# **Proje 3: Veritabanı Güvenliği ve Erişim Kontrolü**

Hazırlayan: Mert Efe Kandemir, Kaan Kaya

Numara: 21290233, 21290436

Teslim: 25.04.2025

Github: https://github.com/kayakaan02/-BLM4522-A-Tabanl-Paralel-Da-t-m-Sistemleri-Proje-Videolari/blob/main/proje3.mp4

## **1. Giriş**

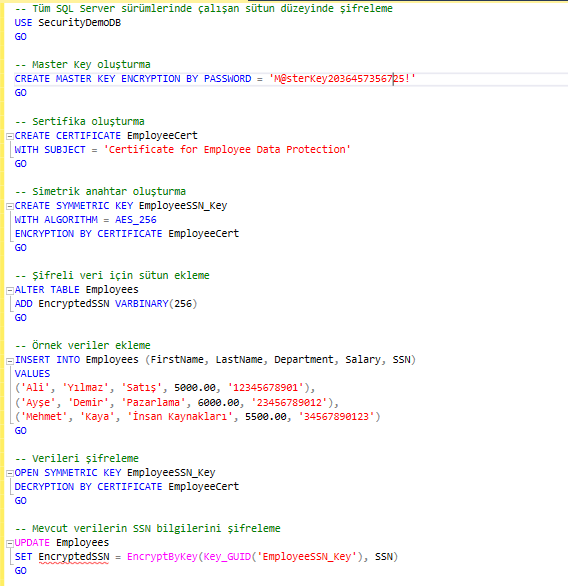
Bu proje kapsamında, veritabanı güvenliği ve erişim kontrolü teknikleri incelenmiştir. Veritabanı güvenliği, kurumsal bilgi sistemlerinin en kritik unsurlarından biridir. Projemizde, kullanıcı erişimi, veri şifreleme ve güvenlik duvarı yönetimi gibi konular ele alınmış, SQL Server üzerinde güvenlik önlemleri uygulanmıştır.

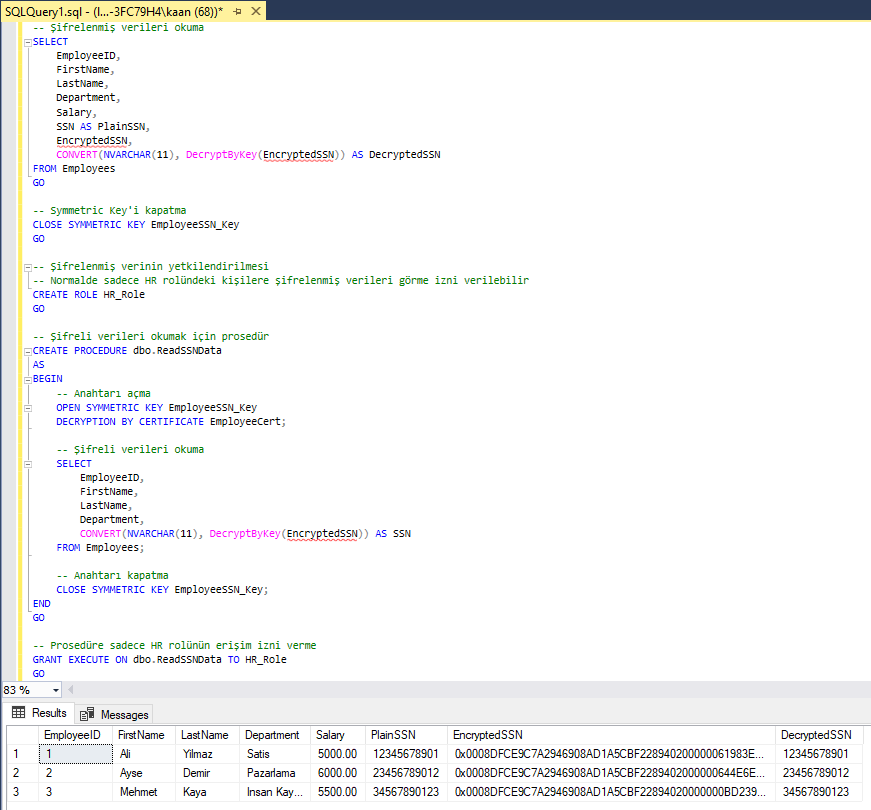
## **2. Erişim Yönetimi**

Erişim yönetimi aşamasında, kullanıcıların verilere erişim yetkilerini kontrol etmek için SQL Server Authentication ve Windows Authentication kullanılmıştır. Farklı kullanıcı türleri oluşturulmuş ve bu kullanıcılara farklı yetki seviyeleri atanmıştır.

## **3. Veri Şifreleme**

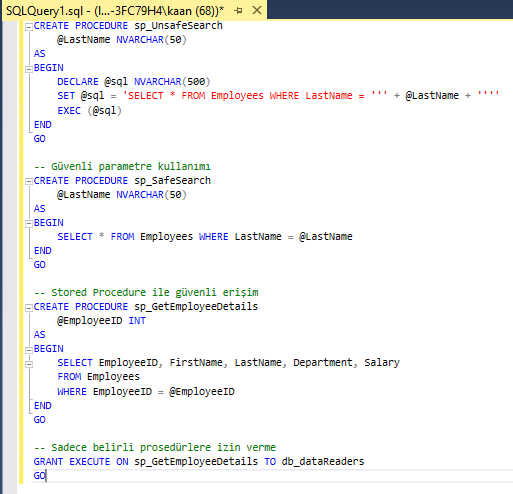
Veri şifreleme aşamasında, veritabanındaki hassas bilgilerin korunması için SQL Server'ın şifreleme özellikleri kullanılmıştır. Bu örnekte, sütun düzeyinde şifreleme uygulayarak hassas kişisel verileri koruyoruz.





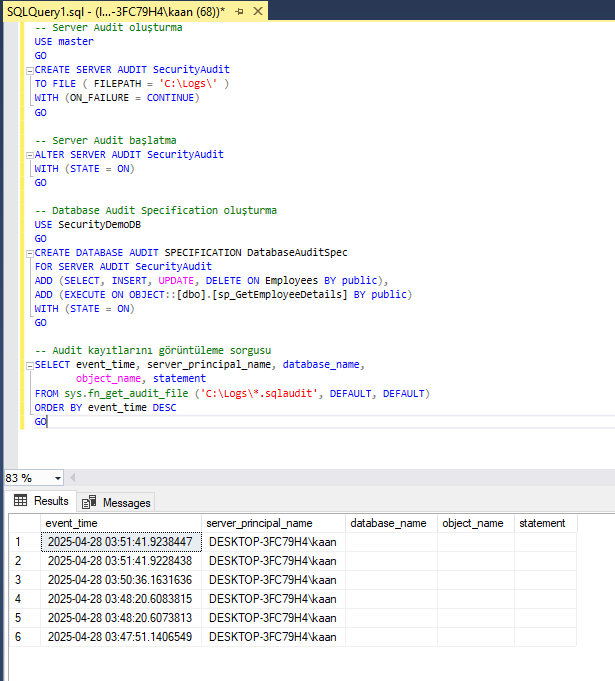
## **4. SQL Injection Testleri**

SQL Injection saldırılarına karşı veritabanının korunması için çeşitli testler yapılmış ve güvenlik önlemleri alınmıştır. Stored Procedure kullanımı, parametreli sorgular ve input validation teknikleri uygulanmıştır.



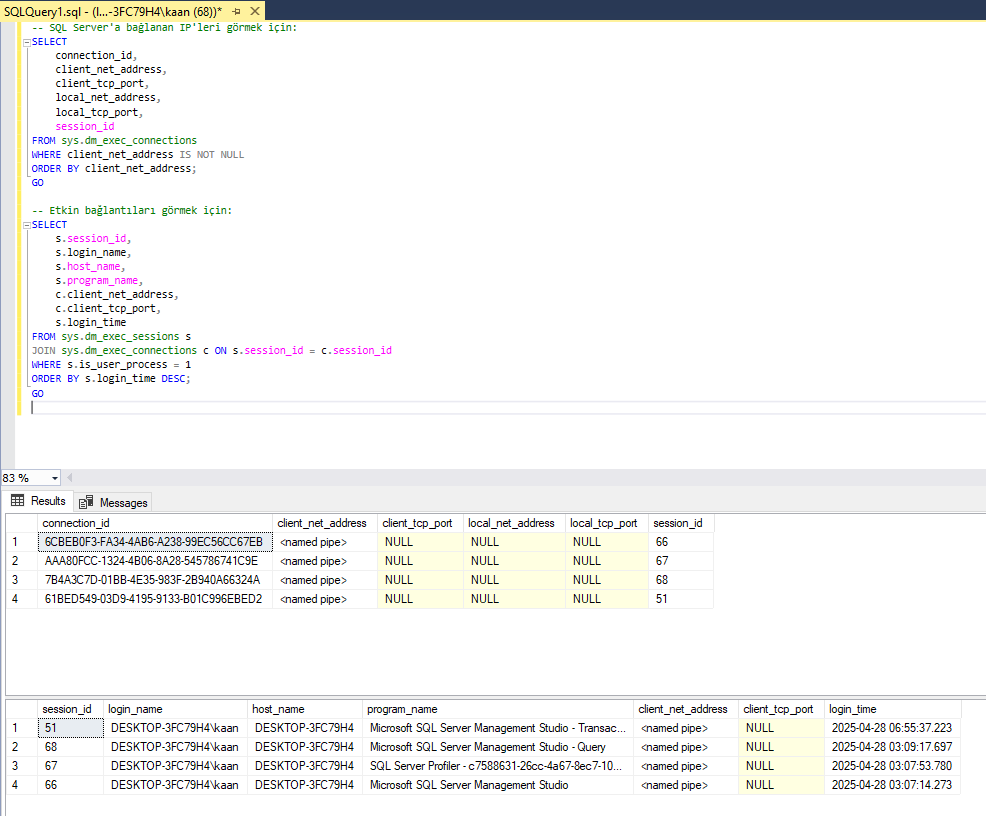
## **5. Audit Logları**

Kullanıcı aktivitelerini izlemek için SQL Server Audit özellikleri kullanılmıştır. Veri değişiklikleri, erişim denemeleri ve güvenlik olayları kaydedilmiş ve incelenmiştir.



## **6. Güvenlik Duvarı Yapılandırma**

SQL Server güvenlik duvarı yapılandırılarak, sadece belirli IP adreslerinden veya ağlardan erişime izin verilmiştir. Bu sayede yetkisiz erişimler engellenmiştir.



## **7. Sonuç**

Bu projede, veritabanı güvenliği ve erişim kontrolü başarıyla uygulanmıştır. Kullanıcı yetkilendirme, veri şifreleme, SQL injection koruması ve audit logları kullanılarak veritabanı sistemi güvenli hale getirilmiştir. Sonuçta, veritabanındaki hassas bilgiler yetkisiz erişimlerden korunmuş ve olası güvenlik ihlalleri takip edilebilir hale getirilmiştir.

Projenin ana kazanımları şunlar olmuştur:

1. Farklı kullanıcı türleri ve yetki seviyeleri ile erişim kontrolü sağlanmıştır.
2. TDE ve sütun düzeyinde şifreleme ile hassas veriler korunmuştur.
3. SQL Injection saldırılarına karşı önlemler alınmıştır.
4. Audit logları ile veritabanı üzerindeki tüm aktiviteler izlenmiştir.
5. Güvenlik duvarı ayarları ile yetkisiz network erişimleri engellenmiştir.

Bu güvenlik önlemleri sayesinde, veritabanı sistemi hem iç hem de dış tehditlere karşı korunaklı hale getirilmiştir.