OWASP

The Open Web Application Security Project

Uygulama Güvenliği Doğrulama Standardı (2014)

Önsöz

Standardın bu sürümü ile kabul edilebilirliğinin artırılması hedeflenmiştir.

Böyle bir standart oluşturmanın en büyük zorluklarından birisi, iki tane birbirinden çok ayrı birimi memnun edebilmeye çalışmaktır: organizasyonlarda yazılım güvenliği programını yürüten birimler ve uygulamaların doğrulamalarını yapan profesyonel yazılım güvenliği uzmanları. Her ne kadar iki birim de ortak olarak endüstri standardında bir uygulama doğrulama hedeflese de, ikisi de farklı koşullar altında çalışmaktadır. Örneğin, ASVS 2009 standardının en çok dile getirilen eleştirisi, otomatik taramaların bir seviye olarak sunulmasıydı. Birçok büyük organizasyon otomatik taramaları doğrulama hiyerarşisine bir giriş noktası olarak görmektedir ve bu yüzden bu konsept onlar için uygundur. Ancak güvenlik uzmanları yapılacak otomatik taramaların derinliğinin ve kapsamının, kullanılan araç ve yöntemlere bağlı olarak çok değişebileceğini ve bu yüzden standartta boşluklar olduğunu dile getirdiler. ASVS 2014 bu zorluğu aşma da esneklik sağlamak için hazırlanmıştır.

Benzer bir not olarak, bu standart sürümü ile genel olarak “Nasıl?” sorusundan çok “Ne?” sorusuna odaklanılması hedeflenmiştir. Bir önceki sürümde dinamik analiz, statik analiz, tehdit modelleme ve tasarım gözden geçirme gibi terimler üzerinde durulmuş olmasına karşın bu sürümde bu gibi terimlerin yer almadığı fark edilecektir. Bunların yerine bu dokümanda bir uygulamanın herhangi bir seviyeye erişmesi için ne gibi gereksinimlere sahip olması gerektiği üzerinde durulmuştur. Bu gereksinimlerin nasıl doğrulandığı, doğrulamayı yapan tarafa bırakılmıştır.

Bu standartları oluştururken karşılaştığımız diğer bir zorluk ise, tasarım ve kapsam için gerekli gereksinimlerin birbirinden keskin olarak nasıl ayrılması gerektiğidir. Bir önceki sürüm bu ayrımı tam olarak yapamamakta ve bu yüzden karışıklıklar oluşmaktadır. Bu sürümde Seviye 3 getirilerek, bu seviyede tasarım gereksinimleri ve detaylı doğrulama gereksinimleri keskin olarak birbirinden ayrılmıştır. Bunlara ek olarak, bu sürümde kapsamın daha detaylı olarak belirlenmesine imkan sunacak yeni (+) sembolü getirilmiştir. Bu sembol, doğrulama yapan kişinin üçüncü parti bileşenleri ve uygulama çatısını da doğrulamaya dahil ettiğini belirtmektedir.

Bu standart üzerinde de %100 anlaşma olmayacağı düşünülmektedir. Risk analizi incelenen ortama göre değişen ve subjektif olmakla beraber, bu yönleri dolayısıyla bu analizi standart hale getirmek gerçekten zor görünmektedir. Ancak tüm bunlara rağmen, bu sürümde son yapılan güncellemeler ile doğru bir yönde ilerlediğimizi düşünüyor ve giderek bu önemli endüstri standardındaki konseptleri genişletmeyi umuyoruz.

Teşekkür

2014 Sürümü
Proje Lideri: Sahba Kazerooni (Security Compass, http://www.securitycompass.com), Daniel Cuthbert (SensePost, http://www.sensepost.com/)

Baş Yazarlar: Andrew van der Stock, Sahba Kazerooni, Daniel Cuthbert, Krishna Raja

Değerlendiriler ve Katkı Sunanlar: Jerome Athias, Boy Baukema, Archangel Cuison, Sebastien Deleersnyder, Antonio Fontes, Evan Gaustad, Safuat Hamdy, Ari Kesäniemi, Scott Luc, Jim Manico, Mait Peekma, Pekka Sillanpää, Jeff Sergeant, Etienne Stalmans, Colin Watson, Dr Emin Tatli.

Ek olarak, uygulama güvenliği doğrulama topluluğuna ve güvenli web programlama ile ilgilenip istekli bir şekilde bu dokümana yardımcı olan herkese teşekkürlerimizi sunarız.

2014 Türkçe Çeviri
Yazarlar: OWASP-Türkiye, Ayhan Çakın, Adil Hafa, Can Demirel, Onur Karasalihoğlu, Fatih Ersınadım, Emin İslam Tatlı, Bünyamin Demir.

2009 Versiyonu
ASVS 2014 birçok yeni doğrulama gereksinimi içerse de, ilk aşamada orjinal Uygulama Güvenliği Doğrulama Standartı(ASVS)'nin oluşturulmasına katkıda bulunan aşağıdaki kişilere teşekkürlerimizi sunarız:

Mike Boberski, Jeff Williams, Dave Wichers, Pierre Parrend (OWASP Summer of Code), Andrew van der Stock, Nam Nguyen, John Martin, Gaurang Shah, Theodore Winograd, Stan Wisseman, Barry Boyd, Steve Coyle, Paul Douthit, Ken Huang, Dave Hausladen, Mandeep Khera Scott Matsumoto, John Steven, Stephen de Vries, Dan Cornell, Shouvik Bardhan, Dr. Sarbari Gupta, Eoin Keary, Richard Campbell, Matt Presson, Jeff LoSapio, Liz Fong, George Lawless, Dave van Stein, Terrie Diaz, Ketan Dilipkumar Vyas, Bedirhan Urgun, Dr. Thomas Braun, Colin Watson, Jeremiah Grossman.

Lisans ve Yayın Hakları

Giriş

OWASP Uygulama Güvenliği Doğrulama Standardı(ASVS)'nin asıl amacı, web uygulama güvenliği doğrulama prosedürlerinin uygulanması/gerçekleştirilmesi esnasında ortaya çıkan zorlukların/eksiklerin giderilmesi ve doğrulama kapsamının en iyi seviyede standart hale getirilmesidir.

OWASP (Open Web Application Security Project), kurumların güvenli uygulamalar geliştirmeleri, güvenli uygulamalar satın almaları ve uygulamaları güvenli bir şekilde sürdürmelerine yardımcı olmak amaçlarını benimsemiş açık bir topluluktur. OWASP'a ait tüm kaynaklar (araçlar, dokümanlar vb.), uygulama güvenliği alanı ile ilgilenen herkese açıktır. OWASP olarak, uygulama güvenliğine insan, süreç ve teknoloji problemi olarak yaklaşılması gerektiğini savunuyoruz, çünkü uygulama güvenliğindeki en etkin yaklaşımlar bu üç alandaki gelişmeleri de kapsayan yaklaşımlardır. Bize www.owasp.org adresinden erişebilirsiniz. OWASP ticari kaygı taşımayan yeni tip bir organizasyondur ve bu ticari bağımsızlık, uygulama güvenliği alanında tarafsız, daha pratik ve maliyetsiz bilgiyi sunmamızı sağlamaktadır. OWASP, hiçbir teknoloji şirketi ile ilişkili değildir ancak bilinçli olarak ticari güvenlik araçlarının kullanılmasını desteklemektedir. Birçok açık kaynak kodlu yazılım projeleri gibi, OWASP da açık kaynak kodlu olmak üzere birçok tipte materyal üretmektedir.

ASVS standartları, uygulamaların temel teknik güvenlik kontrollerinin yerine getirilmesine yardımcı olmayı amaçlarken aynı zamanda Siteler Arası Betik Çalıştırma(XSS) ve SQL Enjeksiyonu gibi kritik zafiyetlere karşı da bir koruma sağlamayı amaçlamaktadır. Bu standartlar, web uygulamaları güvenliğinde kabul edilebilir bir güven seviyesi oluşturmak için kullanılabilir.

Bu Standardın Kullanımı

ASVS standartları, müşteriler ve servis/araç sağlayıcı kuruluşlar tarafından iki taraflı olarak da kullanılabilir.

ASVS'nin aşağıdaki figürlerde belirtilen iki temel amacı vardır:

- Organizasyonların güvenli uygulamalar geliştirmeleri ve mevcut uygulamaları güvenli şekilde muhafaza etmeleri
- Müşteriler ve güvenlik araç/servis sağlayıcıları arasında öneri ve gereksinimlerin ortak bir payda çerçevesinde belirlenmesi

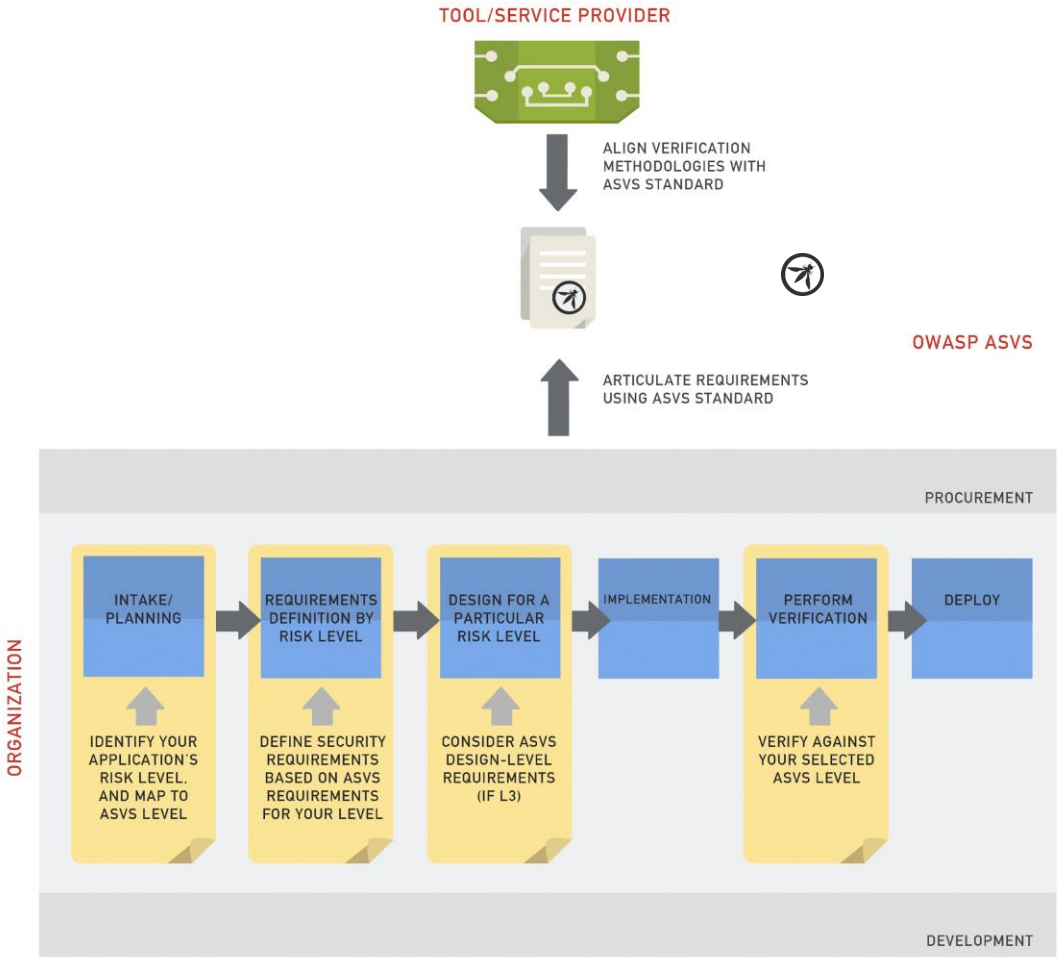

Figure 1 – Uses of ASVS for organizations and tool/service providers

Aşağıdaki örnek senaryolar, kurgusal bir şirket (ACME Bank) ve kurgusal bir güvenlik servis sağlayıcısı (Hack All the Things) arasında ASVS standartlarının örnek kullanım senaryolarını göstermek amaçlıdır.

Use Case 1: Uygulamanın Onaylanması

ACME Bank yeni bir internet bankacılığı uygulaması geliştirmiş olup, uygulama şuanda canlı ortamlarına konuşlandırılıp müşteri kullanımına açılma aşamasında bulunmaktadır. Uygulama bankanın standart Yazılım Geliştirme Yaşam Döngüsü (SDLC) ile geliştirilmiş ve mevcutta güvenli durumda olması beklenmektedir. ACME Bank'ın iç güvenlik ekibi, uygulamanın paylaşılan bir sunucuda konuşlandırılmasından dolayı, başka uygulamalara risk oluşturmayacak şekilde yapılandırılması için görevlendiriliyor. İçeride yapılan bir tehdit modelleme çalışmasından sonra, bu uygulamanın ortam ve içindeki sakladığı bilgiler açısından yüksek risk taşıdığı belirleniyor.

Ekip, çok bilinen bir web uygulama tarama aracını kullanıyor ve uygulamayı bu araçla otomatize olarak

tarama yapabilmek için gerekli ayarlar yapılıyor. Tüm bunlar bitince tarama aracı başlatılıyor ve tarama bitince zafiyet raporu çıkartılıyor. Güvenlik analisti, rapordaki false-positive bulguları ayıklayarak rapora son halini veriyor ve bulguları sistem sahipleri ve geliştiricilere gönderiyor. Tüm bulgular giderildikten sonra bir tarama daha yapılarak bulguların uygun yöntemlerle çözüldüğü kontrol ediliyor.

Bu örnekte, eğer ASVS standartları kullanılmış olsaydı; iç ekip uygulamayı bilinen uygulama zafiyetleri için test edebilir ve aynı zamanda bu uygulamanın bankanın belirlemiş olduğu standartlara göre geliştirilip geliştirilmediğini kontrol edebilirdi.

Use Case 2: Taşeron Servis Sağlayıcının Seçilmesi

ACME Bank yeni internet bankacılığı uygulamasının geliştirme süreçlerini en sonunda tamamladı. Banka denetçileri, dış bir danışmanlık firmasının bu uygulamanın güvenlik açısından denetim gereksinimlerini sağlayıp sağlamadığını değerlendirmesini istiyor.

ACME Bank servis sağlayıcıları listesinden HATT(Hack All the Things) ile bu değerlendirmeyi yapmak üzere anlaşıyor. Banka, danışmanlık firmasına tüm kaynak kodları ve dokümantasyonu sunarak değerlendirmenin zamanını planlıyorlar. Yapılan testler tam otomatize olarak yapılan bir kaynak kod analizi ve elle yapılan bir uygulama değerlendirmesini içeriyor. Bunlara ek olarak, uygulamanın iş akışı mantığı da test edilerek, uygulama dokümantasyonunda yer alan fonksiyonel gereksinimlerin karşılanıp karşılanmadığı da test ediliyor. Tüm bu testler tamamlanınca, bir değerlendirme raporu hazırlanıp ACME Bank çalışanına sunuluyor.

Eğer her iki taraf da bu süreçlere ASVS standartlarını adapte etmiş olsalardı, uygulanacak değerlendirme/testler için iki tarafın da katıldığı bir seviye seçilmiş ve belirlenmiş olurdu. Bunun sonucunda ACME Bank ve HATT firması, bu değerlendirmelerde nelerin yapıldığı ve nelerin sonuç olarak çıkması gerektiği konusunda hemfikir olup, ortak zeminde çalışabilirlerdi.

Uygulama Güvenliği Doğrulama Seviyeleri

ASVS, dört adet doğrulama seviyesi tanımlar ve doğrulamanın üste çıktığı her seviyede derinliği artar.

Her seviyedeki derinlik, bu seviyede adreslenen güvenlik doğrulama gereksinimlerinin sayı ve çeşidi ile belirlenmektedir (Takip eden bölümlerde bu seviyelere ait örnek tablolar bulunmaktadır). Bir denetimde, hedeflenen seviyedeki gereksinimlerin hepsinin karşılandığının kontrolü doğrulamayı yapan kişinin sorumluluğundadır. Eğer bir uygulama bir seviyedeki tüm gereksinimleri karşılıyor ise, o uygulama artık OWASP ASVS N Seviyesi bir uygulama olarak düşünülebilir (N, uygulamaya zorunlu kılınan doğrulama seviyesidir). Eğer uygulama hedeflenen belli bir seviyedeki tüm gereksinimleri karşılamıyor ancak daha düşük bir seviyedeki tüm gereksinimleri karşılıyor ise, düşük olan seviyedeki doğrulamayı sağlamış sayılabilir.

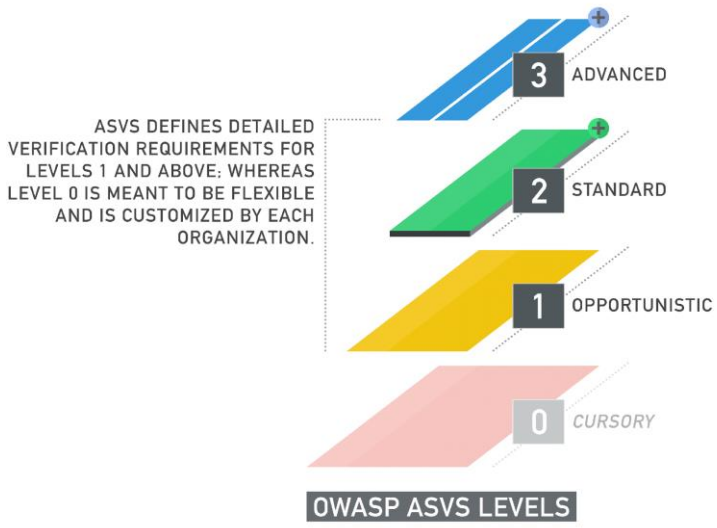

Figure 2 – OWASP ASVS Levels

Doğrulamanın kapsamı, her güvenlik gereksinimi için uygulamanın hangi bölümlerinin doğrulamaya dahil edildiği ile belirlenmektedir. Örneğin bir doğrulamanın kapsamı üçüncü parti uygulamaları da kapsayabilir. Böylesine detaylı bir incelemeyi kapsayan doğrulama seviyesi, yanına konan "+" işareti ile belirtilir.

Seviye 0: Yüzeysel (Cursory)

Seviye 0 (yüzeysel), uygulamanın bazı doğrulamalardan geçtiğini belirten, tercihe bağlı bir belgelendirmedir.

Figure3 – OWASP ASVS Level 0

Seviye 0, doğrulama hiyerarşisine giriş yapmak amacıyla esnek olarak tasarlanmış ve uygulama üzerinde bazı değerlendirmelerin yapıldığını belirten bir seviyedir. Detaylı doğrulama gereksinimleri ASVS tarafından sunulmaz, organizasyonlar kendi minimum kriterlerini belirlerler (Güçlü kimlik doğrulama mekanizmaları vb.).

Bu seviye, çok fazla uygulamaya sahip ve doğrulama seviyelerine düşük bütçe ile girmesi gereken organizasyonlar için uygundur. Örneğin bir organizasyon Seviye 0'ı, firmanın sahip olduğu internete açık tüm uygulamalarının, firmanın sahip olduğu kurumsal araç ile yüzeysel olarak otomatize şekilde taranması olarak belirleyebilir.

Diğer ASVS seviyelerinin aksine, Seviye 0 diğer seviyeler için önkoşul değildir. Eğer organizasyon Seviye 0'ı tanımlamamışsa, bir uygulama direkt olarak Seviye 1'e erişebilir.

Seviye 0 gereksinimleri belirlenirken, aynen bu dokümandaki detaylı doğrulama gereksinimi tanımları gibi düzenli, gerçekçi, doğrulanabilir şekilde belgelendirilmesi tavsiye edilmektedir.

Doğrulama Gereksinimleri Hakkında Açıklama

Seviye 0 ASVS bu seviye için detaylı doğrulama gereksinimlerini tanımlamaz. Bu seviyede uygulamalar organizasyonun belirlediği gereksinimlere göre değerlendirilir.

Seviye 1: Fırsatçı (Opportunistic)

Bir uygulama, eğer tespiti kolay zafiyetlere karşı korumalı ise, Seviye 1 seviyesindedir.

Figure 4 – OWASP ASVS Level 1

Seviye 1'e özel doğrulama gereksinimleri, Detaylı Doğrulama Gereksinimleri bölümünde belirtilmiştir. Ancak bu seviyedeki zafiyetler tipik olarak doğrulama yapan kişinin en az çaba ile belirleyebileceği gruptadır. Bu sebepten dolayı bu seviye, uygulamanın detaylı bir değerlendirmesi değil, daha çok uygulamaya hızlı bir bakış olarak değerlendirilmelidir.

Seviye 1, tipik olarak daha çok güvenlik kontrollerinin yerinde kullanıldığı konusunda bir güven oluşturulmasına ihtiyaç duyulan uygulamalar için uygundur. Ya da kurumsal uygulamaların tamamına genel bir bakış atılarak, daha ilerideki denetimler için bir yol haritası çıkarmak amacıyla Seviye 1 kullanılabilir.

Uygulamalara gelen tehditler genel olarak, tespit etmesi ve istismar etmesi kolay zafiyetleri tespit etmek için basit teknikler kullanan saldırganlar tarafından oluşturulur.

Doğrulama Gereksinimleri Hakkında Açıklama

Seviye 1 Belgelendirilmiş uygulama, "Detaylı Doğrulama Gereksinimleri" bölümündeki Seviye 1 gereksinimlerine göre değerlendirilmiştir.

Seviye 2: Standart

Seviye 2 seviyesindeki bir uygulama, ortalama ve ciddi seviyede risklere yol açan zafiyetlere karşı yeterli seviyede korumalıdır.

Figure 5 – OWASP ASVS Level 2

Seviye 2'ye özel doğrulama gereksinimleri, Detaylı Doğrulama Gereksinimleri bölümünde detaylı belirtilmiş olmasına karşın bu seviye OWASP Top 10 zafiyetleri ve iş mantığı zafiyetlerini de kapsayabilir.
Seviye 2, uygulanan güvenlik kontrollerinin yerinde ve etkili kullanıldığını ve bu sayede uygulamaya özel politikaların zorlandığını garanti eder.

Seviye 2, organizasyonların hassas uygulamaları için harcadıkları çabalar için bir endüstri standartıdır. Bu seviye tipik olarak, işten-işe hassas aktarım (transaction) yapan (sağlık bilgisi içeren, hassas fonksiyonlar içeren ve

diğer hassas aktifleri işleyen) uygulamalar için uygundur.

Bu seviyedeki tehditler fırsatçı ve odaklanmış saldırganlar tarafından oluşturulan, elle yapılan test tekniklerini içeren tehditlerdir.

Doğrulama Gereksinimleri Hakkında Açıklama

Seviye 2 Belgelendirilmiş uygulama, "Detaylı Doğrulama Gereksinimleri" bölümündeki Seviye 2 gereksinimlerine göre değerlendirilmiştir.

Seviye 3: Gelişmiş (Advanced)

Seviye 3 seviyesindeki bir uygulama, tüm gelişmiş uygulama güvenliği zafiyetlerine karşı korumalıdır ve ayrıca iyi bir güvenlik tasarımına sahiptir.

Figure 6 – OWASP ASVS Level 3

Seviye 3'e özel doğrulama gereksinimleri, Detaylı Doğrulama Gereksinimleri bölümünde detaylı belirtilmiştir fakat bu seviye istismar etmesi zor ve ancak tecrübeli saldırganlar tarafından istismar edilebilecek zafiyetleri kapsayabilir.

Seviye 3, tüm ASVS seviyeleri içinde uygulamanın tasarımının incelenmesini gerektiren tek seviyedir. Ayrıca buna ek olarak beraberinde aşağıdaki gibi gereksinimler getirir:

- Birden fazla alternatifi olabilecek tüm önemli güvenlik kontrollerinin (girdi doğrulama, oturum/yetki yönetimi vb.) tek bir merkezde geliştirilmesi ve tüm uygulama geliştirme süreçlerinde bu ortak kontrollerin uygulanması gerekmektedir.
- Doğrulama yapılan tüm güvenlik kontrollerinde, "Beyaz Liste" yaklaşımının uygulanması gerekmektedir.
- Betik enjeksiyonu bulgularında, tek savunma mekanizması olarak girdi doğrulama yeterli görülmemelidir. Girdi doğrulama yöntemlerinin yanında, parametrik kullanım (parameterization) ve çıktı kodlama yöntemleri de uygulanmalıdır.

Seviye 3 doğrulama tipik olarak; yaşam ve güvenliği koruyan kritik uygulamalar, kritik altyapıya sahip uygulamalar ya da savunma mekanizmaları ve istismar edilmesi durumunda organizasyona büyük derecede zarar verecek uygulamalar için uygundur. Hassas bilgileri işleyen uygulamalar için de Seviye 3 uygundur.

Bu seviyedeki tehditler, saldırı amaçlı kullanılan özel tarama araçları ile uygulamayı istismar etmeye çalışan, odaklanmış ve uzman saldırganlar tarafından oluşturulur.

Doğrulama Gereksinimleri Hakkında Açıklama

L3.1 Seviye 3 belgelendirilmiş uygulama, "Detaylı Doğrulama Gereksinimleri" bölümündeki Seviye 3 gereksinimlerine göre değerlendirilmiştir.

L3.2 Seviye 3 belgelendirilmiş uygulamanın, aşağıdaki en iyi uygulama yöntemlerini takip ettiği doğrulanmıştır:

- Tüm güvenlik kontrolleri uygulamada tek bir merkezden yönetilmekte ve uygulanmaktadır.
- Doğrulama yapan tüm güvenlik kontrolleri "Beyaz Liste" yaklaşımını kullanmaktadır.
- Veri doğrulama kontrolleri, çıktı kodlama (output encoding) metotları ile desteklenmektedir.
- Güvenilmeyen kaynaktan gelen ve SQL cümleciklerine giren tüm girdiler, parametrik ya da hazır ifadeler (prepared statements) aracılığıyla kullanılmalı ve uygun bir doğrulamadan geçmelidir.

Doğrulama Kapsamı

Doğrulamanın kapsamı, bir doğrulama seviyesine erişmek için gerekli olan gereksinimlerden ayrıdır.

ASVS temel olarak doğrulama kapsamının, uygulamanın geliştirilmiş ve iyileştirilmiş tüm kodlarını içerdiğini varsayar. Ancak bazı durumlarda organizsyonlar, uygulama tarafından kullanılan ve uygulama güvenliğine etkide bulunduğunu düşündükleri üçüncü parti çatılar, kütüphaneler ve servis fonksiyonlarını doğrulamanın parçası olarak ekleyebilirler. Bu şekilde ulaşılan sıkı bir doğrulama seviyesi, seviyenin yanına "+" işareti eklenerek gösterilebilir. Örneğin bir uygulamada ASVS Seviye3+ olarak işaretlenebilir.

Üçüncü parti bileşenleri eklemek, herhangi bir ASVS seviyesine erişmek için gerekli değildir, sadece opsiyoneldir. Bu sıkılıkta bir doğrulama, yüksek seviyede kritik görevdeki uygulamalar için uygun olabilir. Zaten bu sıkılıktaki bir uygulamanın "+" belgelendirilmesi muhtemelen Seviye 3 ile ilişkili olacaktır.

Bir doğrulamaya üçüncü parti bileşenler katıldığı zaman, bu bileşenler üzerinde tüm detaylı doğrulama gereksinimlerinin uygulanması gerekli değildir. Aslına bakılırsa, birçok detaylı doğrulama gereksinimi zaten üçüncü parti bileşenler üzerinde uygulanamaz durumda olup, sadece temel kod ile alakalı olanlar uygulanabilir olacaktır.

Detaylı doğrulama gereksinimleri uygulamanın tüm temel kodu üzerinde doğrulanmalı ve üçüncü parti bileşenlere ancak uygulanabilir olduğunda doğrulanmalıdır. Yalnızca bu koşulda bir uygulama "+" belgelendirmesine erişebilir.

Detaylı Doğrulama Gereksinimleri

OWASP Uygulama Güvenliği Doğrulama Standardı (ASVS)'nin bu bölümünde, her seviyede bulunan yüksek seviyedeki gereksinimlerden türetilen detaylı doğrulama gereksinimleri tanımlanmaktadır. Her bölüm, ilgili alanlar çerçevesinde gruplanmış detaylı doğrulama gereksinimlerini içermektedir.

ASVS, aşağıdaki güvenlik gereksinimlerini tanımlar. Güncelleme yapmak isteyenlere kolaylık olması için, numaralandırma şeması bir önceki ASVS sürümü ile aynı tutulmuştur.

V2. Kimlik Doğrulama (Authentication)
V3. Oturum Yönetimi (Session Management)
V4. Erişim Kontrolleri (Access Control)
V5. Giriş Verisi Doğrulama (Malicious Input Handling)
V7. Doğrulama İşlemi Şifreleme (Cryptography at Rest)
V8. Hata Ayıklama ve Kayıt Tutma (Error Handling and Logging)
V9. Veri Koruma (Data Protection)
V10. Haberleşme Güvenliği Doğrulama (Communications)
V11. HTTP Güvenliği Doğrulama (HTTP)
V13. Zararlı Kontroller (Malicious Controls)
V15. İş Mantığı Doğrulama (Business Logic)
V16. Dosya ve Kaynaklar (File and Resource)
V17. Mobil Doğrulama (Mobile)

V2: Kimlik Doğrulama Gereksinimleri

Altta ki tablo, doğrulamanın her aşamasında kullanılan ilgili doğrulama gereksinimlerini tanımlamaktadır. Sıfır (0) seviyesi için doğrulama gereksinimleri bu standardın kapsamında değildir.

	KİMLİK DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V2.1	Özel olarak genel paylaşıma açık sayfa ve bileşenler dışında tüm gerekli alanlarda kimlik doğrulama mekanizmalarının olduğu doğrulanmalıdır.	✓	✓	✓
V2.2	Kullanıcıların parola alanlarına girdikleri parola bilgisinin gösterilmediği doğrulanmalıdır.	✓	✓	✓
V2.4	Bütün kimlik doğrulama kontrollerinin sunucu tarafında yapıldığı doğrulanmalıdır.	✓	✓	✓
V2.5	Tüm kimlik doğrulama kontrollerinin (harici kimlik doğrulama servislerini çağıran kütüphaneler dahil) merkezi bir uygulamadan yapıldığı doğrulanmalıdır.			✓
V2.6	Kimlik doğrulama esnasında meydana gelen hataların detaylarının kullanıcılara bildirilmediği doğrulanmalıdır.	✓	✓	✓
V2.7	Parola girdi alanlarının uzun ve karmaşık parolaların kullanımına izin verdiği ve böylece parola tahmini saldırılarına karşı korunma sağlandığı doğrulanmalıdır.		✓	✓

	KİMLİK DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V2.8	Hesaba erişim sağlayabilecek tüm hesap yönetim işlevlerinin (kayıt olma, profil güncelleme, parolamı unuttum, kullanıcı bilgilerini unuttum, devre dışı/kayıp anahtar, yardım paneli ya da interaktif sesli cevap sistemi) en azından birincil kimlik doğrulama mekanizması kadar güvenli olduğu doğrulanmalıdır.		✔	✔
V2.9	Parola değiştirme mekanizmasının an az birincil kimlik doğrulama mekanizması kadar güvenli olduğu doğrulanmalıdır.		✔	✔
V2.12	Lineer geciktirme işlemleri ve yazılımsal veya programsal kilitlemeler dahil olacak şekilde tüm kimlik doğrulama kararlarının kayıt altına alındığı doğrulanmalıdır.		✔	✔
V2.13	Kullanıcı parolalarının, o hesaba özgü (örneğin iç kullanıcı ID'si veya hesap bilgisi) bir değerle tuzlanmadığı (salted) ve depolanmadan önce bcrypt, scrypt veya PBKDF2 fonksiyonu ile özet'lendiği (hash'lendiği) doğrulanmalıdır.		✔	✔
V2.16	Uygulama tarafından işlenen parolalar ve tüm kişisel bilgilerin şifrelenmemiş veya yeterince güçlü olmayan algoritmalarla şifrelenmiş bağlantılar üzerinden iletilmediği doğrulanmalıdır.	✔	✔	✔
V2.17	Parolamı unuttum ve diğer parola kurtarma işlevleri mevcut parolayı kullanıcıya hiç bir şekilde göstermemeli ve yeni şifrenin açık metin olarak kullanıcıya gönderilmediği doğrulamalıdır.	✔	✔	✔
V2.18	Giriş, parola sıfırlama veya parolamı/hesabımı unuttum işlevleri aracılığı ile kullanıcı adları listelemenin mümkün olmadığı doğrulanmalıdır.	✔	✔	✔
V2.19	Uygulama çatısı ya da uygulamanın herhangi bir bileşeninde öntanımlı (default) parola kullanılmadığı doğrulanmalıdır ("admin/password" gibi).	✔	✔	✔

	KİMLİK DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V2.20	Kaynak yöneticisinin, dikey(tek bir hesabın olası tüm parolalar test edilmesi) ve yatay(tüm hesapların tek bir parola ile test edilmesi) kaba kuvvet saldırılarına karşı koruma sağladığı doğrulanmalıdır. Doğru kullanıcı girdileri gecikmeye tabi olmamalıdır. Bu koruyucu önlemler, diagonal ve dağıtık saldırılara karşı eş zamanlı aktif olmalıdır.		✔	✔
V2.21	Uygulamanın dışarıdaki servislere erişim için kullandığı kimlik doğrulama verilerinin şifrelenmiş olduğu ve korunaklı bir yerde saklandığı/depolandığı (kaynak kod içerisinde kesinlikle olmamalı) doğrulanmalıdır.		✔	✔
V2.22	Parolamı unuttum ve diğer kurtarma işlevlerinin şifrenin kendisi yerine zaman sınırlı aktivasyon anahtarları içeren bir link gönderdiği doğrulanmalıdır. Link gönderilmeden önce sanal-jeton (soft-token) (sms sanal-jetonu, mobil uygulama jetonları gibi) doğrulanması da ek kimlik doğrulama metodu olarak entegre edilebilir.		✔	✔
V2.23	Kullanıcı parolasını başarılı bir şekilde değiştirene kadar 'Parolamı unuttum' işlevinin kullanıcı hesabını kitlenmediği ya da devre dışı bırakmadığı doğrulanmalıdır. Bu asıl kullanıcı hesaplarının kilitlenmesini engellemek için gereklidir.		✔	✔
V2.24	Parola sıfırlama için gizli soru ve cevap mekanizmasının kullanılmadığı doğrulanmalıdır.		✔	✔
V2.25	Sistemin 'tanımlanan sayıda' önceden kullanılmış parolaların kullanımına izin vermeyecek şekilde yapılandırılabilir olduğu doğrulanmalıdır.		✔	✔
V2.26	Uygulamanın risk profilini dikkate alarak uygulamaya spesifik hassas işlemler yaparken kimlik doğrulama tekrarı, 'yükselten veya uyarlanabilir kimlik doğrulama, SMS veya diğer iki seviyeli kimlik denetimi veya işlem imzalamalarının kullanıldığı doğrulanmalıdır.			✔

V3: Oturum Yönetimi Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için varolan doğrulama gereksinimlerini kapsamamaktadır.

	OTURUM YÖNETİMİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V3.1	Uygulamanın, çatı yapı tarafından sunulan varsayılan/ön tanımlı oturum yönetimi kontrollerinin kullandığı doğrulanmalıdır.	✓	✓	✓
V3.2	Kullanıcı oturumu sonlandırıldığında oturumun geçersiz kılındığı doğrulanmalıdır.	✓	✓	✓
V3.3	Belirli bir süre boyunca aktif olmayan oturumların, zaman aşımına uğrayarak sonlandırıldığı doğrulanmalıdır.	✓	✓	✓
V3.4	Kullanıcı aktifliğinden bağımsız olarak, yönetim seviyesinde ayarlanabilir bir mutlak zaman aşımı süresi sonrası oturumların sonlandırıldığı doğrulanmalıdır.		✓	✓
V3.5	Yalnızca kimlik doğrulaması ile erişilebilen sayfaların tümünün " oturumu sonlandır" linkine sahip olduğu doğrulanmalıdır.	✓	✓	✓
V3.6	Oturum anahtarının çerez başlıkları dışında hiç bir yerde ifşa edilmediği, özellikle de URL üzerinde, hata mesajları ve tutulan kayıtlar içinde tutulmadığı/geçmediği doğrulanmalıdır. Bu kapsamda, uygulamanın oturum çerezlerinin, URL içinde tekrar yazılmasını da desteklemediği ayrıca doğrulanmalıdır.	✓	✓	✓

	OTURUM YÖNETİMİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V3.7	Oturum sabitleme saldırılarından korunmak için, başarılı bir kullanıcı girişi sonrası oturum anahtarının değiştiği doğrulanmalıdır.		✓	✓
V3.8	Yeniden kimlik doğrulama sonrasında oturum anahtarının değiştiği doğrulanmalıdır.		✓	✓
V3.10	Uygulamanın, yalnızca uygulama çatısı tarafından üretilen oturum anahtarlarını geçerli olarak kabul ettiği doğrulanmalıdır.		✓	✓
V3.11	Kimlik doğrulamada kullanılan oturum anahtarlarının, tahmin saldırılarından korunmaya yetecek seviyede uzun ve karmaşık olduğu doğrulanmalıdır.		✓	✓
V3.12	Kimlik doğrulamada kullanılan oturum anahtarlarını içeren çerezler, oturum anahtarını sitenin sadece belirli bir bölümüne erişim sağlayacak şekilde kısıtlayan dizin değerleri içermelidir. Özel bir iş gereksinimi olmadığı takdirde (single sign on, vb.), dizin değeri olarak tüm domain/alan adını içeren çerezler kullanılmamalıdır.		✓	✓
V3.14	Kimlik doğrulamada kullanılan oturum anahtarlarını içeren ve HTTP üzerinden gönderilen çerezlerin "HttpOnly" olarak işaretlendiğ i doğrulanmalıdır.	✓	✓	✓
V3.15	Kimlik doğrulamada kullanılan oturum anahtarlarını içeren çerezlerin "secure" özelliği ile korunduğu ve sıkı bir taşıma güvenliği başlığına (Strict-Transport-Security: max-age=60000; includeSubDomains) sahip olduğu doğrulanmalıdır.	✓	✓	✓
V3.16	Uygulamanın, aynı kullanıcı için farklı makinalarda eş zamanlı kullanıcı oturumuna izin vermediği doğrulanmalıdır.		✓	✓

Tablo 1 - OWASP ASVS Oturum Yönetimi Doğrulama Gereksinimleri (V3)

V4: Erişim Kontrolleri Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	ERİŞİM KONTROLLERİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V4.1	Kullanıcıların, belirli yetkiler ile kullanmak üzere sadece güvenli işlevler veya servislere eriştiği doğrulanmalıdır.	✔	✔	✔
V4.2	Kullanıcıların, belirli yetkiler ile kullanmak üzere sadece güvenli URL'lere eriştiği doğrulanmalıdır	✔	✔	✔
V4.3	Kullanıcıların, belirli yetkiler ile kullanmak üzere sadece güvenli veri dosyalarına eriştiği doğrulanmalıdır	✔	✔	✔
V4.4	Direkt nesne erişimlerinin yetki kontrolü ile korunduğu doğrulanmalıdır, öyle ki her kullanıcı sadece yetkisi olan nesnelere erişebilmelidir.	✔	✔	✔
V4.5	Özellikle istenmediği sürece dizin geziniminin kapalı olduğu doğrulanmalıdır.	✔	✔	✔
V4.8	Erişim kontrolleri hatalarının güvenli bir şekilde ele alındığı doğrulanmalıdır.	✔	✔	✔
V4.9	Belirli bir kullanıcı rolü için sunum katmanı tarafından belirtilen erişim		✔	✔

	ERİŞİM KONTROLLERİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
	kontrollerinin, sunucu tarafında da uygulanmasının dayatıldığı doğrulanmalıdır, öyle ki bu kontroller ve değişkenler daha yüksek yetkili bir kullanıcı tarafından yeniden etkinleştirilememeli veya yeniden eklenememelidir.		✓	✓
V4.10	Özel olarak yetkilendirilmediği sürece, erişim kontrollerinin kullandığı tüm kullanıcı ve veri yetkilerinin ve ayrıca politika bilgilerinin son kullanıcı tarafından değiştirilemediği doğrulanmalıdır.		✓	✓
V4.11	Tüm erişim kontrollerin sunucu tarafında da uygulanmaya zorlandığı doğrulanmalıdır.	✓	✓	✓
V4.12	Korunan her türlü kaynağa erişimin kontrolü için merkezi bir mekanizmanın(Dış yetkilendirme servislerini çağıran kütüphaneler dahil) olduğu doğrulanmalıdır.			✓
V4.14	Tüm erişim kontrolü hareketlerinin veya tüm yetkisiz erişim hareketlerinin kayıtlarının tutulduğu doğrulanmalıdır.		✓	✓
V4.16	Uygulama veya uygulama çatısının, yüksek değerli hareketler ya da hassas verilere erişim sırasında, yeterince güçlü karmaşıklığa sahip bir anti-CSRF (siteler arası istek sahteciliği) anahtarı yarattığından emin olunmalı ve sunucunun bu tarz istekleri işlemeden önce, bu anahtarın mevcut kullanıcı için uygun olup olmadığını kontrol ettiği doğrulanmalıdır.	✓	✓	✓
V4.17	Erişim kontrol korumaları birleştirilmelidir. Sistemin, güvenli fonksiyonlara, kaynaklarına ya da verilerine sürekli erişime karşı korumalı olduğu doğrulanmalıdır. Örneğin, bir kaynak yöneticisi yardımı ile bir saat boyunca kaynağın düzenleme sayısına sınırlama getirilmesi ya da tek bir kullanıcı tarafından tüm veritabanının erişilmez hale gelmesi sistem tarafından engellenmelidir.		✓	✓

Tablo 2 - OWASP ASVS Erişim Kontrolleri Doğrulama Gereksinimleri (V4)

V5: Giriş Verisi Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	GİRİŞ VERİSİ GEÇERLEME GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V5.1	Canlı ortamın 'buffer overflow-arabellek taşması-' olanak tanımadığı veya güvenlik önlemlerinin 'buffer overflow-arabellek taşması-'a karşı koruma sağladığı doğrulanmalıdır.	✓	✓	✓
V5.3	Tüm giriş verisi geçerleme hatalarının, girilen veriyi reddettiği veya zararlı alanlarından arındırdığı doğrulanmalıdır.	✓	✓	✓
V5.4	UTF-8 gibi kullanılan karakter setinin, tüm giriş alanlarına tanımlandığını doğrulanmalıdır.		✓	✓
V5.5	Giriş verisi geçerleme ve şifreleme işlemlerinin sunucu taraflı yapıldığı ve bu işlemlerin sunucu taraflı yapılmaya zorlandığı doğrulanmalıdır.	✓	✓	✓
V5.6	Uygulama üzerinde, uygulamanın işleme aldığı her tip veri için tek noktadan veri geçerleme kontrollerinin uygulandığı doğrulanmalıdır.			✓

	GİRİŞ VERİSİ GEÇERLEME GEREKSİNİMLERİ	SEVİYE 1	2	3
V5.7	Tüm hatalı giriş veri geçerleme işlemlerinin kayıt altına alındığı (loglandığı) doğrulanmalıdır.			✔
V5.8	Doğrulama öncesi 'downstream' kod çözücü veya dil yorumlayıcıları için giriş verisinin standartlaştırıldığı doğrulanmalıdır.		✔	✔
V5.10	Canlı ortamın 'SQL Injection-SQL Enjeksiyonu-'a olanak tanımadığı veya güvenlik önlemlerinin 'SQL Injection-SQL Enjeksiyonu -'a karşı koruma sağladığı doğrulanmalıdır.	✔	✔	✔
V5.11	Canlı ortamın 'LDAP Injection-LDAP Enjeksiyonu-'a olanak tanımadığı veya güvenlik önlemlerinin 'LDAP Injection-LDAP Enjeksiyonu-'a karşı koruma sağladığı doğrulanmalıdır.	✔	✔	✔
V5.12	Canlı ortamın 'OS Command Injection-İşletim Sistemi Komut Enjeksiyonu-'a olanak tanımadığı veya güvenlik önlemlerinin 'OS Command Injection-İşletim Sistemi Komut Enjeksiyonu-'a karşı koruma sağladığı doğrulanmalıdır.	✔	✔	✔
V5.13	XML External Entity ataklarına karşın, çalışma ortamının güvenlik kontrollerini sağladığı doğrulanmalıdır.	✔	✔	✔
V5.14	XML Injection ataklarına karşın, çalışma ortamının güvenlik kontrollerini sağladığı doğrulanmalıdır.	✔	✔	✔
V5.16	HTML çıktısı (HTML elementleri, HTML özellikleri, JavaScript veri değerleri, CSS blokları, URI) üreten tüm güvenilmeyen verilerden uygulanabilir bir içerik ile uygun bir biçimde kaçınıldığı doğrulanmalıdır.	✔	✔	✔
V5.17	Eğer uygulama otomatik parametre atamasına izin veriyorsa (otomatik değişken bağlama- automatic variable binding -) hassas alanların(Rol, parola, Hesap Özeti) zararlı parametrelerden korunduğu doğrulanmalıdır.		✔	✔

	GİRİŞ VERİSİ GEÇERLEME GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V5.18	Özellikle uygulama çatısı sorgu parametrelerinin (GET, POST, çerezler, başlıklar) kaynağına ilişkin bir ayrım yok ise uygulamanın HTTP Parametre Kirliliği Saldırılarına karşı koruma sağladığı doğrulanmalıdır.		✔	✔
V5.19	Her bir kaçınma/çıkış kodlama'nın uygulama tarafından gerçeklendiği ve istenilen hedefe bu türden çıktıların tek bir güvenlik mekanizması üzerinden üretildiği doğrulanmalıdır.			✔

Tablo 3 - OWASP ASVS Giriş Verisi Doğrulama Gereksinimleri (V5)

V7: Doğrulama İşlemi Şifreleme Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için varolan doğrulama gereksinimlerini kapsamamaktadır.

	DOĞRULAMA İŞLEMLERİ ŞİFRELEME GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V7.1	Uygulama kullanıcısının görmemesi gereken verileri korumak için kullanılan şifreleme işlevlerinin sunucu tarafında uygulandığı doğrulanmalıdır.		✔	✔
V7.2	Tüm şifreleme modüllerinin güvenli şekilde hata durumuna geçtiği doğrulanmalıdır.		✔	✔
V7.3	Yüksek dereceli koruma gerektiren verilerin, yetkilendirilmeyen erişimlerden korunduğu doğrulanmalıdır. (Yüksek dereceli korunması gereken veriye örnek verecek olursak, güvenlik yapılandırma bilgilerine erişimi korumak için diske kaydedilmiş kullanıcı şifresinin açık metin olarak kayıt edilmesi diyebiliriz.)		✔	✔
V7.6	Tüm rastgele üretilen sayılar, dosya isimleri, global eşsiz kimlikleyiciler (GUID) ve karakter dizilerinin saldırgan için tahmin edilemez olmasını sağlama açısından şifreleme modülünün onaylanmış rasgele sayı üretecisini kullanarak üretildiği doğrulanmalıdır.		✔	✔

	DOĞRULAMA İŞLEMLERİ ŞİFRELEME GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V7.7	Uygulama tarafından kullanılan şifreleme modüllerinin FIPS 140-2 veya eşiti bir standarda uygunluğu doğrulanmalıdır.			✔
V7.8	Şifreleme modüllerinin yayınlanmış güvenlik politikaları çerçevesinde işlevselliklerini yerine getirdikleri doğrulanmalıdır.			✔
V7.9	Şifreleme anahtarlarının nasıl yönetileceğine dair açık / belirgin bir politika olduğu doğrulanmalıdır. (Mesela, üretilmesi, dağıtılması, iptali, süresinin dolması v.b.) Bu politikanın da doğru şekilde uygulandığı doğrulanmalıdır.		✔	✔

Tablo 4 - OWASP ASVS Doğrulama İşlemi Şifreleme Gereksinimleri (V7)

V8: Hata Ayıklama ve Kayıt Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için varolan doğrulama gereksinimlerini kapsamamaktadır.

	HATA AYIKLAMA VE KAYIT DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V8.1	Uygulamanın, saldırganın işini kolaylaştıracak hata mesajları veya yığın yapıları (stack) gibi hassas verileri oturum bilgisi ve kişisel bilgiler de dahil olmak üzere açığa çıkarmadığı doğrulanmalıdır.	✔	✔	✔
V8.2	Güvenilir cihazlar üzerinde hata işleme kontrolü yapıldığı doğrulanmalıdır.		✔	✔
V8.3	Kayıt kontrollerinin tamamının sunucu tarafında uygulandığı ve yapıldığı doğrulanmalıdır.		✔	✔
V8.4	Güvenlik kontrollerindeki hata işleme mantığının "varsayılan/fabrika tanımlı" (default) erişimleri reddettiği doğrulanmalıdır.		✔	✔
V8.5	Güvenlik kayıt kontrol mekanizmalarının, güvenlik ile ilgili başarılı ve başarılı olmayan olayları kayıt kabiliyeti sunduğu doğrulanmalıdır.		✔	✔
V8.6	Her kayıt şu özelliklere sahip olmalıdır: - Güvenilir kaynaktan zaman damgası,		✔	✔

	HATA AYIKLAMA VE KAYIT DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
	- Olayın önem derecesi, - Güvenlik dışı kayıtlar ile beraber tutuluyorsa, kaydın bir güvenlik kaydı olduğunu belirten belirteç, - Olaya sebebiyet veren kullanıcı bilgisi (eğer olay ile ilgili kişi iliştirilmişse), - Başarılı olsun veya olmasın, olaya dair kaynak IP adresi, - Olayın tarifi/tanımlanması.		✓	✓
V8.7	Güvenilir olmayan veriyi işleme esnasında kullanılan programın, olaylar içerisindeki verileri kod olarak çalıştırmadığı doğrulanmalıdır.			✓
V8.8	Güvenlik kayıtlarının izinsiz erişimlere ve değişikliklere karşı korunduğu doğrulanmalıdır.		✓	✓
V8.9	Uygulama tarafından kullanılan bir/tek kayıt mekanizması olduğu doğrulanmalıdır.			✓
V8.10	Uygulamanın, saldırganın işini kolaylaştıracak uygulamaya özel hassas verileri oturum bilgisi ve kişisel bilgiler de dahil olmak üzere açığa çıkarmadığı doğrulanmalıdır		✓	✓
V8.11	Kayıt analiz programı/programları, kayıtları analiz eden, kombinasyonlar kurarak kayıtlar içeresinde arama yapan analiste V6.6 gereksiniminde yer alan tüm kayıt özelliklerini sağlayacak şekilde mevcut olduğu doğrulanmalıdır.		✓	✓
V8.13	Güvenilir olmayan veriyi işleme esnasında kullanılan programın, olaylar içerisindeki verileri kod olarak çalıştırmadığı doğrulanmalıdır.			✓
V8.14	Güvenilir ve Güvenilir olmayan kaynaklardan elde edilen kayıtların, kayıt girdilerinde açık bir şekilde birbirinden ayırt edilebilir olduğu doğrulanmalıdır.			✓
V8.15	İşlem veya işlemler gerçeklenmeden önce kayıt altına alındığı			✓

HATA AYIKLAMA VE KAYIT DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
doğrulanmalıdır. Eğer kayıt herhangi bir sebeple başarılı olmaz ise (disk doluluğu, yetersiz yetki vs.) o zaman uygulama güvenli şekilde hata verip durmalıdır. Bu gereksinim özellikle, bütünlük ve inkar edememezliğin geçerli olduğu durumlarda bir zorunluluktur.			

Tablo 5 - OWASP ASVS Hata Ayıklama ve Kayıt Doğrulama Gereksinimleri (V8)

V9: Veri Koruma Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	VERİ KORUMA DOĞ RULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V9.1	Hassas veri içeren tüm formların son kullanıcı tarafında önbellekte ya da otomatik tamamlama özellikleri ile saklanmasının önlendiği doğrulanmalıdır.	✔	✔	✔
V9.2	Uygulama tarafından işlenen tüm hassas verilerin bir listesinin tanımlı olduğu ve ayrıca bu verilere nasıl erişileceği ve verilerin nasıl şifrelenip gönderileceği/saklanacağı hakkında belirli bir politikanın var olduğu doğrulanmalıdır. Bu politikanın uygulanmasının dayatıldığı da doğrulanmalıdır.			✔
V9.3	Tüm hassas verilerin sunucuya HTTP mesaj gövdesinde gönderildiği doğrulanmalıdır. (Hiçbir hassas veri URL parametresi olarak gönderilmemelidir.)	✔	✔	✔
V9.4	Son kullanıcı tarafına gönderilen, önbellekteki veya geçici tüm hassas verilerin yetkisiz erişimlere karşı korumalı olduğu ya da yetkili kullanıcı tarafından kullanıldıktan sonra temizlendiği/geçersiz kılındığı		✔	✔

	doğrulanmalıdır. (Uygun no-cache ve no-store Cache-Control başlıklarının gönderilmesi gerekmektedir.)		
V9.5	Sunucu üzerinde bulunan önbellekteki veya geçici tüm hassas verilerin yetkisiz erişimlere karşı korumalı olduğu ya da yetkili kullanıcı tarafından kullanıldıktan sonra temizlendiği/geçersiz kılındığı doğrulanmalıdır.	✓	✓
V9.6	Her tipteki hassas verinin, saklama süresi dolduğu zaman uygulamadan silinmesini sağlamak üzere bir metodun mevcut olduğu doğrulanmalıdır.		✓
V9.7	Uygulamanın, gizli alanlar, Ajax değişkenleri, çerezler ve başlık değerleri gibi güvenilmeyen sistemlere gönderilecek olan değişken sayısını minimum seviyede tuttuğu doğrulanmalıdır.		✓
V9.8	Uygulamanın, olağandışı istek sayısı veya ekran dönüşümü (screen scraping), otomatize çağrılan web servisleri ve bilgi kaybı gibi durumları tespit edebildiği ve gerekli yerlere alarm mesajları gönderebildiği doğrulanmalıdır. Örneğin ortalama bir kullanıcı, saatte 5, günde ise en fazla 30 kayıt sorgulamalı ya da sosyal ağına dakikada 10 arkadaştan fazla kişi eklememelidir.		✓

Tablo 6 - OWASP ASVS Veri Koruma Doğrulama Gereksinimleri (V9)

V10: Haberleşme Güvenliği Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	HABERLEŞME GÜVENLİĞİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V10.1	Güvenilir bir sertifika otoritesinden tüm Taşıma Katmanı Güvenliği (TLS) sunucu sertifikalarına bir yol(path) sağlanabildiği ve tüm sertifikaların geçerli olduğu doğrulanmalıdır.	✔	✔	✔
V10.2	Taşıma Katmanı Güvenliği (TLS) bağlantılarının, başarısız oldukları anda güvensiz bir HTTP bağlantısına dönüşmedikleri doğrulanmalıdır.			✔
V10.3	Yetkilendirilmiş (authenticated) ya da hassas veriler taşıyan tüm bağlantıların Taşıma Katmanı Güvenliği(TLS)'ni kullandığı doğrulanmalıdır.(dış ve iç(backend) bağlantıları da kapsamak üzere)		✔	✔
V10.4	İç taraftaki(backend) bağlantıların Taşıma Katmanı Güvenliği(TLS) başarısız olduğunda kayıt altına alındığı doğrulanmalıdır.		✔	✔
V10.5	Tüm istemci sertifikaları için sertifika yollarının önceden yapılandırılmış güvenilir referans noktaları(trust anchors) ve iptal(revocation) bilgileri kullanılarak oluşturulduğu/ doğrulandığı			✔

	doğrulanmalıdır.		
V10.6	Dış sistemlere yapılan ve hassas veri/bilgiler ya da işlevler içeren her bağlantının yetkilendirildiği doğrulanmalıdır.	✓	✓
V10.7	Dış sistemlere yapılan ve hassas veri/bilgiler ya da işlevler içeren her bağlantının, uygulama işlevselliğinin düzgün işlemesi için minimum yetkilere sahip olacak şekilde ayarlanmış bir kullanıcı hesabı kullandığı doğrulanmalıdır.	✓	✓
V10.8	Onaylanmış operasyon modunda (approved operation mode) çalışan uygulamaların tek bir standart Taşıma Katmanı Güvenliği gerçeklemesi kullandığı doğrulanmalıdır. (Detaylar için http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf)		✓
V10.9	Tüm bağlantılar için özel karakter kodlamalarının (UTF-8 gibi) tanımlandığı doğrulanmalıdır.		✓

Tablo 7 - OWASP ASVS Haberleşme Güvenliği Doğrulama Gereksinimleri (V10)

V11: HTTP Güvenliği Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	HTTP GÜVENLİĞİ DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V11.2	Uygulamanın GET, POST gibi sadece izin verilen bir dizi HTTP istek yöntemlerini kabul ettiği ve bu dizi dışındaki tüm yöntemleri özellikle blokladığı doğrulanmalıdır.	✓	✓	✓
V11.3	Tüm HTTP cevaplarının UTF-8 vb. gibi güvenli bir karakter setini belirten içerik türü başlığı (content type header) içerdiği doğrulanmalıdır.	✓	✓	✓
V11.6	HTTP istek ve cevaplarının her ikisinin de sadece yazılabilir ASCII karakterleri içerdiği doğrulanmalıdır.		✓	✓
V11.8	Clickjacking saldırılarından korunmak için eski tarayıcılara yönelik HTTP başlıklarının ya da diğer koruyucu mekanizmaların HTTP iletişimine eklendiği doğrulanmalıdır.	✓	✓	✓
V11.9	X-Real-IP gibi ön uçlar (frontend) tarafından eklenen ve uygulama tarafından kullanılan HTTP başlıklarının kullanıcı tarafından aldatıcı olarak değiştirilemediği (spoofing) doğrulanmalıdır.		✓	✓

V11.10	İçeriğinin üçüncü parti bir X-Frame tarafından görüntülenmesi istenmeyen web sitelerinin HTTP başlıklarında X-Frame-Options kullanıldığı doğrulanmalıdır. Genel kabul görmüş bir yöntem, bir web sitesini sadece aynı kaynağa sahip web sitelerinin görüntüleyebilmesi (framing) anlamına gelen SAMEORIGIN göndermektir.	✔	✔
V11.12	HTTP başlıklarının sistem bileşenleri hakkında detaylı sürüm bilgisi açığa çıkarmadığı doğrulanmalıdır.	✔	✔

Tablo 8 - OWASP ASVS HTTP Güvenliği Doğrulama Gereksinimleri (V11)

V13: Zararlı Kontroller Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	ZARARLI KONTROLLER DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
V13.1	Uygulamayı oluşturan herhangi bir kod parçasının içinde zararlı bir kod parçası bulunmadığı veya önceden var olup değiştirilmediği doğrulanmalıdır.			✔
V13.2	Yorumlanmış kodlar, kütüphaneler, çalıştırılabilir dosyalar ve konfigürasyon dosyalarının bütünlüklerinin sağlama toplamı (checksum) ve hash'ler yardımı ile doğrulandığı doğrulanmalıdır.			✔
V13.3	Kimlik doğrulama kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.			✔
V13.4	Oturum yönetimi kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.			✔
V13.5	Erişim/yetki kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.			✔

V13.6	Girdi (input) verisi doğrulama kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.	✓
V13.7	Çıktı (output) verisi doğrulama kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.	✓
V13.8	Şifreleme modülunu destekleyen ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.	✓
V13.9	Hata yönetimi ve kayıt (logging) kontrollerini uygulayan ya da kullanan kodların hiçbir zararlı kod içermediği/zararlı koddan etkilenmediği doğrulanmalıdır.	✓
V13.10	Tüm zararlı aktivitelerin yeterli/etkili bir şekilde kum havuzu içerisine alındığı doğrulanmalıdır. (sandboxed)	✓
V13.11	Hassas verilerin ihtiyaç duyulmayan duruma geldikleri anda hemen bellekten silindiği ve uygulama çatısı/işletim sistemi tarafından sunulan metodlarca ele alındığı doğrulanmalıdır.	✓

Tablo 9 - OWASP ASVS Zararlı Kontroller Doğrulama Gereksinimleri (V13)

V15: İş Mantığı Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	İŞ MANTIĞI DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V15.1	Uygulamanın, korumalı ve izlenen bir sunucu gibi güvenli bir ortamda, tüm yüksek dereceli iş mantığı akışlarını işlediği ve doğruladığı doğrulanmalıdır.		✔	✔
V15.2	Uygulamanın yüksek değerdeki aldatıcı işlemlere (spoofed) izin vermediği doğrulanmalıdır. Örneğin A kullanıcısı bir işlemi B kullanıcısının oturumunu, işlem durumunu, işlem ya da kullanıcı bilgilerini kullanarak gerçekleştirmeye çalıştığında, uygulama gerekli kontroller yardımı ile buna engel olmalıdır.		✔	✔
V15.3	Uygulamanın, fiyat, faiz, indirim, PII, hesap bilgileri, stok kayıtları gibi yüksek değerdeki iş mantığı değişkenlerinin yetkisiz değiştirilmesine (tamper) izin verilmediği doğrulanmalıdır.		✔	✔
V15.4	Uygulamanın, reddetme saldırılarına (repudiation attacks) karşı önleyici tedbirler aldığı doğrulanmalıdır. Bu saldırılar, doğrulanabilir ve korumalı işlem kayıtlarının, denetleme geçmişlerinin ve sistem		✔	✔

	İŞ MANTIĞI DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
	kayıtlarının zarar görmesi ya da kullanıcı aktiviteleri ve işlemlerin gerçek zamanlı izlendiği yüksek değerdeki sistemlerin çalışmasının engellenmesi ile gerçekleşebilir.			
V15.5	Uygulamanın, direk nesne referansı (direct object reference), değiştirme (tampering), oturuma kaba kuvvet (session brute force) gibi bilgi açığa çıkarma saldırılarına karşı korumalı olduğu doğrulanmalıdır.		✔	✔
V15.6	Uygulamanın kava kuvvet saldırıları veya servis dışı bırakma saldırılarına karşı yeterli tespit ve yönetim kontrollerinin olduğu doğrulanmalıdır.		✔	✔
V15.7	Uygulamanın yetki zafiyeti saldırılarından korunmak için yeterli/etkili yetki kontrollerinin olduğu doğrulanmalıdır. Bu kontrollerin yetersiz olduğu durumlarda, oturum açmamış kullanıcılar korunan veri ya da metotlara erişebilir veya oturum açmış kullanıcılar bir diğer kullanıcının hassas bilgilerine yetkisiz erişebilir.		✔	✔
V15.8	Uygulamanın iş mantığı akış adımlarını sıralı ve her adımı gerçek insan benzeri bir zamanda işlediği, kullanılmayan ve başka bir kullanıcıya ait adımları işlemediği veya çok hızlı gönderilen işlemleri işlemediği doğrulanmalıdır.		✔	✔
V15.9	Uygulamanın "adaptive authentication" veya "step up" gibi düşük değerli sistemler için ek yetki kontrollerine sahip olduğu doğrulanmalıdır. Ayrıca uygulamanın, yüksek değerdeki uygulamalar için, geçmiş sahtekârlıklar ve uygulama riski açısından hile-karşıtı kontrolleri (anti-fraud controls) dayatmasını sağlamak amacıyla görevlerin ayrılmasına sahip olduğu doğrulanmalıdır.		✔	✔
V15.10	Uygulamanın işlem limitlerine sahip olduğu ve bunları güvenli bir lokasyon (güvenli bir sunucu vb. gibi) üzerinde kullanıcı bazlı ya da günlük olmak üzere dayatarak uyguladığı ve ayrıca bu dayatmaların		✔	✔

İŞ MANTIĞI DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
	1	2	3
ayarlanabilir bir alarm ve otomatize saldırılara otomatik cevap verebilme gibi özelliklere sahip olduğu doğrulanmalıdır. Bu durumlara örnek olarak: - Bir forumun günlük yalnızca 100 tane yeni kullanıcıya izin vermesi ya da yeni kullanıcıların hesapları onaylanana kadar yorum ve özel mesaj haklarının kısıtlanması, - Bir sağlık sisteminin, bir doktorun günlük bakabileceği hasta sayısından daha fazla hastayı doktora atamaması, - Küçük bir finans siteminin kullanıcılar arasında günlük en fazla 1000 ödemeye izin vermesi vb. Her koşulda, işlem limitleri ve toplamları bahsedilen iş için mantıklı olmalıdır.			

Tablo 10 - OWASP ASVS İş Mantığı Doğrulama Gereksinimleri (V15)

V16: Dosya ve Kaynaklar Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	DOSYA VE KAYNAKLAR DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V16.1	URL yönlendirmeleri ve iletimlerinin onaylanmamış verileri içermediği doğrulanmalıdır.	✔	✔	✔
V16.2	Güvenilmeyen kaynaklardan elde edilen dosya isimleri ve dizin bilgilerinin, dizin gezinme saldırılarını engellemek için kontrolden geçtiği doğrulanmalıdır.	✔	✔	✔
V16.3	Güvenilmeyen kaynaklardan elde edilen dosyaların, zararlı içerik yüklenmesini engellemek amacıyla antivirüs sistemleri tarafından taramadan geçirildiği doğrulanmalıdır.	✔	✔	✔
V16.4	Lokal Dosya Yerleştirme (Local File Inclusion) saldırılarını önlemek amacıyla, güvenilmeyen kaynaklardan elde edilen değişkenlerin girdi doğrulamadan geçmeden dosya isimlerinde, dizin isimlerinde ya da herhangi bir sistem dosya nesnesinde kullanılmadığı doğrulanmalıdır.	✔	✔	✔
V16.5	Uzaktan Dosya Yerleştirme (Remote File Inclusion) saldırılarını önlemek amacıyla, güvenilmeyen kaynaklardan elde edilen	✔	✔	✔

	değişkenlerin girdi doğrulamasından geçtiği, standartlaştırıldığı ve kodlanmış şekilde çıktıya gönderildiği doğrulanmalıdır. Bu kontrollerden geçmeyen girdiler, uygulamada başlık, kaynak kod veya sayfa şablonu olarak çalıştırılabilir.			
V16.6	Uygulamada bulunan IFRAME ve HTML5 alanlar arası (cross-domain) kaynakların, sayfaya gelişi güzel uzak kaynak eklemesine izin verilmediği doğrulanmalıdır.	✓	✓	✓
V16.7	Güvenilmeyen kaynaklardan elde edilen dosyaların uygulamanın kökdizini (webroot)'nin dışında bir yerde tutulduğu doğrulanmalıdır.		✓	✓
V16.8	Uygulama sunucusunun uzak/yabancı kaynaklara veya uygulama sunucusu dışındaki kaynaklara erişiminin varsayılan olarak engellenecek şekilde yapılandırıldığı doğrulanmalıdır.		✓	✓
V16.9	Uygulamanın güvenilmeyen kaynaklarca yüklenen kaynakları çalıştırmadığı doğrulanmalıdır.		✓	✓
V16.10	Uygulama eğer Flash, Silverlight ve benzeri zengin internet uygulaması (RIA) barındırıyorsa, bu uygulamaların alanları arası kaynak paylaşımlarının yetkisiz erişim ya da kimlik doğrulamaya karşı zafiyetli olmadığı doğrulanmalıdır.		✓	✓

Tablo 11 - OWASP ASVS Dosya ve Kaynaklar Doğrulama Gereksinimleri (V16)

V17: Mobil Doğrulama Gereksinimleri

Alttaki tablo, her bir doğrulama seviyesine karşılık gelen doğrulama gereksinimlerini tanımlamaktadır. Bu standart, Seviye Sıfır (0) için var olan doğrulama gereksinimlerini kapsamamaktadır.

	MOBİL DOĞRULAMA GEREKSİNİMLERİ	SEVİYE		
		1	2	3
V17.1	İstemcinin, SSL sertifikaların geçerliliğini kontrol ettiği doğrulanmalıdır.	✓	✓	✓
V17.2	Tekil Cihaz Kimlik Bilgisi (UDID) değerlerinin güvenlik kontrolü için kullanılmadığı doğrulanmalıdır.	✓	✓	✓
V17.3	Mobil uygulamanın hassas verileri cihaz üzerindeki herkes tarafından erişilebilir alanlar (SD Kart, paylaşımlı dosyalar) üzerinde saklamadığı doğrulanmalıdır.	✓	✓	✓
V17.4	Hassas verilerin cihaz üzerindeki SQLite veritabanlarında saklanmadığı doğrulanmalıdır.	✓	✓	✓
V17.5	Gizli anahtarların (secret-key) ve parolaların çalıştırılabilir mobil uygulama (executable) üzerinde gömülü kodlanmış olarak bulunmadığı doğrulanmalıdır.		✓	✓
V17.6	Mobil uygulamanın, hassas verilerin iOS'un auto-snapshot özelliği		✓	✓

	MOBİL DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
	(home butonuna basıldığında o anki ekran görüntüsünün kaydedilmesi) ile sızmasını önlediği doğrulanmalıdır.			
V17.7	Uygulamanın Jailbreak yapılmış veya root'lanmış cihazlar üzerinde çalışmadığı doğrulanmalıdır.		✔	✔
V17.8	Oturum zaman aşımı değerinin makul bir süre olarak ayarlandığı doğrulanmalıdır.		✔	✔
V17.9	Talep edilen izinler ve kaynakların, erişim yetkisi kontrollerinden geçtiği doğrulanmalıdır. (Örnek olarak, AndroidManifest.xml, iOS Entitlements).		✔	✔
V17.10	Uygulamanın hata kayıtlarının hassas veri içermediği doğrulanmalıdır.		✔	✔
V17.11	Derlenmiş uygulama kodlarının (binary) kod karıştırma teknikleri ile korunduğu doğrulanmalıdır.			✔
V17.12	Tüm test verilerinin, .ipa, .apk, .bar gibi uygulama paketlerinin içerisinden kaldırıldığı/temizlendiği doğrulanmalıdır.		✔	✔
V17.13	Uygulamanın hassas verileri sistem kayıtlarında (system log) veya dosya sistemi üzerindeki kayıtlarda tutmadığı doğrulanmalıdır.		✔	✔
V17.14	Uygulamanın, parola ve kişisel bilgiler/kredi kartı bilgisi gibi hassas veri içeren girdi alanlarında otomatik tamamlama özelliğine izin vermediği doğrulanmalıdır.		✔	✔
V17.15	Uygulamanın, uygulamaya ilişkin trafiğin proxy üzerinden iletilmemesi ve proxy üzerinde HTTPS trafiğin açılarak incelenmesini önlemek amacıyla, sertifika iğneleme/sabitleme (certificate pinning) kullandığı doğrulanmalıdır.			✔
V17.16	Uygulamanın yapılandırma dosyalarında hatalı yapılandırma			✔

	MOBİL DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
	bulunmadığı (debug modun açık kalması, okuma/yazma izinlerinin değiştirilebilmesi) ve bu yapılandırma ayarlarının varsayılan değerlerinin en güvenli değerlere sahip olduğu doğrulanmalıdır.			
V17.17	Kullanılan üçüncü parti kütüphanelerin güncel olduğu ve hiçbir güvenlik açığı içermediği doğrulanmalıdır.			✔
V17.18	HTTPS trafiği gibi web verilerinin önbellekte saklanmadığı doğrulanmalıdır			✔
V17.19	Hassas veri içeren sorgu isteklerinin GET talebi ile URL üzerinden değil, SSL üzerinden iletilen ve CSRF anahtarı (token) ile korunan POST talepleri aracılığıyla gönderildiği doğrulanmalıdır.			✔
V17.20	Kişisel hesap bilgilerinin cihaz üzerinde saklanmadan önce - eğer mümkünse - kırpıldığı veya maskelendiği doğrulanmalıdır.			✔
V17.21	Uygulamanın ASLR (Address Space Layout Randomization) yöntemini/korumasını kullandığı doğrulanmalıdır.			✔
V17.22	iOS işletim sistemine sahip cihazlarda otomatik yazım düzeltme fonksiyonunun çalışması için kaydedilen klavye girdileri içerisinde, kullanıcı kimlik bilgileri, finansal bilgiler ya da herhangi bir hassas verinin bulunmadığı doğrulanmalıdır.			✔
V17.23	Eğer uygulama bir Android uygulaması ise, uygulamanın dosyaları MODE_WORLD_READABLE veya MODE_WORLD_WRITABLE yetkileri ile oluşturmadığı doğrulanmalıdır.			✔
V17.24	Hassas verilerin kriptografik olarak güvenli şekilde saklandığı doğrulanmalıdır (iOS Keychain üzerinde saklandığı durumlar da dahil olmak üzere.)			✔
V17.25	Uygulamanın, hata ayıklamayı engelleyici (anti-debugging) ve tersine			✔

	MOBİL DOĞRULAMA GEREKSİNİMLERİ	SEVİYE 1	2	3
	mühendislik (reverse engineering) saldırılarına karşı önleyici mekanizmalar bulundurduğu doğrulanmalıdır.			
V17.26	Android uygulamalarının, uygulama için hassas düzeyde olan aktiviteleri, intent nesnelerini ve içerik sağlayıcılar (content provider)'ı diğer uygulamaların kullanımına açmadığı (export) doğrulanmalıdır.			✔
V17.27	Hesap numaraları gibi hassas veriler için değiştirilebilir (mutable) veri tiplerinin kullanıldığı ve bu hassas verilerin kullanılmadığı zamanlarda üzerine yazılarak (overwritten) bellek analizi saldırılarına karşı önlem alındığı doğrulanmalıdır.			✔
V17.28	Android uygulamalarında, diğer uygulamaların kullanımına açılan (export) içerik sağlayıcıların (content provider), yayın alıcıların (broadcast receiver) ve intent nesnelerinin eksiksiz bir girdi denetimine tabi tutulduğu doğrulanmalıdır.			✔

Tablo 12 - OWASP ASVS Mobil Doğrulama Gereksinimleri (V17)

Ek A: ASVS'nin Pratikte Uygulanması

Farklı tehditler farklı motivasyonlara ve bazı endüstriler, benzersiz teknoloji varlıklarına, benzersiz bilgilere ve benzersiz uyumluluk denetimlerine sahiptir.

Aşağıda, ilgili ASVS seviyeleri için endüstriye özel kılavuzlar sunuyoruz. Her ne kadar her endüstrinin kendine özel kriterleri ve farklılıkları olsa da, tüm endüstriler için geçerli olan ortak görüş; internete açık olan uygulamaların fırsatçı saldırganlar tarafından istismar edilmesi her zaman mümkündür. Bu sebeple ASVS seviye 1, endüstri bağımsız olarak tüm internete açık uygulamalar için tavsiye edilmektedir. Az sayıda risk faktörünü kapsadığı için bu bir başlangıç noktası olarak görülebilir. Organizasyonlar bu seviyeden sonra mutlaka kendi iş alanlılarını ilgilendiren risk faktörlerine derinlemesine eğilmelidirler. En üst seviye olan ASVS Seviye 3 ise insan güvenliğini ilgilendiren veya organizasyonun tamamı açısından kritik uygulamalar gibi yüksek risk taşıyan uygulamalar için tavsiye edilmektedir.

İŞ ALANLARI	TEHDİT PROFİLİ	ÖNERİLEN ASVS SEVİYESİ
Finans ve Sigorta (Finance and Insurance)	Her ne kadar bu iş alanındaki uygulamalar ilk aşamada fırsatçı saldırganların ilgisini çekse de, özellikle finansal alana motive olmuş tecrübeli saldırganlar da bu iş alanları için büyük bir tehdittir. Saldırganlar genel olarak kullanıcılara ait özel bilgileri ve hesap bilgilerini ele geçirmeye çalışmaktadır. Bunun yanında uygulamalar aracılığı ile yapılan para hareketleri ve fonksiyonlarında sahtekarlık yapmaya çalışmaktadırlar. Teknik olarak kullanıcı giriş bilgilerinin çalınması, uygulama seviyesindeki saldırılar ve sosyal mühendislik saldırıları gibi saldırılar kullanılmaktadır. Bazı büyük uyum hususları (compliance considerations) Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leech Bliley act, Sarbanes Oxley (SOX)'i kapsamaktadır.	*Seviye 1: internete açık tüm uygulamalar.* *Seviye 2: Sınırlı yollardan sınırlı paraları taşınmasına sebep olabilecek, kredi kartı numarası ve diğer hassas bilgileri içeren uygulamalar. Örnek olarak: Aynı kurum içinde iki hesap arasında para aktarımı* *Seviye 3: Hızlı bir şekilde büyük miktarlarda para transferine ya da bireysel küçük para transferleri toplamı ile büyük para transferine sebep olabilecek, birçok hassas bilgi içeren uygulamalar.*

Üretim, Profesyonel Ulaşım, Teknoloji, Kamu Kuruluşları, Altyapı ve Savunma	Bu alanlar ilk bakışta pek ortak bir nokta barındırmıyor gibi gözükse de, bu iş alanlarına tehdit olabilecek saldırganlar ortak olarak daha deneyimli, işine odaklanmış ve daha zengin kaynaklara sahip kişilerdir. Bu alanlarda, hassas bilgilerin ve sistemlerin yerini tespit etmek zordur ve genel olarak bunların tespiti için içerden yardım almak ya da sosyal mühendislik gibi teknikler uygulamak gerekir. Saldırganlar içerden, dışardan veya ikisinin birleşimi de olabilir. Saldırılar, akıllı/değerli sistemlere erişim kazanma ya da teknik olarak avantaj sağlama gibi yöntemler içerebilir. Ayrıca uygulamanın işleyişini aksatıp hassas sistemlere zarar vermek isteyecek saldırganlar da göz ardı edilmemelidir.	*Seviye 1: İnternete açık tüm uygulamalar.*	
		Seviye 2: Sosyal mühendislik saldırılarında kullanılabilecek personel bilgilerini içeren uygulamalar. Değerli fikir ve ticaret sırlarını saklayan uygulamalar.	
		Seviye 3: Organizasyonun devamı ve başarısı için gerekli olan gizli bilgileri, sırları, devlet sırlarını saklayan uygulamalar. İnsan hayatını tehlikeye atabilecek kritik sistemlere sahip uygulamalar. (ulaşım sistemleri parçaları üretimi, kontrol sistemler)	

Sağlık	Birçok saldırgan, kimlik doğrulama sonucu yapılan para transferi işlemlerini istismar etmek için kimlik bilgisi gibi hassas bilgileri ele geçirmeye çalışmaktadır. Elde edilen bu bilgiler, kimlik çalınması ile yapılan hileli ödemeler ve birçok dolandırıcılık işlemde kullanılmaktadır.	*Seviye 1: internete açık tüm uygulamalar.*
		Seviye 2: Orta düzeyde hassas sağlık bilgisi taşıyan uygulamalar. (Sağlık ödemeleri, ilaç ödemeleri, ilaç bilgileri)
		Seviye 3: Medikal cihazları, sistemleri ve kayıtları kontrol eden ve insan hayatını etkileyebilecek uygulamalar. *Dolandırıcılık için kullanılabilecek birçok hassas bilgi barındıran POS sistemleri. Bunlar aynı zamanda bu uygulamarın yönetim ekranlarını da kapsar.*
Tüketim, Gıda, Konaklama	Bu alandaki saldırganlar genel olarak "kap kaç" taktikleri uygulamaktadır. Bunun yanında ödeme sistemleri ve kimlik bilgileri gibi hassas sistemler için de her zaman genel tehditler mevcuttur. Çok fazla rastlanmamakla beraber, ayrıca organizasyonun hassas bilgilerine ve gizli sırlarına erişmeye çalışan daha kapsamlı saldırılar da görülmektedir.	*Seviye 1: internete açık tüm uygulamalar.*

	Seviye 2: Kısıtlı kullanıcı bilgisi, şirket anlaşmaları, ürün katalog bilgileri içeren iş uygulamarı için uygundur. Orta düzey ödeme bilgileri ve sistemleri içeren uygulamalar.
	Seviye 3: Dolandırıcılık için kullanılabilecek birçok hassas bilgi barındıran POS sistemleri. Bu aynı zamanda bu uygulamarın yönetim ekranlarını da kapsar. *Kredi kartı bilgisi, anne kızlık soyadı, tc kimlik numarası gibi birçok hassas bilgi içeren uygulamalar.*

Tablo 14 – ASVS'nin Pratikte Uygulanması

Ek B: Sözlük

- *Erişim Kontrolü* – Kullanıcıların içinde bulundukları kimlik veya gruba göre dosyalara, URL'lere veya diğer kaynaklara erişiminin sınırlanmasıdır.
- *Uygulama Bileşeni* – Doğrulamayı yapan kişi tarafından tanımlanan uygulamaya ait bir veya birden çok dosya, kütüphane vb. kaynaktır.
- *Uygulama Güvenliği* – Open Systems Interconnection Reference Model(OSI Modeli)'nin uygulama seviyesinde yer alan ve uygulama seviyesindeki güvenlik açıklarına odaklı olarak uygulamanın bileşenlerinin analizidir. Uygulama güvenliği, işletim sistemi veya bağlı olunan ağları odak noktası olarak almaz.
- *Uygulama Güvenliği Doğrulama* – Bir uygulamanın OWASP ASVS baz alınarak teknik olarak incelenmesidir.
- *Uygulama Güvenliği Doğrulama Raporu* – Bir uygulama için yapılan doğrulama ile ilgili genel sonuçları ve destekleyici analizleri içeren dokümandır.
- *Uygulama Güvenliği Doğrulama Standardı (ASVS)* – Uygulamalar için dört seviyeden oluşan bir uygulama güvenliği doğrulaması sunan bir OWASP standartıdır.
- *Kimlik Doğrulama* – Sunulan kullanıcı kimliğinin doğrulanmasıdır.
- *Otomatize Doğrulama* – Zafiyet imzalarını kullanarak sorunları tespit eden otomatize araçların kullanılmasıdır.(dinamik, statik ya da ikisinin birlikte kullanıldığı araçlar)
- *Arka Kapı(Back Door)* – Bir uygulamaya yetkisiz giriş sağlayan zararlı kod parçası.
- *Kara Liste(Blacklist)* – İzin verilmeyen bir liste halindeki veri ya da operasyonlar.
- *Sertifika Otoritesi(Certificate Authority -CA)* – Dijital sertifikalar dağıtan kurum.
- *Ortak Kriter (Common Criteria - CC)* – IT ürünlerindeki üzerinde güvenlik kontrollerinin tasarım ve uygulanışının doğrulamalarında kullanılabilecek çok aşamalı standart.
- *İletişim Güvenliği* – Uygulamaya ait verilerin, uygulama bileşenleri, istemci-sunucu ve dış sistemlerle uygulama arasında iletişimi sırasında korunması.
- *Siteler Arası Betik Çalıştırma (XSS)* – Tipik olarak web uygulamalarında görülen ve istemci tarafındaki içeriğe müdahale edilmesine izin veren bir zafiyet.
- Basamaklı Biçim Sayfaları *(CSS)* - HTML gibi biçimleme dillerinde yazılan dokümanlarda, sunum işaretlerini tanımlamaya yarayan stil sayfalarıdır.
- *Tasarım Doğrulama* – Bir uygulamanın güvenlik tasarımının değerlendirilmesidir.

- İçerden Doğrulama – Bir uygulamadaki güvenlik tasarımına ait spesifik varlıkların OWASP ASVS standardında tanımlandığı şekilde teknik olarak değerlendirilmesidir.
- *Kriptografik Modül (Cryptographic module)* – Şifreleme algoritmaları ya da şifreleme anahtarları üreten donanım veya yazılım.
- *Servis Dışı Bırakma Saldırıları (DOS)* – Bir uygulamanın kaldırabileceğinden daha fazla istek ile servis veremez duruma getirilmesidir.
- *Dinamik Doğrulama* – Zafiyet imzalarını kullanarak zafiyetlerini tespit eden otomatik araçlar yoluyla yapılan doğrulama.
- *Easter Eggs* – Özel bir olay veya kullanıcı tarafından tetiklenen ve bu tetikleme anına kadar çalışmayan zararlı kod parçası.
- *Harici Sistemler* – Uygulamanın bir parçası olmayan sunucu taraflı uygulama ya da servis.
- *FIPS 140-2* – Şifreleme modüllerinin tasarımı ve uygulanması sırasında temel alınabilecek bir standart.
- Genel Benzersiz Tanımlayıcı (Globally Unique Identifier - *GUID)* – Bir yazılımda tanımlayıcı olarak kullanılan benzersiz referans numarası.
- Hiper Metin Transfer Protokolü *(HTTP)* – Dağınık, işbirlikçi hiper-medya bilgi sistemleri için tasarlanmış bir uygulama protokolü. An application protocol for distributed, collaborative, hypermedia information systems. World Wide Web veri iletişimi temelidir.
- Hiper Metin Biçim Dili *(HTML)* – Tarayıcıda gösterilen web sayfaları ve diğer verilerin yaratılması için kullanılan ana biçim dilidir.
- *Girdi Doğrulama* – Güvenilmeyen kullanıcı girdilerinin doğrulanması ve standartlaştırılmasıdır (canonicalization).
- Basit Dizin Erişim Protokolü (*LDAP)* – Bir ağdaki dağınık dosya bilgi servislerine erişmek ve idame ettirmek için kullanılan uygulama protokolü.
- *Zararlı Kod (Malicious Code)* – Bir kodun geliştirilmesi esnasında uygulama sahibinden gizli olarak yerleştirilen ve uygulama güvenliği politikasını bozan kod parçacığı. Code introduced into an application during its development unbeknownst to the application owner, which circumvents the application's intended security policy. Zararlı yazılım(malware), virüsler ya da solucanlar (worm)'dan farklıdır.
- *Zararlı Yazılım (Malware)* – Uygulama kullanıcısı ya da yöneticisinin haberi olmadan, uygulama koşarken içine yerleştirilen çalışabilir zararlı kod parçası.
- *Open Web Application Security Project (OWASP)* – Kurumların güvenli uygulamalar geliştirmeleri, güvenli uygulamalar satın almaları ve uygulamaları güvenli bir şekilde sürdürmelerine yardımcı olmak amaçlarını benimsemiş açık bir topluluktur. Bkz: http://www.owasp.org/
- *Çıktı Doğrulama* – Tarayıcı ya da harici sistemlere gönderilen uygulama çıktısının doğrulanması ve standartlaştırılmasıdır.
- *OWASP Enterprise Security API (ESAPI)* – Güvenlik yazılım geliştirmek için geliştiricilerin ihtiyaç duyacağı tüm güvenlik metodlarını barındıran açık kaynak kodlu kütüphanelerdir. Bkz: http://www.owasp.org/index.php/ESAPI
- *OWASP Risk Rating Methodology* – Uygulama güvenliği için özelleştirilmiş bir risk oranlama/belirleme metadolojisidir. Bkz: http://www.owasp.org/index.php/How_to_value_the_real_risk

- *OWASP Testing Guide* – Organizasyonlara bir test programının neler içerdiğini anlatmak ve kendi test programlarını yaratmada yardımcı olmak amacıyla oluşturulmuş döküman. Bkz: http://www.owasp.org/index.php/Category:OWASP_Testing_Project
- *OWASP Top Ten* – Geniş mutabakat ile belirlenen en kiritik Web uygulama güvenliği zafiyetlerini sunan döküman. Bkz: http://www.owasp.org/index.php/Top10
- *Salami Saldırısı (Salami Attack)*– Finansal para aktarımlarında fark edilmeden az miktarlardaki parayı saldırganların hesaplarına yönlendiren zararlı kod parçası.
- *Güvenlik Mimarisi* – Uygulama tasarımında güvenlik kontrollerinin nerde ve nasıl kullanıldığını tanımlayan bir soyutlamadır.
- *Güvenlik Kontrolü* – Güvenlik kontrolü yapan bir fonksiyon ya da bileşen. (Ör: Erişim yetkisi kontrolü)
- *Güvenlik Yapılandırması* – Güvenlik kontrollerinin nasıl kullanılacağını etkileyen işyeliş zamanı uygulama yapılandırmasıdır.
- *Statik Doğrulama* – Uygulama kaynak kodundaki sorunları zafiyetlerin imzalarını kullanarak tespit etmeye çalışan otomatik araçların kullanılması.
- *SQL Enjeksiyonu (SQLi)* **–** Veri tabanlı uygulamalarda, bir girdi noktasına zararlı SQL cümleciklerinin yerleştirilmesi ile gerçekleştirilen bir kod yerleştirme saldırısıdır.
- *Doğrulama Hedefi (TOV)* – Eğer OWASP ASVS gereksinimlerine göre bir uygulama doğrulaması gerçekleştiriyorsanız, doğrulama belli bir uygulama üzerinde olacaktır. Bu da kısaca "Doğrulama Hedefi"(Target of Verification) olarak anılmaktadır.
- *Tehdit Modelleme* - Önemli teknik iş varlıklarını, güvenlik alanlarını ve tehdit ajanlarını belirlemek için iyileştirilmiş güvenlik mimarilerinin sürekli geliştirilmesidir.
- *Zaman Bombası (Time Bomb)* – Belli bir zaman gelmeden ya da geçmeden çalışmayan zararlı kod parçası.
- *İletişim Katmanı Güvenliği* – İnternet üzerindeki iletişimde güvenliğin sağlanması için uygulanan şifreleme protokolleridir.
- *Kullanıcı Kabul Testi (UAT)* **–** Canlıya çıkmadan önce tüm yazılımların canlı ortamdaki gibi davranan bir ortamda test edilmesi.
- *URI/URL* **–** Tekdüze Kaynak Tanımlayıcı(URI), bir ismi ya da web kaynağını tanımlamak için kullanılan karakter dizisidir. Tekdüze Kaynak Yer Belirleyici(URL) ise genellikle bir kaynağa referans olarak kullanılır.
- *Doğrulayıcı* - Uygulamayı OWASP ASVS gereksinimlerine göre gözden geçiren takım ya da kişidir.
- *Beyaz Liste (Whitelist)*– İzin verilen veri ya da operasyonların listesidir. Ör: girdi doğrulamada kabul edilen karakterler listesi.
- Genişletilebilir İşaretleme Dili (*XML)* **–** Dokümanların kodlanması(encoding) için bir dizi kurallar sunan işaretleme dili.

Ek C: Kaynaklar

OWASP ASVS yaşayan bir dokümandır. Eğer ASVS standartlarını uyguluyorsanız, ASVS proje sayfasında bulunan makalelere her zaman göz atmanızı öneririz. Bkz:http://www.owasp.org/index.php/ASVS

- *OWASP Top Ten Project* - http://www.owasp.org/index.php/Top_10
- *OWASP Kod Analizi Rehberi*- http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- *OWASP Testing Guide* - http://www.owasp.org/index.php/Testing_Guide
- *OWASP Enterprise Security API (ESAPI) Project* - http://www.owasp.org/index.php/ESAPI
- *OWASP Legal Project* - http://www.owasp.org/index.php/Category:OWASP_Legal_Project

Genel Kaynaklar:

- *OWASP* - http://www.owasp.org
- *MITRE* - Common Weakness Enumeration – Vulnerability Trends, http://cwe.mitre.org/documents/vuln-trends.html
- *PCI Security Standards Council* - publishers of the PCI standards, relevant to all organizations processing or holding credit card data, https://www.pcisecuritystandards.org
- *PCI Data Security Standard (DSS) v2.0* - https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0