VERITABANI TASARIMI

Öğretim Görevlisi A. Berika VAROL MALKOÇOĞLU



İçindekiler

- Join ifadeleri
- Veritabanı güvenliği
- Savunma yöntemleri



Join

- Veritabanı tasarımı ve tablo oluşturma sırasında tablolar çeşitli parçalara ayrılarak veri tekrarının önüne geçilmiş olur.
- Parçalara ayrılan tablolar tek başına bir anlam ifade etmeyebilir.
- Parçaların anlamlı olabilmesi için tabloların birleştirme işlemine tabi tutulması gerekir.
- SQL join ifadeleri kullanılarak tablolar sanal olarak birleştirilir.
- JOIN ifadeleri iki veya daha fazla tabloyu birleştirmek için kullanılır.



Join

Tabloları birleştirmek için;

```
SELECT tablo_A.sutun_adi FROM tablo_A {INNER JOIN | LEFT JOIN | RIGHT JOIN} tablo_B ON tablo_A.sutun_adi = tablo_B.sutun_adi;
```



Join Türleri

- INNER JOIN: Birden çok tablodaki verileri birleştirmek için kullanılır.
- LEFT (OUTER) JOIN: Birden çok tablodaki eşleşen kayıtlar ve eşleşmeyen sol kayıtlar için kullanılır.
- RIGHT (OUTER) JOIN: Birden çok tablodaki eşleşen kayıtlar ve eşleşmeyen sağ kayıtlar için kullanılır.
- FULL OUTER JOIN: Birden çok tablodaki eşleşen kayıtlar ve eşleşmeyen sağ ve sol kayıtlar için kullanılır. LEFT ve RIGHT JOIN birleşimidir.

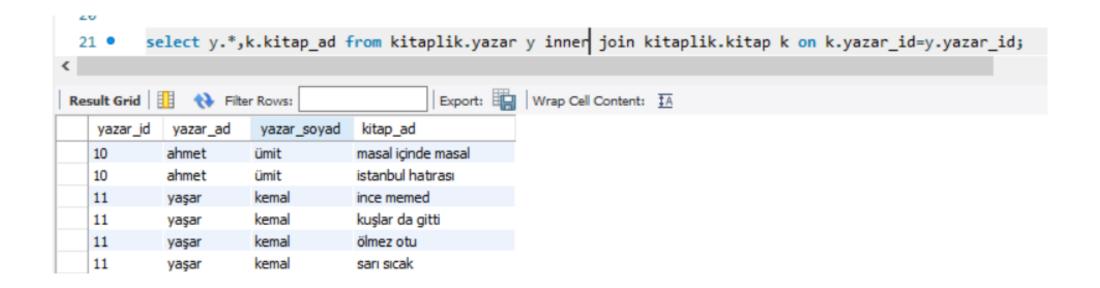


```
SELECT musteri.ad, musteri.soyad, musteri.urun_adet, urun.ad,urun.fiyat as "Bir ürün için"
  8 .
         FROM eczane.musteri
  9
         INNER JOIN urun ON musteri.urun = urun.urun_no;
 10
 11
Result Grid
                                            Export: Wrap Cell Content: IA
              Filter Rows:
                                       Bir ürün
                 urun_adet
   ad
          soyad
                            ad
                                       için
  Aslı
         Can
                            Aspirin
                                      3.98
                           Katarin
                                      7.99
  Ayşe
  Fatma
         Saygin 1
                           Bepanthen
                                      17.49
```

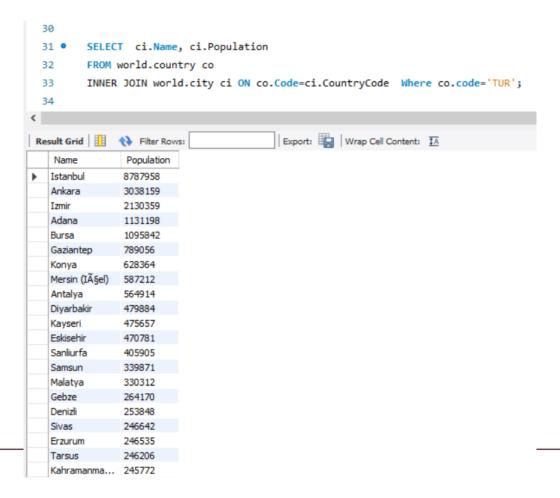


```
13 •
          SELECT kitap.kitap_ad, yazar.yazar_ad,yazar.yazar_soyad, kategori.kategori_ad
 14
          FROM kitaplik.kitap
 15
          INNER JOIN kitaplik.yazar ON kitap.yazar_id = yazar.yazar_id
 16
          INNER JOIN kitaplik.kategori ON kitap.kategori_id = kategori.kategori_id;
                ♦ Filter Rows:
                                                 Export: Wrap Cell Content: IA
Result Grid
   kitap_ad
                         yazar_ad
                                     yazar_soyad
                                                  kategori_ad
                        sabahattin
                                                  türk klasikleri
  kürk mantolu madonna
   kuyucaklı yusuf
                         sabahattin
                                                  türk klasikleri
   kağnı
                         sabahattin
                                                  roman
   benim adım kırmızı
                         orhan
                                     pamuk
                                                  roman
                         orhan
                                    pamuk
                                                  roman
   kırmızı saçlı kadın
                         orhan
                                    pamuk
                                                  roman
   masumiyet müzesi
                         orhan
                                     pamuk
                                                  roman
   XXXX KİTABI
                                                  fantastik
                         orhan
                                    pamuk
   sevgi duvarı
                                     yücel
                         can
   can yücel'in şiirleri
                                                  siir
                                    yücel
                         can
                                    kulin
   adı: aylin
                                                  roman
                         ayşe
   sevdalinka
                                     kulin
                         ayşe
                                                  roman
                                    kulin
   tutsak güneş
                         ayşe
                                                  roman
   veda
                                    kulin
                         ayşe
                                                  roman
   sinekli bakkal
                        halide edip
                                    adıvar
                                                  türk klasikleri
                                                  türk klasikleri
   ateşten gömlek
                        halide edip
                                    adıvar
```



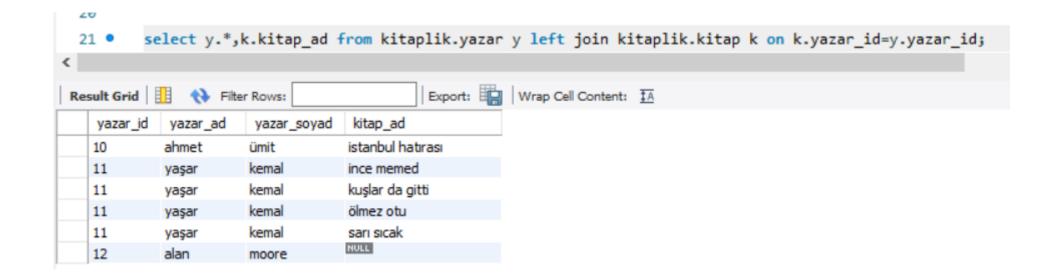








Left Join





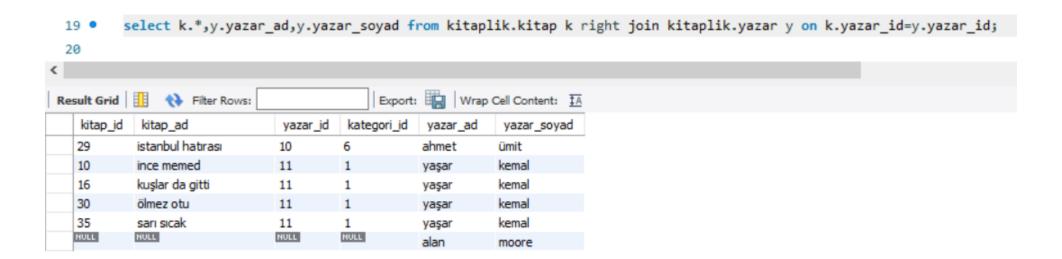
Left Join

29 • SELECT c.calisan_no, c.ad, c.soyad, m.* FROM eczane.calisan c LEFT JOIN musteri m ON c.calisan_no = m.calisan;

<									
R	esult Grid	alt Grid 🔠 🙌 Filter Rows			Export: Wrap Cell Content: TA				
	calisan_no	ad	soyad	musteri_no	ad	soyad	urun	urun_adet	calisan
۰	10	Ali	Öz	100	Aslı	Can	1	2	10
	10	Ali	Öz	104	HULL	NULL	5	1	10
	11	Ayşe	İz	101	Ayşe	Al	4	1	11
	11	Ayşe	İz	102	Fatma	Saygin	5	1	11
	12	Burak	Ulutaş	103	Emine	Yılmaz	6	1	12
	13	Ceren	Çubuk	HULL	NULL	NULL	NULL	NULL	HULL
	14	Zeynep	Güven	HULL	NULL	NULL	NULL	NULL	NULL



Right Join





Right Join

-SELECT m.*, u.ad, u.fiyat FROM eczane.musteri m RIGHT JOIN urun u ON M.urun = u.urun no; Result Grid Export: Wrap Cell Content: IA Filter Rows: urun_adet calisan musteri_no ad ad fiyat soyad urun Aslı 10 Aspirin 3.98 100 Can 2 NULL NULL NULL NULL NULL NULL Parol 8.18 7.99 101 Katarin Ayşe 11 Saygin 17.49 Fatma 11 Bepanthen 102 NULL NULL 10 104 Bepanthen 17.49 Yılmaz 12 aferin 6.89 103 Emine NULL HULL NULL HULL HULL HULL 18.5 majezik HULL NULL HULL NULL HULL HULL

coraspin

13.69



Veri Tabanının Ele Geçirilmesine Neden Olan Tehditler



Kullanıcı İzinleri

- Veritabanındaki kullanıcı izinlerinin iyi bir kontrol mekanizması ile yönetilmemesi
- Kullanıcılara ihtiyaçlarının üzerinde haklar verilmesi,
- Bu kullanıcıların
 - Hesap bilgilerinin çalınması,
 - Bilgizilikten/dikkatsizlikten kaynaklanan hataları veya
 - Kötü niyettli davranışları sonucunda sistemin kolayca ele geçirilmesine neden olacaktır.



SQL Enjeksiyon

- Veri tabanlarına yönelik gerçekleştirilen en yaygın ataklardan biridir.
- SQL enjeksiyon saldırıları veri tabanı veya veri tabanına ara yüz olarak çalışan web uygulamalarını hedef alarak sisteme ulaşmaya çalışmaktadır.
- SQL enjeksiyon atakları saldırganın veri tabanı üzerindeki hassas bilgilere erişmesini, kullanıcı haklarını yükseltmesini ve database işletim sistemi komutlarına ve veri tabanının kendisine ulaşması gibi tehlikeli işlemleri yapmasına neden olabilmektedir.



Zararlı Yazılım Bulaştırma

- Çalışanın;
 - Mail hesabına gönderilen oltalama maili,
 - Zararlı usb belleğin bilgisayarına takılması veya
 - Bilinmeyen sitelerden program indirmesi ile zararlı yazılımın veritabanı kullanıcısının bilgisayarı üzerinden veri tabanı sistemine bulşaması olabilir.



Raporlama ve Yedekleme Sorunu

- Otomatize edilmiş olay kayıtları veri tabanı sistemlerinin güvenliği için büyük önem taşımaktadır.
- Kayıtlar düzenli raporlanmadığı takdirde çeşitli sorunlara yol açacaktır.
- Yada olan sorunları çözümlemeyi engelleyebilir.
- Genelde canlı sistemler daha iyi korunmaya alınmaktadır.
- Ancak yedekleme dosyalarının ve yedekleme ortamının güvenliği de canlı sistemler kadar önemlidir.
- Saldırganlar şifrelenmemiş bir yedekleme dosyası üzerinden sisteme sızabilir.



DOS Saldırısı

- Hizmet engelleme saldırısı olarak adlandırılan DOS atakları ağ cihazlarına veya verilere erişimi engelleyen bir saldırı türüdür.
- Veri tabanı sistemlerine karşı gerçekleştirilen DOS saldırılarında, sistemde büyük oranda bir kaynak kullanımına neden olan arama yapma ve istek gönderme işlemleri gerçekleştirilerek sunucuya aşırı yük bindirilmesi ve hizmet veremez hale getirilmesi hedeflenir.



Veri Tabanı Güvenliği Yöntemleri



Veri Tabanı Güvenliği Yöntemleri

- Verilerin sınıflandırılması
 - Bu yöntemle asıl güvene alınması gereken hassas verilerin daha kolay tanımlanabilmesinin sağlar.
 - Yalnızca veritabanını değil, verileri korumayı hedefler.
- Üçüncü parti bir denetim yazılımı ve ağ cihazı kullanılması
 - Hem koruma hem de monitoring servisi veren bu cihazlar veri tabanı sunucusundan ayrı olarak kuruldukları için sunucuya ek yük bindirmezler.
 - Kullanıcının gereksinimlerine göre özelleştirilebilen bu çözümler birçok özelliğe sahip olmasının yanı sıra aynı zamanda yüksek oranda analiz sonucu alabilmek için detaylı denetim yaparlar.



- Durağan haldeki datanın şifrelenmesi kadar hareket halindeki datanın da güçlü kimlik doğrulama kontrolleri ile iletimi de büyük önem taşımaktadır.
- Durağan haldeki veriler için AES şifreleme algoritması önerilmektedir.
- Varsayılan kullanıcı şifrelerini değiştirmek.
- Kullanılmayan kullanıcı hesaplarını kilitlemek.
- Daha güçlü şifreler uygulamak.



- Şifrenin ömrü kontrol edilmeli, kullanım süresi dolduğunda uyarı mesajı verilmeli.
- Eski şifrelerin yeniden kullanılmasını engelleyecek bir kısıtlama getirilmeli.
- Analiz edilip güvenliğinin sağlanması gereken veri tabanını tespit etmek.
- Veri tabanını zafiyetler, yanlış yapılandırmalar ve kritik değişiklikler için taramak.



- Dataların sınıflandırılması esas alınarak yüksek önemdeki açıklıkların öncelik verilerek kapatılması.
- Zafiyetler için uygun bir düzeltme tespit etmek, zafiyetleri kapatmak ve sistemi güncellemek için yamaları uygulamak
- Zafiyet düzeltme işlemlerinin etkisini ölçmek için düzeltmeden sonra denetim işlemi tekrarlanmalıdır ve bu döngü periyodik olarak tekrarlanmalıdır.
- Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılmalıdır.



- İhtiyacınız olmayan modülleri ve hizmetleri ve/veya paketleri çıkartılmalı.
- Veritabanları için doküman onaylı yapılandırma referansı kullanılmalıdır.
- Girdi/Çıktı kontrolleri, kullanıcı girdisinde problem yaratabilecek SQL'e özel karakterler var mı? Girilen veri, veri tipine uyumluluk gösteriyor mu?
- Girilen veri limitler dahilinde mi? (Taşma hataları)



- Gerekli hata denetimi fonksiyonlarıyla program çıktısı seçenekleri kontrol edilmelidir.
- Uygulamalar ve veritabanı, özellikle Web uygulaması arasındaki oturumları şifrelenmeli.
- Veritabanı güncellemelerini kontrol edilmeli.
- Uygulama tasarımı ve programlanması sırasında güvenlik ilkeleri ve oluşabilecek problemler dikkate alınmalıdır.
- Sistem üzerinde bilgi toplanmasına neden olabilecek başlık bilgileri ve hata mesajlarının açık bırakılmaması gereklidir.



- Fiziksel bütünlüğü sağlamak için hesap verebilirlik ve denetim kontrolleri gereklidir.
- Veri tabanı trafiğini analiz eden, çalıştırmayı algılayan, engelleyen, yetkisiz sorgular ve SQL enjeksiyonları tespit eden gerçek zamanlı çözümler araştırılmalı.



- Bu algılanan tehditler hakkında uyarılar ve raporları yönetici belirlenen kişilere e-posta veya anlık mesajlaşma ile uyarı gönderilmeli.
- Güncel olmayan kimlik doğrulama sistemlerine ait istemcilerin bağlantıları engellenmeli.
- Veri kaybolduğunda veya çalındığında ne yapacağınıza dair bir plan yapılmalı.
- Kullanıcıların sadece belirttikleri sistem üzerinden bağlanmalı.
- Kullanıcıyı yönetmek (yaratmak, silmek, denetlemek) için politikalar oluşturulmalı.
- Kullanıcı izleme politikasını belirlenmeli.

