|  |  |  |  |
| --- | --- | --- | --- |
| **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** | **Uygu n (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** | | | | | | | | | | | | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | | Yüksek | |  | |  | |  | |
|  | | gibi) en kısa sürede ilgili haklar iptal edilmelidir. | |  | |  | |  | |  | |
| 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, gereken adımlar atlanmamak, adımların insanların yapabileceği süreler içinde gerçekleştirildiği kontrol edilmeli ve çok yüksek sıklıkla gönderilen istekler tespit edilmelidir. | | Yüksek | |  | |  | |  | |
| **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 | | URLyeniden 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 | |  | |  | |  | |
| 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 | | Kritik | |  | |  | |  | |
|  | | önleyebilecek denetimler yapılmalıdır. | |  | |  | |  | |  | |
| 82 | | XSS saldırılarına karşı bütün kullanıcı girdileri dışarı aktarılmadan önce sunucu tarafında özel karakter kodlama (output encoding) işleminden geçirilmelidir. | | Yüksek  Yüksek | |  | |  | |  | |
| 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 veri 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 | |  | |  | |  | |
| 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 bombalama, dış varlık saldırısı, kusurlu XML yapısı, tekrarlamalı girdi vb.) kontrol etmelidir. | | Yüksek | |  | |  | |  | |
| 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 | | Iz 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 | |  | |  | |  | |
| 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.