Güvenlik Testi

Elektronik Ticarette Güven Damgası Hakkında Tebliğ'de, Güven Damgası başvurusunda bulunan e-ticaret sitesinin sızma testi yaptırması gerektiğine ilişkin bir madde bulunmaktadır. Bu maddede Güven Damgası başvurusunda bulunmadan en fazla üç ay önce ve her takvim yılı içinde en az bir defa, Türk Standartları Enstitüsü tarafından onaylı A veya B sınıfı sızma testi firmalarına sızma testi yaptırarak gerekli önlemleri alması ve bu önlemleri aldığına ilişkin doğrulama testi yaptırması gerektiğine ifade edilmektedir.

Bu doğrultuda güvenlik testi için kabul görmüş standartlar seviyesinde ortak bir kapsam oluşturulmuştur. Güven damgasına başvuran e-ticaret siteleri, son bir yıllık işlem hacmine göre aşağıdaki tabloda belirlenen içeriklerde güvenlik testini yaptırmalıdır. İşlem sayısı aralıkları PCI DSS standardına göre belirlenmiştir.

İşlem sayısına göre e-ticaret sitesinin yaptırması gereken güvenlik testi içerikleri tablodaki gibi olacaktır.

<table>
<tr><th>Seviye</th><th>İşlem Sayısı</th><th>Sistem Yapılacaklar</th><th>Uygulama Yapılacaklar</th><th>Sonuç</th></tr>
<tr><td>Düşük İşlem Hacmi</td><td>0 – 20 000</td><td>2 araçla loginli test (Gartner, Nexus vb.)</td><td>ASVS Seviye 1 (3.0.1 veya üstü)</td><td><6 (CVSS v2'ye göre skor)</td></tr>
<tr><td>Orta İşlem Hacmi</td><td>20 000 – 1 milyon</td><td>2 araçla loginli test (Gartner, Nexus vb.)</td><td>ASVS Seviye 2 (3.0.1 veya üstü)</td><td><6 (CVSS v2'ye göre skor)</td></tr>
<tr><td rowspan="2">Yüksek İşlem Hacmi</td><td>1 milyon – 6 milyon</td><td colspan="2">PCI DSS (Seviye 1 veya Seviye 2)
Yerinde denetim yapılmayacaktır.</td><td rowspan="2">PCI DSS raporu</td></tr>
<tr><td>> 6 milyon</td><td colspan="2">PCI DSS (Seviye 1 veya Seviye 2)
Yerinde denetim yapılacaktır.</td></tr>
</table>

Altyapı sağlayıcıdan hizmet alan e-ticaret siteleri güvenlik testi yaptırmayacaktır. Ancak altyapı sağlayıcının ilgili güvenlik testinden başarıyla geçmesi ve başvuruda bulunan e-ticaret sitesinin bu sonucu başvurusunda kullanması beklenmektedir.

OWASP-Uygulama Güvenliği Doğrulama Standardı için 3.0.1 ve üstü versiyonları kabul edilecektir. ASVS kontrol noktaları uluslararası kabul görmüş CVSS versiyon 2'ye göre skorlanacaktır. Bu sayede her zafiyet etki kapasitesiyle birlikte değerlendirilecek ve toplam bir skor elde edilecektir. Uygulama tarafında ASVS Seviye 1 için 86 ve Seviye 2 için de 147 kontrol noktası bulunmaktadır. Bu kontrollerin içerikleri aşağıda yer almaktadır.

- *İşlem sayısı aralıkları PCI DSS standardına göre belirlenmiştir. İşlem sayısına göre e-ticaret sitesinin yaptırması gereken güvenlik testi içerikleri BKM A.Ş'den alınacak verilerle doğrulanacaktır. Sızma testi firmaları ve e-ticaret siteleri yıllık işlem hacmini TOBB'dan öğrenip akabinde güvenlik testi süreçlerini netleştirmelidir.*
- *ASVS Level 1 için 86 ve Level 2 için de 147 kontrol noktası bulunmaktadır. Bu kontrollerin içerikleri Ek-1a ve Ek-1b'de yer almaktadır.*
- *İşlem sayısı 0 – 20 000 Aralığında olan e-ticaret sitesi sistem tarafında 2 araçla loginli teste maruz kalacak uygulama tarafında ise ASVS Level 1'e göre değerlendirilecek ve 6'nın üzerindeki sonuçlarda başarısız sayılacaklardır. Bu seviye için otomatik tarama olmamalıdır.*
- *İşlem sayısı 20 000 – 1Milyon Aralığında olan e-ticaret sitesi sistem tarafında 2 araçla loginli teste maruz kalacak uygulama tarafında ise ASVS Level 2'ye göre değerlendirilecek ve 6'nın üzerindeki sonuçlarda başarısız sayılacaklardır.*
- *İşlem sayısı 1Milyonun üzerinde olan e-ticaret sitesi için firma PCI DSS Seviye 1 veya seviye 2'den geçmişse güvenlik testi sonucu kabul edilecektir.*
- *İşlem sayısı 1 milyon ile 6 milyon arasındaki firmalar için yerinde denetim yapılmayacaktır. Ancak 6 Milyonun üzeri için yerinde denetim yapılacaktır.*
- *Orta ve düşük işlem hacimleri için firmanın fiziki adresine gidilmesini gerektirmeyecek içerikler tasarlanmıştır.*
- *Yüksek işlem hacmi kategorisindeki firmalarda güven damgası kapsamında güvenlik testlerinin QSA imzalı bir PCI raporu ile yapılması şart değildir. TSE onaylı firma tarafından PCI/DSS denetim kapsamında gerçekleştirilmesi kabul edilmektedir.*
- *Tüm kategorilerdeki denetimler mobil tarafını da içermelidir.*
- *Altyapı sağlayıcı firmalar güvenlik testi sonucunu yaptırdıktan sonra en geç üç ay içerisinde TOBB'a tebliğ edecektir. Güvenlik testi sonucu, testin yapıldığı tarih itibariyle altyapı sağlayıcıdan hizmet alan e-ticaret firmaları için 3 ay boyunca geçerli olacaktır. Ayrıca altyapı sağlayıcı firmalar üzerlerindeki işlem hacmine göre ilgili testi yaptıracaktır.*
- *Teknik güvenlik testinde yetkili sızma testi firmasının kaşesi, imzası ve testin sonuçlandığı andaki tarih bulunmalıdır.*
- *Altyapı sağlayıcı firma, hizmet verdiği e-ticaret sitelerinin yıllık işlem hacmine göre (bünyesinde yer alan ve en fazla işlem hacmine sahip e-ticaret sitesi baz alınmaktadır.) güvenlik testi yaptıracaktır.*

EK-1a: ASVS Seviye 1 Kontrol Noktaları

ID	ADI	KATEGORİSİ	Seviye
1.1	Tüm uygulama bileşenlerinin tanımlandığını ve gerekli olduğunu doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	1
2.1	Dışarı açık olanlar dışında tüm sayfa ve kaynakların varsayılan olarak kimlik denetimi gerektirdiğini doğrulayın. (Tümden aracılık prensibi)	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1

2.2	Tüm parola alanlarının kullanıcı girişlerini ekrana yansıtmadığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.4	Tüm kimlik denetimi kontrollerinin sunucu tarafında yapılmaya zorlandığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.6	Tüm kimlik denetimi kontrollerinin bir hata surumunda saldırganın giriş yapmasına olanak sağlamayacak şekilde yapılandırıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.7	Tüm parola alanlarının yüksek karmaşıklıktaki/uzun parolaları girişini engellemediğini/kullanmayı önerdiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.8	Hesaba tekrar erişime olanak tanıyan tüm hesap kimlik denetimi fonksiyonlarının (profil güncelleme, parola unutma, kilitli/kayıp token, yardım masası veya IVR gibi) en az birincil kimlik denetimi mekanizması kadar saldırılara karşı dayanıklı olduğunu doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.9	Parola değiştirme işlevinin eski parola, yeni parola ve parola doğrulamayı içerdiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.17	Unutulmuş parola ve diğer kurtarma yollarının halihazırda kullanılan parolayı açığa çıkarmadığını ve yeni oluşturulan parolanın kullanıcıya açık yazı olarak iletilmediğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.18	Kullanıcı girişi, parola sıfırlama veya hesap unutma işlevleri üzerinden bilgi dökümünün mümkün olmadığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.19	Uygulama çerçevesi veya uygulama tarafından kullanılan bileşenlerin hiçbirisinde varsayılan parola kullanılmadığını (örneğin "admin/password") doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.20	Kimlik doğrulamaya yönelik kaba kuvvet saldırıları veya hizmet dışı bırakma saldırılarını engellemek amacı ile istek kısıtlama mekanizmaları konumlandırıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.22	Unutulmuş parola ve diğer kurtarma yollarının soft token, mobil push veya çevrimdışı kurtarma mekanizması kullandığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.24	Bilgi tabanlı sorular ("gizli sorular" olarak da bilinir) gerekli ise, bu soruların	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1

	uygulamayı koruyacak yeterlilikte güçlü olduğunu doğrulayın.		
2.27	Ortak seçilen ve zayıf parola kullanımını engelleyecek önlemlerin konumlandırıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.30	Bir uygulama kullanıcılarının kimlik doğrulaması yapmasına izin veriyor ise, onların kanıtlanmış güvenli bir kimlik doğrulaması mekanizması kullandığı onaylanmalıdır.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.32	Yönetimsel ara yüzlerin güvensiz taraflarca erişilemediğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
3.1	Özel geliştirilmiş bir oturum yönetici kullanılmadığı veya geliştirilen oturum yöneticisinin genel oturum yönetimi ataklarına karşı dirençli olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.2	Kullanıcı oturumu kapattığında oturumun geçersiz hale getirildiğini doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.3	Belirtilen bir zaman süresince işlem yapılmadığında oturumun sonlandırıldığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.5	Kimlik doğrulama gerektiren tüm sayfaların kolay ve görünür biçimde oturum sonlandırma işlevine sahip olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.6	Oturum anahtarının URL, hata mesajları ve loglarda gösterilmediğini doğrulayın.. Bu aynı zamanda uygulamanın oturum çerezi ile URL yeniden yazmayı desteklemediğini de doğrular.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.7	Tüm başarılı kimlik denetimi ve yeniden girişlerin yeni oturum ve oturum anahtarı oluşturduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.11	Oturum anahtarlarının yeterince uzun, rastgele ve tekil olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.12	Oturum anahtarı değerini tutan çerez yolunun uygulamaya kısıtlı olacak şekilde ayarlandığı ve kimlik doğrulama oturum anahtarlarına ait "HttpOnly" ve "secure" niteliklerinin ayarlandığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.16	Uygulamanın eş zamanlı oturum sayısını sınırladığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1

3.17	Her kullanıcı için aktif oturum listesinin hesap profili veya benzeri alanda gösterildiğini doğrulayın. Kullanıcı herhangi bir aktif oturumu sonlandırabilmelidir.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.18	Kullanıcı parolasını başarılı bir şekilde değiştirdikten sonra aktif olan diğer tüm oturumları sonlandırması için seçenek sunulduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
4.1	En az yetki prensibinin varlığını doğrulayın. - kullanıcılar yalnızca kendilerine ait olan yetkilendirmenin izin verdiği fonksiyonlara, veri dosyalarına, URL'lere, kontrollere, hizmetlere ve diğer kaynaklara erişebilmelidir. Bu, kandırma ve yetki yükseltme saldırılarına karşı koruma anlamına gelir.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.4	Her bir kullanıcının sadece yetkilendirildiği nesne veya verilere ulaşabilecek şekilde hassas kayıtların korunduğunu doğrulayın. (örneğin, kullanıcı parametreyi değiştirerek başka hesaplara ait bilgileri görememelidir.)	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.5	Kasten istenmediği takdirde dizin listelemesi işlevinin kapalı olduğunu doğrulayın. Ek olarak uygulamalar, dosya veya klasör üstverisi sızdıran thumbs.db, .DS_Store, .git veya .svn gibi dosya ve klasörlere izin vermemelidir.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.8	Erişim kontrolünün güvenli bir şekide hata oluşturduğunu doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.9	Sunum katmanında uygulanan erişim kontrolü kurallarının sunucu tarafında da uygulandığını doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.13	Uygulama veya kütüphanenin CSRF engelleyici token veya benzeri işlem koruma mekanizmasına sahip olduğunu doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.16	Uygulamanın bağlam duyarlı yetkilendirmeyi doğru bir şekilde - parametre değiştirerek yetkisiz manipülasyon yapılmaması - uyguladığını doğrulayın	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
5.1	Çalışma ortamının tampon bellek taşmalarına elverişli olmadığı veya güvenlik kontrollerinin tampon bellek taşmalarını engellediğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1

5.3	İstek reddine sebep olan sunucu tarafı girdi doğrulama hatası sonuçlarının kayıt altına alındığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.5	Girdi doğrulama rutinlerinin sunucu tarafında uygulandığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.10	Tüm SQL sorguları, HQL, OSQL, NOSQL ve kayıtlı yordamların, kayıtlı yordamların çağırılmasının, hazır ifadeler veya parametrik sorgular kullanılarak yapıldığını, böylelikle SQL sokuşturmaya karşı dayanıklı olduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.11	Uygulamanın LDAP sokuşturmaya karşı dayanıklı olduğu veya güvenlik kontrollerinin LDAP sokuşturmayı engellediğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.12	Uygulamanın işletim sistemi komut sokuşturmaya karşı dayanıklı olduğu veya güvenlik kontrollerinin işletim sistemi komut sokuşturmayı engellediğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.13	Uygulamanın içerikte bir dosyaya yol kullanıldığı durumlarda Uzak Dosya Katma (RFI) veya Yerel Dosya Katma (LFI) zafiyetleri barındırmadığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.14	Uygulamanın genel XML saldırılarına - Xpath sorgu değiştirmesi, XML Dış Varlık ,ve XML sokuşturma - karşı dayanıklı olduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.15	HTML içeriğine veya diğer web tabanlı kodlara yerleştirilen yazı değişkenlerinin düzgün bir şekilde elle kodlanarak veya şablonlar vasıtasıyla otomatik olarak kodlanarak Yansıtılmış, Kayıtlı ve DOM tabanlı Sitelerarası Betik Çalıştırma (XSS) saldırılarına karşı dayanıklı olduğunu doğrulayın	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.22	WYSIWYG editorler veya benzeri kaynaklardan gelen güvensiz HTML içerikleri HTML arındırıcılar ile arındırılmalı ve girdi doğrulama ile kodlama görevlerinin düzgün bir şekilde ele alındığından emin olunmaldır.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
7.2	Kriptografik modüllerin güvenli bir şekilde hata oluşturdukları ve hataların "oracle padding" gibi zafiyetlere yol açmadığını doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	1

7.7	Uygulama tarafından kullanılan kriptografik algoritmaların FIPS140-2 veya eşdeğer bir standart tarafından geçerli kabul edildiğini doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	1
8.1	Uygulamanın saldırgana yardımcı olabilecek şekilde oturum anahtarı, yazılım/çerçeve versiyonu ve kişisel bilgileri sızdıran hata mesajları veya yığın dökümü oluşturmadığını doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	1
9.1	Hassas veri içeren tüm form alanlarının otomatik tamamlamayı da içerecek şekilde istemci tarafında depolanmasının engellendiğini doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	1
9.3	Tüm hassas verilerin HTTP mesaj içeriği ve başlıklarında sunucuya gönderildiğini doğrulayın. (Hassas verileri göndermek için URL parametreleri kullanılmamalıdır)	V9: Veri koruması doğrulama gereksinimleri	1
9.4	Uygulamadaki her riskli alan için uygun bir önbellek engelleyici başlığın ayarlandığını doğrulayın. Örneğin: Expires: Tue, 03 Jul 2001 06:00:00 GMT Last-Modified: {now} GMT Cache-Control: no-store, no-cache, must-revalidate, max-age=0 Cache-Control: post-check=0, pre-check=0 Pragma: no-cache	V9: Veri koruması doğrulama gereksinimleri	1
9.9	İstemci taraflı depolamada - HTML5 yerel depolama, oturum depolama, IndexedDB, genel çerezler veya Flash çerezleri gibi- hassas veri ve kişisel verilerin tutulmadığını doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	1
10.1	Her bir Transport Layer Security (TLS) sunucu sertifikasına güvenilir bir sertifika otoritesinden (CA) yol oluşturulabildiğini ve her sunucu sertifikasının geçerli olduğunu doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
10.3	Kimlik denetimi yapılan veya hassas veri veya fonksiyonlarla ilgili tüm bağlantılar (dış ve arka taraf-sunucu bağlantıları da dahil olmak üzere) için TLS kullanıldığı veya bu bağlantıların güvensiz veya şifrelenmemiş protokollere dönüştürülemediğini doğrulayın. En güçlü alternatifin tercih edilen algoritma olduğudan emin olunmalıdır.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1

10.11	HTTP Strict Transport Security başlıklarının tüm istekler ve tüm alt domainler için uygulandığını doğrulayın. Örneğin: Strict-Transport-Security: max-age=15724800; includeSubdomains	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
10.13	Trafiği kaydeden pasif saldırganları etkisiz hale getirmek için ileri gizlilik (forward secrecy) şifrelemesi kullanılmalıdır.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
V10.14	Uygun sertifika silme - Online Certificate Status Protokol (OCSP) gibi-yöntemlerinin etkinleştirildiği ve yapılandırıldığını doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
V10.15	Sertifika otoritesinin kök ve ara sertifikaları da dahil olmak üzere tüm sertifika hiyerarşisi boyunca yalnızca güçlü algoritma, şifreleme ve protokollerin kullanıldığını doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
V10.16	TLS ayarlarının güncel en iyi uygulama deneyimleri ile, özellikle ortak konfigürasyonlar, şifrelemeler ve güvensiz hale gelen algoritmalar ile eşgüdümlü olduğunu doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
11.1	Uygulamanın sadece gerekli olduğu tanımlanan HTTP istek metodlarını - GET, POST gibi - kabul ettiği ve kullanılmayan metodların (örneğin TRACE, PUT ve DELETE) kesin olarak engellendiğini doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.2	HTTP cevaplarının güvenli karakter seti belirten içerik tipi başlığına (örneğin , UTF-8, ISO 8859-1) sahip olduğunu doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.5	HTTP başlıklarının veya herhangi bir HTTP cevabı bölümünün sistem bileşenleri hakkında detaylı sürüm bilgisi ifşa etmediğini doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.6	Tüm API cevaplarının X-Content-Type-Options: nosniff ve Content-Disposition: attachment; filename="api.json" (veya içerik tipine uygun başka dosya adı) başlıklarını içerdiğini doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.7	Content Security Policy V2'nin (CSP) satıriçi Javascript kullanımını devredışı bıraktığı veya satıriçi Javacript'I CSP nonce veya özetleme ile bütünlük kontrolü sağladığını doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.8	X-XSS-Protection: 1; mode=block başlığının cevaplara konulduğunu doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1

16.1	URL yönlendirmenin yalnızca beyaz listedeki hedeflere izin verdiğini veya potansiyel olarak güvenilmeyen içeriklere yönlendirilirken uyarı gösterildiğini doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.2	Uygulamaya gönderilen güvensiz dosya verilerinin; dizin gezinimi, yerel dosya içerme, dosya mime tipi ve işletim sistemi komut çalıştırma gibi zafiyetlere karşı korunmak için doğrudan dosya girişi/çıkış komutları ile kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.3	Güvenilmeyen kaynaklardan edinilen dosyaların beklenen tipte olduğunun doğrulandığını ve bilinen zararlı içeriğe sahip dosyaların yüklenmesinin engellenmesi için antiviruslerce tarandığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.4	Uzak/yerel dosya katma (RFI/LFI) zafiyetlerini engellemek için güvenilmeyen verinin katma, sınıf yükleme veya yansıtma yetenekleri ile kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.5	Uzaktan zararlı içeriklerden korunmak için, güvenilmeyen verinin Cross-Origin Resource Sharing (CORS) isteklerinde kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.8	Uygulama kodunun güvenilmeyen kaynaklardan edinilerek yüklenen verileri çalıştırmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.9	Flash, Active-X, Silverlight, NACL, istemci taraflı Java veya W3C web tarayıcı standartlarınca doğal olarak desteklenmeyen istemci taraflı teknolojileri kullanmayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
17.1	UDID veya IMEI gibi cihaz üzerinde depolanan ve diğer uygulamalar tarafından da elde edilebilen ID değerlerinin kimlik doğrulama anahtarları olarak kullanılmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.2	Mobil uygulamanın hassas verileri potansiyel olarak cihazda bulunan şifrelenmemiş paylaşılan kaynaklarda (SD kart veya paylaşılan klasörler gibi) depolamadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.3	Hassas verinin cihaz üzerinde korunmasız bir şekilde - anahtar zincirleri gibi sistem korumalı alanlarda bile - depolanmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1

17.7	Uygulamaya hassas kodun bulunduğu alanın hafızada tahmin edilebilir olmadığını (ASLR gibi) doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.9	Uygulamanın aynı cihazdaki diğer uygulamaların istismar etmesi için hassas aktiviteleri, intent'leri ve içerik sağlayıcıları dışarı sunmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.11	Uygulamanın dışarı açılan aktivitelerinin, intent'lerinin, içerik sağlayıcılarının vb. tüm girdileri doğruladığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
18.1	İstemci ve sunucu arasında aynı yazı kodlama stili kullanıldığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.2	Web Servis Uygulaması içerisindeki yönetim ve idare fonksiyonlarına erişimin yalnızca web servisi yöneticilerine kısıtlandığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.3	Girdileri kabul etmeden önce XML veya JSON şemalarının var olduğu ve onaylandığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.4	Tüm girdilerin uygun boyutta sınırlandırıldığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.5	SOPA tabanlı web servislerinin minimum olarak Web Services-Interoperability (WS-I) Basic Profile ile uyumlu olduğunu doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.6	Oturum tabanlı kimlik denetimi ve yetkilendirme kullanıldığını doğrulayın. Bölüm 2,3 ve 4 detaylı yok gösterici olarak kullanılmalıdır. Sabit "API anahtarları" ve benzeri kullanımlardan sakınılmalıdır.	V18: Web servisleri doğrulama gereksinimleri	1
18.7	REST servisinin Cross-Site Request Forgery ataklarına karşı korumalı olduğunu doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
19.1	Tüm bileşenlerin güncel güvenlik konfigürasyonları ve versiyonları ile birlikte güncel olduğunu doğrulayın. Bu işlem, gereksiz örnek uygulamalar, platform dokümantasyonu ve varsayılan veya örnek kullanıcıların kaldırılmasını da içermelidir.	V19. Yapılandırma	1

EK-1b: ASVS Seviye 2 Kontrol Noktaları

ID	ADI	KATEGORİSİ	Seviye
1.1	Tüm uygulama bileşenlerinin	V1: Mimari, tasarım ve tehdit modellemesi	1

	tanımlandığını ve gerekli olduğunu doğrulayın.		
1.2	Kütüphane, modül ve dış sistemler gibi uygulamanın parçası olmayan ama uygulamaların güvendiği tüm bileşenlerin tanımlandığını doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
1.3	Uygulama için üst seviye mimarinin tanımlandığı nı doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
1.7	Tüm güvenlik kontrollerinin - harici güvenlik hizmetlerini çağıran kütüphaneler de dâhil- merkezi olarak uygulandığını doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
1.8	Bileşenlerin birbirlerinden ağ ayrıştırması, firewall kuralları veya bulut tabanlı güvenlik önlemleri gibi güvenlik kontrolleri ile ayrıştırıldığını doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
1.9	Güvenlik kararlarının güvenilen sistemler üzerine zorlanabilecek şekilde, uygulamanın veri, kontrol ve gösterim katmanları arasında açık bir ayrım olduğunu doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
1.10	Hassas iş süreçleri, gizli anahtarlar veya diğer önemli bilgilerin istemci tarafındaki kod içerisinde bulunmadığını doğrulayın.	V1: Mimari, tasarım ve tehdit modellemesi	2
2.1	Dışarı açık olanlar dışında tüm sayfa ve kaynakların varsayılan olarak kimlik denetimi gerektirdiğini doğrulayın. (Tümden aracılık prensibi)	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.2	Tüm parola alanlarının kullanıcı girişlerini ekrana yansıtmadığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.4	Tüm kimlik denetimi kontrollerinin sunucu tarafında yapılmaya zorlandığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.6	Tüm kimlik denetimi kontrollerinin bir hata surumunda saldırganın giriş yapmasına olanak	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1

	sağlamayacak şekilde yapılandırıldığını doğrulayın.		
2.7	Tüm parola alanlarının yüksek karmaşıklıktaki/uzun parolaları girişini engellemediğini/kullanmayı önerdiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.8	Hesaba tekrar erişime olanak tanıyan tüm hesap kimlik denetimi fonksiyonlarının (profil güncelleme, parola unutma, kilitli/kayıp token, yardım masası veya IVR gibi) en az birincil kimlik denetimi mekanizması kadar saldırılara karşı dayanıklı olduğunu doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.9	Parola değiştirme işlevinin eski parola, yeni parola ve parola doğrulamayı içerdiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.12	Tüm şüpheli kimlik denetimi kararlarının kayıt altına alındığını doğrulayın. Bu kayıt, güvenlik soruşturmaları için gerekli olan ilgili üst verileri istek ile birlikte içermelidir.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.13	Tüm hesap parolaları için yeterli sağlamlıkta şifreleme kullanıldığı ve bu şifrelemenin kaba kuvvet saldırılarına karşı dayanaklı olduğunu doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.16	Kimlik bilgilerinin uygun bir şifreli kanal üzerinden aktarıldığını ve kullanıcıların kimlik bilgilerini girmesi gereken tüm sayfaların/fonksiyonların bu şifreli kanaldan aktarıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.17	Unutulmuş parola ve diğer kurtarma yollarının hâlihazırda kullanılan parolayı açığa çıkarmadığını ve yeni	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1

	oluşturulan parolanın kullanıcıya açık yazı olarak iletilmediğini doğrulayın.		
2.18	Kullanıcı girişi, parola sıfırlama veya hesap unutma işlevleri üzerinden bilgi dökümünün mümkün olmadığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.19	Uygulama çerçevesi veya uygulama tarafından kullanılan bileşenlerin hiçbirisinde varsayılan parola kullanılmadığını (örneğin "admin/password") doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.20	Kimlik doğrulamaya yönelik kaba kuvvet saldırıları veya hizmet dışı bırakma saldırılarını engellemek amacı ile istek kısıtlama mekanizmaları konumlandırıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.21	Dışarıdan uygulamadaki servislere erişim için kullanılan tüm kimlik denetimi bilgilerinin şifrelendiğini ve korumalı bir alanda saklandığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.22	Unutulmuş parola ve diğer kurtarma yollarının soft token, mobil push veya çevrimdışı kurtarma mekanizması kullandığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.23	Hesap kilitleme işleminin birbirinden bağımsız olarak yumuşak ve sert olarak ayrıştırıldığını doğrulayın. Bir hesap kaba kuvvet saldırısı sonucu yumuşak olarak kilitlenirse, bu durum sert kilitlemeyi sıfırlamamalıdır.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.24	Bilgi tabanlı sorular ("gizli sorular" olarak da bilinir) gerekli ise, bu soruların uygulamayı koruyacak yeterlilikte güçlü olduğunu doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1

2.25	Sistemin ayarlanabilir sayıda önceden kullanılan parola kullanımını yasaklayabildiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.26	Uygulama için hassas ve yüksek risk düzeyine sahip her bir işlem için tekrar kimlik denetimi, basamaklı veya ayarlanabilen kimlik denetimi, iki faktörlü kimlik denetimi veya işlem imzalama gerektiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.27	Ortak seçilen ve zayıf parola kullanımını engelleyecek önlemlerin konumlandırıldığını doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.30	Bir uygulama kullanıcılarının kimlik doğrulaması yapmasına izin veriyor ise, onların kanıtlanmış güvenli bir kimlik doğrulaması mekanizması kullandığı onaylanmalıdır.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
2.31	Bir uygulama, kullanıcılarının kimlik doğrulaması yapmasına izin veriyor ise, kullanıcı adı ve parola sızmalarına karşı iki faktörlü kimlik doğrulama veya diğer güçlü kimlik doğrulama korumaları kullanılabildiğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	2
2.32	Yönetimsel ara yüzlerin güvensiz taraflarca erişilemediğini doğrulayın.	V2: Kimlik Doğrulaması Doğrulama Gereksinimleri	1
3.1	Özel geliştirilmiş bir oturum yönetici kullanılmadığı veya geliştirilen oturum yöneticisinin genel oturum yönetimi ataklarına karşı dirençli olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.2	Kullanıcı oturumu kapattığında oturumun geçersiz hale getirildiğini doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1

3.3	Belirtilen bir zaman süresince işlem yapılmadığında oturumun sonlandırıldığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.5	Kimlik doğrulama gerektiren tüm sayfaların kolay ve görünür biçimde oturum sonlandırma işlevine sahip olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.6	Oturum anahtarının URL, hata mesajları ve loglarda gösterilmediğini doğrulayın. Bu aynı zamanda uygulamanın oturum çerezi ile URL yeniden yazmayı desteklemediğini de doğrular.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.7	Tüm başarılı kimlik denetimi ve yeniden girişlerin yeni oturum ve oturum anahtarı oluşturduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.10	Sadece uygulama tarafından oluşturulan oturum anahtarlarının uygulama tarafından aktif olarak tanındığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	2
3.11	Oturum anahtarlarının yeterince uzun, rastgele ve tekil olduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.12	Oturum anahtarı değerini tutan çerez yolunun uygulamaya kısıtlı olacak şekilde ayarlandığı ve kimlik doğrulama oturum anahtarlarına ait "HttpOnly" ve "secure" niteliklerinin ayarlandığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.16	Uygulamanın eş zamanlı oturum sayısını sınırladığını doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
3.17	Her kullanıcı için aktif oturum listesinin hesap profili veya benzeri alanda gösterildiğini doğrulayın. Kullanıcı herhangi bir aktif oturumu sonlandırabilmelidir.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1

3.18	Kullanıcı parolasını başarılı bir şekilde değiştirdikten sonra aktif olan diğer tüm oturumları sonlandırması için seçenek sunulduğunu doğrulayın.	V3: Oturum Yönetimi Doğrulama Gereksinimleri	1
4.1	En az yetki prensibinin varlığını doğrulayın. - kullanıcılar yalnızca kendilerine ait olan yetkilendirmenin izin verdiği fonksiyonlara, veri dosyalarına, URL'lere, kontrollere, hizmetlere ve diğer kaynaklara erişebilmelidir. Bu, kandırma ve yetki yükseltme saldırılarına karşı koruma anlamına gelir.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.4	Her bir kullanıcının sadece yetkilendirildiği nesne veya verilere ulaşabilecek şekilde hassas kayıtların korunduğunu doğrulayın. (örneğin, kullanıcı parametreyi değiştirerek başka hesaplara ait bilgileri görememelidir.)	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.5	Kasten istenmediği takdirde dizin listelemesi işlevinin kapalı olduğunu doğrulayın. Ek olarak uygulamalar, dosya veya klasör üst verisi sızdıran thumbs.db, .DS_Store, .git veya .svn gibi dosya ve klasörlere izin vermemelidir.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.8	Erişim kontrolünün güvenli bir şekilde hata oluşturduğunu doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.9	Sunum katmanında uygulanan erişim kontrolü kurallarının sunucu tarafında da uygulandığını doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.10	Erişim kontrolü için kullanılan tüm kullanıcı ve veri nitelikleri ile politika bilgilerinin özel olarak yetkilendirilmedikçe sın	V4: Erişim Kontrolü Doğrulama Gereksinimleri	2

	kullanıcılar tarafından değiştirilemediğini doğrulayın.		
4.12	Tüm erişim kontrol kararları kayıt altına alınabildiğini ve tüm başarısız kararlar kayıt altına alındığını doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	2
4.13	Uygulama veya kütüphanenin CSRF engelleyici token veya benzeri işlem koruma mekanizmasına sahip olduğunu doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
4.14	Sistemin güvenli işlev, kaynak veya verilere toplu veya sürekli erişime karşı korumalı olduğunu doğrulayın. Örneğin bir yönetici kaynağın kullanılmasını kısıtlayabilmeli, böylelikle bir kullanıcının tüm veritabanını bozmaması için kullanıcıya bir saat içerisinde belirli bir sayıda kayıt güncelleme sınırı getirilebilmelidir.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	2
4.15	Uygulamanın, dolandırıcılığı engellemek amacıyla uygulama riskine ve geçmişteki dolandırıcılık örneklerine bakarak, düşük değerli sistemler için ek yetkilendirmeye (basamaklı veya ayarlanabilen kimlik denetimi) sahip olduğu ve/veya yüksek değerli uygulamalar için yetki ayrılığı olduğunu doğrulayın.	V4: Erişim Kontrolü Doğrulama Gereksinimleri	2
4.16	Uygulamanın bağlam duyarlı yetkilendirmeyi doğru bir şekilde - parametre değiştirerek yetkisiz manipülasyon yapılmaması - uyguladığını doğrulayın	V4: Erişim Kontrolü Doğrulama Gereksinimleri	1
5.1	Çalışma ortamının tampon bellek taşmalarına elverişli olmadığı veya güvenlik kontrollerinin tampon bellek	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1

	taşmalarını engellediğini doğrulayın.		
5.3	İstek reddine sebep olan sunucu tarafı girdi doğrulama hatası sonuçlarının kayıt altına alındığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.5	Girdi doğrulama rutinlerinin sunucu tarafında uygulandığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.10	Tüm SQL sorguları, HQL, OSQL, NOSQL ve kayıtlı yordamların, kayıtlı yordamların çağırılmasının, hazır ifadeler veya parametrik sorgular kullanılarak yapıldığını, böylelikle SQL sokuşturmaya karşı dayanıklı olduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.11	Uygulamanın LDAP sokuşturmaya karşı dayanıklı olduğu veya güvenlik kontrollerinin LDAP sokuşturmayı engellediğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.12	Uygulamanın işletim sistemi komut sokuşturmaya karşı dayanıklı olduğu veya güvenlik kontrollerinin işletim sistemi komut sokuşturmayı engellediğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.13	Uygulamanın içerikte bir dosyaya yol kullanıldığı durumlarda Uzak Dosya Katma (RFI) veya Yerel Dosya Katma (LFI) zafiyetleri barındırmadığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.14	Uygulamanın genel XML saldırılarına - Xpath sorgu değiştirmesi, XML Dış Varlık ve XML sokuşturma - karşı dayanıklı olduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.15	HTML içeriğine veya diğer web tabanlı kodlara yerleştirilen yazı	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1

	değişkenlerinin düzgün bir şekilde elle kodlanarak veya şablonlar vasıtasıyla otomatik olarak kodlanarak Yansıtılmış, Kayıtlı ve DOM tabanlı Sitelerarası Betik Çalıştırma (XSS) saldırılarına karşı dayanıklı olduğunu doğrulayın		
5.16	Uygulama çerçevesi gelen isteklerden modele otomatik toplu parametre atamasına (ayrıca otomatik değişken bağlama olarak da adlandırılır) izin veriyor ise, güvenliği hassas olan "hesapTutarı", "rol" veya "parola" gibi alanların zararlı otomatik bağlamadan korunduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.17	Uygulamanın HTTP parametre kirletme saldırılarına karşı -özellikle uygulama çerçevesinin istek parametreleri kaynağı hakkında ayrım yapmadığı (GET, POST, çerezler, başlıklar, çevre değişkeneri vs.) - korumalı olduğunu doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.18	Sunucu tarafı doğrulamaya ek olarak kullanıcı tarafı doğrulamanın da kullanıldığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.19	Sadece HTML form alanları için değil, REST çağrıları, sorgu parametreleri, HTTP başlıkları, çerezler, yığın komut dosyaları, RSS beslemeleri gibi noktalar için de gri liste (bilinen kötü girdileri silme) veya kötü girdileri reddetme (kara liste) yerine positif doğrulama (beyaz liste) kullanıldığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.20	Yapılı verinin güçlü tip olarak yapılandırıldığı ve izin verilen karakterler, uzunluk ve örgüsel olarak	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2

	onaylandığını doğrulayın. (örneğin kredi kartı numaraları veya telefon, veya ilişkili iki alanın mantıklı olması - posta kosu ile bölgenin eşleşmesi gibi-)		
5.21	Yapısız verinin genel güvenlik önlemlerini zorlayacak şekilde - izin verilen karakterler, uzunluk ve potansiyel olarak zarar verebilecek karakterlerin (örneğin Unicode karakter barındıran isimler veya kesme işareti - ねこ veya O'Hara gibi -) dönüştürüldüğü / temizlendiğini doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.22	WYSIWYG editorler veya benzeri kaynaklardan gelen güvensiz HTML içerikleri HTML arındırıcılar ile arındırılmalı ve girdi doğrulama ile kodlama görevlerinin düzgün bir şekilde ele alındığından emin olunmaldıır.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	1
5.23	Otomatik dönüştüren şablon teknolojileri için, UI dönüştürmesi devre dışı bırakılmış ise, HTML arındırmanın devreye alındığından emin olunmalıdır.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.24	Bir DOM içeriğinden diğerine veri taşınacağı zaman val ve.innerText gibi güvenli JavaScript metodlarının kullanıldığını doğrulayın.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.25	Tarayıcılarda JSON çözümlemesi yapılırken JSON. parse kullanıldığını doğrulayın. İstemcide JSON çözümleme için eval() kullanılmamalıdır.	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2
5.26	Oturum sonlandırıldıktan sonra yetkilendirilmiş verinin istemci depolamasından -tarayıcı	V5: Zararlı Girdi Kontrolü Doğrulama Gereksinimleri	2

	DOM'u vb. - temizlendiğini doğrulayın.		
7.2	Kriptografik modüllerin güvenli bir şekilde hata oluşturdukları ve hataların "oracle padding" gibi zafiyetlere yol açmadığını doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	1
7.6	Rastgele sayılar, rastgele dosya isimleri, rastgele GUID'ler ve random karakter dizilerinin - saldırgan tarafından tamin edilmemesi bekleniyor ise - kriptografik modüllerin onaylanmış rastgele sayı üreteci tarafından oluşturulduğunu doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	2
7.7	Uygulama tarafından kullanılan kriptografik algoritmaların FIPS140-2 veya eşdeğer bir standart tarafından geçerli kabul edildiğini doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	1
7.9	Kriptografik anahtarların nasıl yönetileceğine dair (oluşturma, dağıtım, iptal ve zaman dolması) dair kesin bir politika olduğunu doğrulayın. Anahtar yaşam döngüsünün uygun bir şekilde uygulandığını doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	2
7.12	Kişisel veriler şifreli olarak saklanmalı ve iletilirken güvenlik kanallar üzerinden aktarılmalıdır.	V7: Sabit kriptografi doğrulama gereksinimleri	2
7.13	Anahtar ve şifreler yok edildiğinde -mümkünse- sıfırlandığını doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	2
7.14	Tüm anahtar ve parolaların değiştirilebilir olduğu, uygulamanın kurulum zamanında oluşturulduğu veya değiştirildiğini doğrulayın.	V7: Sabit kriptografi doğrulama gereksinimleri	2
8.1	Uygulamanın saldırgana yardımcı olabilecek şekilde oturum anahtarı, yazılım/çerçeve versiyonu ve kişisel bilgileri sızdıran	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	1

	hata mesajları veya yığın dökümü oluşturmadığını doğrulayın.		
8.2	Güvenlik kontrollerindeki hata ele alış mantığının varsayılan olarak erişimi engellediğini doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
8.3	Güvenlik kayıt kontrollerinin güvenlik ilişkili başarılı ve kısmen hatalı olayları kaydetme yeteneği olduğunu doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
8.4	Bir olay oluştuğunda her bir kaydın zamansal olarak soruşturma yapmaya izin verecek bilgileri içerdiğini doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
8.6	Güvenlik kayıtlarının yetkisiz erişim ve değişimden korunduğunu doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
8.7	Uygulamanın mahremiyet yasaları ve düzenlemeleri ile tanımlanan hassas verileri, risk değerlendirmesi sonucu tanımlanan organizasyonel hassas verileri veya kullanıcı oturum anahtarı, parolalar, özetler veya API anahtarları gibi saldırganlara yardımcı olabilecek kimlik doğrulama verilerini kayıt altına almadığını doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
8.10	Denetim kayıtları veya benzer yöntemlerin önemli işlemler için inkar edilemezliği sağladığını doğrulayın.	V8: Hata yönetimi ve loglama doğrulama gereksinimleri	2
9.1	Hassas veri içeren tüm form alanlarının otomatik tamamlamayı da içerecek şekilde istemci tarafında depolanmasının engellendiğini doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	1
9.3	Tüm hassas verilerin HTTP mesaj içeriği ve başlıklarında sunucuya gönderildiğini doğrulayın. (Hassas verileri göndermek	V9: Veri koruması doğrulama gereksinimleri	1

	için URL parametreleri kullanılmamalıdır)		
9.4	Uygulamadaki her riskli alan için uygun bir önbellek engelleyici başlığın ayarlandığını doğrulayın. Örneğin: Expires: Tue, 03 Jul 2001 06:00:00 GMTLast-Modified: {now} GMTCache-Control: no-store, no-cache, must-revalidate, max-age=0Cache-Control: post-check=0, pre-check=0Pragma: no-cache	V9: Veri koruması doğrulama gereksinimleri	1
9.5	Sunucu tarafında hassas verilerin önbelleklenmiş ve geçici kopyalarının yetkisiz erişimden korunduğu veya yetkilendirilmiş kullanıcının hassas veriye erişiminden sonra temizlendiği/geçersiz hale getirildiğini doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	2
9.7	Uygulamanın isteklerdeki parametre sayılarını - gizli alanlar, Ajax değişkenleri, çerezler ve başlık değerleri gibi- minimize ettiğini doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	2
9.9	İstemci taraflı depolamada - HTML5 yerel depolama, oturum depolama, IndexedDB, genel çerezler veya Flash çerezleri gibi- hassas veri ve kişisel verilerin tutulmadığını doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	1
9.10	Veri ilişkili veri koruma direktifleri altında toplanmışsa veya erişimlerin kayıt altına alınması gerekiyorsa, hassas verilere erişimin kaydedildiğini doğrulayın.	V9: Veri koruması doğrulama gereksinimleri	2
9.11	Hassas verilerin ihtiyaç biter bitmez hafızadan temizlendiği ve çerçeve/kütüphane/işletim sisteminde desteklenen uygun fonksiyon ve	V9: Veri koruması doğrulama gereksinimleri	2

	tekniklerle işlendiğini doğrulayın.		
10.1	Her bir Transport Layer Security (TLS) sunucu sertifikasına güvenilir bir sertifika otoritesinden (CA) yol oluşturulabildiğini ve her sunucu sertifikasının geçerli olduğunu doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
10.3	Kimlik denetimi yapılan veya hassas veri veya fonksiyonlarla ilgili tüm bağlantılar (dış ve arka taraf-sunucu bağlantıları da dahil olmak üzere) için TLS kullanıldığı veya bu bağlantıların güvensiz veya şifrelenmemiş protokollere dönüştürülemediğini doğrulayın. En güçlü alternatifin tercih edilen algoritma olduğudan emin olunmalıdır.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
10.6	Hassas bilgi ve fonksiyonlar ile ilgili tüm dış bağlantıların kimlik doğrulaması yaptığını doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	2
10.11	HTTP Strict Transport Security başlıklarının tüm istekler ve tüm alt domainler için uygulandığını doğrulayın. Örneğin: Strict-Transport-Security: max-age=15724800; includeSubdomains	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
10.13	Trafiği kaydeden pasif saldırganları etkisiz hale getirmek için ileri gizlilik (forward secrecy) şifrelemesi kullanılmalıdır.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
V10.14	Uygun sertifika silme - Online Certificate Status Protokol (OCSP) gibi- yöntemlerinin etkinleştirildiği ve yapılandırıldığını doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
V10.15	Sertifika otoritesinin kök ve ara sertifikaları da dâhil olmak üzere tüm sertifika	V10: Haberleşme güvenliği doğrulama gereksinimleri	1

	hiyerarşisi boyunca yalnızca güçlü algoritma, şifreleme ve protokollerin kullanıldığını doğrulayın.		
V10.16	TLS ayarlarının güncel en iyi uygulama deneyimleri ile özellikle ortak konfigürasyonlar, şifrelemeler ve güvensiz hale gelen algoritmalar ile eşgüdümlü olduğunu doğrulayın.	V10: Haberleşme güvenliği doğrulama gereksinimleri	1
11.1	Uygulamanın sadece gerekli olduğu tanımlanan HTTP istek metodlarını - GET, POST gibi - kabul ettiği ve kullanılmayan metodların (örneğin TRACE, PUT ve DELETE) kesin olarak engellendiğini doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.2	HTTP cevaplarının güvenli karakter seti belirten içerik tipi başlığına (örneğin UTF-8, ISO 8859-1) sahip olduğunu doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.3	Güvenilen proxy veya SSO cihazlarından eklenen HTTP başlıklarına - örneğin bearer token- uygulama tarafından kimlik denetimi yapıldığını doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	2
11.4	İçeriğin 3. taraf X-Frame içerisinde görüntülenmemesi gereken siteler için Content Security Policy V2 (CSP) kullanıldığını doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	2
11.5	HTTP başlıklarının veya herhangi bir HTTP cevabı bölümünün sistem bileşenleri hakkında detaylı sürüm bilgisi ifşa etmediğini doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.6	Tüm API cevaplarının X-Content-Type-Options: nosniff ve Content-Disposition: attachment; filename="api.json" (veya içerik tipine uygun başka	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1

	dosya adı) başlıklarını içerdiğini doğrulayın.		
11.7	Content Security Policy V2'nin (CSP) satıriçi Javascript kullanımını devredışı bıraktığı veya satıriçi Javacript'I CSP nonce veya özetleme ile bütünlük kontrolü sağladığını doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
11.8	X-XSS-Protection: 1; mode=block başlığının cevaplara konulduğunu doğrulayın.	V11: HTTP güvenlik yapılandırması doğrulama gereksinimleri	1
V15.1	Uygulamanın tüm adımları gerçekçi insan zamanında işlenen sıralı adımlarla yapılan iş mantık akışlarını işleme aldığı, sırası bozulmuş, atlanmış adımları olan diğer kullanıcılardan adım içeren veya çok hızlı gönderilen hareketleri işleme almadığını doğrulayın.	V15: İş mantığı doğrulama gereksinimleri	2
V15.2	Uygulamanın iş limitlerine sahip olduğu ve kullanıcılar için doğru bir şekilde uygulandığı, otomatize veya sıradışı saldırılara karşı ayarlanabilir uyarı verdiğini veya otomatikleştirilmiş aksiyon aldığını doğrulayın.	V15: İş mantığı doğrulama gereksinimleri	2
16.1	URL yönlendirmenin yalnızca beyaz listedeki hedeflere izin verdiğini veya potansiyel olarak güvenilmeyen içeriklere yönlendirilirken uyarı gösterildiğini doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.2	Uygulamaya gönderilen güvensiz dosya verilerinin; dizin gezinimi, yerel dosya içerme, dosya mime tipi ve işletim sistemi komut çalıştırma gibi zafiyetlere karşı korunmak için doğrudan dosya girişi/çıkış komutları ile kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1

16.3	Güvenilmeyen kaynaklardan edinilen dosyaların beklenen tipte olduğunun doğrulandığını ve bilinen zararlı içeriğe sahip dosyaların yüklenmesinin engellenmesi için antiviruslerce tarandığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.4	Uzak/yerel dosya katma (RFI/LFI) zafiyetlerini engellemek için güvenilmeyen verinin katma, sınıf yükleme veya yansıtma yetenekleri ile kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.5	Uzaktan zararlı içeriklerden korunmak için, güvenilmeyen verinin Cross-Origin Resource Sharing (CORS) isteklerinde kullanılmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.6	Güvenilmeyen kaynaklardan edinilen dosyaların web kök dizini dışında, sınırlı izinlerle, tercihen güçlü doğrulama ile depolandığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	2
16.7	Web veya uygulama sunucularının, varsayılan olarak web veya uygulama sunucuları dışındaki kaynak ve sistemlere erişim engelli olarak yapılandırıldığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	2
16.8	Uygulama kodunun güvenilmeyen kaynaklardan edinilerek yüklenen verileri çalıştırmadığını doğrulayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1
16.9	Flash, Active-X, Silverlight, NACL, istemci taraflı Java veya W3C web tarayıcı satandartlarınca doğal oalrak desteklenmeyen istemci taraflı teknolojileri kullanmayın.	V16: Dosya ve kaynakları doğrulama gereksinimleri	1

17.1	UDID veya IMEI gibi cihaz üzerinde depolanan ve diğer uygulamalar tarafından da elde edilebilen ID değerlerinin kimlik doğrulama anahtarları olarak kullanılmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.2	Mobil uygulamanın hassas verileri potansiyel olarak cihazda bulunan şifrelenmemiş paylaşılan kaynaklarda (SD kart veya paylaşılan klasörler gibi) depolamadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.3	Hassas verinin cihaz üzerinde korunmasız bir şekilde - anahtar zincirleri gibi sistem korumalı alanlarda bile - depolanmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.4	Gizli anahtarlar, API anahtarları veya parolaların mobil uygulamalarda dinamik olarak oluşturulduğunu doğrulayın.	V17: Mobil doğrulama gereksinimleri	2
17.5	Mobil uygulamanın hassas verileri sızdırmayı engellediğini doğrulayın.	V17: Mobil doğrulama gereksinimleri	2
17.6	Uygulamanın gereken çalışabilirlik ve kaynaklar için minimum düzeyde hak talebinde bulunduğunu doğrulayın.	V17: Mobil doğrulama gereksinimleri	2
17.7	Uygulamaya hassas kodun bulunduğu alanın hafızada tahmin edilebilir olmadığını (ASLR gibi) doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.9	Uygulamanın aynı cihazdaki diğer uygulamaların istismar etmesi için hassas aktiviteleri, intent'leri ve içerik sağlayıcıları dışarı sunmadığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1
17.11	Uygulamanın dışarı açılan aktivitelerinin, intent'lerinin, içerik sağlayıcılarının vb. tüm girdileri doğruladığını doğrulayın.	V17: Mobil doğrulama gereksinimleri	1

18.1	İstemci ve sunucu arasında aynı yazı kodlama stili kullanıldığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.2	Web Servis Uygulaması içerisindeki yönetim ve idare fonksiyonlarına erişimin yalnızca web servisi yöneticilerine kısıtlandığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.3	Girdileri kabul etmeden önce XML veya JSON şemalarının var olduğu ve onaylandığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.4	Tüm girdilerin uygun boyutta sınırlandırıldığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.5	SOPA tabanlı web servislerinin minimum olarak Web Services-Interoperability (WS-I) Basic Profile ile uyumlu olduğunu doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.6	Oturum tabanlı kimlik denetimi ve yetkilendirme kullanıldığını doğrulayın. Bölüm 2,3 ve 4 detaylı yok gösterici olarak kullanılmalıdır. Sabit "API anahtarları" ve benzeri kullanımlardan sakınılmalıdır.	V18: Web servisleri doğrulama gereksinimleri	1
18.7	REST servisinin Cross-Site Request Forgery ataklarına karşı korumalı olduğunu doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	1
18.8	REST servisinin gelen Content-Type değerlerinin kesin bir biçimde beklenen biçimde -application/xml veya application/json gibi- olduğunun kontrol ettiğini doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	2
18.9	İstemci ve servis arasında güvenli aktarımdan emin olmak için mesaj içerik kısmının imzalı olduğunu doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	2
18.10	Alternatif ve daha az güvenli bir erişim yolunun olmadığını doğrulayın.	V18: Web servisleri doğrulama gereksinimleri	2

19.1	Tüm bileşenlerin güncel güvenlik konfigürasyonları ve versiyonları ile birlikte güncel olduğunu doğrulayın. Bu işlem, gereksiz örnek uygulamalar, platform dökümantasyonu ve varsayılan veya örnek kullanıcıların kaldırılmasını da içermelidir.	V19. Yapılandırma	1
19.2	Bileşenler arası haberleşmeler - uygulama sunucusu ve veritabanı sunucusu arasında gibi - özellikle farklı barındırıcılar veya sistemlerde iseler, şifreli olmalıdır.	V19. Yapılandırma	2
19.3	Bileşenler arası haberleşmeler - uygulama sunucusu ve veritabanı sunucusu arasında gibi - gerekli olan en düşük kullanıcı hakları ile kimlik doğrulaması yapılarak gerçekleştirilmelidir.	V19. Yapılandırma	2
19.4	Uygulama dağıtımlarının, saldırganların diğer uygulamalara saldırmasının engelleyecek ya da geciktirecek şekilde yeterince kum havuzuna alındığını, barındırıcılarda tutulduğunu veya izole edildiğini doğrulayın.	V19. Yapılandırma	2
19.5	Uygulama yapım ve dağıtım süreçlerinin güvenli yöntemlerle yapıldığını doğrulayın.	V19. Yapılandırma	2