SDU International Journal of Technological Sciences
Vol. 10, No 2, August 2018
pp. 22-46

ORACLE VE MS SQL SERVER VERİ TABANLARI İÇİN VERİ TABANI YÖNETİM SİSTEMLERİ GÜVENLİK KONTROL İLKELERİNİN TAKİP EDİLMESİ VE UYGULANMASI

Bekir Eray Katı*, Ecir Uğur Küçüksille

Geliş Tarihi/ Received: 30.09.2018, Kabul tarihi/Accepted: 12.11.2018

Özet

Veri tabanı yönetim sistemleri, veri tabanlarını tanımlamak, oluşturmak, kullanmak, değiştirmek ve veri tabanı sistemleriyle ilgili her türlü işletimsel gereksinimleri karşılamak için tasarlanmış sistem ve yazılımlardır. DB-Engines verilerine göre günümüzde 300'ün üzerinde veri tabanı yönetim sistemi geliştirilmiştir.

Bu tez çalışmasında Oracle ve MS SQL Server veri tabanı yönetim sistemleri için kendi şirketleri tarafından oluşturulan güvenlik kontrol ilkeleri incelenmiş ve bu ilkelerin uygulanmadığı takdirde ortaya çıkabilecek olası sonuçlar ortaya konulmuştur. Güvenlik kontrol ilkelerinin detaylıca tanımlanmasının ardından, java server faces aracılığı ile güvenlik kontrol ilkelerini Oracle ve MS SQL Server veri tabanlarına uygulayan bir uygulama geliştirilmiştir. Uzak sunucu ihtiyacı için sanal laboratuvar ortamı oluşturulmuştur.

Uygulama hem uzak sunucu üzerinde hem de ana bilgisayar üzerinde test edilmiştir. Güvenlik kontrol ilkelerine göre yönetilmeyen veri tabanı yönetim sistemlerinin aslında birçok güvenlik açığı bulundurduğu tespit edilmiştir. Kullanıcı verileri, giriş bilgileri ve hatta ana bilgisayardaki diğer özel verilerin bile saldırı altında olabileceği sonucu ortaya konulmuştur.

Anahtar Kelimeler: veri tabanı yönetim sistemleri, veri tabanı güvenlik kontrol ilkeleri, veri tabanı güvenliğinde korunma yöntemleri

SUBMITTING AND IMPLEMENTING SECURITY CONTROL PRINCIPLES FOR DATABASE MANAGEMENT SYSTEMS FOR ORACLE AND MS SQL SERVER DATABASES

Abstract

Database management systems are systems and software designed to define, create, use, modify databases and meet all operational requirements related to database systems. According to DB-Engines data, today more than 300 database management systems have been developed.

In this thesis study, the security control policies created by their own companies for Oracle and MS SQL Server database management systems have been examined and the possible results that could arise if these principles were not applied. After a detailed description of the security control policies, an application has been developed that applies security control policies to Oracle and MS SQL Server databases via java server faces. A virtual laboratory environment was created for remote server needs. The application has been tested on both the remote server and the host computer.

It has been found that database management systems that are not managed by security control policies actually have many security deficiencies. User data, login information, and even other private data on the host computer are the result of being under attack

* Bilgisayar Mühendisliği, Süleyman Demirel Üniversitesi, Isparta, Türkiye
E-posta: bekireraykati@gmail.com

Key Words: database management systems, database security control list, protection methods of database security

1. Giriş

Veri işlenmemiş bilgi parçası olarak adlandırılır. Herhangi bir olay üzerinde gözlem, deney ve ölçüm yapılarak o olay hakkında çeşitli veriler elde edilebilir. Bilgisayar bilimleri bakımından incelendiğinde veriler binary (ikili) veya karakter kodlama ile kaydedilir [1]. Bulunan veriler birbirinden bağımsız, çok sayıda farklı yapıda olabilir. Bu çok sayıdaki veri, veri tabanı adı verilen bir sistemde tutulmaktadır.

Veri tabanı birçok kullanıcı tarafından kullanılan büyük veri kümelerini düzenleyip belirli bir formatta depolar. Büyük miktardaki bilgileri depolamada geleneksel yöntem olan "dosya-işlem sistemine" alternatif olarak getirilmiştir [2]. Veri tabanları, veri tabanı yönetim sistemleri aracılığıyla oluşturulur ve yönetilir. Veri tabanı sistemlerinin kurulumu, kullanıcılara yetki ve rol atama işlemleri, veri düzeni, sorgulaması, güvenliği ve denetimi gibi çok sayıda işin kontrol altına alınabilmesi için veri tabanı yöneticiliği kavramını ortaya çıkarmıştır [3].

Veri tabanı yönetim sistemleri dört farklı veri modeline göre sınıflandırılmaktadır. Sıradüzensel (hiyerarşik) veri modeli, ana bilgisayar ortamlarında çalışan yazılımlar tarafından kullanılmaktadır. IBM tarafından gelitirilen IMS, bu türde en çok kullanılan yazılımdır. İlk çıkan veri modeli olmasına rağmen, bilgisayar ortamında kullanılan hiyerarşik veri modeli bulunmamaktadır [4]. Hiyerarşik veri tabanları, bilgileri bir ağaç (tree) yapısında kayıt altına alır. Kayıt (kök) ve bu köke bağlı kayıtlar (dal) bu veri tabanının temelini oluştururlar.

Ağ veri modeli karmaşık bir model olup hiyerarşik modele benzemektedir. Ancak bu modelde bir dosyanın birden fazla dosyayla doğrudan ilişkisi vardır. Hiyerarşik modele göre düşünülürse bir dalın birden fazla kökü; benzer şekilde bir kökün birden fazla dalı olabilmektedir.
Nesneye yönelik veri modelinde veriler nesne olarak modellenir ve oluşturulur. Nesneye yönelik programlamada kullanılan sınıf ve miras kavramlarına sahiptir. Karmaşık veriler üzerinde işlem yaparken yüksek performans sunan bir yaklaşımdır. Arama işlemleri diğer veri modellerine göre oldukça hızlıdır [4].

İlşkisel veri modeli günümüzde en çok kullanılan veri modelidir. Bu sistemde veriler tablolarda satır ve sütunlar şeklinde saklanır. Çeşitli tablolar arasında organize edilmiş verilerden oluşan veri modeli olarak açıklanabilir. Bu farklı tablolar arasındaki veriler, çeşitli anahtarlar vasıtası ile birbirine bağlanırlar. Bu anahtar sütün aracılığı ile birden çok tablo verileri birbiriyle bağlantı sağlayabilir ve herhangi bir sorgulamada birlikte görüntülenebilir. İlişkisel veri tabanı yönetim sistemlerine örnek olarak Microsoft SQL Server, Oracle, MySQL, Microsoft Access ve Postre SQL örnek olarak verilebilir [3].

Şekil 1.1.'de kullanım oranı en yüksek ilk beş veri tabanı yönetim sistemi gösterilmiştir. Oracle veri tabanı 12c sürümü ile birlikte bulut depolama teknolojisinde kendini geliştirerek verilerin sanal ortamda güvenli bir şekilde tutulduğunu göstermiştir. Windows, linux, os x, solaris, aix, hp-ux, z/os gibi geniş bir işletim sistemi aralığında sunucu olarak hizmet verebilmektedir. Ayrıca içinde Java, Pythonn, C#, C++, Ruby gibi popüler programlama dillerinin de bulunduğu yirmi dört farklı programlama dili desteği sunmaktadır. Bu sebepten dolayı çok fazla kullanıcıya ulaşmış ve günümüzdeki en popüler veri tabanı olmuştur. Oracle

veri tabanını takip eden MySQL'in beş işletim sistemi ve on dokuz programlama diline desteği vardır. Üçüncü sırada olan MS SQL Server' ın ise iki işletim sistemi ve on programlama dili desteği bulunmaktadır. [5]

Şekil 1.1. Günümüzde Veri Tabanı Kullanım Oranları [6]

Bir veri tabanı yönetim sistemi, kurulumuyla beraber yazılımsal ve varsayılan yapılandırmalardan kaynaklanan birçok güvenlik açığını beraberinde getirir. Varsayılan yapılandırmalardan kaynaklanan açıkların temel sebebi, kurulum esnasında yönetici tarafından kullanılmayacak pek çok özelliğin sunucu üzerinde aktif edilmesi ve varsayılan olarak bırakılmasıdır. Sunucuya veri tabanı yönetim sistemi kurulmadan önce, iyi bir planlama yapılıp, bu plan doğrultusunda bir veri tabanı ve network uzmanıyla beraber gerekli konfigurasyonlar yapılmalıdır.

Veriler insan yaşamında önemli bir noktada bulunmaktadır. Bir bireyin kişisel verileri, bir şirketin yüksek kâr sağlayabileceği planlama verileri veya bir bankadaki müşterilerin hesap hareketlerini tutan veriler saldırganlar tarafından tehdit altındadır. Her ne kadar güvenlik yamaları ile yazılımsal güvenlik açıklıkları kapatılmaya çalışılsa da yapılandırmadan kaynaklanan açıklar için bu durum geçerli değildir. Yapılandırmalardan kaynaklanan güvenil akçılarını öneleyebilmek amacı ile veri tabanı yönetim sistemlerini geliştiren şirketler kendi güvenlik kontrol ilkelerini oluşturmuşlardır.

Bu çalışmada, SQL Server ve Oracle veri tabanı yönetim sistemleri için gerekli güvenlik kontrol ilkelerini test ederek veri tabanı yöneticisini bilgilendirerek isterse ilgili özelliği düzeltmesi konusunda yardımcı olan bir web tabanlı yazılım geliştirilmiştir. Literatürde yapılan çalışmalar sadece güvenlik doğrulama ilkelerini tanımlayıp SQL Server veya Oracle'ın kendi arayüzleri kullanılarak bir çözüme ulaşılmasını konu almıştır. Bu çalışmada ise Sistem yöneticisinin her hangi bir T-SQL veya PL/SQL kodu yazmadan tek bir arayüz üzerinden güvenlik ilkelerini tarayıp, herhangi bir güvenlik açığında müdahale etmesine olank sağlamaktadır.

2. Literatür Özetleri

Muralidhar K. vd. (1999) çalışmalarında, veri güvenliğini sağlamak için matematiksel metotlar kullanmışlardır. Bu metotlarla veri analizi ve veri gizliliğini eş zamanlı olarak yürütmüşlerdir [7].

Bertino E. ve Sandhu R. (2005) çalışmalarında, veritabanında geliştirdikleri isteğe bağlı veya zorunlu ve rol tabanlı erişim kontrol modelleri üzerinde çalışmalar yapmışlardır Ayrıca veri yönetim sistemleri ve XML (Extensible markup Language) üzerinde veri kontrolü üzerine tartışmışlardır [8].

Mehta R. (2006) çalışmasında, oracle veritabanı şifre yönetiminde, kullanıcı yetkilendirme yöntemlerinde, veri tabanı bağlantı kurulum çeşitlerini ideal bir şekilde oluşturmayı açıklamıştır. İşletim sisteminden kaynaklanabilecek sistem açıkları için önerilerde bulunmuştur [9].

Aaron N. (2006) çalışmasında, oracle veritabanındaki sunucu – dinleyici arasındaki iletişimi irdelemiştir. Dinleyici verilerinin farklı işletim sistemleri üzerinden uzak bağlantı ile nasıl kontrol edilebileceğini yorumlamıştır [10].

Vural Y. ve Sağıroğlu Ş. (2010) çalışmalarında, veritabanı yönetim sistemleri güvenliğini etkileyen doğrudan veya dolaylı bileşenleri açıklamışlar ve bu bileşenlere tek bir çatıdan farklı bir bakış açısıyla bakılmasını sağlayan bir yaklaşım sunmuşlardır [11].

Titrade C. – M. (2011) çalışmalarında, oracle veri tabanında oracle kullanıcı, kaynak ve şifre yönetimi konularında güvenlik önlemlerinin nasıl alınacağından bahsetmişlerdir. Oracle http (hyper text transfer protocol) server ve oracle access control hakkında detaylı bilgi verilmişlerdir [12].

Türköz T. vd. (2012) çalışmalarında, Oracle veri tabanı mimarisinin nasıl oluşturulacağı, veri tabanını geliştirme ortamını, veri tabanı yönetim sürecini, bağlantı yönetimlerini ve güvenlik yapılandırılmasının nasıl yapılacağından bahsetmişlerdir [13].

Qian K. vd. (2017) çalışmalarında, mobil veri tabanlarına ve mobil cihazların ön belleklerine yapılan saldırıları incelemiştir. Ayrıca öğrenciler için mobil veri tabanının RSA ile nasıl kriptolanacağını anlatmışlardır [14].
Gupta A. M. ve Gore Y. R. (2016) çalışmalarında, dağıtık veri tabanı sistemlerini ve veri güvenliğindeki güvenlik sorunlarının eş zamanlı denetimini incelemişlerdir. Dağıtık veri tabanları sistemlerinde çok seviyeli erişim kontrolüne, gizlilik, güvenilirlik ve bütünlük konularına çözüm yolları sunmuşlardır [15].

Gupta K. vd. (2016) çalışmalarında, verileri saldırganalara karşı korumak için bilgi tabanlı gizili ve kişisel bilgileri birleştirerek iki yönlü bir kimlik doğrulama yöntemini önermişlerdir [16].

Grachev V. M. vd. (2014) çalışmalarında, veri tabanının evrensel model örneğiyle saklanan kurumsal verilerin güvenliğini sağlayan araçlar ve yöntemler göz önüne almışlardır. Veri tabanı şemasında uygulanan platform ve özel veri koruma aracı olarak kullanılan evrensel veri modelini tartışmışlardır [17].

Hamdi Mohammed. vd. (2014) çalışmalarında, ağ modelinde geliştirilen veri tabanlarının kripto-sistem mimarisiyle analizini ele almışlardır. Veri tabanlarının uygulama ve depolama seviyesindeki kiriptolama ve çözümleme işleyişini tartışmışlardır. Maskelenen verinin kriptolama işlemini açıklayarak ağ modeli veri tabanlarında korunma yöntemlerini belirlemişlerdir [18].

3. Ms Sql Server Veri Tabanı İçin Güvenlik Doğrulama Listesinin Tanımlanması Ve Uygulanması

Veri tabanı kontrol listeleri, bir veri tabanının kurulum sırasında ve sonrasında oluşan güvenlik açıklıklarını kapatmak için uygulanan kurallar bütünüdür. Veri tabanı kurulurken bilinçsiz bir kullanıcı tarafından kuruluyorsa varsayılan olarak gelen tüm ayarları kabul edilmekte, üzerinde bir değişiklik yapılmamaktadır. Sunucu üzerinde bulunan birçok özellik veri tabanı ile etkileşimde bulunabilmektedir. Bu gibi durumlarda, veri tabanı kontrol listesi aracılığı ile veri tabanı ve sistem kullanıcıları, rolleri ve bağlantı ayarları taranarak olası güvenlik açıklıkları önlenecektir.

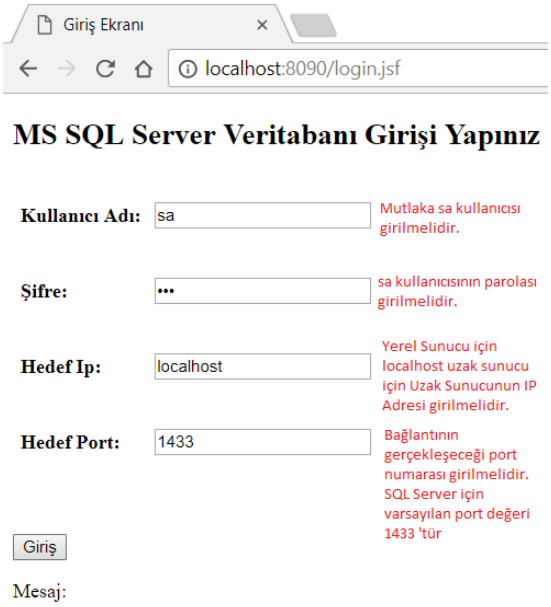
Tablo 3.1.'de geliştirilen uygulamanın MS SQL Server veri tabanı üzerinde otomatik olarak güvenlik açığı oluşturabilecek kullanıcıların ve rollerin tespit edilmesi ve bu açıklıkları yönetici izniyle otomatik olarak kapatılması işlemleri gösterilmiştir. Tabloda işaretlenmeyen hücreler ise arayüzü üzerinden yöneticinin ilgili programlara yönlendirilmesi amaçlanmıştır. Uzak sunucu testleri sanal makine üzerine kurulan MS SQL Server 2014 Enterprise sürümü üzerinde test edilmiştir. Otomatikleştirme niteliğinin amacı, sistem yöneticisinin SQL Server Management Studio arayüzünü kullanmadan sadece JSF üzerinde geliştirilen uygulama panelinden hazır olarak yapabilmesidir.

Tablo 3.1. MS SQL Server Güvenlik Açıklıklarının Tespiti ve Kapatılması İşlemleri

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A	x	x	x	x	x	x	x	x	x		x	x	x		x	x	x
B	x	x	x	x	x	x	x	x	x	x	x	x	x	x			x
C	x	x	x	x	x	x	x	x	x		x	x	x		x		
D	x	x	x	x	x	x	x	x	x	x	x	x					

A. Yerel Sunucu Üzerinde Zaafiyetlerin Tespit Edilmesi
B. Yerel Sunucu Üzerinde Zaafiyetlerin Kapatılması
C. Uzak Sunucu Üzerinde Zaafiyetlerin Tespit Edilmesi
D. Uzak Sunucu Üzerinde Zaafiyetlerin Kapatılması
1. System Administrator (SA) Kullanıcısının Şifre Uygunluğu
2. SA Kullanıcısının Varsayılan Kullanıcı Adı
3. SA Kullanıcısının Aktifliği
4. Boş Şifreye Sahip Olan Kullanıcılar
5. Kullanıcı Adı ve Şifresi Aynı Olan Kullanıcılar
6. Ortak Şifreye Sahip Kullanıcılar
7. Uzun Süredir Aktif Olarak Kullanılmayan Kullanıcılar
8. Builtin Hesaplar
9. Guest (konuk) Kullanıcılar
10. Uzak Bağlantıların Kullanımı
11. Kullanıcılara Verilen Yüksek Seviyeli Ayrıcalıklar
12. Public Role Ayrıcalıkları
13. Kimlik Doğrulama
14. Anonim Oturumlar
15. Bağlantı Protokolleri
16. Hizmetler
17. Güvenlik Yamaları

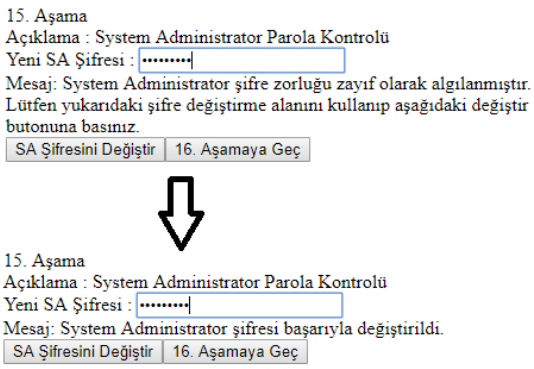
MS SQL Server üzerinde veri tabanı yönetim sistemleri güvenlik ilkelerinin taranabilmesi ve uygulanabilmesi için veri tabanı bağlantısının kurulması gerekmektedir. Şekil 3.1.'de görüldüğü üzere uygulamanın sistem üzerinde geniş yetkilere sahip olabilmesi için sistem yöneticisi bilgileri ile giriş yapılması gerekmektedir. Eğer varsayılan değer olan "sa" kullanıcı adı değiştirildiyse değiştirilen yeni isim kullanılmalıdır. Kimlik doğrulama modu mixed mode konumuna getirilmeli ve sistem yöneticisi aktif olarak tutulmalıdır.



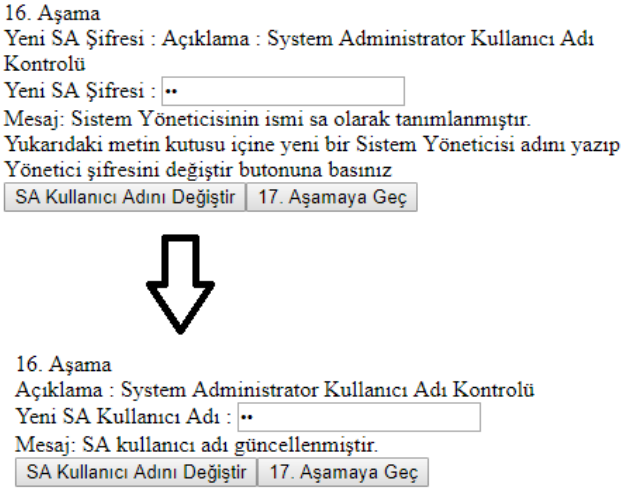
Şekil 3.1. MS SQL Server Veri Tabanı Bağlantısının Kurulması

Eğer yerel makine üzerinde liste kontrol edilecekse "Hedef IP" kısmına "localhost" değeri; eğer uzak sunucu üzerinde liste kontrol edilecekse "Hedef IP" kısmına hedef sunucunun IP adresi girilmelidir. Port numarası değiştirilmediyse varsayılan değer olan 1433 numaralı port numarası kullanılabilmektedir.

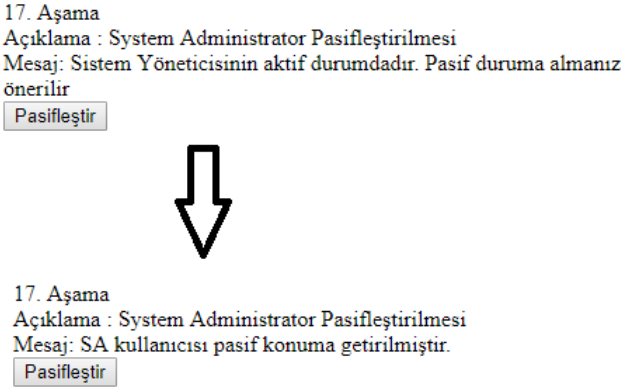
Uygulamanın geniş yetkilere sahip olabilmesi için giriş yaparken System Administrator (SA) kullanıcısının kimlik bilgileri kullanılmıştır. SA kullanıcısı SQL Server üzerinde en geniş yetki ve rollere sahip olduğu için saldırganların odak noktası durumundadır. Herhangi bir tahmin veya sözlük saldırısı durumunda sunucunun tüm kontrolü saldırgan tarafından ele geçirilmesi kaçınılmazdır [19]. Bu kullanıcının güvenliği için tarama işlemi bittikten sonra parolasının karmaşıklığı ve varsayılan kullanıcı adı olan "sa" adını kullanıp kullanmadığı kontrol edilmiştir [20]. Uygunluğu yeterli olmadığı durumda şekil 3.3., şekil 3.3. ve şekil 3.4.'te gösterildiği üzere panel üzerinde bulunan textbox ve buton yardımıyla yöneticinin kullanıcı adı ve şifresinin değiştirmesi önerilmiştir. Ayrıca SA kullanıcısının bir sonraki kullanımına kadar pasifleştirilmesi de teklif edilmiştir.



Şekil 3.2. SA Kullanıcısının Şifre Kontrol Aşaması

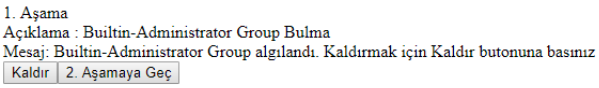


Şekil 3.3. SA Kullanıcı Adının Değiştirilmesi



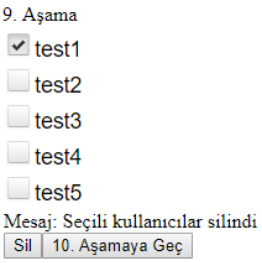
Şekil 3.4. SA Kullanıcısının Pasif Duruma Alınması

Builtin Administrator Grupları sunucu üzerinde açılmış yan yönetici hesap gruplarına verilen isimdir. Bu gruplar SQL Server kurulumundan sonra SA kullanıcı haklarınının çoğuna sahip olabilmektedirler [21]. Şekil 3.5.'te gösterildiği üzre geliştirilen uygulama önce bu grupların server üzerinde bulunup bulunmadığını tespit edip; eğer aktif bir gruba rastlarsa yöneticiye bir buton vasıtasıyla kaldırılma işlemini önermektedir.



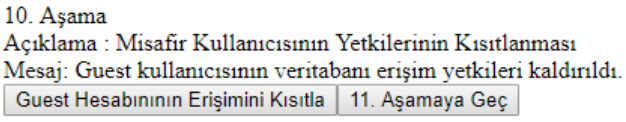
Şekil 3.5. Builtin Administrators Gruplarının Tespiti

Kullanılmayan ve sistemde açık bir şekilde bırakılan kullanıcılar da veri tabanı güvenliği açısından tehlike arz etmektedir. Bu kullanıcılar birçok farklı yetkiye sahip olabilmektedir. Ayrıca uzun süredir şifre değişikliklerine uğramadıkları için uzun süreli bir kaba kuvvet saldırısına olanak sağlamaktadırlar. SQL Server güvenlik ilkelerine göre bir kullanıcının en son kullanım süresi 42 günü geçtiği takdirde bu kullanıcıların şifre değişikliğine; kullanılmıyorsa da sistemden kaldırılması gerektiği ön görülmüştür [22]. Şekil 3.6.'da gösterildiği üzere uygulama, yöneticiye 42 gün boyunca aktif olmayan kullanıcıları multibox yardımıyla göstermektedir. Yönetici, bu kullanıcılardan istediklerini seçip kaldırma hakkına sahiptir.



Şekil 3.6. Son 42 Gün Aktif Olmayan Giriş Listesi

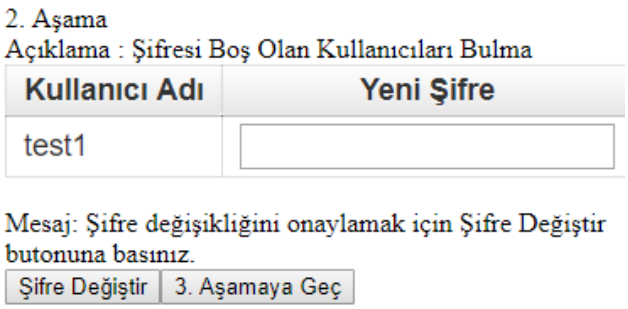
SQL Server üzerinde bir tabloyla işlem yaparken herhangi bir kullanıcının aktif olmadığı durumlarda otomatik olarak konuk kullanıcısı kullanılmaktadır. Tüm tablolarda varsayılan olarak oluşturulan bir kullanıcı olduğundan; herhangi bir yetki yükseltmesinde tüm tablolar üzerinde geniş haklara sahip olabilmektedir. Bu kullanıcı silinememektedir. Bu nedenle veri güvenlik kontrol ilkelerine göre konuk kullanıcısının veri tabanı tabloları üzerinden bağlanma yetkisi kaldırılmalıdır [23]. Şekil 3.7.'de gösterildiği üzere geliştirilen uygulamada konuk kullanıcısının üzerinde "connect" yetkisine sahip olan veritabanları bulunmuştur. Bu veri tabanlarından guest kullanıcısının bağlanma erişimininin kaldırılmasını bir buton aracılığıyla yöneticiye sunmuştur.



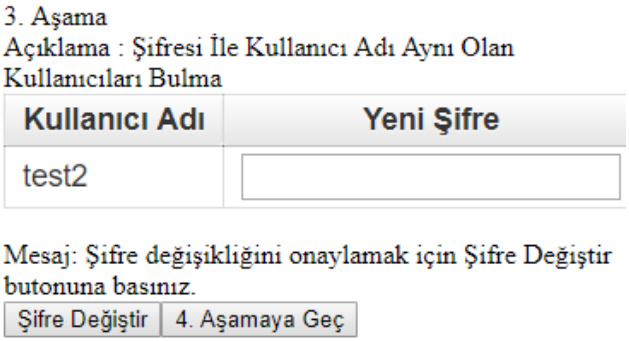
Şekil 3.7. Aktif Olan Konuk Hesabın Erişim Yetkilerinin Kaldırılması

Veri tabanı girişleri (login) üzerinde herhangi bir şifre güvenlik politikası windows ayarları üzerinden açılmadıysa; kullanıcıların istediği şekilde şifre girebilmelerine neden olmaktadır. Kullanıcılar istediği gibi şifre kısımını boş bırakabilmekte, kullanıcı adı ve şifresini birebir aynı girebilmekte veya farklı kullanıcılar aynı şifreleri kullanabilmektedir. Böyle bir güvenlik açığı ile saldırganların sisteme hiçbir çaba sarfetmeden ulaşabileceklerdir. SQL Server'ın PWDCOMPARE fonksiyonu yadımıyla uygulamada ilgili kullanıcılar tespit edilmiştir [24]. Şekil 3.8. , şekil 3.9. ve şekil 3.10. 'da görüldüğü üzere tespit edilen bu

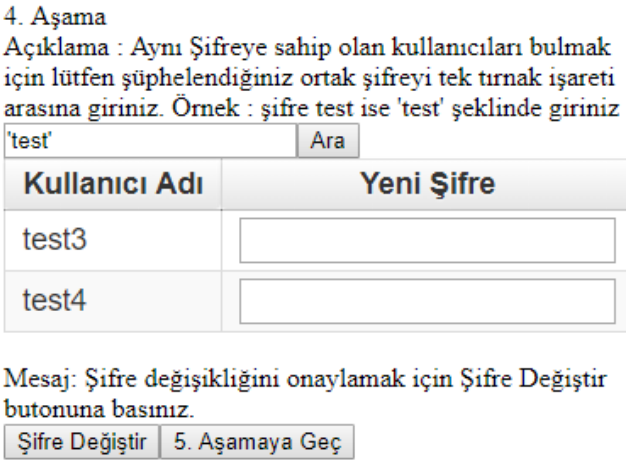
kullanıcıların şifrelerinin değiştirilmesi için password box ve buton yardımıyla yöneticiye sunulmuştur.



Şekil 3.8. Boş Şifreye Sahip Olan Kullanıcıların Tespiti



Şekil 3.9. Kullanıcı Adı ve Şifresi Aynı Olan Kullanıcıların Tespiti



Şekil 3.10. Ortak Şifreye Sahip Kullanıcıların Tespiti

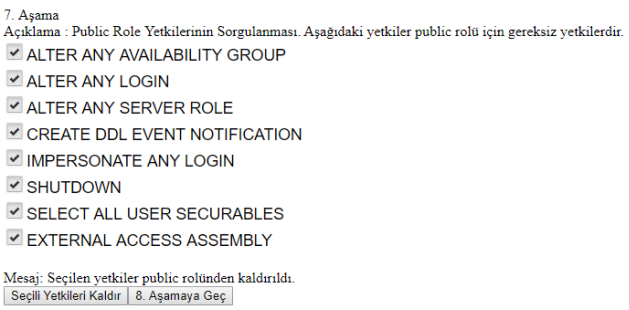
SQL Server'da her bir veritabanına özel çeşitli kullanıcılar oluşturulmaktadır. Bu kullanıcılar ilk oluşturulduklarında public role haklarına sahip olmaktadır. Bu kullanıcılar veri tabanındaki konumuna göre çeşitli haklara yükseltilebilmektedir. Gereksiz yere yükseltilen yetkiler saldırganlar için bir davet noktası oluşturacaktır. "db_owner" yetkisine yükseltilmiş bir kullanıcı veri tabanı üzerinde geniş bir yetkiye sahip olacaktır. Kullanıcı için oluşturulan şifre güvenlik ilkeleri sistem yöneticisinkine göre daha basit kalacağı için saldırganlar için kolay bir hedef olacaktır. Böylelikle saldırgan kolaylıkla "db_owner" yetkisine sahip olup kendi için daha güvenli bir giriş yetkisi açıp habersiz saldırılar gerçekleştirebilecektir. Sistem

yöneticilerinin tüm kullanıcıların yetkilerini gözden geçirip gereksiz yere yetkisi yükseltilen kullanıcıların yetkilerini kısıtlaması gerekmektedir [22]. Şekil 3.11.'de gösterildiği üzere geliştirilen uygulamada kullanıclar üzerinde "db_owner", "db_accessadmin", "db_backupoperator", "db_datareader", "db_datawriter", "db_ddladmin", "db_danydatareader", "db_danydatawriter" ve "db_securityadmin" rollerinin olup olmadığı tespit edilmiştir. Bu kullanıcılar yöneticiye sunularak istediği kullanıcıyı seçmesine olanak sağlanmıştır. Şekil 3.12.'de görüldüğü üzere seçili olan kullanıcı üzerindeki istenmeyen haklar checkbox yardımıyla seçilip silinebilmektedir.

Şekil 3.11. Üst Seviyeli Yetkilere Sahip Olan Kullanıcıların Gösterildiği DataGrid Sayfası

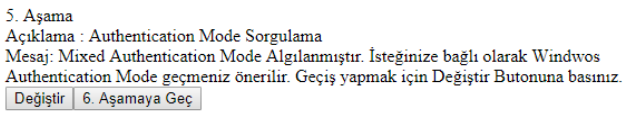
Şekil 3.12. Seçilen Kullanıcıya ait Yetkilerin Kaldırılması

SQL Server tüm veri tabanları üzerinde varsayılan olarak public rolü bulunmaktadır. Sonradan oluşturulan kullanıcılar, gruplar ve roller ilk olarak bu rol yekisine sahip olarak gelmektedir. Public rolü kaldırılamamaktadır. Bu yüzden public rolü yetkisi kesinlikle hiçbir yetkiye yükseltilmemelidir [22]. Aksi takdirde oluşturulan en basit bir kullanıcı bile, istenmeyen geniş yetkilere sahip olacaktır. Public rolü varsayılan olarak "Connect" ve "View Any Database" yetkilerine sahiptir. Şekil 3.13.'te gösterildiği üzere geliştirilen uygulamada bu roller dışında kalan roller tespit edilip, yöneticiden bu rollerin kaldırılması istenmiştir.



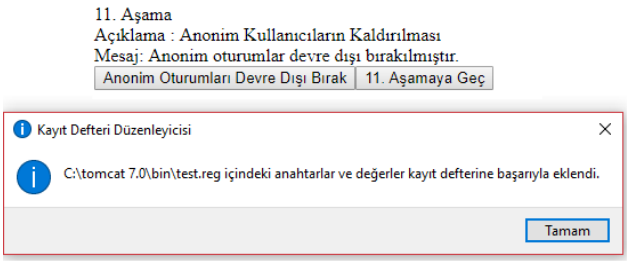
Şekil 3.13. Public Rolü İçin Gereksiz Yetkilerin Tespiti

SQL Server veri tabanı bağlantısı yapılırken kimlik doğrulamak için iki seçenek mevcuttur. Bunlardan ilki sunucunun kurulu olduğu windows kullanıcısı (Windows Authentication) ile yapılan girişi diğeri ise SQL Server için özel oluşturulan kullanıcılar ve windows kullanıcısının birlikte olduğu karışık moddur (Mixed Mode). SQL Server güvenliği için sadece windows kullanıcısının giriş yapıldığı "windows only mode" seçilmelidir."Windows only mode" seçimi "mixed mode" seçimine göre daha güvenlidir. Giriş bilgileri ağ üzerinden iletilmek zorunda değildir. Kullanıcı adları ve parolalarını veri dizileri ile aktarılmak zorunda kalınmaz. Tek windows güvenlik modeli ile çalışıldığından dolayı karışık moda göre güvenlik işlemleri daha kolay yürütülür [25]. Şekil 3.14.'te gösterildiği üzere uygulamada T-SQL yardımıyla kimlik doğrulama modeli tespit edilmiştir. "Mixed Mode" algılandığı takdirde yöneticiden bir buton aracılığıyla "Windows Only Mode" 'a çevirmesi istenmiştir. Değiştirilmesi için yeniden T-SQL kullanılarak kayıt defteri üzerindeki "N'HKEY_LOCAL_MACHINE\\N'Software\\Microsoft\\MSSQLServer\\MSSQLServer'N'LoginMode"'un dword değeri 1 olarak ayarlanmaktadır.



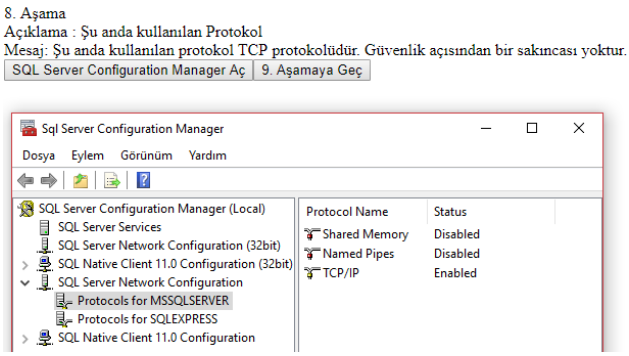
Şekil 3.14. SQL Server Kimlik Doğrulama Modunun Tespiti

Anonim erişim iki bilgisayar arasında kurulan kimliği doğrulanmamış ve anonim oturumlardır [26]. Anonim erişimi önlemek için boş oturumlar devre dışı bırakılmalıdır. Boş oturumlar devre dışı bırakılmadığı sürece bir saldırgan sunucuya anonim olarak bağlanabilir. Kimlik doğrulama gerekmediği için saldırganlar verilere çok rahat bir şekilde erişebilmektedir. Anonim oturumla birlikte; bilgi türü, etki alanı ve güven ayrıntıları, paylaşımlar, gruplar ve kullanıcı hakları da dâhil olmak üzere kullanıcı bilgileri, kayıt defteri anahtarları ve daha fazlasına ulaşılabilmektedir. Bu nedenle anonim oturumlar devre dışı bırakılmalıdır [22]. Şekil 3.15.' te gösterildiği üzere geliştirilen uygulamada bir adet reg uzantılı dosya oluşturulmuştur. Reg uzantılı dosya kayıt defteri içindeki HKEY_Local_Machine\SYSTEM\CurrentControlSet\ Control\Lsa dizini içerisindeki "restrictanonymous" 'un dword değerini 1 olarak değiştirecek şekilde ayarlanmıştır. Oluşturulan reg uzantılı dosya buton vasıtasıyla çalıştırılarak kayıt defterindeki ilgili değeri güncellemektedir. Bir sonraki aşamaya geçildiğinde oluşturulan reg uzantılı dosya otomatik olarak silinmektedir.



Şekil 3.15. Anonim Oturumların Devre Dışı Bırakılması

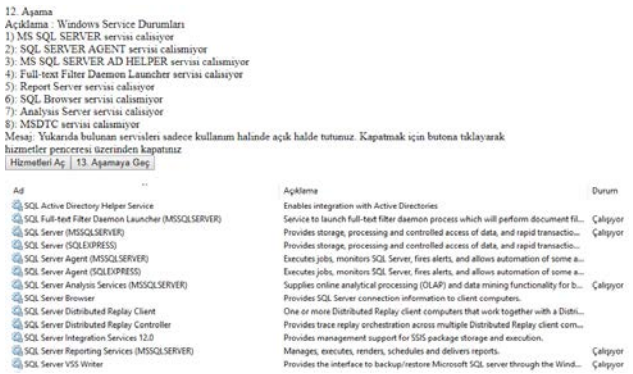
MS SQL Server üzerinde bağlantılar için kullanabilen dört adet protokol mevcuttur. Bunlar Named Pipes, TCP/IP, Shared Memory ve VIA'dır. Birden fazla ağ protokolünü kullanmak hem ağ trafiğini yoğunlaştıracak hem de saldırganlar tarafından istismara uğramasını kolaylaştıracaktır. Varolan protokollerden sadece TCP/IP protokolü kullanılmalıdır. Gerekmedikçe diğer protokoller devre dışı bırakılmalıdır [27]. Şekil 3.16.'da gösterildiği üzere geliştirilen uygulamada T-SQL yardımıyla hangi protokolün kullanıldığı öğrenilmiştir. TCP/IP dışında bir protokol algılandığında yöneticiye SQL Server Configuration Manager Programına yönlendirme işlemi yapmıştır.



Şekil 3.16. SQL Server Network Protokol Tespiti

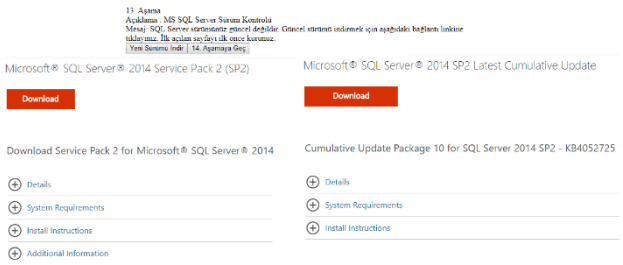
Veri tabanı güvenliğini sağlamak için kullanılmayan veri tabanı servisleri ve veri tabanı ile iletişim halinde olan diğer kullanılmayan servislerin kapatılması gerekmektedir. MSSQLSERVER servisi SQL Server veri tabanı motorudur ve veri tabanının çalışması için zorunludur. Ne kadar örnek veri tabanı sunucusu varsa bu servisten o kadar sayıda üretilir. Kullanılmayan örnek veri tabanı sunucularına ait bu servisler kapatılmalıdır. SQLSERVERAGENT servisi ile çeşitli veri tabanı komutları önceden zamanlanabilir ve olası hata durumlarını operatörlere bildirebilir. Bu servis sayısı da örnek veritabanı sunucu sayısı ile aynı olup kullanılmayanları kapatılmalıdır. MSSQLServerADHelper servisi veri tabanı örnek kaydını yapar ve aktif dizin uyumlarını gerçekleştirir. MSSQLFDLauncher servisi tam metin arama özelliğini sağlar. Bir sorgu sonucunda istenilen sonuç tam olarak bulunamadığı durumlarda istenilen sonuca en yakın verileri getirir. SQL Service Reporting Services hizmeti tüm veri manipülasyonlarını hakkında rapor hazırlar. Browser Servisi, SQL Server eğer dinamik port kullanıyorlarsa suncuya bağlanmaya çalışan kullanıcılara hangi portu kullanması gerektiği konusunda bilgi verir. Analysis Service veri üzerindeki istatistik sonuçların elde edilmesini sağlar. Açıklanan bu servisler kullanılmadığı zamanlarda kapalı olarak tutulmalıdır. Bunlardan bağımsız olarak MicrosoftDTC (MSDTC) servisi birden çok sunucu arasındaki işlemleri yönetmek için kullanılır [28]. Bu servis de kullanılmıyorsa devre dışı bırakılmalıdır. Şekil 3.17.'da gösterildiği üzere geliştirilen uygulamada bahsi geçen servisler

cmd komutları yardımıyla tespit edilmiştir. Tespit edilen hizmetlerden istenilenin kapatması için, yönetici hizmetler penceresine yönlendirilmiştir.



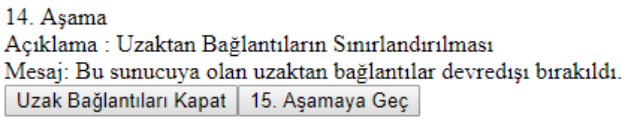
Şekil 3.17. Kullanılmayan Hizmetlerin Kapatılması

MS SQL Server için düzenli bir şekilde güvenlik yaması Microsoft tarafından yayımlanmaktadır [29]. Bu yamalarla birlikte SQL Server üzerinde var olan zero day açıklıkları kapatılmaktadır. Saldırganlar tarafından da kontrol edilen bu güvenlik yamaları eski sürümlerdeki güvenlik açıklıklarını rahat bir şekilde bulmalarını sağlamaktadır. Zamanında yapılmayan güvenlik yamalarının saldırganlar tarafından bilinen güvenik açıklarının istismarına neden olacağı yadsınamaz bir gerçektir. Güvenlik yaması yapılmadan önce bir test sunucusuna uygulanmalı, sistemde herhangi bir sorun oluşmadıysa gerçek sunucu üzerine uygulanmalıdır. Geliştirilen uygulamada SQL Server dizini içerisindeki ERRORLOG metin belgesi okutularak ilk satırında yer alan sürüm bilgileri kayıt altına alınmıştır. Bu satırda var olan sürüm ve yıl bilgileri birbirinden ayrılmıştır. JSOUP kütüphanesi kullanılarak https://sqlserverupdates.com adresinden ilgili yıl bilgisine göre sürüm bilgileri çekilmiştir. Metin belgesi içindeki sürüm numarası ile sitedeki sürüm numarası karşılaştırılmıştır. Şekil 3.18.'de görüldüğü üzere eğer sistem üzerindeki SQL Server sürüm numarasının daha küçük olduğu tespit edilirse yönetici, ilgili yıla ait iki adet yamaya yönlendirilmiştir.



Şekil 3.18. SQL Server Sürümlerinin Kıyaslanması ve Yöneticinin İlgili Linklere Yönlendirilmesi

SQL Server'a yerel olmayan ağ üzerinden yapılan bağlantılar güvenlik ilkeri açısından tehlikelidir. Eğer bu bağlantılar kullanılmıyorsa kesinlikle kapatılması gereklidir [30]. Şekil 3.19.'da gösterildiği üzere yönetici tarafından "Uzak Bağlantıları Kapat" butonu yardımıyla SQL Server üzerinde remoteaccess değeri "0" yapılarak uzaktan bağlantılar kapatılmıştır.



Şekil 3.19. SQL Server Uzaktan Bağlantıların Kapatılması ((Disabling SQL Server Remote Connections)

4. Oracle Veri Tabanı İçin Güvenlik Doğrulama Listesinin Tanımlanması Ve Uygulanması

Tablo 4.1.'de geliştirilen uygulamanın Oracle veri tabanı üzerinde otomatik olarak güvenlik açığı oluşturabilecek kullanıcıların ve rollerin tespit edilmesi ve bu açıklıkları yönetici izniyle otomatik olarak kapatılması işlemleri gösterilmiştir. Uzak sunucu testleri sanal makine üzerine kurulan Oracle 12c 1.0.2 sürümü üzerinde test edilmiştir. Otomatikleştirme niteliğinin amacı, sistem yöneticisinin SQL Developer arayüzünü kullanmadan sadece JSF üzerinde geliştirilen uygulama panelinden hazır olarak yapabilmesidir.

Tablo 4.1. Oracle Veri Tabanı Güvenlik Açıklıklarının Tespiti ve Kapatılması İşlemleri

	1	2	3	4	5	6	7	8	9	10
A	x	x	x	x	x	x	x	x	x	x
B	x	x	x	x	x	x	x	x	x	x
C	x	x	x	x	x	x	x	x	x	x
D	x	x	x	x	x	x	x	x	x	x

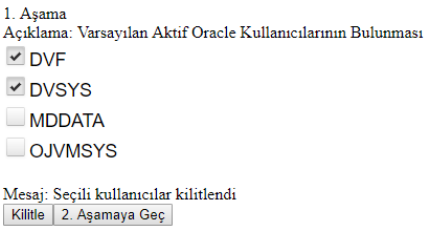
A. Yerel Sunucu Üzerinde Zaafiyetlerin Tespit Edilmesi
B. Yerel Sunucu Üzerinde Zaafiyetlerin Kapatılması
C. Uzak Sunucu Üzerinde Zaafiyetlerin Tespit Edilmesi
D. Uzak Sunucu Üzerinde Zaafiyetlerin Kapatılması
1. Varsayılan Kullanıcıların Aktifliği
2. Varsayılan Kullanıcıların Şifreleri
3. Veri Sözlüğü Değeri
4. EM_EXPRESS_ALL Yetkisi
5. Kullanıcılara Verilen Yüksek Seviyeli Ayrıcalıklar
6. Public Role Ayrıcalıkları
7. Remote_Os_Authent Değeri
8. Şifre Doğrulama Fonksiyonları
9. Varsayılan Profil Özellikleri
10. Güvenlik Yamaları

Oracle üzerinde veri tabanı yönetim sistemleri güvenlik ilkelerinin taranabilmesi ve uygulanabilmesi için veri tabanı bağlantısının kurulması gerekmektedir. Şekil 4.1.'de görüldüğü üzere uygulamanın sistem üzerinde geniş yetkilere sahip olabilmesi için sistem yöneticisi bilgileri ile giriş yapılması gerekmektedir. Eğer "sys as sysdba" kullanıcı adı kilitli konumdaysa geçici süreliğine aktif konuma getirilmelidir.

Şekil 4.1. Oracle Veri Tabanı Bağlantısının Kurulması

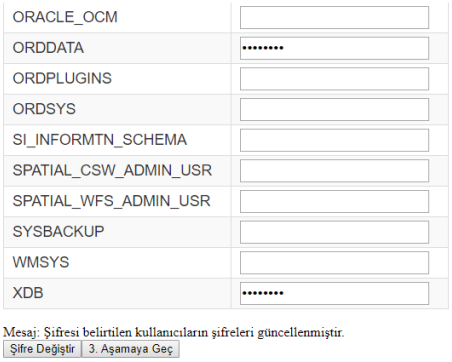
Eğer yerel makine üzerinde liste kontrol edilecekse "Hedef IP" kısmına "localhost" değeri; eğer uzak sunucu üzerinde liste kontrol edilecekse "Hedef IP" kısmına hedef sunucunun IP adresi girilmelidir. Port numarası değiştirilmediyse varsayılan değer olan 1521 numaralı port numarası kullanılabilmektedir.

Oracle veri tabanı kurulum sırasında yirmiyi aşkın varsayılan kullanıcı oluşturur [31]. Kurulum uygun bir şekilde gerçekleştirilirse Database Configuration Asistant ile tüm varsayılan kullanıcılar kilitlenip pasif konuma getirilmektedir. Ancak kurulum aşamasında Database Configuration Asistan kullanılmayıp, gerekli ayarlamalar manuel yolla yapılırsa varsayılan kullanıcılar serbest ve aktif bir şekilde veri tabanı üzerinde işlem gerçekleştirebilmektedirler. Ayrıca, veri tabanı eski sürümden yeni bir sürüme güncellendiği zaman bazı varsayılan kullanıcıların kilitleri açılabilmektedir. Bu kullanıcılar kolay bir şekilde istismara uğrayarak, saldırganların veri tabanı erişimini kolaylaştırmaktadır. Bu kullanıcıların aktif olanları tespit edilip; bunların kilitlenip devre dışı konumuna getirilmesi gerekmektedir [32]. İlk kurulumdan sonra, veri tabanı eklentilerinin ve bileşenlerinin kurulması da ekstra varsayılan kullanıcıları beraberinde getirmektedir. Database Configuration Asistant kullanıldığında tekrardan bu kullanıcılar otomatik olarak kilitlenmektedir. Bu kullanıcılar sadece gerektiği takdirde aktif hale getirilmeli ve güçlü parolalar atanmalıdır. Tüm veri tabanları SYS, SYSTEM, DBSNMP ve SYSMAN yönetim hesaplarını içerir [33]. Oracle veri tabanı tarafından sağlanan idari hesaplar sadece yetkili kişiler tarafından kullanılmalıdır. Bu hesapları yetkisiz erişime karşı korumak için, kullanılmadıkları takdirde kilit altına alınmalıdır. Şekil 4.2.'de gösterildiği üzere geliştirilen uygulamada PL\SQL kullanılarak kilitli olmayan varsayılan kullanıcılar bulunmuştur. Yöneticinin bu kullanıcılardan istediklerini işaretleyip kitleme işlemi yapabilmesi sağlanmıştır.



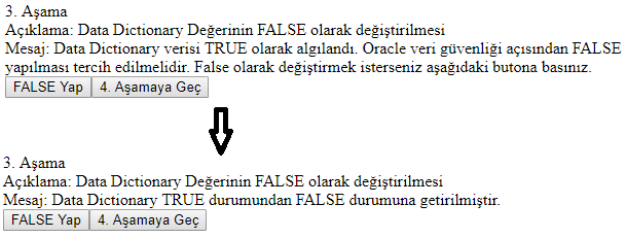
Şekil 4.2. Oracle Veri Tabanında Varsayılan Kullanıcıların Kilitlenmesi

Varsayılan kullanıcılar kullanılmak istenirse şifrelerinin değiştirilmesi gerekmektedir. İnternet üzerinde basit bir arama ile bu varsayılan kullanıcıların şifreleri saldırganlar tarafından öğrenilebilir [34]. Şekil 4.3.'te gösterildiği üzere geliştirilen uygulamada her bir varsayılan kullanıcı için şifre alanı oluşturulmuştur. Veri tabanı yöneticisinin, şifresini değiştirmek istediği kullanıcıların şifresini girip "Şifre Değiştir" butonuna basmasıyla birlikte ilgili kullanıcıların şifreleri değiştirilmiş olur. Diğer kullanıcıların şifrelerinde herhangi bir değer girilmeyerek, boş şifre kontrolü sayesinde herhangi bir değişiklik yapılmaması sağlanmıştır.



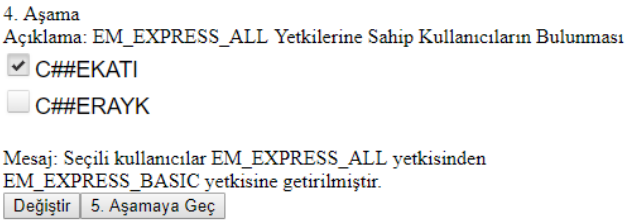
Şekil 4.3. Varsayılan Kullanıcıların Şifrelerinin Değiştirilmesi

Oracle veri tabanın en önemli bölümlerinden biri olan data dictionary (veri sözlüğü), veri tabanı hakkında genel bilgilere sahip tablolardan oluşan olan salt okunur veri yapısıdır. Data dictionary tüm veritabanındaki şema tanımlamalarını, şema nesnelerine ne kadar yer ayrıldığı, sütunlar için varsayılan değerleri, oracle kullanıcı isimleri, her kullanıcı için yükseltilmiş hak ve rolleri, denetim bilgileri gibi verileri saklamaktadır. Oracle; herhangi bir sistem ayrıcalığına sahip olan kullanıcıların, data dictionary veri tablosu üzerinde bu hakları kullanma yetkisi olabildiğinden data dictionary tablosunun korunmasını önermektedir [35]. Data dictionary tablolarındaki verilerin değişimi veya manipüle edilmesi, veri tabanını üzerinde kalıcı hasarlara sebep olabilmektedir. Data dictionary güvenliğini sağlayabilmek için "07_DICTIONARY_ACCESSIBILTY" değeri "FALSE" olarak ayarlanmalıdır. Bu değer ayarlandıktan sonra sadece veri tabanı yöneticileri ve "Select Any Dictionary" yetkisine sahip kullanıcılar data dictionary'e ulaşabileceklerdir. Eğer bu değer "FALSE" olarak ayarlanmazsa, "Drop Any Table" yetkisine sahip kullanıcıların Data Dictionary tablosu üzerindeki verileri silme imkânı oluşmaktadır. Şekil 4.4.'te gsöterildiği üzere geliştirilen uygulamada Data Dictionary değeri tespit edilmiştir. Tespiti ardından elde edilen değer "TRUE" ise "FALSE" yapılması gerektiği uygulama tarafından önerilmiştir. Yönetici tarafından "FALSE Yap" butonu basıldıktan sonra veri tabanı üzerinde "07_DICTIONARY_ACCESSIBILTY" değeri "FALSE" olarak ayarlanmıştır.



Şekil 4.4. Data Dictionary Değerinin False Olarak Ayarlanması

Enterprise Manager (EM), web arayüzü vasıtasıyla oracle veri tabanlarının, kullanıcıların ve rollerin ayarlandığı, sistem izleme özelliği ile sorunların algılanmasını ve bildirilmesini sağlayan bir yazılımdır [36]. Veri tabanı kullanıcılarının EM arayüzüne ulaşması için "EM_EXPRESS_BASIC" ya da "EM_EXPRESS_ALL" yetkilerinden birine sahip olması gerekmektedir. "EM_EXPRESS_BASIC" yetkisi kullanıcılara sadece okuma yetkisinin verildiği yetkidir. "EM_EXPRESS_ALL" yetkisi hem okuma hem de yazma imkânlarını kullanıcılara vermektedir. Sadece okuma yetkisine sahip olması gereken kullanıcılar için "EM_EXPRESS_BASIC" yetkisinin verilmesi yeterlidir. Şekil 4.5.'te gösterildiği üzere geliştirilen uygulamada EM_EXPRESS_ALL yetkisine sahip olan yönetici ve kilitli durumda olan kullanıcılar dışında kalan kullanıcılar tespit edilmiştir. Tespit edilen kullanıcılar veri tabanı yöneticisine sunulmuştur. Yönetici istediği kullanıcıları seçip "Değiştir" butonuna basarak seçili kullanıcıların "EM_EXPRESS_ALL" yetkilerini "EM_EXPRESS_BASIC" yekisine dönüştürebilmektedir.



Şekil 4.5. Seçili Kullanıcıların EM Yetkilerinin ALL Konumundan BASIC Konuma Değiştirilmesi

Veri tabanı kullanıcılarına veya rollerine gerektiğinden fazla yetki verilmesinden kaçınılmalıdır. Kullanıcılara yalnızca etkin şekilde işlerini yapabilecek seviyede gerekli ayrıcalıklar verilmelidir.
En az ayrıcalık ilkesini gerçekleştirmek için;

- SYSTEM ve OBJECT yetkilerine yükseltilmiş olan veri tabanı kullanıcı sayısı,
- SYS yetkisiyle veri tabanı bağlantısı yapan kullanıcıların sayısı,
- İçinde "ANY" kelimesi geçen yetkilere sahip kullanıcıların sayısı,
- Veri tabanı nesneleri oluşturma, değiştirme ve silme yetkisine sahip kullanıcıların sayısı kısıtlanmalıdır.

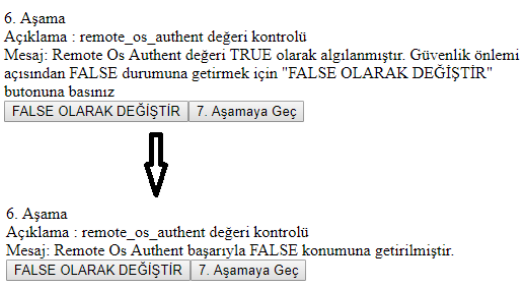
Ayrıca "CREATE ANY JOB", "BECOME USER", "EXP_FULL_DATABASE", "IMP_FULL_DATABASE", "CREATE LIBRARY", "CREATE ANY LİBRARY", "ALTER ANY LİBRARY", "EXECUTE ANY LIBRARY", "CREATE PUBLIC SYNONYM" VE "DROP PUBLİC SYNONYM" yetkilerine sahip kullanıcıları gözeden geçirilmeldir [33]. Şekil 4.6.'da gösterildiği üzere geliştirilen uygulamada dba ve pasif kullanıcılar dışında kalan ve önemli haklara sahip olan kullanıcılar JSF'te bulunan datagrid

aracılığı ile listelenmiştir. Şekil 4.7.'de gösterildiği üzere görüntülenmesi istenilen kullanıcıların altındaki büyüteç işaretine basıldığında ilgili kullanıcıya ait haklar yöneticiye gösterilmiştir. Yönetici tarafından kapatılması istenilen haklar seçilerek "Kaldır" butonuna basıldığı zaman bu haklar ilgili kullanıcıdan kaldırılmıştır.

Şekil 4.6. Yüksek Yetkilere Sahip Olan Kullanıcıların Listelenmesi

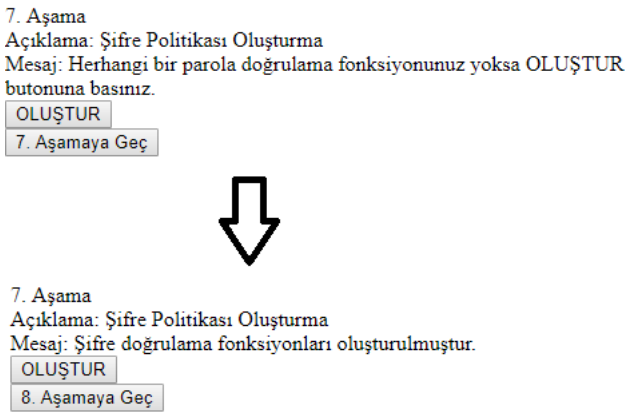
Şekil 4.7. Seçilen Yetkilerin İlgili Kullanıcı Üzerinden Kaldırılması

Varsayılan olarak Oracle veri tabanı, işletim sistemi kimliği ile bağlanma özelliğini sadece güvenli bağlantılarda kabul etmektedir. Böylelikle, uzak istemciden bağlanan bir kullanıcının, bağlandığı sunucu üzerinde kendi işletim sistemi üzerindeki kullanıcı kimlik bilgilerini kullanmasını engeller. "REMOTE_OS_AUTHENT" parametresi varsayılan olarak "FALSE" değerine ayarlıdır. Bu parametreyi "TRUE" olarak ayarlamak, istemci üzerindeki işletim sistemi kullanıcı kimlik bilgilerinin kabul edilmesini sağlamakta ve hesap erişimi için sunucuyu zorlamaktadır. Kişisel bilgisayar gibi istemcilerin işletim sistemi kimlik kontrolü çok güvenli olmadığı için bu özelliğin TRUE olarak kullanılması önerilmemektedir [37]. Bu özelliği "FALSE" olarak ayarlamak kullanıcıların uzak bağlantı yapamayacağı anlamına gelmez. Başka bir deyişle, istemci makinenin işletim sistemi kimliğine güvenmeden, standart kimlik doğrulama sürecini uzak bağlantılar üzerinde uygular. Şekil 4.8.'de gösterildiği üzere geliştirilen uygulamada remote_os_authent değeri tespit PL/SQL yardımıyla tespit edilmiştir. Eğer bu değer "TRUE" olarak algılanmışsa uygulama bu değerin "FALSE" olarak değiştirilmesini yöneticiden istemektedir. Yönetici, "FALSE Olarak Değiştir" butonuna basarak ilgili değeri "FALSE" olarak değiştirmiş olur.



Şekil 4.8. "Remote_os_authent" Değerinin FALSE Olarak Değiştirilmesi

Oracle veri tabanı kullanıcıları için şifre doğrulama fonksiyonları oluşturulmalıdır. Önemli sistem yetkilerine sahip olmayan kullanıcıların şifreleri en az sekiz alfanumerik karakter, en az bir küçük harf ve bir büyük harf; DBA gibi sistem yetkilerine sahip olan kullanıcıların şifreleri en az 8 alfanumerik karakter, en az bir küçük harf, bir büyük harf, bir rakam ve bir sembolden oluşmalıdır [38]. Şifre içerikleri tahmin edilebilir basit kelimelerden oluşmamalıdır. Boş bırakılmamalıdır. Kullanıcı adıyla aynı olmamalıdır. Ayrıca en az 3 farklı harf içeriğine sahip olmalıdır. Şekil 4.9.'da gösterildiği üzre şifre doğrulama fonksiyonlarının Oracle veri tabanı üzerinde oluşması için yöneticiden "Oluştur" butonuna basması istenmiştir. Böylelikle bahsi geçen normal ve strong güçlü doğrulama fonksiyonları Oracle fonksiyon dizinine yazılmıştır.



Şekil 4.9. Şifre Doğrulama Fonksiyonlarının Oluşturulması

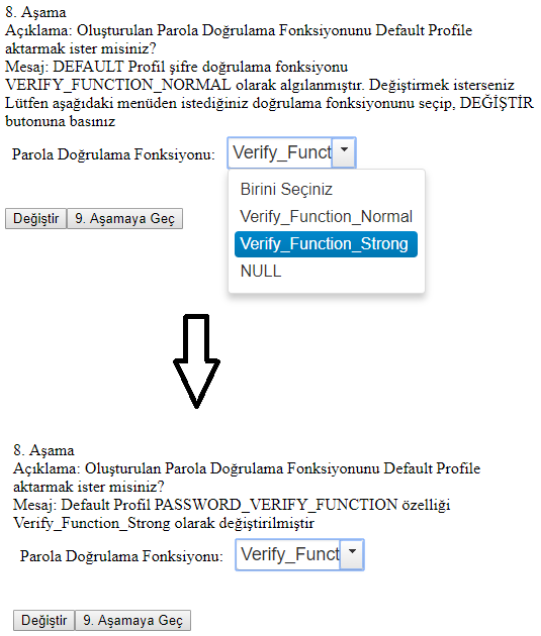
Oracle veri tabanı profili, veri tabanı kullanıcılarının güvenliği için oluşturulan ve kullanıcılara eklenen bir özelliktir. Profil ile kullanıcıların bağlantı süreci ve şifre politikaları ayarlanmaktadır. Yönetici tarafından herhangi bir profil oluşturulmadığı zaman, sistem otomatik olarak varsayılan profil ayarlarını kullanıcılara eklemektedir. Varsayılan profil ayarları, güvenlik kontrolü için yeterli olmadığı için önerilmemektedir. Ancak varsayılan profil ayarlarına karmaşık şifre kontrolü sağlayan bir fonksiyon eklenirse kullanımında herhangi bir sorun teşkil etmeyecektir. Ayrıca DBA gibi sistem yöneticiliği hakkına sahip olan kullanıcılar için varsayılan profil yerine daha karmaşık şifre kontrolü uygulayan bir profil oluşturulmalıdır.

Oluşturulan bir profilde aşağıda gösterilen şifre parametrelerine dikkat edilmelidir.[39]

- Failed_Login_Attempts, belirtilen sayı kadar üst üste girilen yanlış şifre sonucunda kullanıcıyı kilitler. Bu sayı üç olarak belirlenmelidir.
- Password_Life_Time, belirtilen gün kadar zaman geçtikten sonra kullanıcıdan yeni bir şifre girmesini ister. Bu sayı otuz olarak belirlenmelidir.
- Password_Reuse_Time (prt), daha önce atanan bir şifrenin kaç gün sonra yeniden kullanılabileceğini bildirir. Bu sayı 180 olarak belirlenmelidir.
- Password_Reuse_Max (prm), daha önce atanan bir şifrenin belirtilen sayı kadar şifre değişikliği sonrasında yeniden kullanabileceğini bildirir. Bu sayı altı olarak belirlenmelidir.
- Password_Lock_Time, kilitli olan bir hesabın belirtilen dakikadan sonra yeniden aktif hale gelmesini sağlar. 1/1440 değeri girilerek bu süre bir dakika olarak belirlenmelidir.

- Password_Grace_Time, şifre değiştirme süresi dolan kullanıcılar için belirtilen gün kadar daha sisteme giriş yapmasına izin verir ve şifre değiştirilmesi konusunda uyarı verir. Bu sayı 5 olarak belirlenmelidir.
- Password_Verify_Function, kullanıcının hangi şifre doğrulama fonksiyonunu kullanacağını belirtir. Eğer daha öncesinde yönetici tarafından karmaşık şifre doğrulama fonksiyonu oluşturulmuşsa bu fonksiyon atanmalıdır.

Eğer eski şifrelerin bir daha kullanılması istenmiyorsa, prm ya da prt parametrelerinden sadece bir tanesine unlimited değeri verilmelidir. Eğer iki parametreye birden unlimited değeri verilirse eski şifreler sürekli kullanıma açık olup, güvenlik zaafiyetine sebep olacaktır. Şekil 4.10.'da gösterildiği üzere geliştirilen uygulamada Default Profilin hangi şifre doğrulama fonksiyonunu kullandığı tespit edilmiştir. Eğer kullandığı doğrulama fonksiyonu varsayılan bir fonksiyon ise uygulama bu fonksiyonun değiştirilmesini önerir. Eğer daha önceden oluşturulan bir doğrulama fonksiyonu var ise menu üzerinden yönetici tarafından seçilerek değiştirme işlemi gerçekleştirilir.

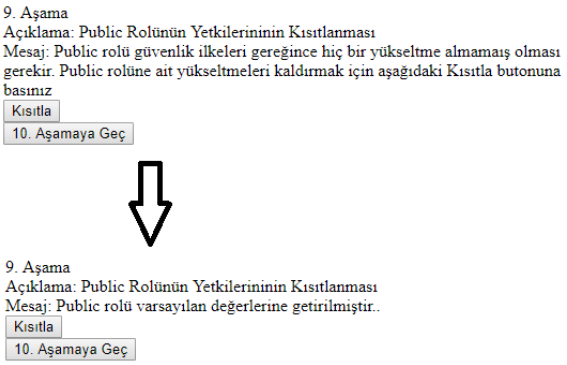


Şekil 4.10. Default Profilin Şifre Doğrulama Fonksiyonunun Değiştirlmesi

Oracle veri tabanı üzerinde yeni bir kullanıcı oluşturulduğunda, bu kullanıcıya sistem tarafından otomatik olarak public rolü atanır. Public rolü varsayılan bir roldür ve silinemez. Tüm kullanıcılarda bulunduğu için kesinlikle yetki yükseltmesi yapılmamalıdır. Oracle kurulumunda varsayılan olarak public rolüne bazı haklar tanınmaktadır. Bu haklardan bir kaçı güvenlik açısından kısıtlanmalıdır. Bu haklar aşağıda tanımlanmıştır. [13]

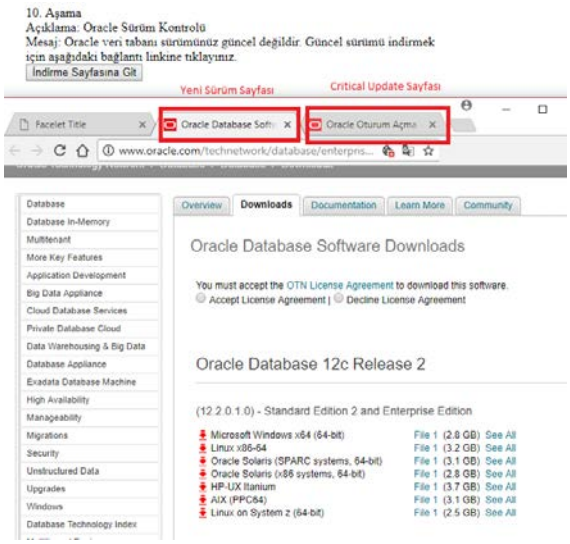
- DBMS_EXPORT_EXTENSION, veri tabanınında export dosyalarının oluşumunu sağlar.
- UTL_FILE, işletim sistemindeki dosyaları okuma ve yazma işlemi için kullanılır.
- UTL_SMTP, veri tabanı sunucusu aracılığıyla e-posta gönderme hizmeti verir.
- UTL_TCP, TCP/IP tabanlı ağ servisleri ile haberleşmek için kullanılır.
- UTL_HTTP, web sunucularla iletişim kurmak için HTTP (Hypertext Tranfer Protocol) çağrılarını yapar.

Şekil 4.11.'de gösterildiği üzere geliştirilen uygulamada "Public Rolünü Kısıtla" butonu vasıtasıyla bu rol üzerinden "DBMS_EXPORT_EXTENSION", "UTL_FILE", "UTL_SMTP", "UTL_HTTP" ve "UTL_TCP" yetkileri kaldırılmıştır.



Şekil 4.11. Public Rolünün Kısıtlanması

Oracle şirketi her yıl ocak, nisan, temmuz ve ekim aylarında olmak üzere düzenli olarak yılda dört kez güvenlik yaması yayımlamaktadır [40]. Yayımlanan her güvenlik yaması bir önceki yamayı da kapsadığı için sadece en son çıkan yamanın kurulması yeterlidir. Oracle tarafından yayımlanan güvenlik yamalarını kontrol etmek için Oracle Technology Network sayfası düzenli olarak kontrol edilmelidir. Ayrıca şu anki veya gelecekte gelecek olan yama ve güncellemeler; Oracle Dünya Destek Hizmetleri sistesi olan Metalink [40] üzerinden kontrol edilmelidir. Güvenlik yaması yapılmadan önce bir test sunucusu üzerinde uygulanmalı, sistemde herhangi bir sorun oluşmadıysa gerçek sunucu üzerine uygulanmalıdır. Geliştirilen uygulamada Oracle veri tabanının sürüm numarası tespit edilmiştir. JSOUP kütüphanesi kullanılarak ilk olarak Oracle'a ait "Critical Patch Updates"[41] adresinden son yamaya ait adres sayfası verisi çekilmiştir. Yeniden JSOUP kütüphanesi kullanılarak son yamaları içeren web sitesi üzerinden veri tabanı sürüm bilgileri çekilmiştir. Şekil 4.12.'de gösterildiği üzere elde edilen 2 sürüm numarası kıyaslanmıştır. Mevcut makinedeki oracle veri tabanı sürüm numarası daha küçük çıkarsa, yöneticinin indirmesi gereken yeni sürümü ve yamayı veri tabanı yöneticisine bildirecektir.



Şekil 4.12. Oracle Veri Tabanı Sürümlerinin Kıyaslanması ve Yöneticinin İlgili Linklere Yönlendirilmesi

5. Sonuç

Sonuç olarak güvenlik kontrol ilkeleri bir veri tabanı yönetim sisteminin (VTYS) güvenlik temelini oluşturmaktadır. Güvenlik kontrol ilkelerinin, veri tabanı yönetim sisteminin kurulumundan itibaren başlayıp yeni tablolar, kullanıcılar, roller ve bağlantılar eklendikçe takip edilmesi gerekmektedir.

Firmalar kendi içinde kullanacakları veri tabanı yönetim sistemlerini güvenlik açığı oluşturmadan kullanmak istedikleri zaman uzman bir veri tabanı yöneticisi ve çok sayıda test görevlilerini kadrolarına katmalıdırlar.

Bir VTYS'nin dikkat edilmesi gereken en önemli güvenlik ilkesi kullanıcılara verilen yetkilerin ve rollerin takip edilmesidir. Yetki ve rol kavramı veri tabanının kullanım ömrü boyunca sürekli olarak kontrol edilmeldir. Gereksiz yere yönetici yetkisi alan kullanıcıların yanlışlıkla ilgili olmadığı tablo yapılarına erişip, verileri bozma olasılığı vardır. Başka bir açıdan bakıldığında, yönetici yetkisine sahip olan bir kullanıcı kendine benzer birçok yönetici hesabı oluşturabilmektedir. Bu durum saldırganlar için davet noktası oluşturmaktadır. Public rolü tüm kullanıcıların sahip olduğu varsayılan roldür. Bu nedenle public rollerin yetkileri hiçbir şekilde yükseltilmemelidir.

VTYS geliştiren şirketlerinin çıkarmış olduğu güvenlik yamaları vakit kaybedilmeden uygulanmalıdır. Güvenlik yamaları VTYS şirketlerinin kendi web siteleri üzerinden takip edilmelidir. Gerekmeyen veri tabanı özellikleri aktif edilmemelidir.
Saldırganların hedef sunucuya ulaşmaları için, hedef sunucunun ip ve saldırılacak olan uygulamanın hangi port numarası ile çalıştığını bilmesi gerekmektedir. Bu nedenle ilgili vtys uygulamasının varsayılan port numarası kurulumdan hemen sonra değiştirilmelidir.

Bu çalışma ile geliştirilen uygulama sayesinde, veri tabanı yöneticisine sorgulama dili kullandırmadan MS SQL Server ve Oracle veri tabanları üzerinde birçok güvenlik ilkesini gerçekleştirme olanağı sağlanmaktadır. Önceki çalışmalar incelendiğinde sadece veri tabanı yönetim sistemlerinin veri güvenlik ilkelerinin bulunduğu; ancak yöneticiye kolaylık sağlayacak herhangi bir uygulamanın geliştirilmediği görülmüştür.

Geliştirilen uygulamada Oracle ve Microsoft'un oluşturduğu güvenlik ilkeleri takip edilmiştir. Ancak veri tabanı yönetim sistemi kullanan firmalar bu ilkeler haricinde kendilerine özel ilkeler tanımlamak isterlerse; bu ilkeler uygulamaya eklenti olarak eklenmesi sonraki aşamalarda düşünülmektedir.

Kaynakça

[1]İnternet: Online İstatistik, Veri Nedir? Veri ve Bilgi İlişkisi Nasıl Açıklanabilir?, https://www.onlineistatistik.com/single-post/2016/12 /03/veri-nedir-veri-bilgi-iliskisi-nasil-aciklanabilir

[2] Özdemir, S., Selçuk, A., Kilitçi, A., (2011), Veri Tabanı Yönetim Sistemleri, İstanbul

[3]İnternet: Vikipedi, Veri Tabanı, https://tr.wikipedia.org/wiki/Veri_taban%C4%B1, 2016.

[4] Vural, Y., Sağıroğlu, Ş., (2010), Veri Tabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri, Politeknik Dergisi, 13(2), 71-8.

[5]İnternet: DB-Engines, DB-Engines Comparison, https://db-engines.com/en/system/Microsoft+SQL+Server%3BMySQL%3BOracle, 2018

[6]İnternet: DB-Engines, DB-Engines Ranking, https://db-engines.com/en/ranking, 2018

[7] Muralidhar, K., Karsa, P., Sarathy, R., (1999) A General Additive Data Perturbation Method for Database Security, Cerias Tech Report, 45(10), 1399-1415, 1999.

[8] Bertino, E., Sandhu, R., (2005), Database Security, Management Science, 2(1), 2-19.

[9] Mehta, R., (2006), Oracle Database Security, Application Program Security, 13(5), 40-52.

[10] Aaron, N., (2006), Oracle Database Security, 10s.

[11] Vural, Y., Sağıroğlu, Ş., (2010), Veri Tabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri, Politeknik Dergisi, 13(2), 71-81.

[12] Titrade, C., Titrade, M., (2011) Oracle Database Security, Romanian Economic Business Review, 5(2), 408-418.

[13] Türköz, T., Sezer, A., Çankaya, Y., Çalışkan, E., (2012), Oracle Veri Tabanı Güvenliği Kılavuzu, Siber Güvenlik Enstitüsü, 75s, Kocaeli.

[14] Qian, K., Lo, D., Shahriar, H., Li, L., Wu, F., Bhattacharya, P., (2017), Learning Database Security with Hands-on Mobile Labs, Frontiers in Education Conference, 18-21.

[15] Gupta, A. M., Gore, Y. R., (2016), Concurrency Control and Security Issue in Distributed Database System, Ijedr, 4(2), 177-181.

[16] Gupta, K., Malik, A., Pawar, S., Patil, J., (2016), Database Security Two Way Authentication Using Graphical Password, Ijera, 6(4), 100-103.

[17] Grachev, V. M., Esin, V. I., Polikhina, N. G., Rassomakin S. G., (2014), Data Security Mechanism Implemented in the Database with Universal Model, Kratkie Soobshcheniya po Fizike, 41(5), 10-16.

[18] Mohammed, H., Safran, M., Hou, W., (2014), A Security Novel for a Networked Database International Conference on Computational Science and Computational Intelligence, 179-284.

[19] Dalabasmaz, H., (2015), Microsoft SQL Server Sızma ve Güvenlik Testi Çalışmaları, Bilgi Güvenliği Akademisi, İstanbul.

[20] İnternet: MSSQLTips, Best practices to secure the sql server sa account, https://www.mssqltips.com/sqlservertip/3695/best-practices-to-secure-the-sql-server-sa-account/, 2015.

[21] İnternet: MSSQLTips, Security issues with the sql server builtin administrators group, https://www.mssqltips.com/sqlservertip/1017/security-issues-with-the-sql-server-builtin-administrators-group/, 2016.

[22] İnternet: Microsoft, Securing Your Database Server, https://msdn.microsoft.com/en-us/library/ff648664.aspx, 2003.

[23] İnternet: Microsoft, Guest User Account in SQL Server, https://blogs.msdn.microsoft.com/batuhanyildiz/2013/03/02/guest-user-account-in-sql-server/, 2013.

[24] İnternet: MSSQLTips, Identify blank and weak passwords for SQL Server logins, https://www.mssqltips.com/sqlservertip/2775/identify-blank-and-weak-passwords-for-sql-server-logins/, 2015.

[25] İnternet: Microsoft, Change server authentication mode, https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode, 2017.

[26] İnternet: Microsoft, Securing Annonymous Account, https://msdn.microsoft.com/en-us/library/ee824255(v=cs.20).aspx, 2002.

[27] İnternet: Mesutx, Sql Server Network Interface Nedir, http://www.mesutx.com/sql-server-network-interface-nedir/, 2015.

[28] İnternet: Microsoft, List of Sql Server Service Name, https://blogs.technet.microsoft.com/fort_sql/2010/05/31/list-of-sql-server-service-names/, 2010.

[29] İnternet: SqlServerUpdates, What are the most recent updates for SQL Server, https://sqlserverupdates.com/, 2018.

[30] İnternet: Microsoft, Configure the Remote Access Server, https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-remote-access-server-configuration-option, 2017.

[31] İnternet: Orafaq, List of Default Database Users, http://www.orafaq.com/wiki/List_of_default_database_users, 2014.

[32] Internet: Lock and Expired Default User Account, https://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm#DBSEG10005, 2014.

[33] İnternet: Oracle, Default Accounts and Passwords, https://docs.oracle.com/cd/A97630_01/win.920/a95490/username.htm, 2002.

[34] Internet: Oracle, The Data Dictionary, https://docs.oracle.com/cd/B28359_01/server.111/b28318/datadict.htm#CNCPT002, 2002.

[35] Internet: Oracle, Enterprise Manager, http://www.oracle.com/technetwork/oem/enterprise-manager/overview/index.html, 2017.

[36] Internet: Oracle, Keeping Your Oracle Database Secure, https://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm#DBSEG98446

[37] Isaca, (2008), Oracle Database Security Checklist, 15s.

[38] Internet: OraDBA, Oracle 12c new password verify function, http://www.oradba.ch/2013/07/oracle-12c-new-password-verify-function/, 2013.

[39] Internet: Oracle, Create Profile, https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_6010.htm, 2014.

[40] Internet: Oracle,Critical Patch Updates Security Alerts and Bulletins, https://www.oracle.com/technetwork/topics/security/alerts-086861.html /a83793/metalink.htm

[41]Internet: Oracle,Critical Patch Updates Security Alerts and Bulletins, https://www.oracle.com/technetwork/topics/security/alerts-086861.html#CriticalPatchUpdates