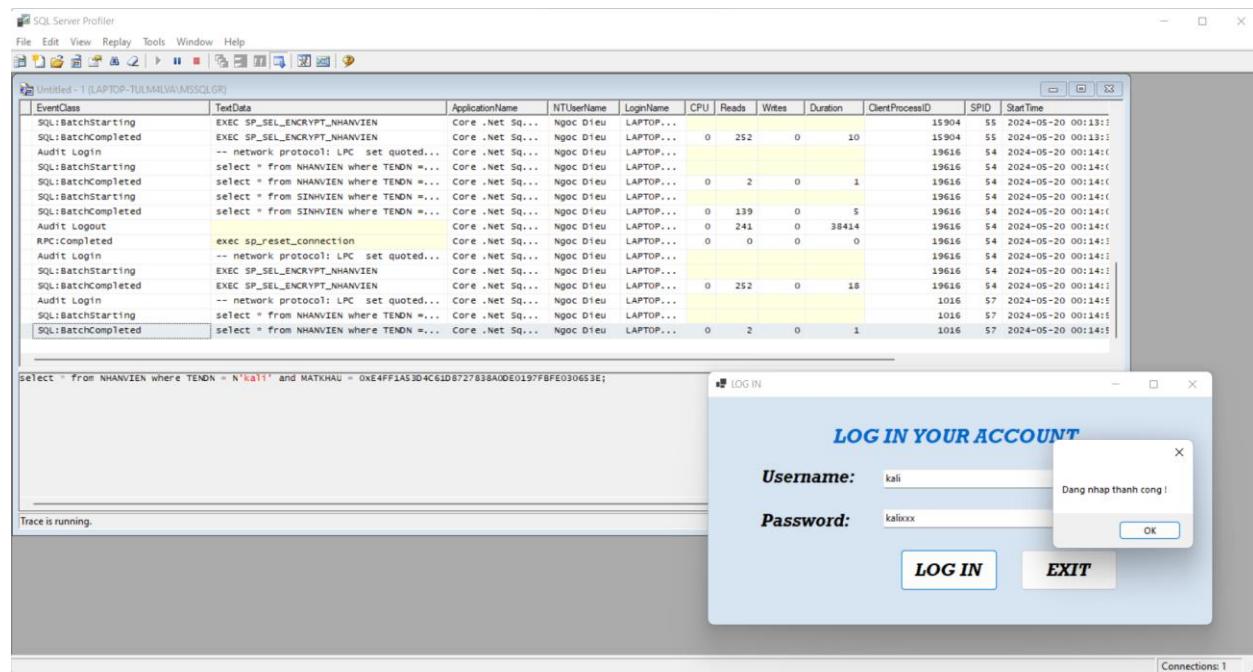
- Thực thi câu lệnh:

```

107 |      121 %
108 |      | select * from SINHVIEN where TENDN = N'21120419' and MATKHAU = 0xD6FDC1A6004C3A44DC40EC97A8961FAE;
      |
      | Results  Messages
      | MASV   HOTEN   NGAYSINH    DIACHI  MALOP  TENDN  MATKHAU
      | 21120419 VŨ THÀNH CÔNG 2003-01-01 00:00:00.000 LÂM ĐỒNG CNTT-K21 21120419 0xD6FDC1A6004C3A44DC40EC97A8961FAE
      |
      | 105 |      121 %
106 |      | select * from SINHVIEN where TENDN = N'35120001' and MATKHAU = 0x192A1A8DDDC67D7CFB5EB7AA692FB143;
      |
      | Results  Messages
      | MASV   HOTEN   NGAYSINH    DIACHI  MALOP  TENDN  MATKHAU
      | 35120001 CÔNG THÀNH VŨ 2017-11-11 00:00:00.000 LONG AN  CNTT-K35 35120001 0x192A1A8DDDC67D7CFB5EB7AA692FB143
  
```

- Đối với NHÂN VIÊN

- Đăng nhập:



- Thực thi câu lệnh:

```
103 | select * from NHANVIEN where TENDN = N'kali' and MATKHAU = 0xE4FF1A53D4C61D8727838A0DE0197FBFE030653E;
104 |
```

Results

MANV	HOTEN	EMAIL	LUONG	TENDN	MATKHAU	
1	NV10	Kali Mall	kali@mail.com	0x65CAE6AE21D77088679DDE132FAB0265	kali	0xE4FF1A53D4C61D8727838A0DE0197FBFE030653E

- Nhận xét:

- Các thuộc tính cần giữ bí mật như mật khẩu hay lương đã bị mã hóa ở phía Client rồi truyền xuống dưới database. Vì vậy nên an toàn đối với người trung gian và kẻ tấn công (chỉ có chuỗi mật khẩu đã bị mã hóa).
- Nếu kẻ tấn công có quyền truy cập vào SQL Profile thì cũng không thể thấy được các thuộc tính nhạy cảm cần được mã hóa.

III. Màn hình load danh sách nhân viên

1. Màn hình load danh sách

a. Màn hình load

Sau khi đăng nhập với tên đăng nhập và mật khẩu đúng sẽ có thông báo hiện lên “Dang nhap thanh cong”. Khi đó, chỉ cần nhấn “OK” thì màn hình load danh sách nhân viên sẽ hiện ra:

The screenshot shows a Windows application window titled "Danh mục nhân viên". The window has a title bar with standard window controls (minimize, maximize, close). Below the title bar is a header with the text "DANH MỤC NHÂN VIÊN". Under the header is a section labeled "Thông tin nhân viên" (Employee Information) containing four input fields: "Mã NV" (NV10), "Họ tên" (Kali Mall), "Email" (kali@mail.com), and "Lương" (5000). Below this is a table with four columns: "MANV", "HOTEN", "EMAIL", and "LUONG". A single row is visible in the table, showing the data from the input fields. At the bottom of the window are six buttons: "Thêm", "Xóa", "Sửa", "Ghi/Lưu", "Không", and "Thoát".

Khi đó, nếu nhấn vào nhân viên nào đó sẽ có thông tin nhân viên đó hiện ra, với dữ liệu LUONG đã được decrypt và dữ liệu TENDN và MATKHAU sẽ được để trống.

b. Thao tác thêm nhân viên

Nhấn vào nút thêm để thực hiện thêm mới nhân viên. Sau đó, điền các thông tin vào các thanh phần thông tin nhân viên

Danh mục nhân viên

DANH MỤC NHÂN VIÊN

Thông tin nhân viên			
Mã NV	NV11	Họ tên	Burp Suite
Email	burpsuite@mail.edu.vn	Lương	6000
Tên đăng nhập	burp	Mật khẩu	burpxxx

	MANV	HOTEN	EMAIL	LUONG
▶	NV10	Kali Mall	kali@mail.com	5000
*				

Sau đó, nhấn vào Ghi/Lưu thì các thông tin vừa rồi ngay lập tức được lưu vào database và phần Data Grid View bên dưới ngay lập tức cập nhật thông tin vừa mới thêm vào.

Danh mục nhân viên

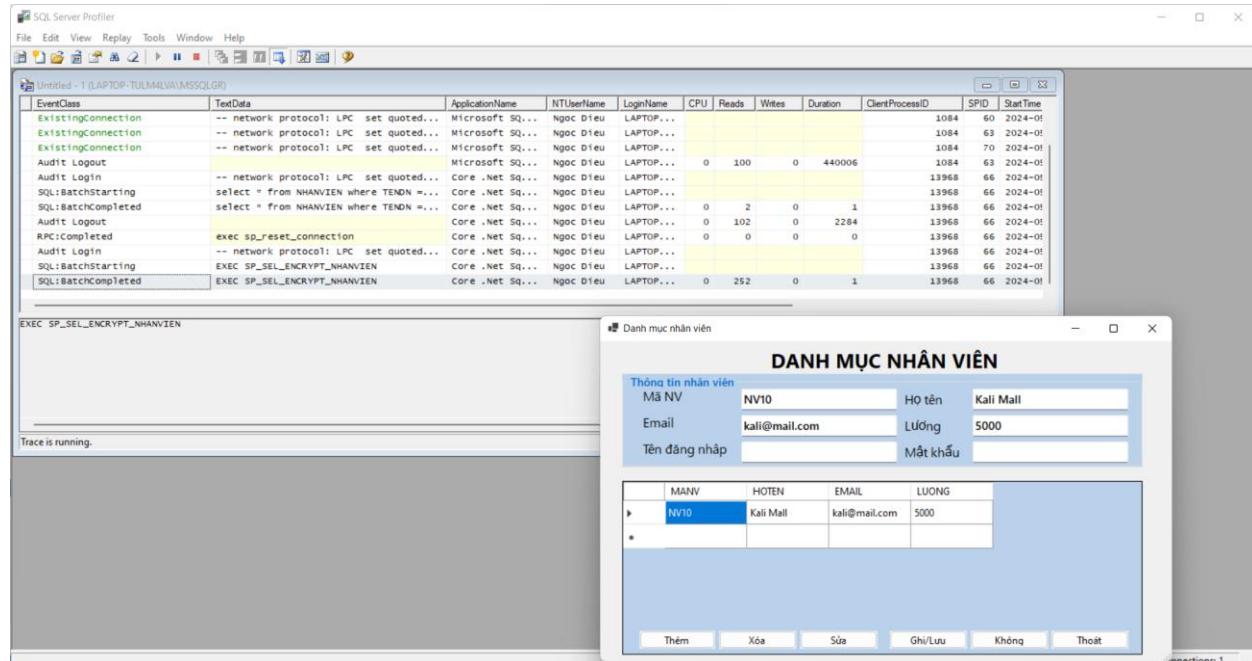
DANH MỤC NHÂN VIÊN

Thông tin nhân viên			
Mã NV	NV11	Họ tên	Burp Suite
Email	burpsuite@mail.edu.vn	Lương	6000
Tên đăng nhập	burp	Mật khẩu	burpxxx

	MANV	HOTEN	EMAIL	LUONG
▶	NV10	Kali Mall	kali@mail.com	5000
	NV11	Burp Suite	burpsuite@mail...	6000
*				

2. Theo dõi load màn hình danh sách nhân viên bằng SQL Profile

Sau khi đăng nhập bằng TENDN với MATKHAU chính xác, màn hình load danh sách nhân viên sẽ hiện ra



Khi đó, trong màn hình SQL Profiler, ta sẽ nhận được câu lệnh đã được thực hiện là: EXEC SP SEL ENCRYPT NHANVIEN

Copy câu lệnh qua SQL để thực hiện, ta được:

```
107 |  
108 EXEC SP_SEL_ENCRYPT_NHANVIEN
```



Nhân xét:

- Câu lệnh được thực thi thông qua stored procedure nên SQL Profiler không thể thấy trực tiếp được câu lệnh thực thi SQL
 - Thuộc tính LUONG của các nhân viên đã được mã hóa và chỉ có người dùng bên phía Client mới có thể giải mã. Đảm bảo bí mật chỉ những người có khóa mới có thể xem được dữ liệu

3. Theo dõi thêm mới nhân viên bằng SQL Profile

Sau khi nhấn nút Ghi/Lưu để thêm thông tin nhân viên mới vào database, chuyển qua SQL Profiler, ta có như sau:

RPC:Completed	exec sp_reset_connection	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	0	0	0	7924	57	2024-05
Audit Login	-- network protocol: LPC set quoted...	Core .Net Sq...	Ngoc Dieu	LAPTOP...					7924	57	2024-05
RPC:Completed	exec sp_executesql N'EXEC SP_INS_ENC...	Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	270	1	15	7924	57	2024-05
Audit Logout		Core .Net Sq...	Ngoc Dieu	LAPTOP...	0	674	1	17	7924	57	2024-05

exec sp_executesql N'EXEC SP_TNS_ENCRYPT_NHANVIEN @MANV, @HOTEN, @EMAIL, @LUONG, @TENDN, @MATKHAU', N'@MANV varchar(4),@HOTEN nvarchar(10),@EMAIL varchar(21),@LUONG varbinary(16),@TENDN nvarchar(4),@MATKHAU varbinary(20)', @MANV='NV11', @HOTEN=N'Burp Suite!', @EMAIL='burpsuite@mail.edu.vn', @LUONG=0xF9459E85B158469E6A38E6366165EE78, @TENDN=N'burp', @MATKHAU=0XCA3AE1B229F2CA5FDE4E1F8A7550FC8529EE18E5

Nhận xét:

- Sau khi nhấn nút Ghi/Lưu, dữ liệu sẽ được lấy từ textbox, sau đó đem đi mã hóa rồi mới được lưu vào database.
- Khi đó, việc mã hóa và giải mã sẽ được thực hiện trước khi truyền vào database, vì vậy khi sử dụng SQL Profiler để theo dõi, thì các thuộc tính nhạy cảm đã được mã hóa và không thể thấy được.
- Khi đó, các dữ liệu sẽ được đảm bảo an toàn hơn.