T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

GÜVENLİ YAZILIM GELİŞTİRME REHBERİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Sivil Havacılık Genel Müdürlüğü
Güvenli Yazılım Geliştirme Rehberi

Güvenli Yazılım Geliştirme Rehberi

Aralık,2020/Ankara

İçindekiler

1.YAZILIM GELİŞTİRME SÜREÇLERİ

1.1.Analiz

Bu aşamanın amacı sistemin işlevlerini ve kesin gereksinimleri açıklığa kavuşturmak ve sonucunda bunları belirli bir formatta dokümante etmektir. Bu çalışma müşteri, yazılım mühendisi, sistem analisti, iş analisti, ürün yöneticisi, Kurumsal Some görevlisi vb. rollerin bir araya geldiği gruplar tarafından yapılabilir. Çeşitli yazılım geliştirme metodolojilerinde bu aşamada kullanım dokümanları ve test plan dokümanları da oluşturulabilir.

1.2.Tasarım

Gereksinimlerin tamamlanmasıyla beraber sistem tasarım aşamasına başlanır. Yazılım ürün tasarımı, gereksinim ve isteklerini karşılamak üzere yazılım ürününün özellikleri, yetenekleri ve ara yüzlerinin belirlenmesi etkinliğidir. İki tür tasarımdan bahsetmek mümkündür (Yüksek düzeyde tasarım — Mimari tasarım ve Detaylı tasarım). Mimari tasarım, yazılım modüllerinin genel yapıları ve organizasyon içerisindeki etkileşimleri ile ilgilenir. Sonucunda mimari tasarım dokümanları oluşturulur. Detaylı tasarım aşamasında Mimari tasarım dokümanları genelde revize edilirler. Tasarım ve analiz aşamalarının ayrımı "Problem Ne?/Problem Nasıl Çözülür?" sorularının kullanımı ile ilgilidir. Gereksinimlerin belirlendiği analiz aşaması problemin ne olduğu ile ilgilidir.

1.3.Kodlama

Tasarım aşamasının belirli bir olgunluğa ulaşmasıyla birlikte kodlama aşaması başlar. Teslim edilecek projeyi programlama aşamasıdır.

1.4.Test

Kodlama süresince ve kodlama sonrasında yapılan diğer önemli aşama test'tir. Erken test et yaklaşımı ile hareket edip, analiz aşamasından itibaren test bakış açısına sahip olmamız hata yapma oranımızı ve maliyetleri düşürecektir. Birim testleri, duman testleri, yanlış değer testleri, kabul testleri, kullanım senaryo testleri, yük testleri, kullanıcı kabul testi, yoldan geçen adam testi, test otomasyonu gibi sürece ve duruma göre uygulanabilecek çok farklı kategoride ve derinlikte test türü bulunmaktadır.

1.5.Bakım

Tüm test aşamaları tamamlandıktan sonra yazılım ürünün sahaya teslim edilebilir bir versiyonu çıkartılır ve teslim aşaması gerçekleştirilir. Teslim çıktısı olarak ürün tek başına yeterli değildir. Mutlaka son kullanıcılar için kullanım kılavuzu ve versiyon fark dokümanı oluşturulmalıdır. Teslim ile birlikte bakım aşaması da başlar. Hata giderici, önleyici, altyapıyı iyileştirici, ürüne yeni özellikler ekletici gibi farklı bakım faaliyetleri mevcuttur.

2.GÜVENLİ YAZILIM GELİŞTİRME

2.1.Girdi Doğrulama

Günümüzde bilinen ve gelecekte de muhtemel tehditlerin çoğu kötü niyetli girdi ile başlamaktadır. Bununla birlikte; basit girdi doğrulama yöntemleri ile büyük güvenlik tehditlerinin önlenmesi mümkündür.

Girdi doğrulama yöntemlerini "beyaz kutu" ve "kara kutu" olmak üzere ikiye ayırmak mümkündür. Beyaz kutu yönteminde bilinen bir şablon girdi olarak kullanılmakta, bu şablonun dışındaki tüm girdiler kötü niyetli olarak kabul edilmektedir. Şablonun kontrolü çok kolay olduğundan bu yöntem oldukça etkili bir yöntemdir. Kara kutu yöntemi ise daha az etkili olmasına rağmen daha çok tercih edilen bir yöntemdir. Bu yöntemde kullanılan belirli bir şablon yoktur, sadece bilinen saldırıların bir listesi mevcuttur. Eğer girdi bilinen bir saldırıya benziyor ise o zaman girdi reddedilecek, onun dışındaki tüm girdiler ise kabul edilecektir. Tüm atak çeşitlerini belirlemek zor iken gelecekteki atakları bilip filtrelemek daha da zor olacağından bu yöntemin etkinliğinin daha az olacağı açıktır. Dolayısıyla veri yapıları, mümkün olduğunca belli bir şablona uygun tasarlanarak geçerleme daha güçlü kılınmalıdır.

İstemci-sunucu uygulamalarında doğrulama hem istemci hem de sunucu tarafında yapılabilmektedir. Bununla birlikte; bir saldırgan istemci tarafındaki doğrulama kontrolünü kolay aşabileceğinden istemci tarafındaki doğrulama hiçbir zaman yeterli bir güvenlik önlemi olarak ele alınmamalıdır. Bunun yerine daha çok sunucu tarafında doğrulama kontrolü yapılarak güvenlik seviyesi arttırılmalıdır. Güvenilir olmayan bir kaynaktan gelen veriler mutlaka onaylanmalıdır.

2.2.Kimlik Doğrulama

Kimlik doğrulama, varlıkların kimlik kontrolünden geçmesi işlemidir ve farklı kimlik doğrulama yöntemleri bulunmaktadır. Genellikle yazılımlar önceleri sadece kullanıcı adı ve şifre kullanması şeklinde zayıf doğrulama yöntemleri kullanılmakta idi. Eğer bir "domain" yapısı varsa, kullanıcılar "Active Directory" kullanılarak doğrulanmakta, "domain" dışında ise kimlik yönetimine ilişkin veritabanı uygulanmaktadır. Daha güçlü doğrulama yöntemleri olarak da biyometrik metotlar veya akıllı kartlar kullanılabilir. Bir diğer doğrulama yöntemi ise üçüncü bir tarafın doğrulama işini yapması ve bu üçüncü tarafa güven duyulması şeklindedir.

2.3.Yetkilendirme

Kullanıcıların tanımlanması aşaması olan kimlik doğrulamadan sonra kullanıcının kimliği doğrultusunda erişim haklarının belirlendiği ve kontrolünün gerçekleştiği aşama yetkilendirmedir.

2.4.Konfigürasyon Yönetimi

Konfigürasyon, uygulama ile ilgili hassas bilgileri içermektedir. Örnek olarak, veri tabanına erişim için gerekli bağlantı bilgilerini içeren dosyalar bu kapsamdadır. Konfigürasyona müdahale uygulamanın işleyişini değiştirebilir veya çalışmamasına sebep olabilir. Konfigürasyon dosyalarının sunucularda saklanıyor olması yeterli güvenlik önlemlerinin alındığı anlamına gelmemektedir. Konfigürasyon dosyaları

hassas bilgi olarak nitelendirilmeli, şifrelenmiş bir şekilde tutulmalı ve bu dosyalara erişim kayıt altında tutulmalıdır.

2.5.Kritik Bilgi Yönetimi

Kritik bilginin ne olduğunun belirlenebilmesi için uygulamanın ve işin bir arada ele alınması gerekir. Uygulama geliştirici işin niteliğini tam olarak bilemediğinden, diğer yandan işin sahibi de uygulamanın teknik altyapısı hakkında sınırlı bilgiye sahip olacağından bu iki taraf tek başlarına kritik bilgi için yeterli tanımlama yapamayacaklardır. İki tarafın ve kurumsal some yetkililerinin bir araya gelmesiyle hassas bilgileri içeren bir liste oluşturulmalı ve bu listeyi koruyacak bir politika oluşturulmalıdır.

2.6.Kriptografi

Veriyi korumanın yollarından biri de şifrelemedir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır. Daha önce kırılması uzun zaman alan algoritmalar günümüzde daha kısa zamanda çözülebilmektedir. Dolayısıyla uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.

2.7.Parametre Manipülasyonu

Dağıtık algoritmalar modüller arasında parametre gönderirler. Eğer bu parametreler arada değiştirilirse, saldırı gerçekleştirilmiş olur.

2.8.Hata Yönetimi

Bazı teknolojiler hataları kullanarak hata yönetimi gerçekleştirmektedirler. Hatalar geliştiriciler ve sistem yöneticileri için uygulama ile ilgili birçok önemli bilgi ihtiva ettiği için çok önemlidirler. Bununla birlikte; geliştirici için bu derece önemli olan bilgi kullanıcı açısından problem oluşturabilmektedir. Her ne kadar kullanıcılar bu hataların ne demek olduğunu anlamasalar da saldırganlar için büyük ipuçları, yazılımla ilgili önemli bilgiler içermektedir. Bundan dolayı sadece genel bir hata mesajının dönmesi, hataların kayıt altında tutulması ve gerçek hataya sadece yöneticiler ulaşmasını sağlayacak sürecin oluşturulması gerekmektedir.

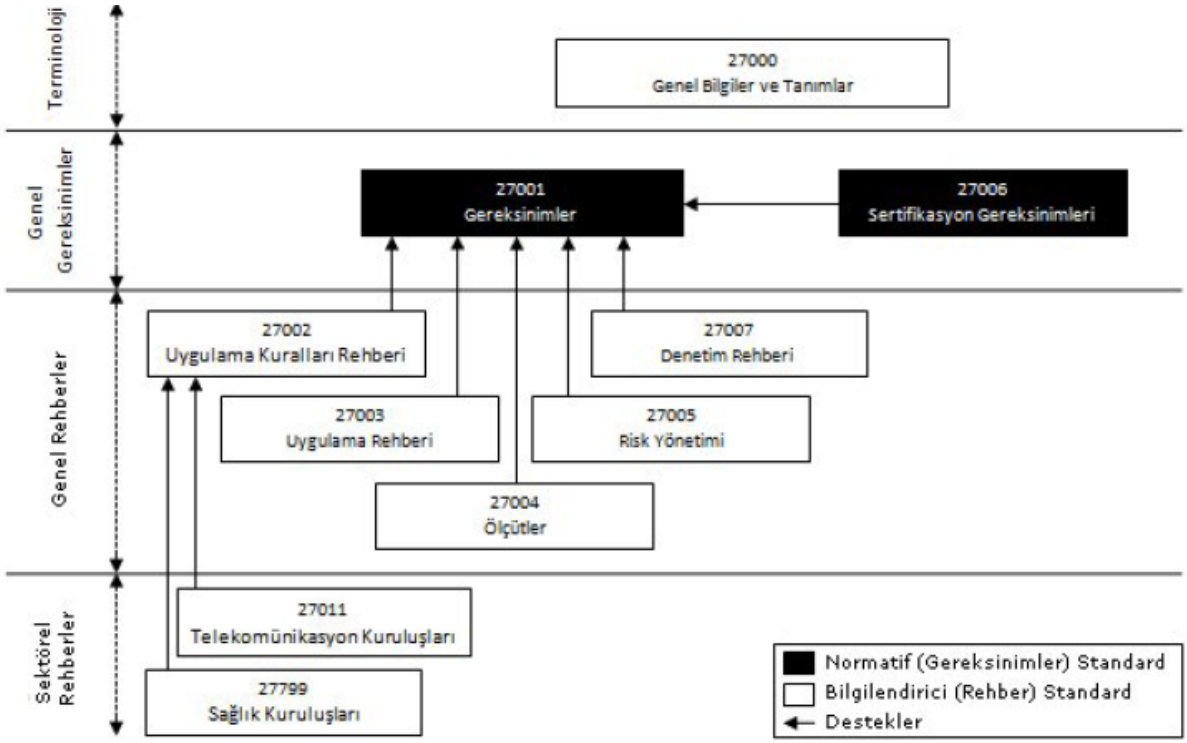
2.9.Kayıt Tutma ve Denetim

Uygulama veya uygulamanın yöneticileri saldırı altında olduklarını anlamalıdır. Bu durum aslında neyin normal neyin anormal olduğunun belirlenmesi ile sağlanır. Bir uygulamaya ilişkin normal süreç ve şablon tanımlanmalı ve bunu dışında bir olay olduğunda saldırı ihtimali, kurumsal some yetkilileri ile birlikte, ele alınmalıdır.

3.ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE GÜVENLİ YAZILIM GELİŞTİRME

Bilgi güvenliği, yazılı, sözlü, elektronik ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişilebilirlik bakımından güvence altına alınması ve bu güvence durumunun sürekliliğinin sağlanmasıdır. Bilgi sistemlerinin hayata geçmesiyle ortaya çıkan depolama ve işleme imkânlarının artması, izinsiz erişimler, bilginin yetkisiz imhası, yetkisiz değiştirilmesi veya yetkisiz görülmesi ihtimallerinin artması gibi hususlar nedeniyle bilgi güvenliği kavramı gündeme gelmektedir. Bilgi güvenliği işletmenizdeki tüm yazılı ve dijital bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir.

Bilgi güvenliği ile ilgili olarak ISO 27000 serisi güvenlik standartları, kullanıcıların bilinçlenmesi, güvenlik risklerinin azaltılması ve de güvenlik açıklarıyla karşılaşıldığında alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır.



ISO 27001, gerek yazılım geliştirme süreçleriyle doğrudan ya da dolaylı ilişki içerisinde olan birçok kontrol içermektedir.

4.YAZILIM GELİŞTİRME AŞAMALARINA İLİŞKİN KONTROLLER

4.1.Analiz Aşamasına İlişkin Kontroller

Yazılım geliştirme sürecinin en önemli aşamasıdır. Bu aşamada yapılacak yanlışlıklar yazılım projesinin başarısını en yüksek düzeyde etkilemektedir. Bu aşamada kurumun mevcut bilgi teknolojileri, varsa sistem veri tabanı yapısı, sistem veri yapıları tanımlanmalıdır. Kullanıcı uygulama ihtiyaçları doğrultusunda yazılım ihtiyaç tanımları, veri yapılarını güncelleyen giriş bilgileri, uygulama yazılım ara yüz tanımları, yazılımın üreteceği çıktı bilgileri, yazılım için istenen sorgular gibi tanımlar belirlemelidir.

Bu kapsamda;

- Yazılım için devreye alınacak yeni bilgi sistemleri için iş gereksinimleri bildirgeleri ya da mevcut bilgi sistemlerine yapılan iyileştirmeler güvenlik kontrolleri için gereksinimleri belirlemelidir.

- Yeni bilgi işleme tesisleri için, bir yönetim yetki süreci tanımlanmalı ve gerçekleştirilmelidir.
- Yetkilendirilmiş kullanıcıların sistemde neler yapabileceği uygun şekilde belirtilmelidir, aksi durumlarda başka kullanıcı haklarını kullanma, yetkisiz olduğu halde verilere erişebilme gibi sakıncalar doğabilir. Kuruluş içinden ya da dışından sağlanmış olsun tüm ağ hizmetlerinin güvenlik özellikleri, hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalıdır.
- İletişimin bütün türlerinin kullanımıyla ve bilgi değişimini korumak için resmi değişim politikaları, süreçleri ve kontrolleri oluşturulmalıdır.
- Yazılımda kullanılacak harici materyaller için fikri mülkiyet haklarına göre materyallerin kullanımı ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla doğan gereksinimlere uyum sağlanmalıdır.
- Kuruluşun dış taraflarla yapacağı bilgi ve yazılım değişimi için anlaşmalar yapılması gerekir, bu gereksinim analiz aşamasında karşılanmalıdır.

4.2.Tasarım Aşamasına İlişkin Kontroller

Tasarım aşamasında, uygulanacak geliştirme safhaları, her safha için girdiler, çıktılar ve kontrol metotları, iş zaman planları, uygulama planlarının yanı sıra yapılacak işlerin neler olduğu, bu işler için gerekli zaman ve kaynak ihtiyaçlarının tespiti, ilerlemenin izlenmesi için kullanılacak metotlar belirlenmelidir. Bu kapsamda;

- Tüm yazılım kullanıcıları için her türlü yazılım sistemine erişim kullanıcı isimleri ve şifreler ile sağlanmalı, bu şifre ve kullanıcı isimleri her kullanıcı için tek ve benzersiz olacak şekilde tasarlanmalıdır.
- Tasarımda kullanıcılar işlevlerine ve sorumluluk alanlarına göre gruplandırılmalı, grup bazında programlara ve veri tabanlarına erişim hakları verilerek yetkisiz kişilerin sistemi kullanmasına imkân verilmemelidir.
- Bilgi sistemlerinin birbirine bağlantısı ile ilişkili bilgiyi korumak için politikalar ve prosedürler geliştirilmeli ve gerçekleştirilmeli, bilgi sızması fırsatları önlenmelidir.
- Yüksek riskli uygulamalara ek güvenlik sağlamak için bağlantı sürelerinde sınırlandırmalar kullanılması gerektiği hesaba katılmalıdır.
- Tehditlerden korunmak için ve iletilmekte olan bilgi dâhil ağı kullanan sistemler ve uygulamalar için güvenliği sağlamak amacıyla ağlar uygun şekilde yönetilmeli ve kontrol edilmelidir.
- Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, oluşturulması önerilen tanımlanmış erişim kontrol politikasına uygun olarak kısıtlanmalıdır.

4.3.Kodlama Aşamasına İlişkin Kontroller

Yazılımlarda kodlamalar yapılırken güvenli yazılım kodlama teknikleri kullanılmalıdır. Bu kapsamda;

- Yazılımlar, modüler planlanmalı, modüler arası ilişkilerde yapısallık göz önünde bulundurulmalı ve programcı müdahalesi asgari seviyede olacak şekilde parametrik hazırlanmalıdır.
- Sisteme yeni modülerin ilavesi, modüllerin değiştirilmesi ya da silinmesi durumda sistemin bütünü etkilenmemelidir.
- Tutarsız kod ve verilerin girişine engel olacak tedbirler alınmalı, veri tipleri ile kullanıcıların giriş yaptıkları alanların birbirleri ile tutarlı olma durumu kod içinde yapılan düzenlemeler ile giriş anında kontrol edilmelidir.
- Uygulamalara gerçekleşen veri girişinin, bu verinin doğruluğunun ve uygunluğunun geçerlenmesi gerekmektedir.
- Kayıt olanakları ve kayıt bilgisi kurcalanma ve yetkisiz erişime karşı korunmalıdır.
- Yazılımda çıkış verisi sistem hakkında bilgi vermemeli veri sızıntısına açıklık bırakmamalıdır.
- Bir uygulamadan gerçekleşecek veri çıktısı, depolanan bilginin işlenmesinin koşullara göre doğruluğunun ve uygunluğunun sağlanması için geçerlenmelidir.
- Veri işleme hataları veya kasıtlı eylemler nedeniyle herhangi bir bilgi bozulmasını saptamak için geçerleme kontrolleri uygulamalar içine dâhil edilmelidir.
- Uygulamalarda verinin kimliğinin doğruluğunu sağlama ve mesaj bütünlüğünü koruma gereksinimleri tanımlanmalı bunlarla ilgili uygun kontroller tanımlanmalı ve gerçekleştirilmelidir.
- Kötü niyetli koda karşı korunmak için saptama, önleme ve kurtarma kontrolleri ve uygun kullanıcı farkındalığı prosedürleri gerçekleştirilmeli, elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.
- Kriptografi teknikleri yazılımlarda güvenliği sağlamada faydalanılan önemli tekniklerdir. Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmeli ve gerçekleştirilmelidir.
- Kriptografi için yeterli rastgeleliği sağlayan kriptografik tekniklerin kullanım desteklenmeli ve anahtar yönetimi bulunmalıdır.
- Yazılım geliştirme hizmetinin kuruluş dışından sağlanması durumunda, hizmeti sunan şirketin hareketleri ve yaptığı işler denetlenmeli ve izlenmelidir.

4.4.Test Aşamasına İlişkin Kontroller

Kodlama aşamasından sonra gerçekleştirilecek test aşamasında yazılım uygulaması modüllerinin nitelik ve nicelik testleri uygulanmalıdır. Bu kapsamda;

- Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmalıdır.
- Veri tabanının büyüklüğü ve listelenen, sorgulanan kayıt sayısı ile sistemin performans ilişkisi kontrol edilmelidir.
- Test verisi dikkatlice seçilmeli, korunmalı ve kontrol edilmelidir.

- Yazılım ürünlerinin, sistemin ve alt sistemlerin modül, fonksiyon, entegrasyon ve performans testlerinden sonra testlerde ortaya çıkan değerlere uygun olarak gerçek bilgi ve verilerle, gerçek kullanıcı donanım ve işletim ortamında tüm ihtiyaçların karşılandığı kontrol edilmelidir.
- Test aşaması bitip uygulama devreye alınırken tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi ve bilgi işleme olanaklarına olan erişim hakları, istihdam, sözleşme veya anlaşmalarının sonlandırılmasıyla birlikte kaldırılmalı ya da değiştirilmesiyle birlikte ayarlanmalıdır.

4.5.Bakım Aşamasına İlişkin Kontroller

Yazılım geliştirme sürecinin son aşaması, bakım aşamasında da alınması gereken bir takım güvenlik önlemlerinden söz etmek mümkündür. Bu kapsamda;

- Yazılım paketlerine yapılacak değişiklikler, belirli bir incelemeden geçirilmeli, gerek duyulanlar gerçekleştirilmeli, bunun dışındakiler önlenmelidir. Tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.
- Kullanıcıların erişim hakları da resmi bir proses kullanarak düzenli aralıklarda gözden geçirmelidir.
- Yazılım Kaynak kodlarının bozulma riskini azaltmak ve bilgi kaybından korumak amacı ile kaynak kodları yazılım uzmanlarının işletim sistemleri içinde değil sunucu terminal üzerinde bulunmalıdır. Program kaynak koduna erişim kısıtlı olmalıdır.
- Yedekleme için kurtarılabilir veri saklama yöntemleri uygulanmalı, bilgi ve yazılımlara ait yedekleme kopyaları düzenli olarak alınmalı ve alınan yedekler belirlenecek bir politikaya göre uygun şekilde düzenli olarak test edilmelidir.
- Eğer yetkilendirme varsa ve bilgi içeren ortamın, kuruluşun fiziksel sınırları ötesinde taşınması söz konusu ise taşıma esnasında, bilgiler yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalıdır.
- Bilgisayar donanımlarının depolama ortamı içeren tüm parçaları, elden çıkarılmadan önce, herhangi bir hassas veri ve lisanslı yazılım varsa kaldırılmasını veya güvenlişekilde üzerine yazılmasını sağlanmalıdır.
- İşletim sistemleri değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.
- Kurumların ve şirketlerin operasyonel sistemlerindeki yazılımların kurulmasını kontrol etmek için prosedürler bulunmalıdır.

5.Ulaştırma ve Altyapı Bakanlığı Güvenli Yazılım Geliştirme Kontrol Listesi

Gözden Geçiren		**Proje Adı**	
Gözden Geçirme Süresi	(Harcanan Toplam Süre Saat Olarak Yazılır)	**İş Büyüklüğü**	
Gözden Geçirme Tarihleri		**Gözden Geçirilen İş Ürünü**	

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
Mimari, Tasarım ve Tehdit Modelleme					
1	Uygulamanın mimarisi Güvenli Yazılım Geliştirme Kılavuzunda belirtilmiş olan güvenli yazılım ilkelerine uygun olmalıdır.	Yüksek			
2	Uygulamadaki bileşenler hata durumlarında varsayılan olarak güvenli durumlara geçmelidir.	Yüksek			
3	Uygulamaya yapılan tüm erişim istekleri hem istek hem de yanıt zamanında yetkilendirmeye tabi tutulmalıdır.	Yüksek			
4	Uygulama bileşenleri birbirlerinden iyi tanımlanmış güvenlik mekanizmalarıyla ayrılmalıdır. Bu bağlamda sanallaştırma, uygulama konteyneri, ağ ayrımı, güvenlik duvarı veya bulut tabanlı güvenlik grupları gibi mekanizmalar kullanılmalıdır.	Yüksek			
Bilgi Toplama					

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
5	Web, uygulama ve veri tabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü vb.) gizlenmelidir.	Orta			
6	Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.	Orta			
7	Uygulamaların üzerinde koştukları sunucular, servis verdikleri dizinlerin içeriklerini listelememelidir.	Orta			
8	Arama motorları tarafından görüntülenmemesi istenen dizinler varsa, bunlar için robots.txt ile önlem alınmalıdır. Yalnız, sayfa içerisinde köprülenmeyen bağlantıların/dizinlerin (örneğin yönetim sayfası) güvenlik sorunu oluşturmaması adına robots.txt dosyasına eklenmemesi gerekmektedir.	Orta			
Yapılandırma Yönetimi					
9	Uygulama çatısı, veri tabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.	Kritik			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
10	Uygulama, güncelleme bildirimlerini ya da güvenlik uyarılarını e-posta, SMS veya alternatif iletişim kanallarıyla iletebilmelidir.	Yüksek			
11	Uygulama, başarısız sistem başlatma, başarısız sonlandırma veya başarısız kapatma gibi işlemlerde güvenli bir duruma geçmelidir.	Yüksek			
12	Ana sistem için gereksiz olan dosyalara (örneğin yedekleme, arşiv, test, geliştirme için kullanılan dosyalar) erişim engellenmeli ve sistemdeki gereksiz uygulamalar kaldırılmalıdır.	Yüksek Yüksek			
13	ASP.NET, PHP, STRUTS gibi kullanılan uygulama çatılarının güvenlik özellikleri aktif hale getirilmelidir.	Yüksek			
14	Ön tanımlı kullanıcı hesapları sistemden, veri tabanından ve uygulamadan kaldırılmalıdır.	Yüksek			
15	Hassas bilgiler içeren web sayfalarının tarayıcılarda belleğe alınmaması için autocomplete, cache-control, pragma gibi gerekli HTTP/HTML başlıkları kullanılmalıdır.	Yüksek			
16	Güvenli web trafiği için (SSL) güçlü şifreleme algoritmaları kullanılmalıdır, güvensiz algoritmalar inaktif hale getirilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
17	SSL sunucusunun "renegotiation" özelliği kapatılarak sunucu servis dışı bırakma ve Man In The Middle (MITM) saldırılarına karşı korunaklı hale getirilmelidir.	Yüksek			
İletişim Güvenliği					
18	Güvenilen bir sertifika otoritesinden her Transport Layer Security (TLS) sunucu sertifikasına bir güven zinciri oluşturulabilmeli ve her sunucu sertifikası geçerli olmalıdır.	Yüksek			
19	Kimlik doğrulaması yapılmış, hassas veriler ya da işlevler içeren ve güvensiz ya da şifrelenmemiş protokollerle yapılan tüm bağlantılar (iç ve dış) için TLS protokolünün yaygın kullanılan son sürümü üzerinden yapılmalıdır.	Yüksek			
20	Uygulamada, ağı dinleyen saldırganların trafiği kaydetmesini engellemek için ileri gizlilik şifrelemeleri kullanılmalıdır.	Yüksek			
21	Uygulama, Çevrimiçi Sertifika Durum Protokolü Damgalama (OCSP stapling) gibi yöntemlerle sertifika iptal denetimi gerçekleştirebilecek şekilde yapılandırılmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
22	Sertifikalarda ve sertifikanın tüm hiyerarşisinde yalnızca güçlü algoritmalar ve protokoller kullanılmalıdır.	Yüksek			
23	Uygulama, kimliği doğrulanmış iletişim oturumlarının güvenilir olarak sonlandırıldığını belirten ve kolay anlaşılabilen bir çıkış iletisi görüntülemelidir.	Yüksek			
Kimlik Doğrulama					
24	Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası maskelenmeli ve açık olarak görünmemelidir.	Yüksek			
25	Tüm şüpheli kimlik doğrulama kararları için özet veri içerecek şekilde iz kaydı oluşturulmalıdır.	Yüksek			
26	Yazılım altyapısında ya da herhangi bir bileşen için kullanılan teknolojide üzerinde varsayılan parolalar yer almamalıdır.	Yüksek			
27	Zayıf parolaların kullanımına izin verilmemelidir.	Kritik			
28	Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.	Kritik			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
29	Uygulama ile son kullanıcı arasında aktarılan kullanıcı adı, parola gibi hassas veriler HTTPS protokolü üzerinden aktarılmalıdır.	Kritik			
30	Herkese açık olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılmalıdır.	Yüksek			
31	Parola Hash değerleri oluşturulurken salt verisi de kullanılmalıdır.	Yüksek			
32	Kullanıcılara (SMS, e-posta yoluyla) dağıtılan başlangıç parolalar, kullanıcılar uygulamaya ilk giriş yaptıklarında değiştirilmeye zorlanmalıdır.	Yüksek			
33	Uygulama üzerinden yapılan kritik işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınmalıdır.	Kritik			
34	Kullanıcı adı ve parola ile kimlik doğrulamasının yapıldığı kontroller tek tip hata mesajı vermek suretiyle kullanıcı adları listeleme saldırılarına engel olmalıdırlar.	Yüksek			
35	Önceden belirlenmiş hatalı giriş sayısından sonra hesap pasif hale getirilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
36	Uygulama giriş yapan kullanıcıya profil bilgilerini (şifre, email adresi) düzenleme imkanı verilmelidir.	Orta			
37	Şifremi unuttum mekanizması olmalıdır ancak bu mekanizma güvenlik zafiyeti içermemelidir.	Yüksek			
38	Uygulama erişim için kullanıcıya otomatik üretilip verilen ilk parola güçlü, benzersiz ve geçerlilik süresine sahip olmalıdır.	Yüksek			
39	Parolalar en az 8 karakterden oluşmalıdır, en az bir büyük bir küçük harf içermeli, en az 1 rakam içermeli, en az bir özel karakter içermeli aynı karakterler peş peşe kullanılmamalıdır.	Yüksek			
40	Parolalar geçerlilik süresi olmalıdır (standart kullanıcı için tavsiye edilen 180 gün).	Yüksek			
41	Parola değiştirilmesi için mutlaka eski parola doğrulanmalıdır.	Yüksek			
Oturum Yönetimi					
42	Kullanıcı oturumu kapattığında tüm oturumlar geçersiz hale getirilebilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
43	Oturum kimlikleri yeterince uzun olmalı, rastgele olmalı ve etkin oturumlar içerisinde tekil olmalıdır.	Yüksek			
44	Oturum sonlandığında oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir.	Yüksek			
45	Uygulama her ürettiği oturum kimliğini yalnızca bir kez kullanmalıdır.	Yüksek			
46	Oturum tekil tanımlayıcısı (Session ID) URL'de gönderilmemeli veya referrer başlığı* içine dâhil edilmemelidir.	Yüksek			
47	Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılmalıdır.	Yüksek			
48	Uygulamalarda başarılı kimlik doğrulama ve tekrarlayan kimlik doğrulama (re-authentication) neticesinde her zaman yeni bir oturum bilgisi oluşturulmalıdır. Çıkış işleminden sonra da var olan oturum bilgisi geçersizleştirilmelidir.	Yüksek			
49	Kritik işlemlerde CSRF saldırılarına karşı "token" veya "CAPTCHA" gibi güvenlik önlemleri alınmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
50	Oturum bilgisini içeren çerezlerin (COOKIE) domain ve yol (path) bilgileri ilgili site için en uygun şekilde sınırlandırılmalıdır.	Yüksek			
51	Kullanılan çerez değerleri için *httponly* parametresi tanımlı olmalıdır. Buna ek olarak, HTTPS protokolü kullanılan bağlantılarda kullanılan çerez değerleri için *secure* parametresi tanımlı olmalıdır.	Yüksek			
52	Başarılı login işlemleri sonrası kullanıcı HTTP 302 ile dahili sayfalara yönlendirilmelidir.	Orta			
53	Başarılı kimlik doğrulaması sonucu erişilen uygulamalarda sistemden tekrar çıkmak (logout) için gerekli linkler sağlanmalıdır.	Orta			
Yetkilendirme					
54	Yetkilendirme yaparken “Rol bazlı” yetkilendirme tercih edilmelidir.	Yüksek			
55	Uygulama, kurumsal bilgi sistemlerinde saklanan ve kendi sorumluluğunda olmayan verilerin değiştirilebilmesini engellemelidir.	Yüksek			
56	Kullanıcı yetkileri, sadece sistem yöneticisi veya yetkilendirilmiş kişiler tarafından yapılmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
57	GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.	Kritik			
58	Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.	Yüksek			
59	Veri tabanı kullanıcısının sadece uygulamanın kullandığı veri tabanı kaynaklarına erişim hakkı olmalıdır.	Yüksek			
60	Veri tabanı kullanıcısının veri tabanına sadece uygulama sunucu IP adresinden bağlantı hakkı olmalıdır.	Yüksek			
61	Web tabanlı istatistiksel bilgi sağlayan uygulamalara erişim herkese açık olmamalı, rol tabanlı yetkilendirme yapılmalıdır.	Orta			
62	Kısıtlı erişim gerektiren bütün URL'lere, fonksiyonlara, obje referanslarına, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.	Yüksek			
63	Yetki hakkının artık gerekmediği durumlarda (görevden ayrılma, projede rol değiştirme gibi) en kısa sürede ilgili haklar iptal edilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
64	Bir kullanıcıya bağlı birden fazla rol varsa oturum kapatılmadan roller arası geçiş yapılabilmesi sağlanmalıdır.	Yüksek			
65	Yetkilendirme dinamik olmalı ve yetki kaldırıldığında kullanıcın ilgili sayfaya erişimi mümkün olmamalıdır.	Yüksek			
66	Uygulama dokümante edilmişse sistemin çalışmasını etkileyebilecek parametreleri ya da kullanıcı hesaplarını içermemelidir.	Yüksek			
67	Her bir İş nesnesi(business object)* için read/write/modify/delete gibi yetkiler tanımlanmalıdır.	Yüksek			
İş Mantığı					
68	Yönetim paneli gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır. (admin, yönetici, administrator, yönetim, panel v.b.).	Orta			
69	Uygulama domain isimlerine ait hassas bilgilerin google/bing gibi arama motorları tarafından indekslenmediği kontrol edilmelidir.	Yüksek			
70	Uygulama iş mantığını doğru bir şekilde gerçekleştirmeli, iş mantığındaki akışlar yazılımda beklenen sırada gerçekleşmeli,	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
	gereken adımlar atlanmamalı, adımların insanların yapabileceği süreler içinde gerçekleştirildiği kontrol edilmeli ve çok yüksek sıklıkla gönderilen istekler tespit edilmelidir.				
Dosyalar ve Kaynakların Güvenliği					
71	Uygulama, ayar ve denetim dosyaları kullanıcı verisiyle aynı konumda depolamamalıdır.	Yüksek			
72	Uygulama, paylaşılan kaynaklar üzerinden yapılan istenmeyen bilgi akışlarını engellemelidir.	Yüksek			
73	URL yeniden yönlendirmelerinin sadece bilinen "beyaz liste" adreslerine yapılması, bilinmeyen adreslere yönlendirme gerekiyorsa kullanıcının uyarılarak onayının alınması sağlanmalıdır.	Yüksek			
74	Güvenilmeyen kaynaklardan alınan dosyaların türü doğrulanmalı ve zararlı bir içeriğe sahip olup olmadığı kontrol edilmelidir.	Yüksek			
75	Güvenilmeyen verinin dinamik olarak yüklenerek çalışan koda dahil edilmesi engellenmelidir.	Yüksek			
76	Karşı alanlar arası kaynak paylaşımında (Cross-domain Resource Sharing, CORS) güvenilmeyen veri kullanılmamalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
77	Web veya uygulama sunucularının, kendi sınırları dışında bulunan kaynak ve sistemlere uzak bağlantı ve erişimi varsayılan olarak engellenmelidir.	Yüksek			
78	Uygulama, güvenilmeyen kaynaklardan alınmış veriyi çalıştırılabilir kod olarak koşturmamalıdır.	Yüksek			
Veri Denetimi					
79	Kullanıcıdan gelen tüm girdiler sunucu tarafında veri kontrolünden geçmelidir.	Yüksek			
80	Kullanıcıdan gelen veriler işletim sistemi komut satırına girmeden kontrol edilmeli ve düzgünleştirme işleminden (escape) geçirilmelidir.	Kritik			
81	Bütün veritabanı sorguları, parametre olarak yapılmalı ve veritabanına erişimde kullanılan dile karşı (SQL, NoSQL vb.) enjeksiyon saldırılarını önleyebilecek denetimler yapılmalıdır.	Kritik			
82	XSS saldırılarına karşı bütün kullanıcı girdileri dışarı aktarılmadan önce sunucu tarafında özel karakter kodlama (output encoding) işleminden geçirilmelidir.	Yüksek Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
83	Güvensiz kaynaklardan veri alarak aritmetik işlem yapan uygulamalar, gerekli tam sayı üst sınır ve alt sınır kontrollerini gerçekleştirmelidirler.	Yüksek			
84	Web uygulamalarında kullanıcıların girmiş olduğu verilerin ver tabanına kaydetmeden önce istenen şartları sağlayıp sağlamadığını kontrol etmek için validation kontrolleri kullanılmalıdır. Bilgi tekrarını önlemek ve veri tutarlılığını sağlamak için de veri tabanına normalizasyon işlemi uygulanmalıdır.	Yüksek			
85	Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılmalıdır.	Yüksek			
86	Kullanıcı parametrelerini kullanarak farklı sitelere yönlendirme yapan uygulamalarda ilgili parametrelere pozitif girdi denetimi uygulanmalı ve bu sayede olta saldırılarına engel olunmalıdır.	Yüksek			
87	Kullanıcıdan veri alarak LDAP'a bağlanan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri LDAP düzgünleştirme işleminden (escape) geçirmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
88	Kullanıcıdan gelen CR/LF karakterleri uygulama tarafında oldukları gibi HTTP cevap başlıklarında kullanılmamalıdır.	Yüksek			
89	Uygulamalar, uygun olan her sayfada çerçeve engelleyici önlemleri (frame busting) almalıdırlar.	Orta			
90	Uygulama hizmete girmeden önce sızma testleri yapılmalıdır.	Yüksek			
91	Uygulama, yetki onaylama hizmetlerinin (LDAP, Active Directory) enjeksiyonu açıklıklarını önleyici güvenlik denetimlerini yapmalıdır.	Yüksek			
92	HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları, RSS beslemeleri gibi veri girdileri için doğrulama denetimi yapılmalıdır.	Yüksek			
Güçlü Kriptografik Mekanizmaların Kullanımı					
93	Tüm kriptografik modüllerin, güvenli bir şekilde hataya düştüğü doğrulanmalıdır. Hata yönetimi “Oracle Padding” atağına imkan tanımayacak şekilde olmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
94	Tüm anahtar ve şifreler kullanımları tamamlandığında, tamamen sıfırlanarak yok edilmelidir.	Yüksek			
95	Tüm rastgele üretilen sayılar, dosya isimleri, global eşsiz değerler (GUID) ve karakter dizilerinin saldırgan için tahmin edilemez olması sağlanmalıdır. Rastgele sayıların yüksek entropiye sahip olarak üretilmelidir	Yüksek			
96	Uygulamada şifreleme, anahtar değişimi, dijital imzalama veya özet alma gibi fonksiyonlar bulunuyorsa TS ISO/IEC 19790-24759 onaylı kriptografik modüller ve rasgele sayı üreteçleri kullanılmalıdır.	Yüksek			
Verinin Korunması					
97	Sunucu üzerinde saklanan önemli verilerin ön belleklenmiş ya da geçici üretilmiş kopyaları şifreli ve güvenli bir şekilde saklanmalıdır.	Yüksek			
98	Bellekte tutulan önemli veriler gereksinimi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde silinmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
99	Uygulama herhangi bir metodu çalıştırmadan önce güvenlik metodlarını çalışır ve ayakta olduğunu garanti etmelidir.	Yüksek			
100	Silinmiş verilere uygulama bileşenleri üzerinden tekrar ulaşım engellenmelidir. Bellekte ye da disk sisteminde oluşturulan nesnelerin (objects)* gizli veri içermesi engellenmelidir.	Yüksek			
101	Uygulama tablolar arasında veri bütünlüğünü garanti altına almalıdır.	Yüksek			
102	Gerçek veri tabanı asla test ortamı için kullanılmamalıdır.	Yüksek			
103	Uygulama, iş tanımlama dokümanında ya da güvenlik gereksinimlerinde belirtilmesi durumunda, uygulama ara yüzlerinden işlenen ya da saklanan bütün verilerin yedeklerinin alınabilmesine imkân sağlamalıdır.	Yüksek			
Hizmet Dışı Bırakma					
104	DoS saldırısı barındıracak veya şifre deneme-yanılma gibi kaba kuvvet saldırılarına açık tüm formlara CAPTCHA kontrolleri uygulanmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
105	Genelde uygulamaların arama özelliğini kötüye kullanarak veri tabanı üzerinde çok detaylı arama yaptırarak işlemciyi meşgul eden SQL genel arama karakter (%,* vb.) saldırılarına karşı arama süresini kısıtlamak suretiyle önlem alınmalıdır.	Orta			
Web Servisleri					
106	SOAP, Restful, XML-RPC gibi teknolojilerle geliştirilmiş web servislerine erişimlerde kimlik doğrulama kontrolü uygulanmalıdır.	Kritik			
107	Web servisleri için kullanılan çatıların klasik XML saldırılarına (örneğin çok büyük XML verileri, çok sık tekrarlanan XML tag'leri) ve parametre manipülasyonlarına karşı korunaklı olmaları sağlanmalıdır.	Yüksek			
108	Uygulama, web servislerini iyi yapılandırılmış en az TLS v1.2 ve muadil güvenlik önlemi sunan bir protokol ile sunacak şekilde tasarlanmalıdır.	Yüksek			
109	Uygulama, web servis girdilerini kullanmadan önce gidilerin şeklini (XML ve JSON şemalarına uygunluk, parametre beyaz listesi) uygunluğunu ve içeriğini çeşitli saldırılara karşı (XML	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
	bombalama, dış varlık saldırısı, kusurlu XML yapısı, tekrarlamalı girdi vb.) kontrol etmelidir.				
110	Uygulama, web servisi ile gönderilen veride betik (script) içermeyecek şekilde tasarlanmalıdır.	Yüksek			
111	Uygulama, web servislerinden şifreli olarak paylaşılan verileri yine şifreli olarak saklayacak şekilde tasarlanmalıdır.	Yüksek			
İzleme ve Denetim					
112	İz kayıtlarının doğru zaman bilgisi ile oluşturulması sağlanmalıdır.	Yüksek			
113	İzleme kayıtlarının yetkisiz silinmeden ve/veya değiştirilmeden korunması gerekmektedir.	Yüksek			
114	İzleme kayıtlarına erişim de, erişim denetimine tabii olmalıdır. Bu bilgilere sadece güvenlik yöneticilerinin erişmeleri sağlanmalıdır.	Yüksek			
115	İzleme kayıtlarının arşivlenmesi ve bu arşivlerin bakımı mümkün olmalıdır.	Yüksek			
116	İzleme kayıtları, güvenlik yöneticisinin belirlediği ya da uygun bir standarda göre belirlenmiş bir süre zarfı müddetince tutulmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
117	İz kaydı bilgileri 5651 sayılı kanuna uygun şekilde elektronik olarak imzalanmalıdır.	Yüksek			
Kişisel Verilerin Korunması					
118	Uygulama, kişisel veriler üzerinde işlem yapılması ana amaç olmayan durumlarda kişisel verileri maskeleyerek görüntülemeli, aktarmalı veya işlemelidir.	Yüksek			
119	Uygulama, kişisel verileri şifreli olarak saklamalı ve bu verilerin taşınmasında korumalı iletişim kanallarını kullanmalıdır.	Yüksek			
120	Kullanılan veritabanının dışarıya aktarımı ancak veritabanı yönetim yetkisi olan hesaplarla yapılmalı ve öncesinde veritabanındaki kişisel verilerin silinmesi sağlanmalıdır.	Yüksek			

***Seviye**

4-Kritik: Bu seviyedeki güvenlik açıkları saldırganlar tarafından genellikle kötüye kullanılabilir, bütün uygulamanın ve sistemin ele geçirilmesiyle veya en azından hassas bilgilerin açığa çıkmasıyla sonuçlanabilir.

3-Yüksek: Bu seviyedeki güvenlik açıkları saldırganlar tarafından kötüye kullanılabilir ve uygulamadaki/sunucudaki güvenlik ve sistem yapılandırma bilgilerinin ele geçirilmesiyle sonuçlanabilir.

2-Orta: Bu seviyedeki güvenlik açıkları saldırganların hassas sistem ve program sürüm bilgilerini ele geçirmesine neden olabilir.

1-Düşük: Bu seviyedeki güvenlik açıkları saldırganların sistemin basit bilgilerini (portlar, servisler, sürüm) ele geçirilmesine neden olabilir.

6.Yararlanılan Kaynaklar

- Dayıoğlu, Burak, “Yazılım Geliştirme Yaşam Döngüsü ve Güvenlik”
- Kartın, Esma, “Güvenli Yazılım Geliştirme”
- Özbilgin, Dr.İzzet Gökhan, “Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi”
- Yılmaz, Yrd.Doç.Dr. Güray, “Yazılım Mühendisliği Gerçeği”,
- Beydağlı, Erkut, “Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standartı”
- Alparslan, Erdem, “Güvenli Yazılım Geliştirme Modelleri”
- Michael, C.C., Radosevich, Will, “Risk-Based and Functional Security Testing”,
- “Yazılım Güvenliği Yaklaşımı”, Labris Teknoloji,
- Cohen, Manu, “Practical Application Security”
- Çetinkaya, Mehtap, “Kurumlarda Bilgi Güvenliği Yönetim Sistemi’nin Uygulanması”
- International Standard, “ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements”
- Ottekin, Fikret, “Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri”
- Calder, Alan, Bon, Jan Van,“Implementing Information Security based on ISO 27001/ISO 17799 - A Management Guide”
- International Standard, ISO/IEC 27000:2009: Information technology –Security techniques – Information security management systems – Overview and vocabulary
- Layton, Timothy P. “Information Security: Design, Implementation, Measurement and Compliance”,
- Brooks, F.P., “No Silver Bullet Essense and Accidents of Software Engineering”
- Microsoft Security Lifecycle (SDL) Version 3.2
- COBİT, IT Governance Institute