TRtest
Test ve Değerlendirme A.Ş.

KİMLİK ve ERİŞİM YÖNETİMİ ÜRÜN GRUBU TEST KRİTERLERİ

No	Başlık/Soru
	1- Ürün Güvenliği
UG_YA	**Yönetim Arayüzleri**
UG_AGO	**1.1 Arayüz Güvenlik Özellikleri (Eğer Varsa)**
UG_AGO_1	Kimlik Doğrulama kontrolü yapılıyor mu?
UG_AGO_2	Parola yönetimi güvenliği sağlanıyor mu?
UG_AGO_3	Erişim yönetimi ve yetkilendirme yapılıyor mu?
UG_AGO_4	Güvenli iletişim kanalları destekleniyor mu?
UG_AGO_5	Sistem yapılandırması doğru, güncel ve güvenli mi?
UG_AGO_6	Tüm ekranlarda form alanlarının biçim doğrulaması (Geçerli veri, Zorunluluk) sağlanabiliyor mu? (Örnek: Tarih alanına harf girilmemesi , TC kimlik alanının 11 karakter uzunlukta numerik karakter dışında kabul etmemesi)
UG_AGO_7	Web arayüzleri varsa OWASP Top 10 saldırılarına karşı desteği var mı? (Injection, Broken Authentication, Sensitive Data Exposure, Xml External, Entities, Broken Access Control, Security Misconfiguration, XSS, Insecure Deserialization)
UG_AGO_8	Güvenli oturum kapatma özelliği var mı?
UG_D	**1.2. Diğer (Uygulama/Web API Vb. Kullanarak Yönetim) (Eğer Varsa)**
UG_D_1	Kullanılan API için yazılımsal güvenlik önlemleri alınmış mı?
UG_D_2	Zararlı girdi kontrolü yapılıyor mu?
UG_D_3	Erişim yönetimi ve yetkilendirme yapılıyor mu?
UG_D_4	Güvenli iletişim kanalları destekleniyor mu?
UG_MT	**Masumiyet Testi**
UG_MT_1	Herhangi bir dış noktaya şüpheli veri gönderiyor mu, içeride görevi dışında bir sisteme erişiyor mu?

TO	2- Temel Özellikler
TO_LOTR	**Log İşleme/ Toplama ve Raporlama**
TO_LOTR_1	Bileşen bazında, detaylı log yönetimi (Akış bilgisi, Exception) yapılıyor mu?
TO_LOTR_2	Sistem erişilecek sistemlerdeki verilere kimler erişmiş ,hangi şekilde erişmiş gibi kullanıcı bazlı bilgileri loglayabiliyor mu?
TO_LOTR_3	Sistemde üreyen tüm loglar yetkili kişilerce izlenebiliyor, istenirse raporlama amacıyla dışarıya alınabiliyor mu? (csv,excel,pdf vb en az biri)
TO_LOTR_4	Sistemde üreyen loglar belirlenecek bir politika dogrultusunda otomatik veya on-demand arşivlenebiliyor mu?
TO_LOTR_5	Log bütünlüğü sağlanıyor mu? (HMAC vb.)
TO_AOY	**Alarm ve Olay Yönetim**
TO_AOY_1	Üretilen uyarılar, tanımlı kullanıcılara e-posta/sms/arayüz pop-up vs yöntemlerinden en az biri ile gönderilebiliyor mu?
TO_AOY_2	Sistem durumu izlenebiliyor mu?
TO_UD	**Ürün Dokümantasyonu**
TO_UD_1	Ürün dokümantasyonu var mıdır?(Yazılı materyal veya Tool Tip vb.)
TO_VDV	**Veri dosyaları ve Veritabanı**
TO_VDV_1	Varsa, Veritabanında tutulan kritik veriler(Örnek: Şifre,TC kimlik no vb) şifreli saklanıyor mu?
TO_VDV_2	Varsa, Veritabanı erişiminde gerekli yetkilendirme unsurları kontrol ediliyor mu?
TO_VDV_3	Veri yedeklemesi sağlanıyor mu?
UGK	**3. ÜRÜN GRUBU KATEGORİLERİ** (Bu bölümün altında bulunan kırmızı başlıklardaki fonksiyonları sağladığını iddia eden üreticiler,kriterleri sağlamalıdır.)
UGK_KD	**Kimlik Doğrulama (Authentication)** Sisteme/Uygulamaya vs giren kişinin kimliğinin doğrulanması, kimlik doğrulamanın sürekliliğin sağlanması
UGK_KD_KF	**KULLANILAN FAKTÖRLER**
UGK_KD_KF_1	Aşağıdaki kimlik doğrulama yöntemlerinden en az ikisini sağlıyor mu?
UGK_KD_KF_2	SMS Tek Kullanımlık Parola Doğrulaması Yapabiliyor mu?
UGK_KD_KF_3	Mobil Uygulama Üzerinden Çevrimiçi Onay Vererek Doğrulama Yapabiliyor mu?
UGK_KD_KF_4	Mobil Push Şeklinde Gönderilen Tek Kullanımlık Parola ile Doğrulama Yapabiliyor mu?

UGK_KD_KF_5	Çevrimdışı Olarak Zaman Bazlı Tek Kullanımlık Parola ile Doğrulama Yapabiliyor mu? (TOTP - RFC-6238)
UGK_KD_KF_6	Çevrimdışı Özet Zincir (Hash Chain) Tabanlı Tek Kullanımlık Parola ile Doğrulama Yapabiliyor mu? (HOTP-RFC 4226)
UGK_KD_KF_7	E-posta Üzerinden Tek Kullanımlık Parola veya Onay ile Doğrulama Yapabiliyor mu?
UGK_KD_KF_8	Davranışsal Biyometri kullanarak doğrulama yapabiliyor mu?
UGK_KD_KF_9	Fiziksel Biyometri (Parmak izi, avuç içi, iris, retina vb.) kullanarak doğrulama yapabiliyor mu?
UGK_KD_KF_10	Güvenli bir donanım (hardware token) üzerinden kimlik doğrulama yapabiliyor mu?
UGK_KD_KF_11	Temaslı akıllı kartlar üzerinden doğrulama yapılıyor mu? (PKI kartları vb.)
UGK_KD_KF_12	Temassız akıllık kartlar üzerinden doğrulama yapılıyor mu? (Mifare, RFID vb.)
UGK_KD_EN	**Entegrasyon Noktaları**
UGK_KD_EN_1	Ağ Erişim Sistemlerinden En Az Bir Tanesi Üzerinden Kimlik Doğrulama Yapabiliyor mu (RADIUS, TACACS vb.)
UGK_KD_EN_2	Active Directory, OpenLDAP, BulutLDAP, Single Sign On(SSO) veya OAuth2 gibi erişim sistemlerinden en az bir tanesi üzerinden kimlik doğrulama yapabiliyor mu?
UGK_KD_EN_3	Windows, Mac, Linux, Android , İoS gibi Client, Mobil İşletim Sistemlerinden En Az Bir Tanesinin Logini ile Entegre Olabiliyor Mu?
UGK_KD_KAPAY	**KRİPTO ALGORİTMALARI, PKI VE ANAHTAR YÖNETİMİ**
UGK_KD_KAPAY_1	Kişiyi tanımlayan kimlik doğrulama verileri, biyometrik veriler veya kullanılan anahtarlar şifreli bir şekilde saklanıyor mu?
UGK_KD_KAPAY_2	Simetrik veya Asimetrik şifreleme kullanıyorsa üretilen anahtarlar için yüksek entropi garanti ediliyor mu?
UGK_KD_KAPAY_3	Simetrik veya Asimetrik şifreleme kullanıyorsa güvenilir açık algoritmalar ve parametreler kullanılıyor mu ? (Simetrik: DES, 3DES, AES vb; Asimetrik: RSA, ECDSA vb.; Özet: SHA-2 vb.)
UGK_HBK	**Hassas Bilgi Kasası (Secret Data Vault Manager)** Kullanıcı erişim bilgileri ve anahtar gibi hassas bilgilerin güvenli bir şekilde saklanması , güncellenmesi , değiştirilmesi (Kullanıcı Cihazı, Veritabanı Şifreleri, Web Uygulama Şifreleri, Yazılım ve Donanım Varlıkları)
UGK_HBK_1	Sistem, hesapların parolalarını güvenli bir şekilde saklıyor mu?
UGK_HBK_2	Sistem, anahtar yönetimini (İptal, Yenileme, Yeniden verme vb) yapabiliyor mu?
UGK_HBK_3	Sistem herhangi biri parolayı kullanım amacıyla aldığında(check out ettiğinde) , başka bir kullanıcıya bu şifreyi vermediği teyit edildi mi?
UGK_EYY	**Erişim ve Yetkilendirme Yönetimi (Access and Authorization Management)** Yetkilendirme ve kısıtlama yönetimi yapılabilmesi , erişimlerin güvenli bir şekilde kayıt altına alınması (Videolog, Keylog vb), erişimler sırasında riskli durumlarda sistemin kendisini koruyabilmesi ve onay mekanizmaları ile güvenliği artırabilmesi , nesne / obje/verinin varoluş amacı dışındaki kullanımlara karşı kendini koruyabilmesi

UGK_EYY_1	Sistem erişim sirasinda güvenliği artırmak amacıyla SSL protokolu ve benzeri yöntemleri destekliyor mu?
UGK_EYY_2	Sistem imkan sağladığı erişimlerde kullanıcı yetkilendirmesi (least privilege) yapabiliyor mu?
UGK_EYY_3	Sistem yapılan erişimlere kural bazlı politika tanımlama (izin verme/vermeme vs) alternatiflerini destekliyor mu?
UGK_EYY_4	Sistem yapılan erişimlere belli bir süre sınırı getirebiliyor ve süresi aşılan erişimleri kesebiliyor mu?
UGK_EYY_5	Kullanıcı ve grup profilleri yönetimi (kullanıcının kullanacağı emtiaların sınıflandırılması ve kullanmaması gereken emtia lara erişimi kısıtlama, asla'lar yönetimi) yapıyor mu?
UGK_EYY_6	Kullanıcıya yetkilendirilen varlıklar görüntülenebiliyor ve yönetilebiliyor mu?
UGK_EYY_7	Kullanıcılara ait erişim yetkilendirme logları log veya Video-log vb methodlarla kayıt altına alınabiliyor mu?
UGK_NY	**Nesne / Ortam / Veri Yönetimi (Object Management)** Erişilen nesne/obje/veri/ortam niteliklerinin kimliklendirilmesi, sertifikalandırılması (PKI vb), yetki tanımının yapılması, çevrimiçi veya çevrimdışı çalışmada nesnenin yetkisiz ve varoluş amacı dışındaki kullanımlara karşı kendini koruyabilmesi
UGK_NY_1	Anahtar yönetiminin güvenliği sağlanıyor mu?
UGK_NY_2	Rasgele anahtar üretimi gerekiyorsa, anahtarların kalite gereksinimleri sağlanıyor mu?
UGK_NY_3	Üretilen ve kullanılan anahtarlar güvenli biçimde saklanıyor mu? (HSM üzerinde saklama, veritabanında şifreli saklama vb.)
UGK_NY_4	Güvenilir açık algoritmalar kullanılıyor mu? (Simetrik: DES, 3DES, AES vb; Asimetrik: RSA, ECDSA vb.; Özet: SHA-2 vb.)
UGK_NY_5	Bu nesnelere / ortamlara erişim SSL , VPN vb güvenli yöntemlerle sağlanıyor mu?
UGK_ATT	**Anomali ve Tehdit Tespiti (Anomally and Threat Detection)** Sistemin çevrimiçi veya çevrimdışı yöntemlerle yapılan kimlik doğrulama ve yetkilendirme erişimlerini zaman, mekan ve davranış özellikleri gibi faktörleri değerlendirerek anomali tespiti yapabilmesi ve buna uygun olarak karşı koyma tedbiri alabilmesi
UGK_ATT_1	Risk Analizinde kural bazlı teknikler kullanılıyor mu? (Rule based)
UGK_ATT_2	Risk faktörü olarak zaman anomalisi kullanılıyor mu? (Time Anomaly, Frekans)
UGK_ATT_3	Risk faktörü olarak tarayıcı parmakizi kullanılıyor mu? (Browser Fingerprint)
UGK_ATT_4	Risk faktörü olarak IP tehdit analizi kullanılıyor mu? (IP Threat)
UGK_ATT_5	Kimlik doğrulama ve erişim yönetimi esnasında tespit edilen anomalilere göre alarm veriyor mu?(SMS, E mail vb)
UGK_ESK	**Erişilen Sistemlerde Kullanıcı / Veri Gizliliği ve Koruması** Veritabanı sistemlerine yapılan erişimlerin kısıtlanabilmesi , erişilen verilerin maskeli bir şekilde görüntülenebilmesi (KVKK veya şirket politikası vb) ve gerekli yetki yönetimi
UGK_ESK_1	Sistem erişilecek sistemlerdeki hassas veri tiplerini tanımlamaya imkan veriyor mu?

UGK_ESK_2	Sistem erişilecek sistemlerdeki verilere kısıtlama getirebiliyor mu? (Bu veriye şu kulanıcılar erişir veya bunlar erişemez şeklinde)
RU	**4- REGÜLASYONLARA UYUM**
RU_1	KVKK uyarınca saklanan ve işlenen verilerin güvenliği/gizliliği sağlanıyor mu?