VERİTABANI GÜVENLİĞİ ve SAVUNMA ALGORİTMALARI

Öğretim Görevlisi A. Berika VAROL MALKOÇOĞLU

BEYKOZ ÜNİVERSİTESİ

Veritabanı Nedir?

- Veritabanı, kolayca güncellenebilen, düzenlenebilen, yönetilen ve erişilebilen düzenli bir veri topluluğudur.
- Birbiriyle ilişkili verilerin depolandığı alandır.
- Veritabanını korumak için bir veritabanı yönetim sistemine ihtiyacımız vardır.

Veritabanı Yönetim Sistemleri (VTYS) Nedir?

- Veritabanının düzenli biçimde tutulduğu ve bu verilerin yazılımlar aracılığı ile yönetildiği ortamlara **veritabanı yönetim sistemleri** denir.
- SQL çeşitleri;
  - **SQL;** veriler üzerinde çalışmak için bir sorgu dilidir.
    Az çok standartlaştırılmıştır ve hemen hemen tüm ilişkisel veritabanı yönetim sistemleri tarafından kullanılır: SQL Server, Oracle, MySQL, PostgreSQL, DB2, Informix, vb.
  - **PL/SQL;** Oracle tarafından kullanılan tescilli bir prosedür dilidir
  - **PL/pgSQL;** PostgreSQL tarafından kullanılan prosedürel bir dildir
  - **TSQL;** Microsoft tarafından SQL Server'da kullanılan tescilli bir prosedür dilidir.

Veritabanı Güvenliği Nedir?

- VTYS, kurumların veya kişilerin önemli bilgilerinin tutulduğu hassas ve korunması gereken yazılımlardır.
- GÜVENLİĞİN TEMEL ELEMANLARI NEDİR?
  - GİZLİLİK, BÜTÜNLÜK, ERİŞEBİLİRLİK
- Yüksek seviyede VTYS güvenliği için teknolojik önlemlere ek olarak iç güvenlik de dikkate alınmalıdır.
  - Teknik seviyeden idari seviyeye kadar tüm kullanıcılarda **bilgi güvenliği** farkındalığı sağlanmalıdır.
- Veritabanları güvenliği **iç** ve **dış** güvenlik olarak ikiye ayrılabilir.

Veritabanı güvenliği için birçok risk bulunmaktadır. Bunlar kısaca aşağıdaki gibi özet olarak listelenebilir (Khanuja & Adane, 2011):

- Veritabanı yönetimi için bütçe kısıtlamalarının olması
- Tehditleri algılayacak mekanizmaların eksikliği
- Birimler arası ilişkilerin olmaması
- Yönetim ve Bilgi Teknolojileri ekipleri arasındaki uyumsuzluklar
- Veritabanı için uygun güvenlik süreçlerinin ve prosedürlerinin zayıf olması
- Veritabanına erişimde kullanıc rolleri ile ilgili karmaşıklıklar
- Tecrübeli ve yetenekli veritabanı güvenlik profesyonellerinin olmaması
- Veritabanı güvenlik sorunlarına bilinçli yaklaşımların getirilmesi ve uygun çözüm yollarının sunulmasında yaşanan eksiklikler
- Veritabanı güvenlik rutinlerinin oluşmamış olması

Veritabanı: İç Güvenlik

- Sistemdeki güvenlik açıkları kapatılmalı.
- Kullanıcıları şifreleri güçlü olmalı.
- Kullanıcıların yetkileri sınırlandırılmalı.
- Veritabanı işlemleri loglanmalı ve bu loglar raporlanmalı.
- Yapılan işlemler işletim sistemine kaydedilmeli.
- Yedekleme yapılırken şifrelenmeli.

Veritabanı: Dış Güvenlik

- Bir veri tabanı internete açıksa, dış tehditlere de açık demektir.
- Firewall olmalı.
- SQL'in yapısı anlık olarak incelenmelidir.
- SQL injection saldırısına karşı yazılımları kullanılmalı.

Veritabanı Güvenliği

- Verinin güvenli bir ortamda saklanması gerekmektedir.
- Veriler güvenli bir şekilde muhafaza edilmeli ve gizli tutulmalıdır.
- Veritabanına sadece izin verilen kullanıcılar erişebilmelidir.
- Veri Tabanı Güvenliği 2 şekilde incelenebilir:
  - Tabii afetlere karşı olan güvenlik
  - Yetkisi olmayan kişilere karşı güvenlik

- **YEDEKLEME**
- Düzenli olarak veritabanın yedeğinin alınması gerekmektedir.
- Kullanıcılar kontrol edilmeli ve sisteme zarar vermemelidirler.
- Bozulan bilgilerin veya herhangi bir nedenden dolayı ulaşılamayan veri tabanlarının düzeltilebilmesi yedeklere bağlıdır.
- Tam yada kısmi yedekleme türleri mevcuttur. Kurum içinde ihtiyaca yönelik yedekleme prosedürü geliştirilmelidir.
- Yedek ve orijinal verinin fiziksel konumları ayrı olmalıdır.

- **SİSTEMİN TEST EDİLMESİ VE BAKIMI**
- Veritabanının doğru ve geçerli işlemler yapıp yapmadığına bakılır.
- Veritabanının sık sık yedeği alınır (backup).
- Disk arızası gibi durumlarda yedekten geri yüklenir (recovery).

Veritabanına Yapılan Saldırı Türleri

- Brute force saldırıları
- SQL injection saldırıları
- Hizmet Reddi (DoS/DDoS) saldırıları
- Zararlı yazılımlar
- İçerideki tehditler

Brute Force

- Kaba kuvvet saldırıları, bir hedef üzerinde kombinasyon yapmaya çalışmasına "Brute Force Attack" denir.
- Brute force (kaba kuvvet) saldırısı, hacker'ların bir hesaba erişebilmek için deneme-yanılma yöntemi kullanmasına denir.
- Bu, duruma bağlı olarak parola ya da kişisel kimlik numarası (PIN) kırılmasını içerebilir.
- Çoğu kaba kuvvet saldırısı otomatiktir, bu yüzden her ölçekten işletme hedef olabilir.
- Zamana ihtiyaç duyar.

Brute Force

- Peki ne kadar zamana?
- ‘parola’ parolasını kırmaya çalışalım;
- 29’un 6’lı kombinasyonu

  29x29x29x29x29x29=594.823.321 farklı parola kombinasyonu olur.

Diyelim ki; saldırgan dışarıdan saldırıyor
(bağlantı hızı saniyede 20 parola denetebilir)

594.823.321 / 20= 29.741.166 sn

~344 Gün
~11 Ay
~1 Yıl

Diyelim ki; saldırgan içeriden saldırıyor
(bağlantı hızı saniyede 5000 parola denetebilir)

594.823.321 / 5000= 118.964 sn

~33 saat
~ 1,5 gün

EN KÖTÜ DURUMDA

Brute Force Saldırılarından Korunmak

- Login işlemlerini kayıt altına almak
- Şart koyarız
  - Logları 3 dk. da bir oku
  - Eğer hata mesajını 100 den fazlaysa saldırı olduğunu tespit et.
  - IP adresi tespit et Admine otomatik mail gönder.
- Belirlenen IP adresi engellemek için firewall'a kural yamak ya da sql triggerler kullanılır.

Brute Force Saldırılarından Korunmak

- Belirli sayıda hatalı giriş yapıldığı taktirde sonraki denemeler engellenmeli.
- Web sitelerinde güvenlik yazılımları yüklü ve aktif durumda olmalı.
- İki faktörlü kimlik doğrulama sistemi kullanılmalı.
- Daha uzun şifre tercih edilmeli.
- Büyük-küçük harf, özel karakter, alfanümerik şifre kombinasyonları kullanılmalı.

SQL Injection

- Bir SQL enjeksiyonu saldırısında saldırgan genellikle güvenlik açığı bulunan bir SQL veri kanalına yetkilendirilmemiş veritabanı yordamları ekler.
- Bu eklenen yordamlar veritabanına aktarılır ve orada çalıştırılır.
- SQL enjeksiyonu ile saldırganlar veritabanına sınırsız yetki ile erişebilir.
- Sıklıkla web uygulamalarında kullanılan formlar aracılığı ile yapılır.
- SQL enjeksiyon ile;
  - Sisteme kullanıcı eklenebilir
  - Sistem formatlanabilir
  - Verilere zarar verilebilir.
  - Veirler dışarı aktarılabilir vs.

SQL Injection

- Kullanıcı adı ve şifre doğruluğunu normalde şöyle kontrol ederiz;

SELECT * FROM users **WHERE** uname=‘uname’ **AND** pass = ‘pass’

- SQL Injeciton kontrolü yapmadıysak ve saldırı yapıldıysa;

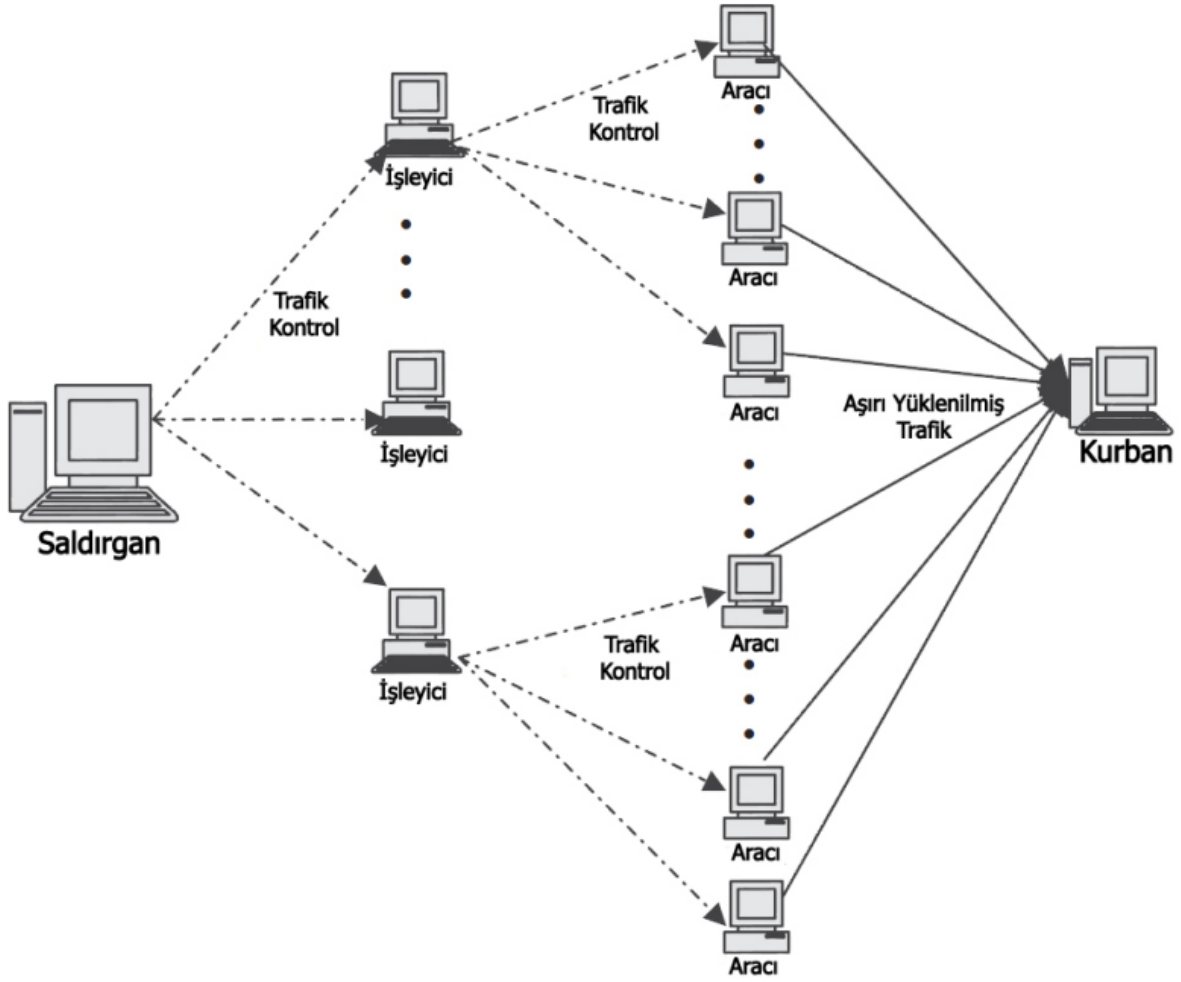
SELECT * **FROM** users **WHERE** username = ’uname’ **OR** 1 = 1 **AND** pass = ‘pass’ **OR** 1= 1

SQL Injection Saldırılarından Korunmak

- Üç yöntem uygulanabilir;
  - Kullanıcıdan alınan her veride ' ve " karakterleri getirilmeli.
  - Kullanıcıdan alınan karakterler karakter koduna çevrilmeli
  - Kullanıcıdan alınan verilerin başına \ eklenmelidir.
- Bu durumda SQL programı o karakterleri komut olarak algılamayacaktır.
- Doğrudan sorgular yerine saklı yordam kullanılması bu durumu önleyebilir.

Hizmet Reddi (DoS/DDoS)

- Dos (Denial Of Service- Servis Hizmet Reddi) saldırısı bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini, kullanıcıların sisteme erişmesini engelleyen bir saldırı türüdür.
- DDos (Distributed Denial of Service- Dağıtılmış Hizmet Reddi) ise saldırının birden fazla sayıda farklı kaynaktan başlatılmasıyla gerçekleşir.



Hizmet Reddi (DoS/DDoS) Saldırılarından Korunmak

- Sistem güncellemeleri zamanında yapılmalıdır.
- -Bant genişliği kurumun ihtiyacı olandan fazla olmalıdır.
- Ağ trafiği izlenilmelidir.
- Yönlendiriciler için sınır özelliği, sahte ve bozuk paketlerin engellenmesi, SYN, ICMP ve UDP paketlerinin eşik değerlerinin belirlenmesi gerekmektedir.
- Veritabanı sunucusuna bağlantı kurma süresi kısaltılmalıdır.
- Kuyruğu azaltmak için dinamik biriktirme listeleri kullanılmalıdır.

Genel olarak

- Yetkilendirmeye dikkat edilmeli
- Log tutulmalı
- Olası saldırılar için önlemler alınmalı
- Ağ izlenmeli
- Kullanıcılar bilinçlendirilmeli
- Yedekleme ve yedekten geri dönme prosedürleri belirlenmeli
- Birden fazla farklı yetkilere sahip VTYS yöneticisi belirlenmeli

Genel olarak

Veritabanı denetimi (auditing): Veritabanı denetimi, veritabanı erişimini ve kullanıcı etkinliğini izlemek için kullanılır. Veritabanı denetimi, veritabanı nesnelerine kimin eriştiğini, hangi eylemlerin gerçekleştirildiğini ve hangi verilerin değiştirildiğini belirlemek için kullanılabilir. Ek olarak veritabanı denetimi, güvenlik ihlallerini engellemez, ancak ihlallerin oluşup oluşmadığını belirlemenin bir yolunu sağlamak için kullanılmaktadır (Murray, 2010).

Genel olarak

Web uygulama güvenlik duvarının kullanımı (firewall): Bir web uygulaması güvenlik duvarı (WAF), uygulama tabanlı ve veritabanı güvenliğinde oldukça etkili olan bir siber güvenlik aracıdır. WAF, HTTP tabanlı kötü amaçlı trafiğini filtreleme, izleme ve engelleme yaparak uygulamaları korumak için tasarlanmış bir güvenlik politika aracıdır (Prandl *vd.*, 2015).

Genel olarak

Fiziksel güvenlik çözümlerinin kullanılması: Fiziksel veritabanı güvenliği, yetkisiz erişimlerden korunmak için veritabanı sunucusu odasının korunmasıdır. Veritabanı sunucusu, güvenli bir binada ve iklim kontrollü bir ortamda bulunmalıdır. Ayrıca RAID tabanlı disk çözümleri de veritabanı güvenliği için kullanılabilecek fiziksel bir güvenlik kontrolüdür.

Genel olarak

Uygulama tabanlı güvenlik yazılımlarının tercih edilmesi: SQL yerleştirmesi gibi tehditlere karşı veritabanı güvenliğinin sağlanması için saklı yordam, görünüm (views) ve güvenlik yazımları gibi ek çözüm yollarından yararlanılmalıdır.

Genel olarak

Güçlü kullanıcı ve yönetici şifrelerinin kullanılması: Veritabanlarında yönetici ve farklı rollere sahip kullanıcıların güçlü şifreler kullanması, bu şifrelerin periyodik olarak değiştirilmesi ve paylaşılmaması veritabanı güvenliği açısından olukça önemlidir.