

ANKARA ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ



BLM4522 Veritabanı Güvenliği ve Erişim Kontrolü Projesi Raporu

Görkem HAZAR – Furkan Yağcı

21290428 – 20290301

GİTHUB Linki : https://github.com/hazargorkem/Vize_SQL

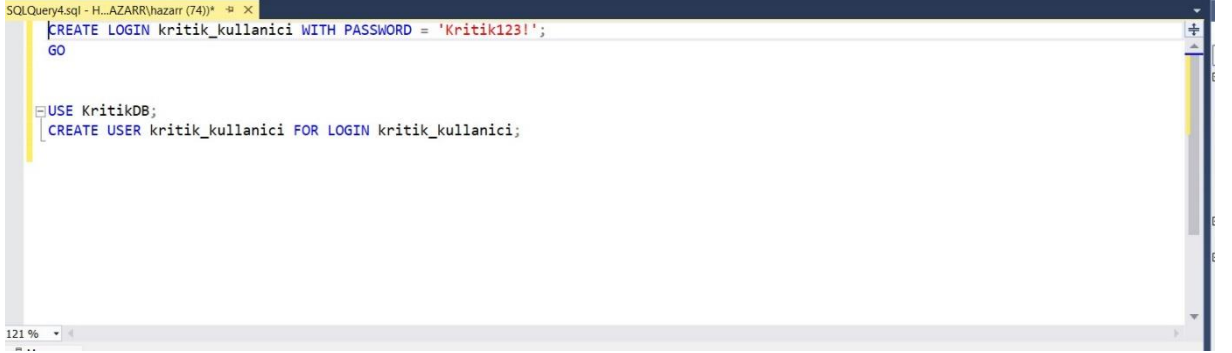
25.05.2025

PROJE : Veritabanı Güvenliği ve Erişim Kontrolü

1.AŞAMA : Erişim Yönetimi

Bu aşamada halihazır bulunan bir veritabanımız kullanılmaktadır. Veritabanı örnek bir personel tablosu ve içerisinde ad-soyad, maaş bilgisi gibi kritik bilgileri içermektedir.

- a) Veritabanına dışarıdan erişebilecek özel bir kullanıcı oluşturulmuştur. Bu kullanıcıya yalnızca gerekli yetkiler verilecek ve güvenlik uygulamaları bu kullanıcı üzerinden test edilecektir.



```
SQLQuery4.sql - H...AZARR\hazarr (74) *  
CREATE LOGIN kritik_kullanici WITH PASSWORD = 'Kritik123!';  
GO  
  
USE KritikDB;  
CREATE USER kritik_kullanici FOR LOGIN kritik_kullanici;
```

- b) Yetki sınırlandırması ile kullanıcının sadece ad-soyad bilgisini görmesi sağlanarak hassas veri olan maaş bilgisinin yetkisiz kişiler tarafından görüntülenmesi engellenmiştir.

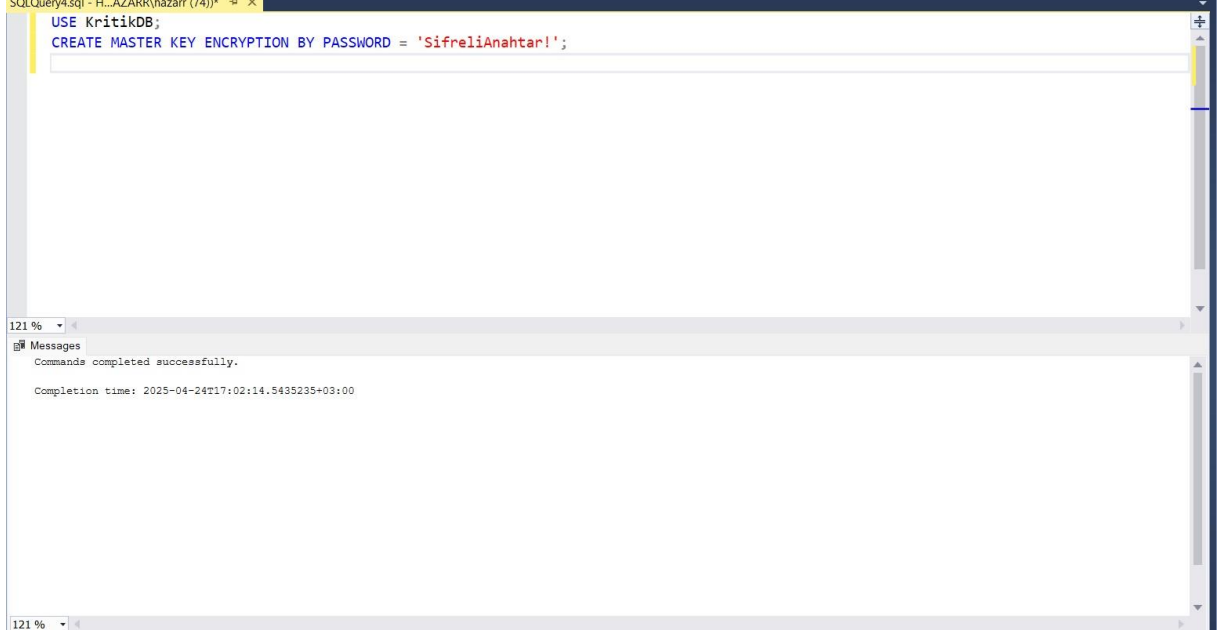


```
SQLQuery4.sql - H...AZARR\hazarr (74) *  
DENY SELECT ON Calisanlar TO kritik_kullanici;  
  
GRANT SELECT (AdSoyad) ON Calisanlar TO kritik_kullanici;
```

Messages
Commands completed successfully.
Completion time: 2025-04-24T17:01:24.5093415+03:00

2.AŞAMA : VERİ ŞİFRELEME

- a) Veri şifreleme işlemlerinde kullanılacak anahtar ve sertifikaların güvenli bir şekilde saklanabilmesi için master key ve sertifika oluşturulmuştur. Bunlar, şifreleme altyapısının temelini oluşturur.

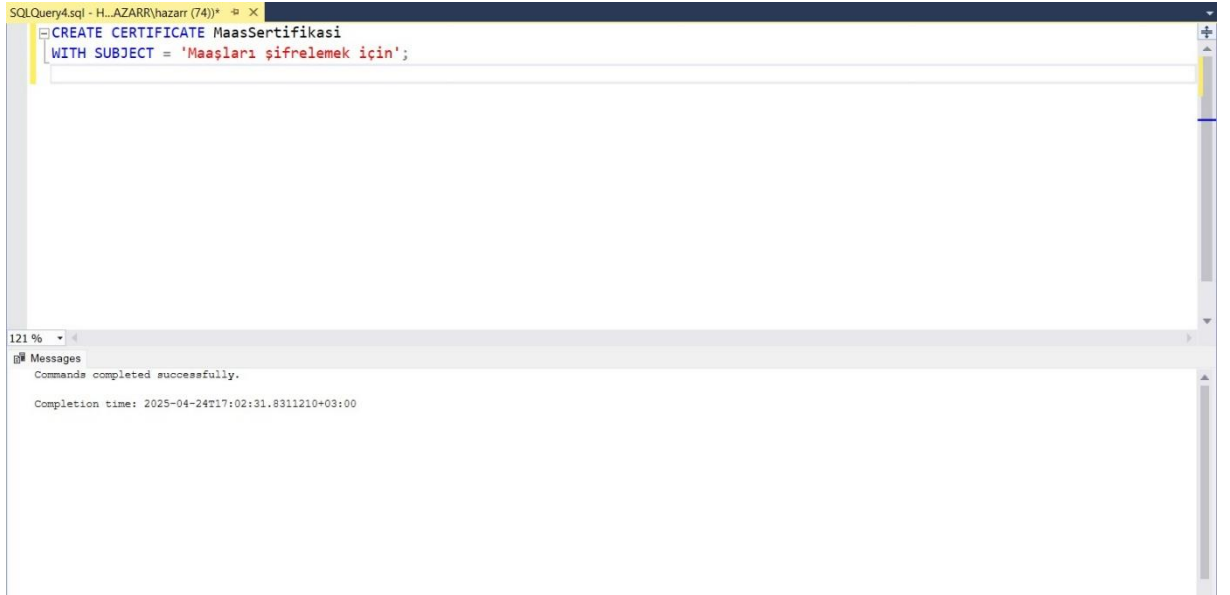


The screenshot shows the SQL Server Enterprise Manager interface. The top pane displays the following T-SQL command:

```
USE KritikDB;  
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'SifreliAnahtar!';
```

The bottom pane shows the execution results:

```
Messages  
Commands completed successfully.  
Completion time: 2025-04-24T17:02:14.5435235+03:00
```



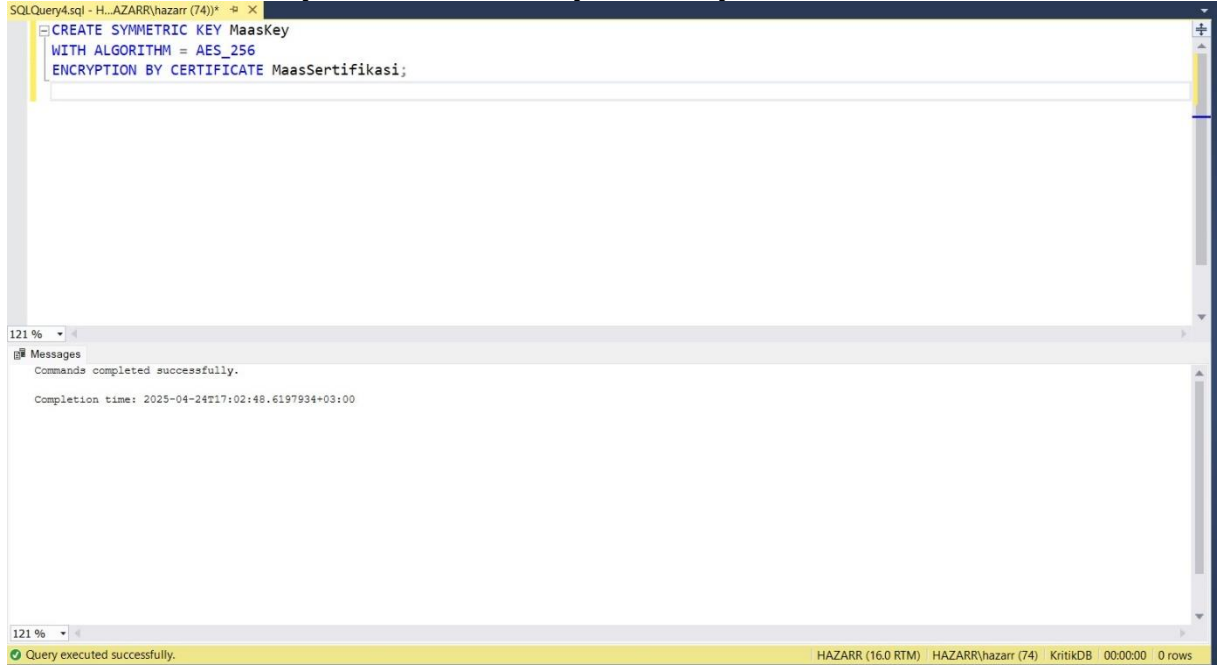
The screenshot shows the SQL Server Enterprise Manager interface. The top pane displays the following T-SQL command:

```
CREATE CERTIFICATE MaasSertifikasi  
WITH SUBJECT = 'Maaşları şifrelemek için';
```

The bottom pane shows the execution results:

```
Messages  
Commands completed successfully.  
Completion time: 2025-04-24T17:02:31.8311210+03:00
```

- b) Simetrik anahtar tanımlama ile güçlü bir şifreleme anahtarı tanımlanmıştır. Bu anahtar, verilerin hem şifrlenmesi hem de çözülmesi için kullanılacaktır.

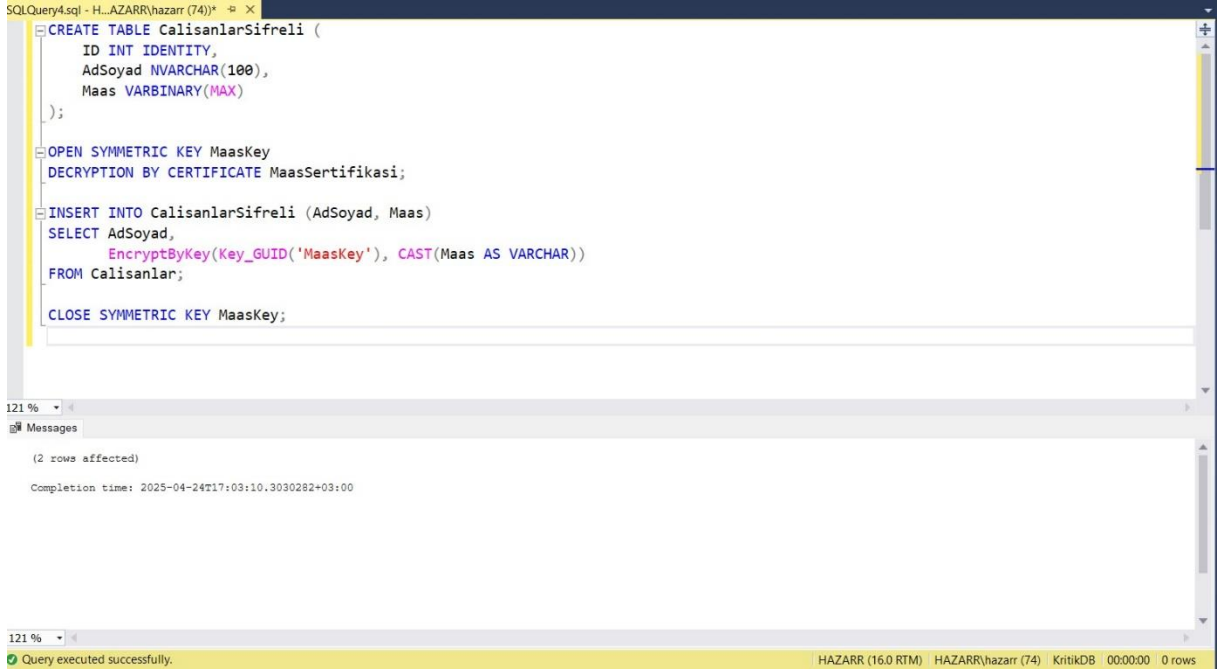


```
SQLQuery4.sql - H...AZARR\hazarr (74) * X
CREATE SYMMETRIC KEY MaasKey
WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE MaasSertifikasi;

121 %
Messages
Commands completed successfully.
Completion time: 2025-04-24T17:02:48.6197934+03:00

121 %
Query executed successfully. HAZARR (16.0 RTM) HAZARR\hazarr (74) KritikDB 00:00:00 0 rows
```

- c) Şifreli Tablo Oluşturma ve Veriyi Şifreleme, Hassas veriler (maaş bilgisi), şifrlenerek yeni bir tabloda saklanmıştır. Böylece veritabanı erişilse bile şifrelenmiş maaş verileri okunamaz hale getirilmiştir.

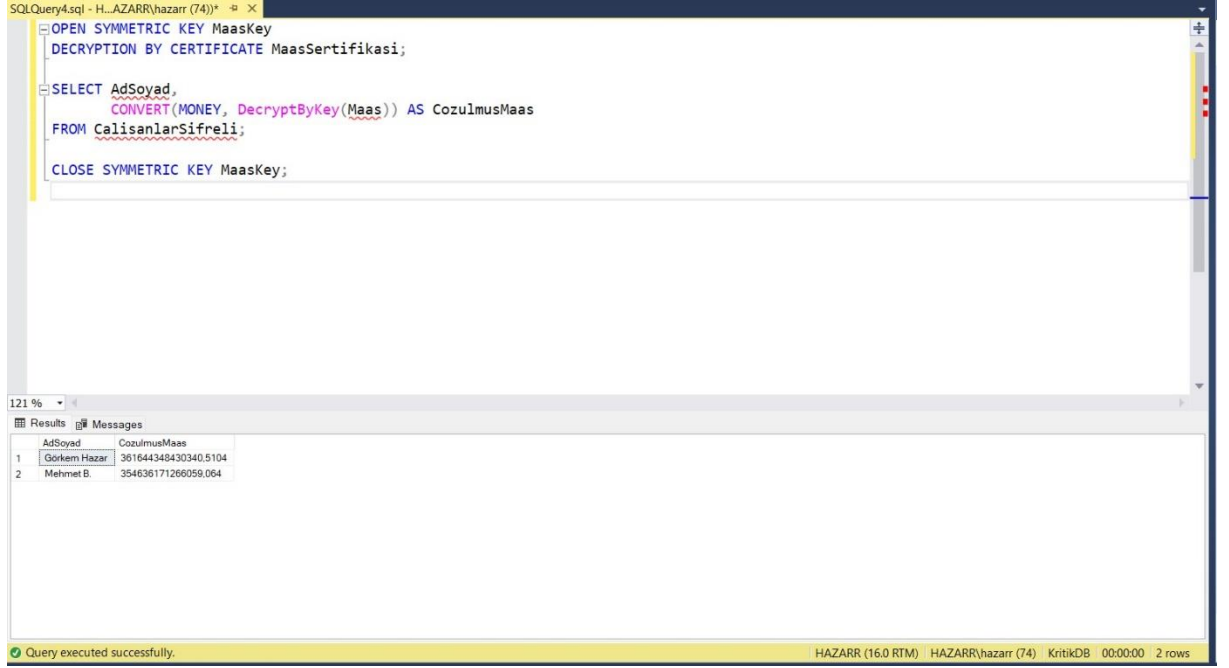


```
SQLQuery4.sql - H...AZARR\hazarr (74) * X
CREATE TABLE CalisanlarSifreli (
    ID INT IDENTITY,
    AdSoyad NVARCHAR(100),
    Maas VARBINARY(MAX)
);
OPEN SYMMETRIC KEY MaasKey
DECRYPTION BY CERTIFICATE MaasSertifikasi;
INSERT INTO CalisanlarSifreli (AdSoyad, Maas)
SELECT AdSoyad,
    EncryptByKey(Key_GUID('MaasKey'), CAST(Maas AS VARCHAR))
FROM Calisanlar;
CLOSE SYMMETRIC KEY MaasKey;

121 %
Messages
(2 rows affected)
Completion time: 2025-04-24T17:03:10.3030282+03:00

121 %
Query executed successfully. HAZARR (16.0 RTM) HAZARR\hazarr (74) KritikDB 00:00:00 0 rows
```

- d) Şifreli Veriyi Çözme, Şifrelenmiş verilerin sadece yetkili kişiler tarafından çözülebileceği gösterilmiştir.



```
SQLQuery4.sql - H:\AZARR\hazarr (74)* X
OPEN SYMMETRIC KEY MaasKey
DECRYPTION BY CERTIFICATE MaasSertifikasi;

SELECT AdSoyad,
        CONVERT(MONEY, DecryptByKey(Maas)) AS CozulmusMaas
FROM CalisanlarSifreli;

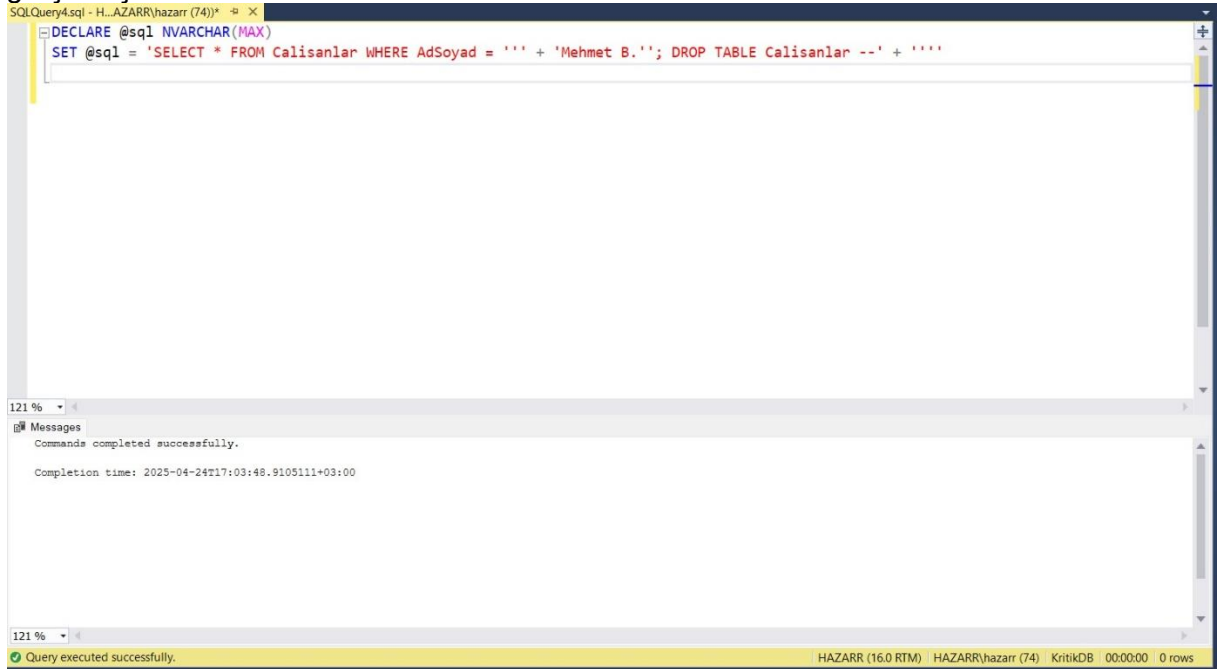
CLOSE SYMMETRIC KEY MaasKey;
```

	AdSoyad	CozulmusMaas
1	Gökrem Hazar	361644348430340.5104
2	Mehmet B.	354636171266059.064

Query executed successfully. HAZARR (16.0 RTM) HAZARR\hazarr (74) KritikDB 00:00:00 2 rows

3.AŞAMA : SQL INJECTION TESTİ

- a) Injection Riski taşıyan Güvensiz Sorgu yaparak veritabanına sızma testi gerçekleştirildi.



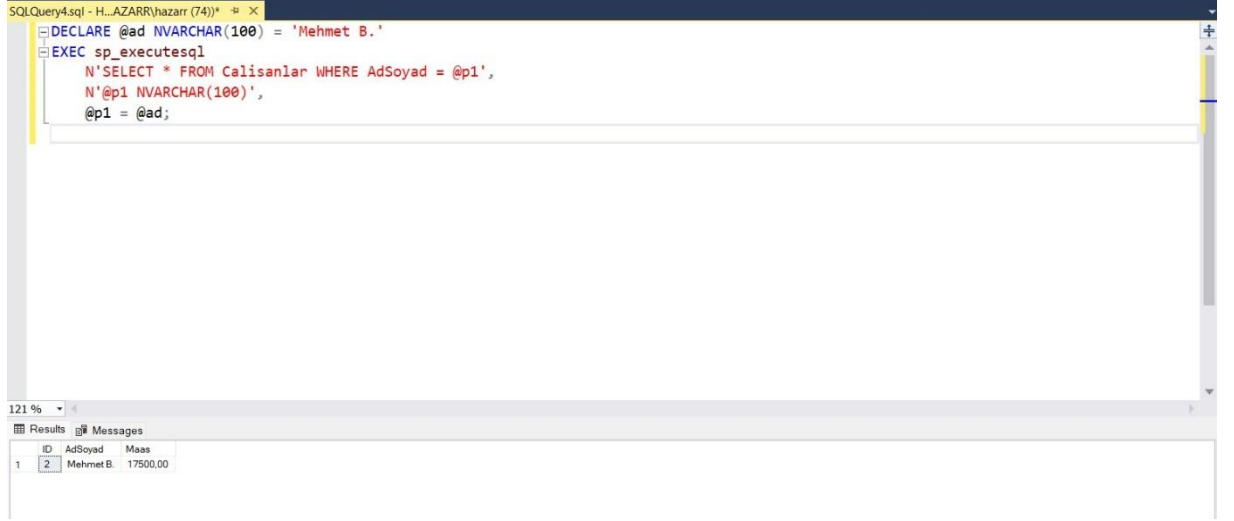
```
SQLQuery4.sql - H:\AZARR\hazarr (74)* X
DECLARE @sql NVARCHAR(MAX)
SET @sql = 'SELECT * FROM Calisanlar WHERE AdSoyad = '' + 'Mehmet B.'; DROP TABLE Calisanlar --' + '''
```

Commands completed successfully.

Completion time: 2025-04-24T17:03:48.9105111+03:00

Query executed successfully. HAZARR (16.0 RTM) HAZARR\hazarr (74) KritikDB 00:00:00 0 rows

- b) Bu riskli sorgulara karşı parametrelili sorgular kullanılarak SQL Injection saldırılarının engellenmesi sağlanmıştır.

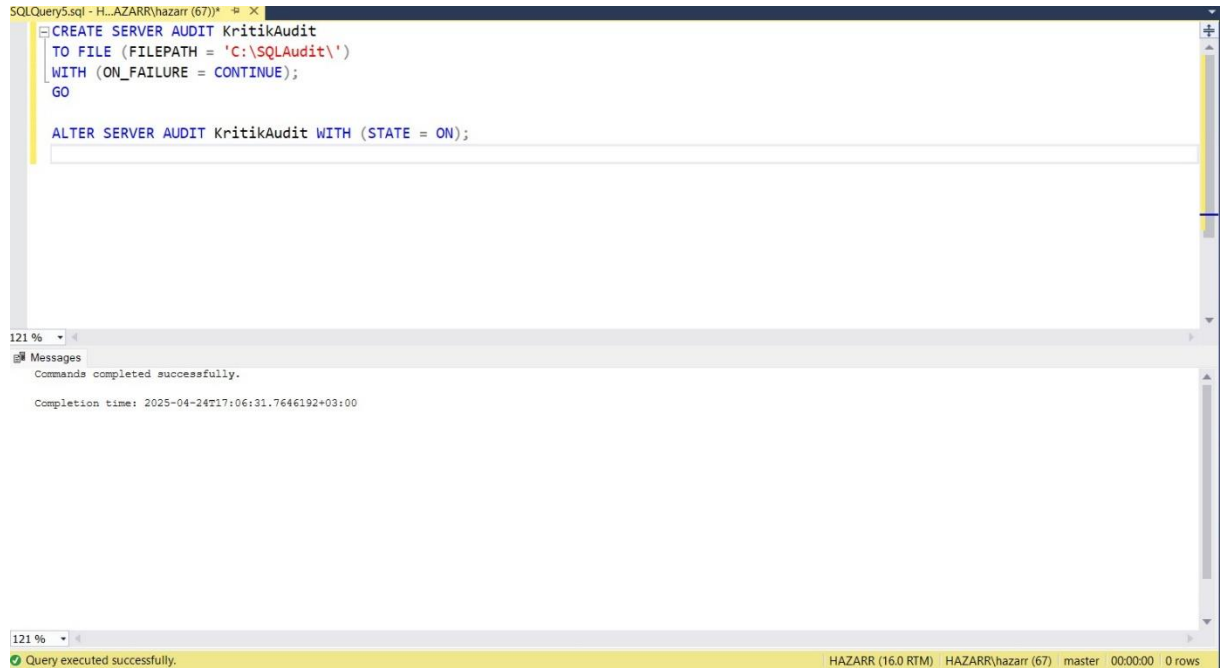


```
SQLQuery4.sql - H...AZARR\hazarr (74) *  X
-- DECLARE @ad NVARCHAR(100) = 'Mehmet B.'
-- EXEC sp_executesql
--     N'SELECT * FROM Calisanlar WHERE AdSoyad = @p1',
--     N'@p1 NVARCHAR(100)',
--     @p1 = @ad;
```

ID	AdSoyad	Maaş
1	Mehmet B.	17500.00

4.AŞAMA : AUDIT LOG – KULLANICI TAKİBİ

- a) Server Audit Tanımlama, Veri tabanı aktivitelerini sistemsel olarak izleyebilmek için SQL Server Audit sistemi devreye alınmış, tüm işlemler log dosyasına kaydedilecek şekilde yapılandırılmıştır.



```
SQLQuery5.sql - H...AZARR\hazarr (67) *  X
-- CREATE SERVER AUDIT KritikAudit
-- TO FILE (FILEPATH = 'C:\SQLAudit\')
-- WITH (ON_FAILURE = CONTINUE);
-- GO
-- ALTER SERVER AUDIT KritikAudit WITH (STATE = ON);
```

Messages

Commands completed successfully.

Completion time: 2025-04-24T17:06:31.7646192+03:00

Query executed successfully.

HAZARR (16.0 RTM) HAZARR\hazarr (67) master 00:00:00 0 rows

- b) Audit Specification Oluşturma, Belirli bir kullanıcı ve tablo özelinde loglama yapılarak, hassas verilere erişimlerin kayıt altına alınması sağlanmıştır.

```
SQLQuery5.sql - H...AZARR\hazarr (67)) *  
USE KritikDB;  
GO  
CREATE DATABASE AUDIT SPECIFICATION KritikAuditSpec  
FOR SERVER AUDIT KritikAudit  
ADD (SELECT ON OBJECT::dbo.Calisanlar BY k_kullanici)  
WITH (STATE = ON);
```

Messages
Commands completed successfully.
Completion time: 2025-04-24T17:08:13.8373843+03:00

c) Kayıt altına alınmış audit log dosyası :

