

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

BÁO CÁO LAB 02

Đề tài: Phân quyền truy cập các đối tượng trong CSDL

Môn học: Bảo mật cơ sở dữ liệu

Sinh viên thực hiện:

Doãn Hoàng Sơn - 22127365

Võ Hữu Tuấn - 22127439

Giáo viên hướng dẫn:

Cô Nguyễn Thị Hường

Thầy Nguyễn Đình Thúc

Thầy Lê Trọng Anh Tú



Mục lục

Bảng phân công công việc	2
Câu a	3
Câu b	3
Câu c	3
Câu d	3
Câu e	5
Câu f	5
Câu g	7
Câu h	8
Câu i	14
Câu j	19
Nhận xét	24

Table 2

Bảng phân công công việc

Nhóm: 03		
1	Doãn Hoàng Sơn	22127365
2	Võ Hữu Tuấn	22127439

Thông tin nhóm

	Hoàng Sơn	Hữu Tuấn
Câu a	x	
Câu b	x	
Câu c	x	
Câu d	x	
Câu e	x	
Câu f		x
Câu g		x
Câu h		x
Câu i		x
Câu j		x
Báo cáo	x	x

Bảng phân công công việc

Câu a

Thực hiện chạy đoạn mã trong script

Câu b

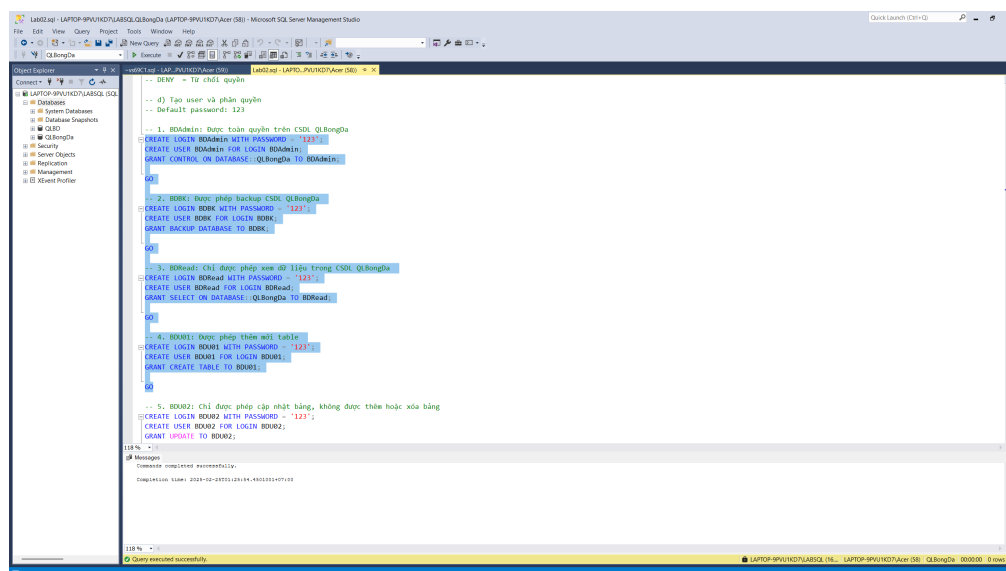
Thực hiện chạy đoạn mã trong script

Câu c

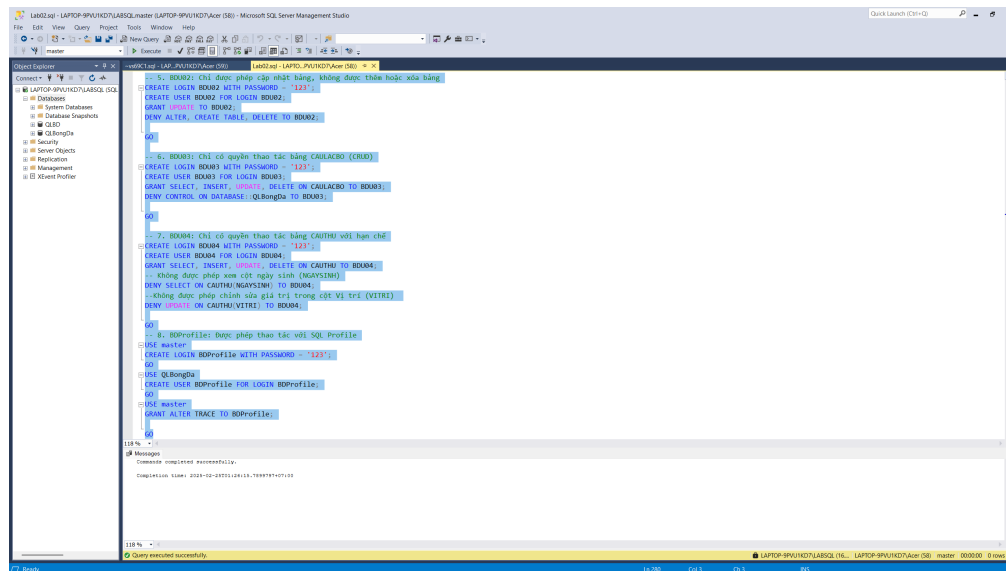
Thực hiện chạy đoạn mã trong script

Câu d

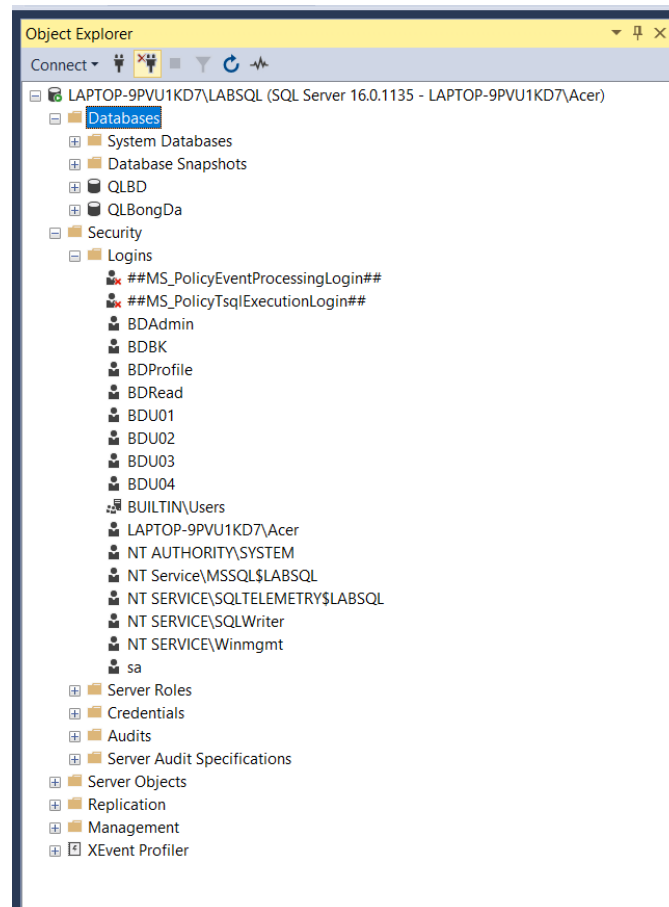
1. Tạo tài khoản LOGIN ở cấp Server
2. Tạo USER ở cấp Database cho LOGIN vừa tạo
3. Cấp quyền hoặc từ chối các quyền cho USER
4. Kiểm tra lại các User đã tạo trong SQL Server → Security → Logins



Mã script và kết quả câu d (4 User đầu tiên)

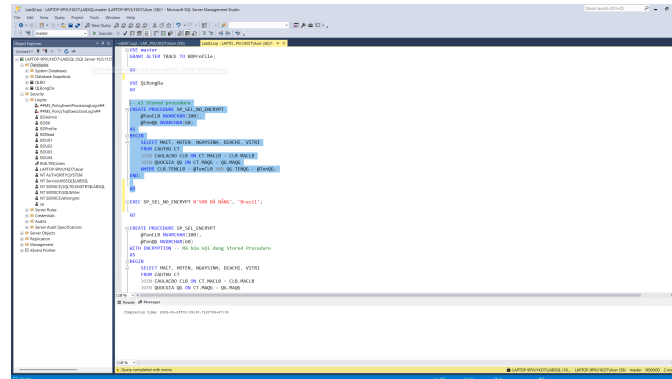


Mã script và kết quả câu d (4 User còn lại)

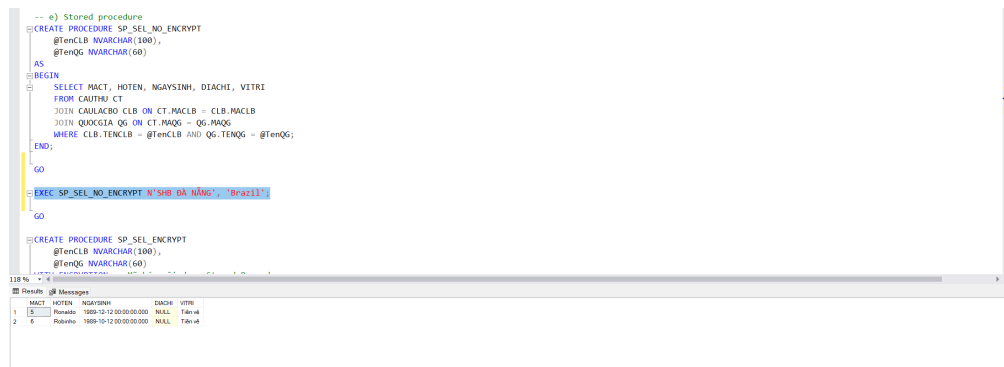


Kết quả sau khi hoàn thành câu d

Câu e



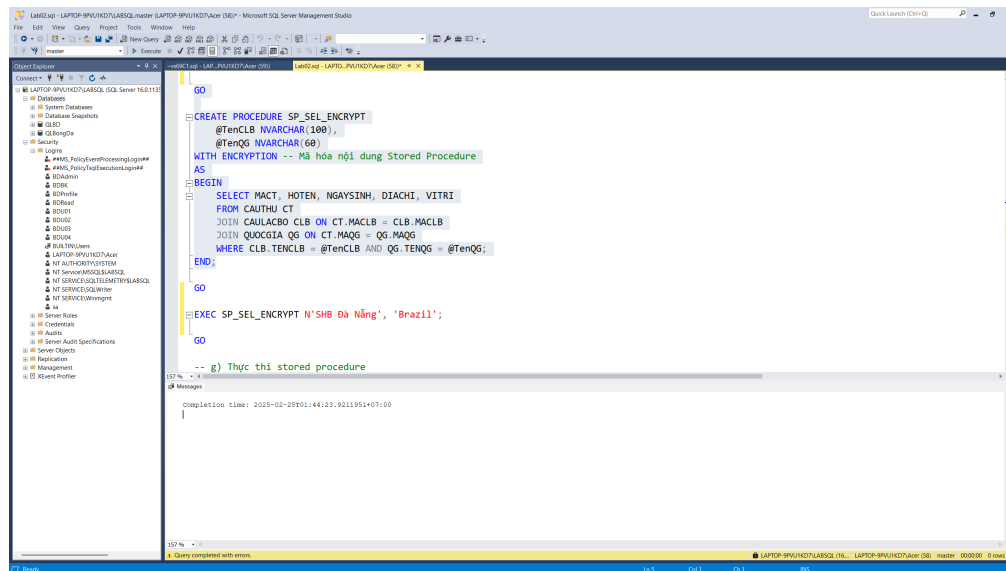
Mã script và kết quả tạo stored procedure **SP_SEL_NO_ENCRYPT**



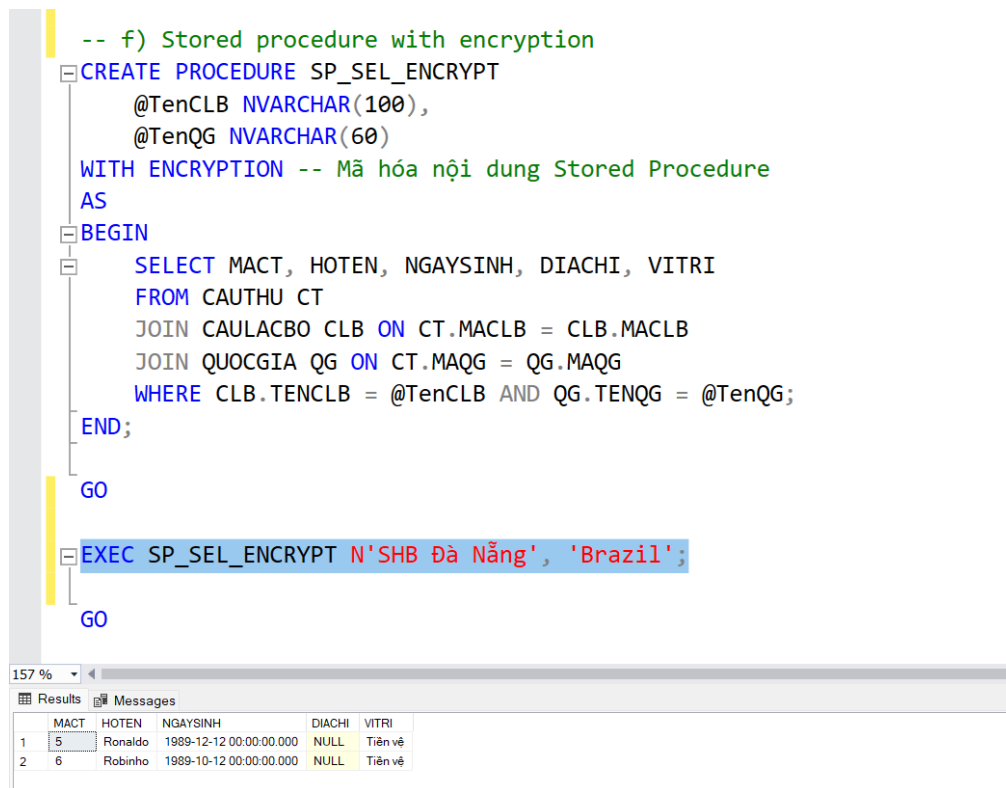
Kết quả thực thi câu e

Câu f

Tương tự như câu e, nhưng stored procedure *được mã hóa*



Mã script và kết quả tạo stored procedure **SP_SEL_ENCRYPT**



Kết quả thực thi câu f

Câu g

```
-- g) Thực thi stored procedure
EXEC SP_SEL_NO_ENCRYPT N'SHB ĐÀ NẴNG', 'Brazil';
EXEC SP_SEL_ENCRYPT N'SHB ĐÀ NẴNG', 'Brazil';

GO

-- Xem mã nguồn stored procedure
EXEC sp_helptext 'SP_SEL_NO_ENCRYPT';
EXEC sp_helptext 'SP_SEL_ENCRYPT';
```

157 %

Results Messages

	MACT	HOTEN	NGAYSINH	DIACHI	VITRI
1	5	Ronaldo	1989-12-12 00:00:00.000	NULL	Tiền vệ
2	6	Robinho	1989-10-12 00:00:00.000	NULL	Tiền vệ

	MACT	HOTEN	NGAYSINH	DIACHI	VITRI
1	5	Ronaldo	1989-12-12 00:00:00.000	NULL	Tiền vệ
2	6	Robinho	1989-10-12 00:00:00.000	NULL	Tiền vệ

Kết quả thực thi stored procedure **SP_SEL_ENCRYPT** và **SP_SEL_NO_ENCRYPT**

* NHẬN XÉT:

- Kết quả thực thi cho thấy stored procedure mặc định và stored procedure được mã hóa **đều** trả về kết quả giống nhau.
- Nhưng **stored procedure được mã hóa** có tính bảo mật cao hơn vì không cho phép xem mã nguồn của nó:


```
-- Xem mã nguồn stored procedure
EXEC sp_helptext 'SP_SEL_NO_ENCRYPT';
EXEC sp_helptext 'SP_SEL_ENCRYPT';
```

157 %

Results Messages

	Text
1	CREATE PROCEDURE SP_SEL_NO_ENCRYPT @TenCLB NV...
2	ERE CLB.TENCLB = @TenCLB AND QG.TENQG = @TenQG; END;

Xem mã nguồn của **SP_SEL_NO_ENCRYPT**

```
-- Xem mã nguồn stored procedure
EXEC sp_helptext 'SP_SEL_NO_ENCRYPT';
EXEC sp_helptext 'SP_SEL_ENCRYPT';
```

157 %

Messages

The text for object 'SP_SEL_ENCRYPT' is encrypted.

Completion time: 2025-02-25T01:57:06.9931482+07:00

Xem mã nguồn của **SP_SEL_ENCRYPT** (bị từ chối)

Câu h

Tuy trong SQL không có hàm có sẵn để thực hiện việc chuyển 1 stored procedure sang stored procedure with Encrypt. Nhưng có thể thực hiện thủ công theo cách sau:

1. Duyệt hết database để kiểm tất cả stored procedure đang có. Với mỗi stored procedure thực hiện các bước sau:
2. Lọc ra các **stored procedure no encrypt**
3. Lấy mã nguồn của stored procedure no encrypt

4. Thêm **"WITH ENCRYPTION"** vào mã nguồn của stored procedure và lưu lại
5. Xóa stored procedure (cũ) đã tạo đó
6. Chạy mã nguồn stored procedure mới lưu

* Lưu ý: Để không ảnh hưởng đến các câu khác, ta sẽ tạo 1 database có dữ liệu tương tự như **QLBongDa**

```
GO

-- Lấy danh sách các stored procedure no encrypt
SELECT p.name AS StoredProcedureName
FROM sys.procedures p
JOIN sys.sql_modules m ON p.object_id = m.object_id
WHERE m.definition IS NOT NULL -- no encrypt

GO

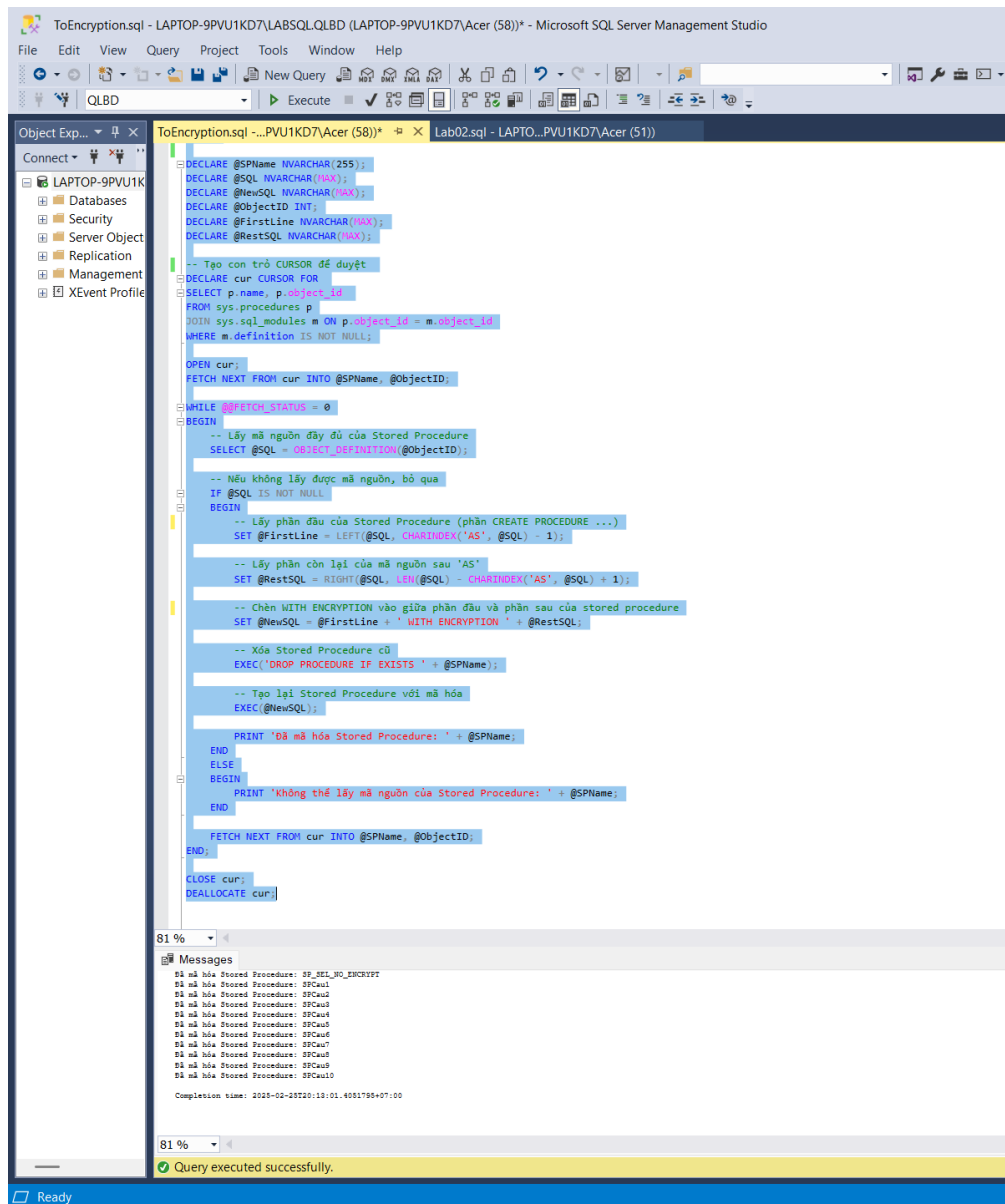
-- Kiểm tra mã nguồn từng stored procedure
EXEC sp_helptext 'SPCau1';
EXEC sp_helptext 'SPCau2';
EXEC sp_helptext 'SPCau3';
EXEC sp_helptext 'SPCau4';
EXEC sp_helptext 'SPCau5';
EXEC sp_helptext 'SPCau6';
EXEC sp_helptext 'SPCau7';
EXEC sp_helptext 'SPCau8';
EXEC sp_helptext 'SPCau9';
EXEC sp_helptext 'SPCau10';
```

143 %

Results Messages

	StoredProcedureName
1	SP_SEL_NO_ENCRYPT
2	SPCau1
3	SPCau2
4	SPCau3
5	SPCau4
6	SPCau5
7	SPCau6
8	SPCau7
9	SPCau8
10	SPCau9
11	SPCau10

Danh sách các stored procedure no encrypt ban đầu



```
DECLARE @SPName NVARCHAR(255);
DECLARE @SQL NVARCHAR(MAX);
DECLARE @NewSQL NVARCHAR(MAX);
DECLARE @ObjectID INT;
DECLARE @FirstLine NVARCHAR(MAX);
DECLARE @RestSQL NVARCHAR(MAX);

-- Tạo con trỏ CURSOR để duyệt
DECLARE cur CURSOR FOR
SELECT p.name, p.object_id
FROM sys.procedures p
JOIN sys.sql_modules m ON p.object_id = m.object_id
WHERE m.definition IS NOT NULL;

OPEN cur;
FETCH NEXT FROM cur INTO @SPName, @ObjectID;

WHILE @@FETCH_STATUS = 0
BEGIN
    -- Lấy mã nguồn đầy đủ của Stored Procedure
    SELECT @SQL = OBJECT_DEFINITION(@ObjectID);

    -- Nếu không lấy được mã nguồn, bỏ qua
    IF @SQL IS NOT NULL
    BEGIN
        -- Lấy phần đầu của Stored Procedure (phần CREATE PROCEDURE ...)
        SET @FirstLine = LEFT(@SQL, CHARINDEX('AS', @SQL) - 1);

        -- Lấy phần còn lại của mã nguồn sau 'AS'
        SET @RestSQL = RIGHT(@SQL, LEN(@SQL) - CHARINDEX('AS', @SQL) + 1);

        -- Chèn WITH ENCRYPTION vào giữa phần đầu và phần sau của stored procedure
        SET @NewSQL = @FirstLine + ' WITH ENCRYPTION ' + @RestSQL;

        -- Xóa Stored Procedure cũ
        EXEC('DROP PROCEDURE IF EXISTS ' + @SPName);

        -- Tạo lại Stored Procedure với mã hóa
        EXEC(@NewSQL);

        PRINT 'Đã mã hóa Stored Procedure: ' + @SPName;
    END
    ELSE
    BEGIN
        PRINT 'Không thể lấy mã nguồn của Stored Procedure: ' + @SPName;
    END

    FETCH NEXT FROM cur INTO @SPName, @ObjectID;
END;

CLOSE cur;
DEALLOCATE cur;
```

Messages

Đã mã hóa Stored Procedure: sp_get_no_encrypt
Đã mã hóa Stored Procedure: spCau1
Đã mã hóa Stored Procedure: spCau2
Đã mã hóa Stored Procedure: spCau3
Đã mã hóa Stored Procedure: spCau4
Đã mã hóa Stored Procedure: spCau5
Đã mã hóa Stored Procedure: spCau6
Đã mã hóa Stored Procedure: spCau7
Đã mã hóa Stored Procedure: spCau8
Đã mã hóa Stored Procedure: spCau9
Đã mã hóa Stored Procedure: spCau10

Completion time: 2025-02-28T20:13:01.4051785+07:00

Query executed successfully.

Thực hiện mã hóa các stored procedure

```
-- Lấy danh sách các stored procedure no encrypt
SELECT p.name AS StoredProcedureName
FROM sys.procedures p
JOIN sys.sql_modules m ON p.object_id = m.object_id
WHERE m.definition IS NOT NULL -- no encrypt
GO

-- Kiểm tra mã nguồn từng stored procedure
EXEC sp_helptext 'SPCau1';
EXEC sp_helptext 'SPCau2';
EXEC sp_helptext 'SPCau3';
EXEC sp_helptext 'SPCau4';
EXEC sp_helptext 'SPCau5';
EXEC sp_helptext 'SPCau6';
EXEC sp_helptext 'SPCau7';
EXEC sp_helptext 'SPCau8';
EXEC sp_helptext 'SPCau9';
EXEC sp_helptext 'SPCau10';
GO

-- h)
```

143 %

Results Messages

StoredProcedureName

Query executed successfully.

Kiểm tra lại danh sách các stored procedure no encrypt

```
-- Test
SELECT *
FROM sys.procedures

EXEC sp_helptext 'SPCau1';
EXEC SPCau1 N'SHB Đà Nẵng', N'Brazil';

EXEC sp_helptext 'SPCau2';
EXEC sp_helptext 'SPCau3';
EXEC sp_helptext 'SPCau4';
EXEC sp_helptext 'SPCau5';
EXEC sp_helptext 'SPCau6';
EXEC sp_helptext 'SPCau7';
EXEC sp_helptext 'SPCau8';
EXEC sp_helptext 'SPCau9';
EXEC sp_helptext 'SPCau10';
```

143 %

Results Messages

	MACT	HOTEN	NGAYSINH	DIACHI	VITRI
1	5	Ronaldo	1989-12-12 00:00:00.000	NULL	Tiền vệ
2	6	Robinho	1989-10-12 00:00:00.000	NULL	Tiền vệ
3	14	Ronaldo	1989-12-12 00:00:00.000	NULL	Tiền vệ
4	15	Robinho	1989-10-12 00:00:00.000	NULL	Tiền vệ

✓ Query executed successfully.

Chạy thử stored procedure **SPCau1**

```
-- Test
SELECT *
FROM sys.procedures

EXEC sp_helptext 'SPCau1';
EXEC SPCau1 N'SHB Đà Nẵng', N'Brazil';

EXEC sp_helptext 'SPCau2';
EXEC sp_helptext 'SPCau3';
EXEC sp_helptext 'SPCau4';
EXEC sp_helptext 'SPCau5';
EXEC sp_helptext 'SPCau6';
EXEC sp_helptext 'SPCau7';
EXEC sp_helptext 'SPCau8';
EXEC sp_helptext 'SPCau9';
EXEC sp_helptext 'SPCau10';
```

143 %

Messages

The text for object 'SPCau1' is encrypted.

Completion time: 2025-02-25T20:17:04.5295976+07:00

143 %

✓ Query executed successfully.

Kiểm tra mã nguồn stored procedure **SPCau1** (đã mã hóa)

Câu i

```
-- View 1. Cho biết mã số, họ tên, ngày sinh, địa chỉ và vị trí của các cầu thủ thuộc đội bóng "SĐB Đà Nẵng" có quốc tịch "Brazil".
CREATE VIEW vCau1 AS
SELECT CT.MACT, CT.HOTEN, CT.NGAYTHAM, CT.DIACHI, CT.VITRI
FROM CAUTHU CT;

-- View 2. Cho biết mã huấn luyện viên, họ tên, ngày sinh, địa chỉ, vai trò và kết quả
-- đang làm việc của các huấn luyện viên có quốc tịch "Việt Nam".
CREATE VIEW vCau2 AS
SELECT TO.NAMTA, TO.NGAYTO, SVD.TENCLB AS TENC1B1, CLB2.TENCLB AS TENC1B2, TO.KETQUA
FROM TRAUQU TO;

-- View 3. Cho biết mã huấn luyện viên, họ tên, ngày sinh, địa chỉ, vai trò và tên CLB
-- đang làm việc của các huấn luyện viên có quốc tịch "Việt Nam".
CREATE VIEW vCau3 AS
SELECT HLV.NHNV, HLV.TENHLV, HLV.NGAYTHAM, HLV.DIACHI, HLV.CLB VAITRO, CLB.TENCLB
FROM HUANLUYENVIEN HLV;

-- View 4. Cho biết mã cầu lạc bộ, tên cầu lạc bộ, tên sân vận động, địa chỉ và số lượng
-- cầu thủ nước ngoài (có quốc tịch khác "Việt Nam") đang thi đấu của cầu lạc bộ.
-- Có nhiều hơn 2 cầu thủ nước ngoài.
CREATE VIEW vCau4 AS
SELECT CLB.MACLB, CLB.TENCLB, SVD.TENSAN, SVD.DIACHI, SVD.CT.MACT AS SoLuongGauThaoKhungGau
FROM CAULACRO CLB;

-- View 5. Cho biết tên cầu lạc bộ, tên sân vận động, địa chỉ và vị trí của cầu thủ đang thi đấu ở vị trí tiền đạo trong các cầu lạc
-- bộ thuộc địa bàn tỉnh độ quận lỵ.
CREATE VIEW vCau5 AS
SELECT T.TENTINH, SVD.CT.MACT AS SoLuongTienDao
FROM TINH T;

-- View 6. Cho biết tên cầu lạc bộ, tên tỉnh mà CLB đang đóng nền ở vị trí cao nhất của
-- bảng xếp hạng của vòng 3, năm 2009.
CREATE VIEW vCau6 AS
SELECT BX.MACLB, CLB.TENCLB, T.TENTINH
FROM BANCON BX;

-- View 7. Cho biết tên huấn luyện viên đang nắm giữ một vị trí trong một cầu lạc bộ mà
-- chưa có số điện thoại.
CREATE VIEW vCau7 AS
SELECT NHNV, TENNHV, NGAYTHAM, DIACHI
FROM HUANLUYENVIEN;

-- View 8. Liệt kê các huấn luyện viên thuộc quốc gia Việt Nam chưa làm công tác huấn
-- luyện tại bất kỳ một cầu lạc bộ nào.
CREATE VIEW vCau8 AS
SELECT NHNV, TENNHV, NGAYTHAM, DIACHI
FROM HUANLUYENVIEN;

-- View 9. Liệt kê các huấn luyện viên thuộc quốc gia Việt Nam chưa làm công tác huấn
-- luyện tại bất kỳ một cầu lạc bộ nào.
CREATE VIEW vCau9 AS
SELECT NHNV, TENNHV, NGAYTHAM, DIACHI
FROM HUANLUYENVIEN;
```

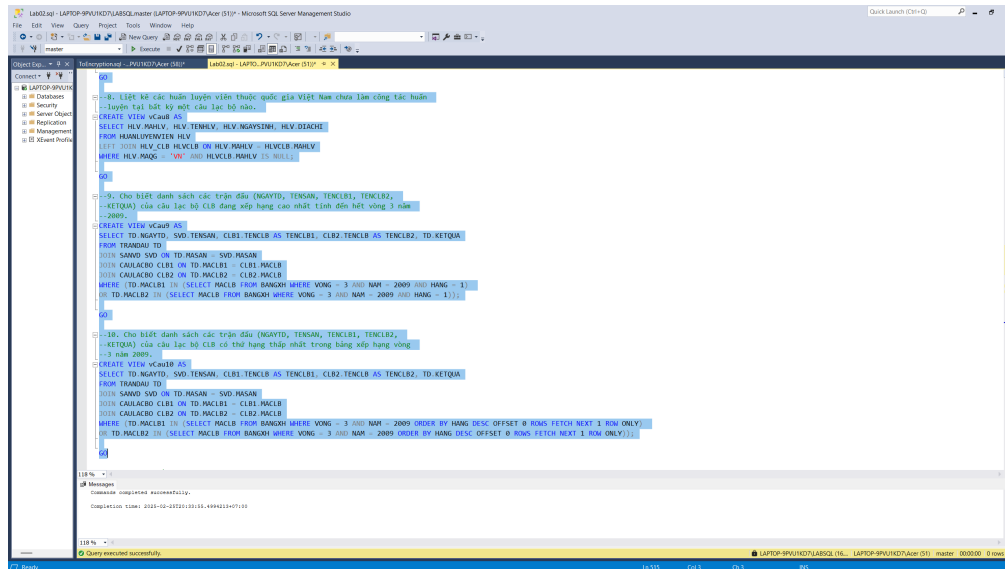
Khởi tạo view 1-4

```
-- View 5. Cho biết tên tỉnh, số lượng cầu thủ đang thi đấu ở vị trí tiền đạo trong các cầu lạc
-- bộ thuộc địa bàn tỉnh độ quận lỵ.
CREATE VIEW vCau5 AS
SELECT T.TENTINH, SVD.CT.MACT AS SoLuongTienDao
FROM TINH T;

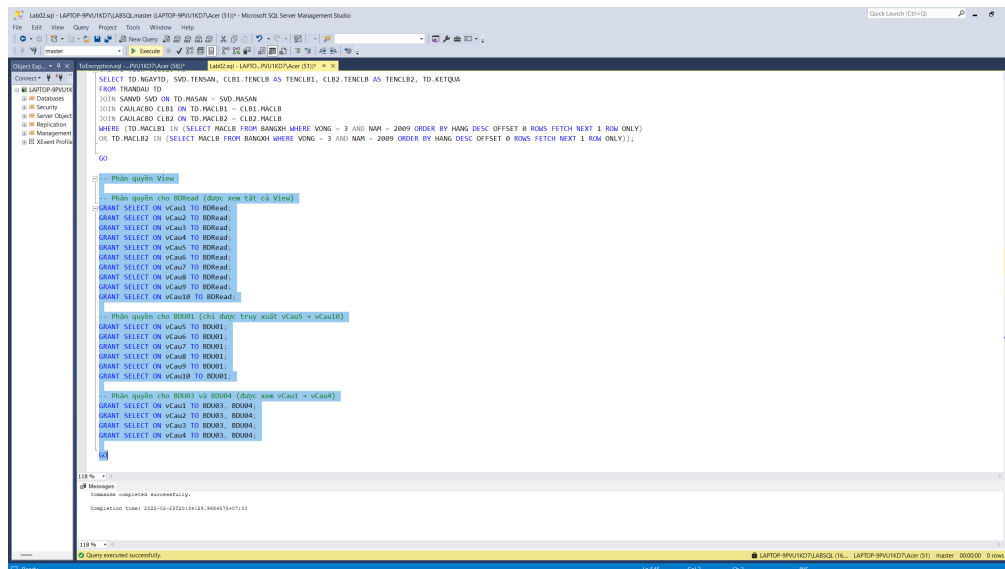
-- View 6. Cho biết tên cầu lạc bộ, tên tỉnh mà CLB đang đóng nền ở vị trí cao nhất của
-- bảng xếp hạng của vòng 3, năm 2009.
CREATE VIEW vCau6 AS
SELECT BX.MACLB, CLB.TENCLB, T.TENTINH
FROM BANCON BX;

-- View 7. Cho biết tên huấn luyện viên đang nắm giữ một vị trí trong một cầu lạc bộ mà
-- chưa có số điện thoại.
CREATE VIEW vCau7 AS
SELECT NHNV, TENNHV, NGAYTHAM, DIACHI
FROM HUANLUYENVIEN;
```

khởi tạo view 5-7



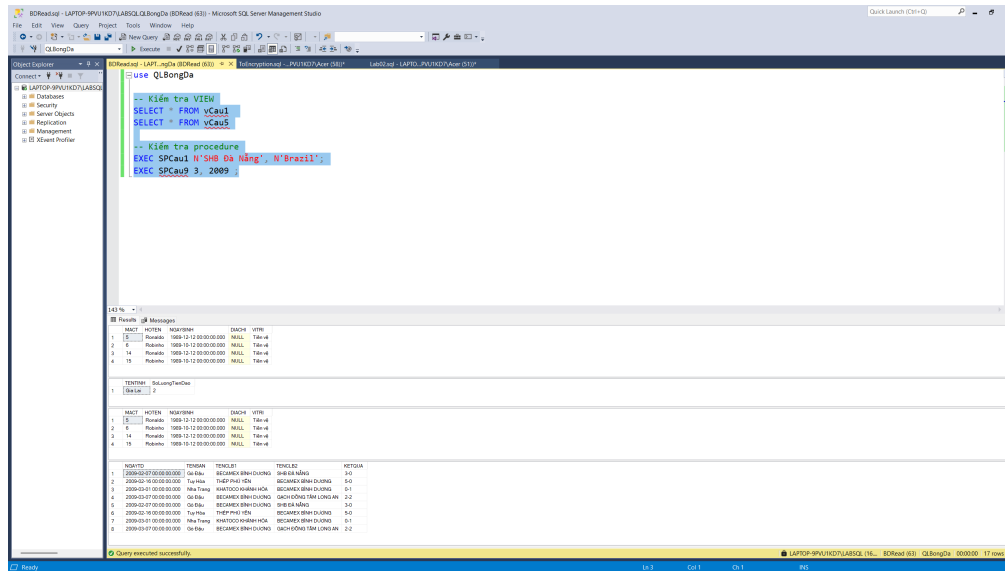
Khởi tạo view 8-10



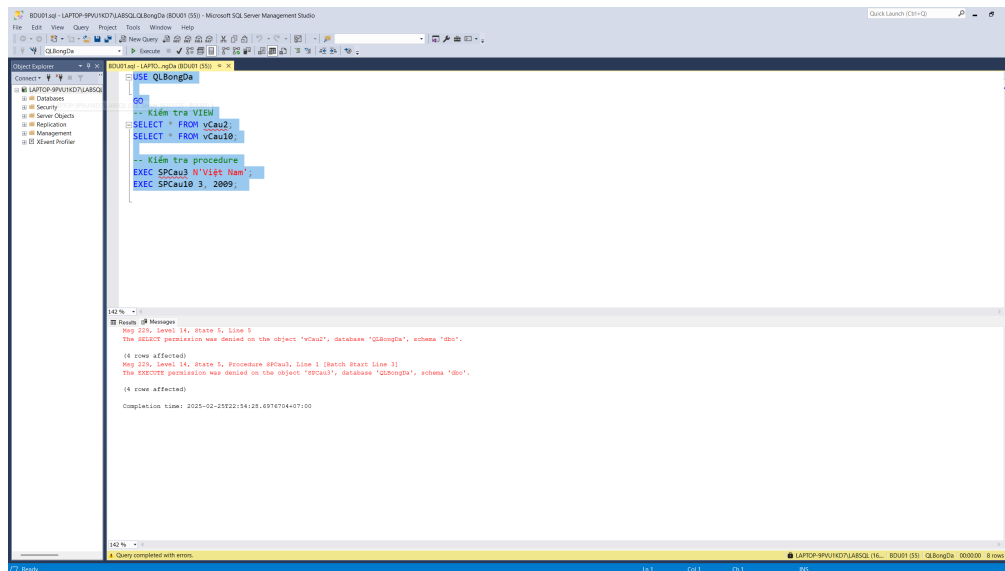
Phân quyền view cho các User

STT	Tên User	Thực thi câu select	Kết quả	Giải thích kết quả
1	BDRead	SELECT* FROM vCau1	Thành công	
	BDRead	SELECT* FROM vCau5	Thành công	
2	BDU01	SELECT* FROM vCau2	Báo lỗi	Chỉ được phép truy cập vCau5 đến vCau10
	BDU01	SELECT* FROM vCau10	Thành công	
3	BDU03	SELECT* FROM vCau1	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT các table khác
	BDU03	SELECT* FROM vCau2	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT các table khác
	BDU03	SELECT* FROM vCau3	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT các table khác
	BDU03	SELECT* FROM vCau4	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT các table khác
4	BDU04	SELECT* FROM vCau1	Báo lỗi	Không được phép xem cột NGAYSINH trong table CAUTHU
	BDU04	SELECT* FROM vCau2	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.
	BDU04	SELECT* FROM vCau3	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.
	BDU04	SELECT* FROM vCau4	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.

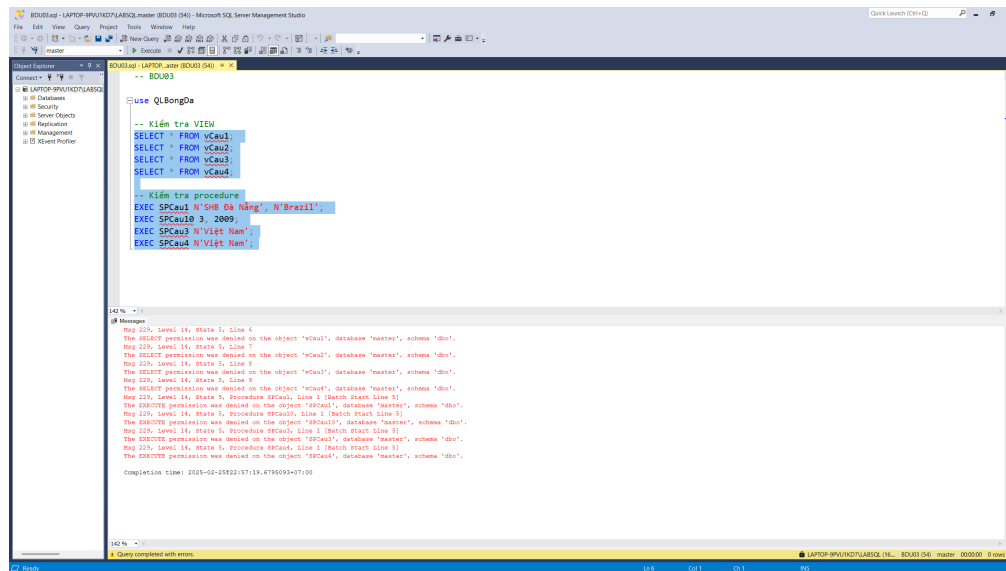
Bảng thực thi câu lệnh SELECT



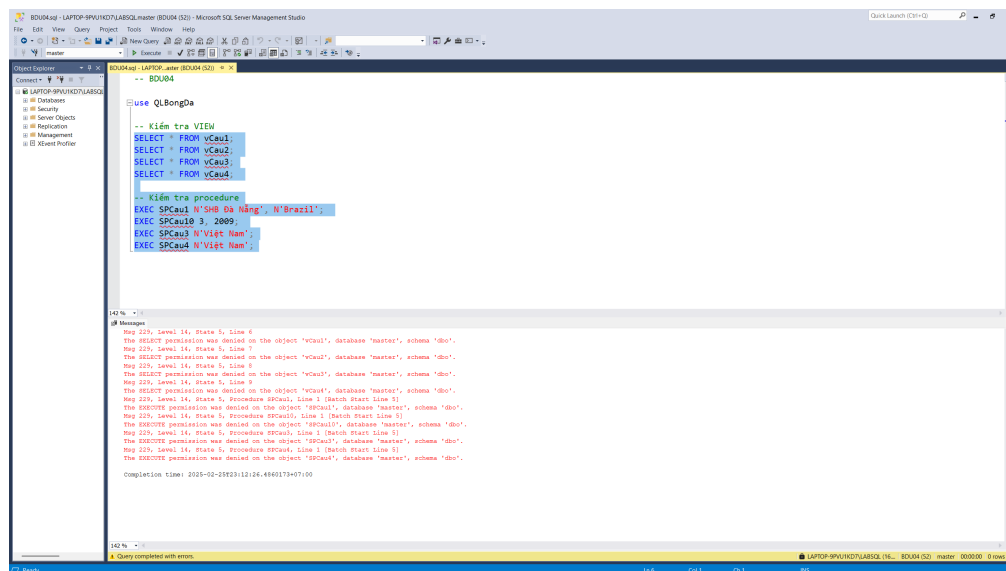
Thực thi với User BDRoad



Thực thi với User BDU01

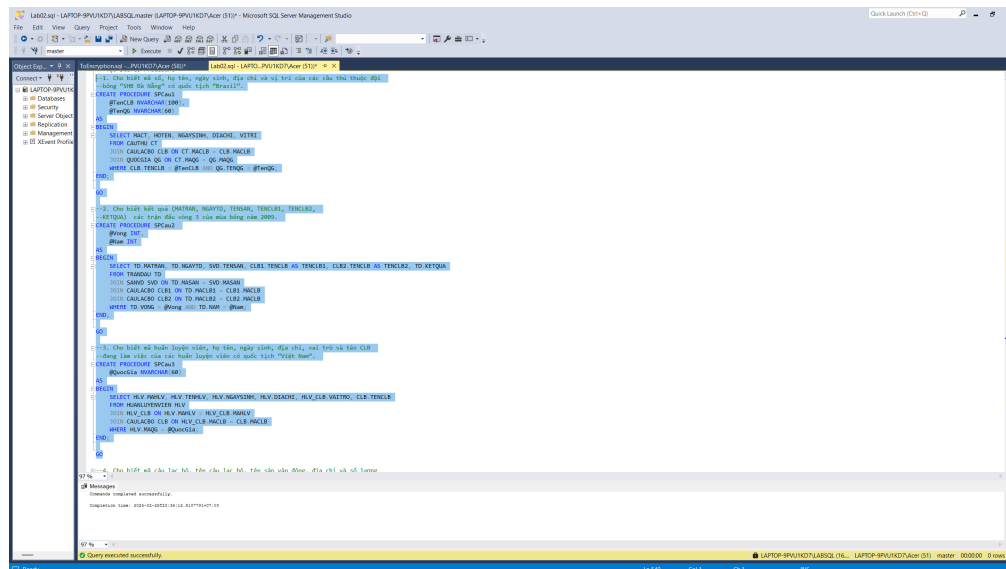


Thực thi với User BDU03

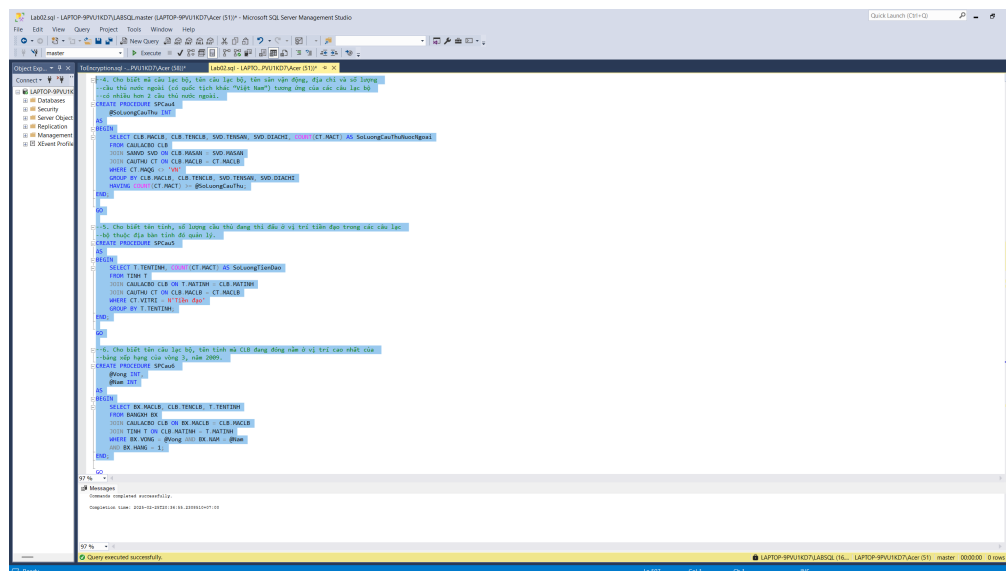


Thực thi với User BDU04

Câu j

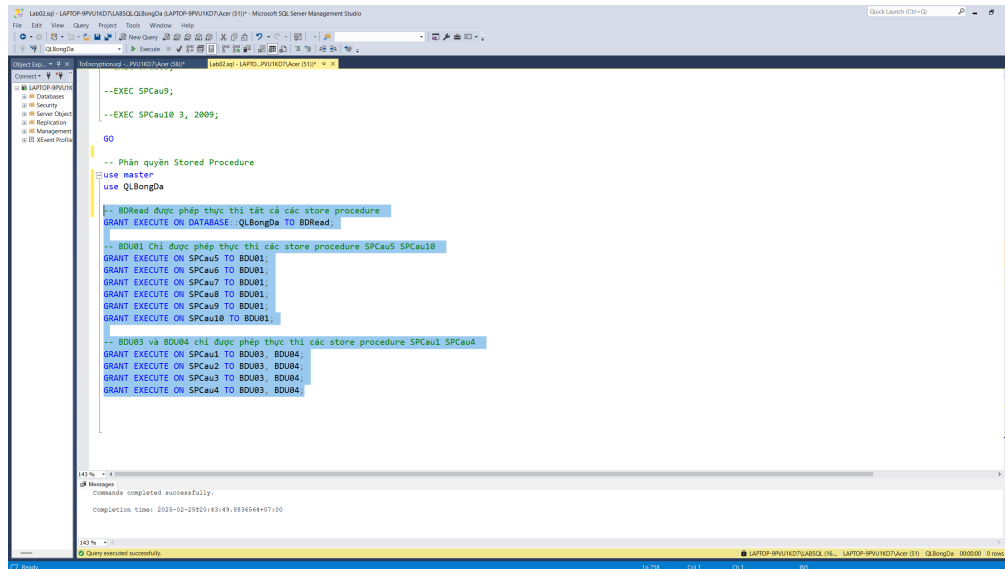


Khởi tạo stored procedure 1-3



khởi tạo stored procedure từ 4-6





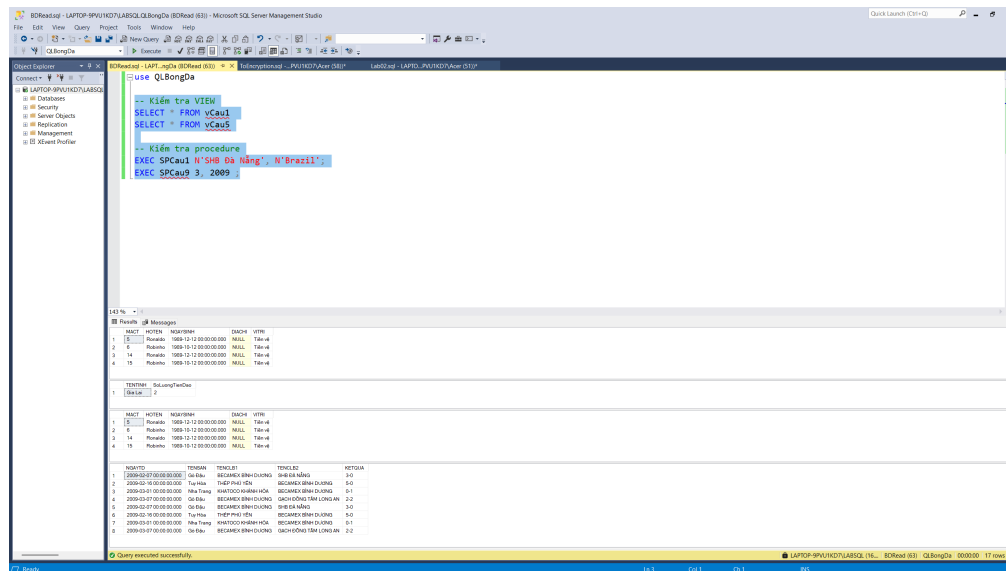
```
--EXEC SPCau9;  
--EXEC SPCau10 3, 2009;  
  
GO  
  
-- Phân quyền Stored Procedure  
use master  
use QLBongDa  
  
-- BDRoad được phép thực thi tất cả các store procedure  
GRANT EXECUTE ON DATABASE::QLBongDa TO BDRoad;  
  
-- BDU01 chỉ được phép thực thi các store procedure SPCau5 SPCau10  
GRANT EXECUTE ON SPCau5 TO BDU01;  
GRANT EXECUTE ON SPCau6 TO BDU01;  
GRANT EXECUTE ON SPCau7 TO BDU01;  
GRANT EXECUTE ON SPCau8 TO BDU01;  
GRANT EXECUTE ON SPCau9 TO BDU01;  
GRANT EXECUTE ON SPCau10 TO BDU01;  
  
-- BDU03 và BDU04 chỉ được phép thực thi các store procedure SPCau1 SPCau4  
GRANT EXECUTE ON SPCau1 TO BDU03, BDU04;  
GRANT EXECUTE ON SPCau2 TO BDU03, BDU04;  
GRANT EXECUTE ON SPCau3 TO BDU03, BDU04;  
GRANT EXECUTE ON SPCau4 TO BDU03, BDU04;
```

143 % -> *
Messages
Commands completed successfully.
Completion time: 2025-10-29 20:43:49.8836564+07:00
143 % -> *
Query executed successfully.

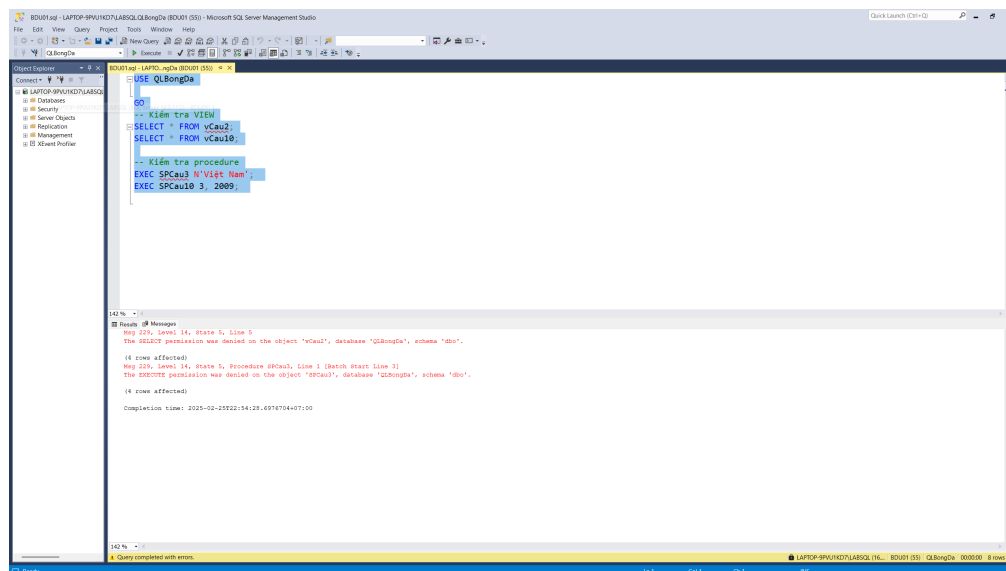
Phân quyền Stored Procedure cho Users

STT	Tên User	Thực thi câu select	Kết quả	Giải thích kết quả
1	BDRead	SELECT * FROM vCau1	Thành công	
	BDRead	SPCau9 3, 2009	Thành công	
2	BDU01	EXEC SP- Cau3 'Việt Nam'	Báo lỗi	Chỉ cho phép truy cập SPCau5 đến SPCau10
	BDU01	EXEC SP- Cau10 3, 2009	Thành công	
3	BDU03	SELECT * FROM vCau1	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT table khác
	BDU03	SELECT * FROM vCau2	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT table khác
	BDU03	SELECT * FROM vCau3	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT table khác
	BDU03	SELECT * FROM vCau4	Báo lỗi	Chỉ được phép thao tác table CauLacBo. Không thể SELECT table khác
4	BDU04	SELECT * FROM vCau1	Báo lỗi	Không được phép xem cột NGAYSINH trong table CAUTHU
	BDU04	SELECT * FROM vCau2	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.
	BDU04	SELECT * FROM vCau3	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.
	BDU04	SELECT * FROM vCau4	Báo lỗi	Chỉ được phép thao tác table CAUTHU. Không được phép thao tác các table khác.

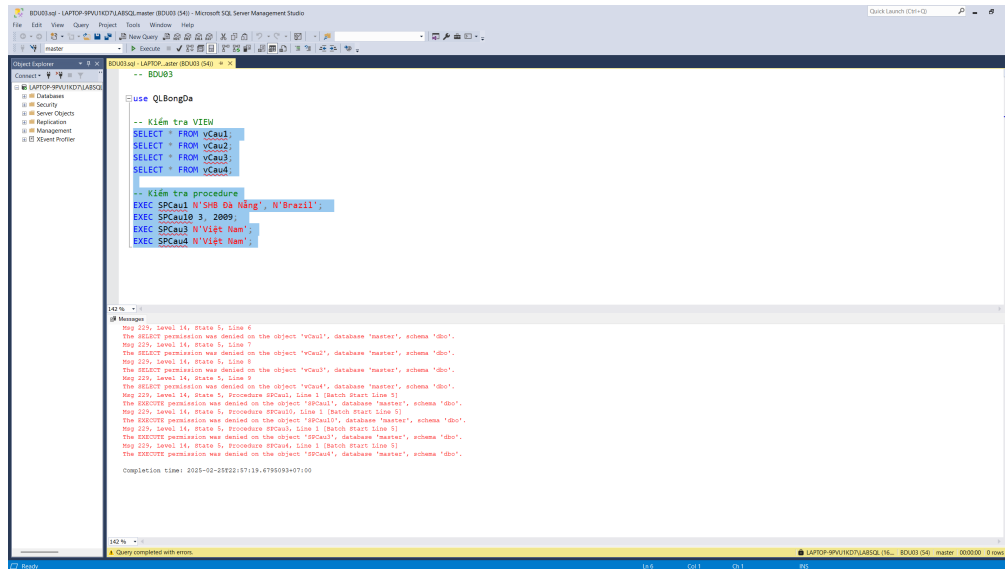
Bảng thực thi câu lệnh SELECT



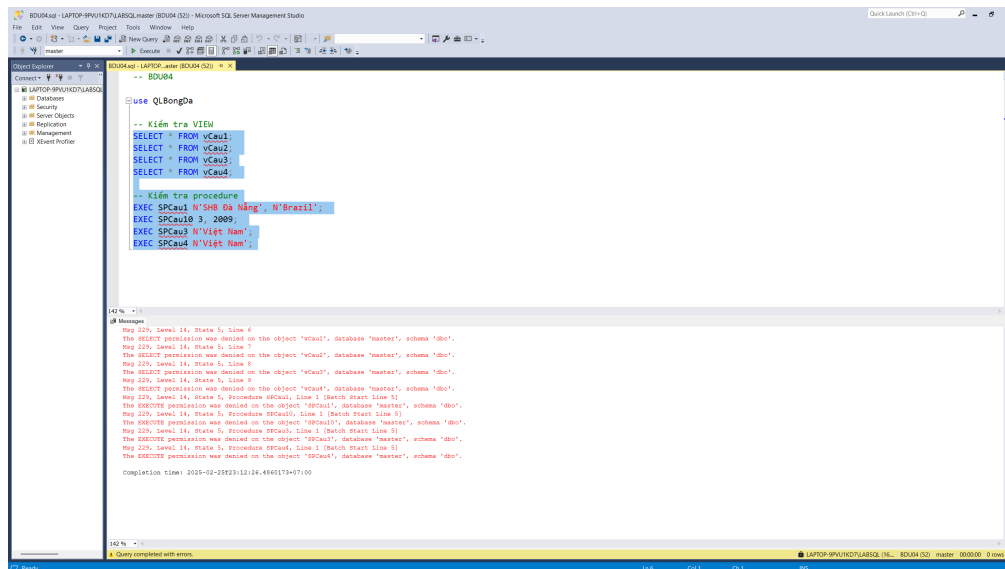
Thực thi với User BDRoad



Thực thi với User BDU01



Thực thi với User BDU03

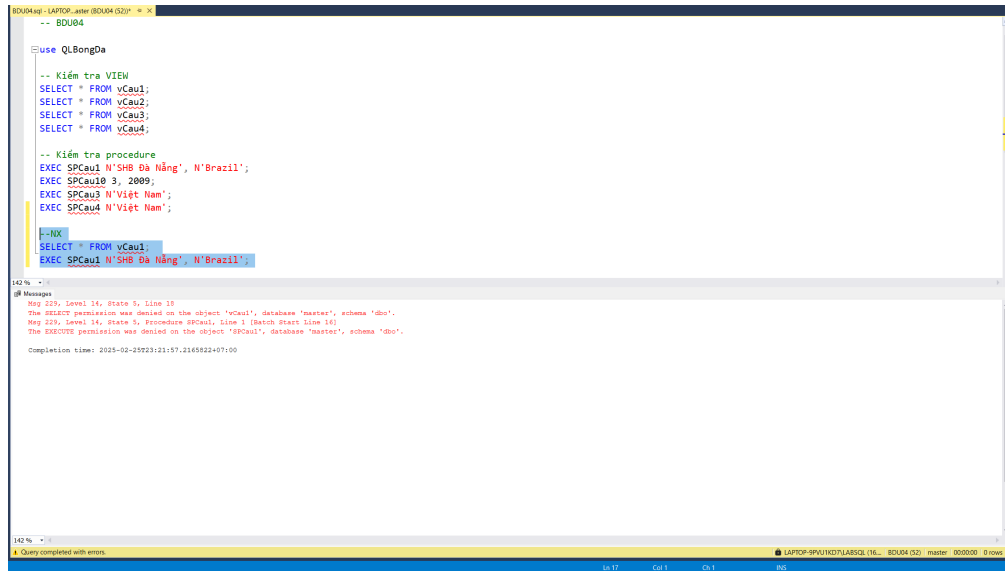


Thực thi với User BDU04

Nhận xét

- Vì mỗi User đều có ràng buộc về các quyền truy cập hoặc chỉnh sửa các table hoặc quyền trên server, database
- Kèm theo đó là các VIEW hay Procedure được cấp cho mỗi User cần quyền như quyền truy cập một số data mà User đó bị cấm thì sẽ bị hệ thống từ chối và báo lỗi

- Ví dụ như user BDU04 có thể truy cập table CAUTHU nhưng không thể xem cột NGAYSINH trong khi view vCau1 hay procedure SPCau1 cần xuất ra NGAYSINH của câu thủ dẫn đến mâu thuẫn và bị từ chối



```
-- BDU04
-- use QLBoongDa
-- Kiểm tra VIEW
SELECT * FROM vCau1;
SELECT * FROM vCau2;
SELECT * FROM vCau3;
SELECT * FROM vCau4;

-- Kiểm tra procedure
EXEC SPCau1 N'Shò Bà Nàng', N'Brazil';
EXEC SPCau10 3, 2009;
EXEC SPCau3 N'Việt Nam';
EXEC SPCau4 N'Việt Nam';

--NX
SELECT * FROM vCau1;
EXEC SPCau1 N'Shò Bà Nàng', N'Brazil';
```

Msg 229, Level 14, State 5, Line 10
The SELECT permission was denied on the object 'vCau1', database 'master', schema 'dbo'.
Msg 229, Level 14, State 5, Procedure SPCau1, Line 1 (Batch Start Line 10)
The EXECUTE permission was denied on the object 'SPCau1', database 'master', schema 'dbo'.
Completion time: 2025-02-25 23:21:57.2165822+07:00

Query completed with errors.

BDU04 bị từ chối thực thi vCau1 và SPCau1