Denetci.org

REFERANS İLKELERİ

Güvenlik Doğrulama ve Test İlkeleri

Rİ-GUV-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Güvenlik Doğrulama ve Test İlkeleri

Güvenlik doğrulama ve test, bir sistemin güvenli olduğuna ilişkin varsayım ve iddiaların uygun kanıtlarla sınanmasını ele alır. Amaç belirli test yöntemleri, araçları veya sıklıkları zorunlu kılmak değil; güvenlik güvencesinin kontrol varlığına veya tek seferlik test sonucuna değil, sistemin gerçek davranışına ilişkin yeterli ve sınırları bilinen kanıta dayanmasını sağlamaktır.

İlke 1: Güvenlik doğrulaması kontrolün varlığını değil güvenlik iddiasının doğruluğunu sınamalıdır.

Bir mekanizmanın yapılandırılmış veya etkin görünmesi beklenen korumayı gerçekten sağladığını göstermez. Doğrulamanın başlangıç noktası "hangi kontrol var?" sorusundan çok "hangi güvenlik özelliğinin doğru olduğuna inanıyoruz?" sorusu olmalıdır.

İlke 2: Test edilen güvenlik iddiası açık ve sınanabilir olmalıdır.

"Güvenli", "izole" veya "korunuyor" gibi genel ifadeler hangi davranışın beklenildiğini açıklamadığında anlamlı biçimde doğrulanamaz. Test, sınırları belli bir güven iddiasına ve onu yanlışlayabilecek koşullara dayanmalıdır.

İlke 3: Test kapsamı sistemin gerçek saldırı ve etki yüzeyini temsil etmelidir.

Yalnızca kolay ulaşılabilen bileşenlerin incelenmesi, dışarıda kalan yolların güvenli olduğunu göstermez. Kimlikler, yönetim yolları, entegrasyonlar, istemciler, bağımlılıklar ve başka anlamlı girişler kapsam belirlenirken dikkate alınmalıdır.

İlke 4: Kapsam dışında bırakılan alanlar test edilmiş gibi değerlendirilmemelidir.

Zaman, yetki veya başka nedenlerle bazı bölümler doğrulanamayabilir. Bu sınırlar sonuçların anlamını değiştirdiği için görünür olmalı ve doğrulanmamış alanlar hakkında testin desteklemediği güven çıkarımları yapılmamalıdır.

İlke 5: Doğrulamanın derinliği olası güvenlik etkisiyle uyumlu olmalıdır.

Bütün sistemler ve bütün iddialar aynı düzeyde inceleme gerektirmez. Kritik bir güven sınırı ile düşük etkili bir özellik aynı test derinliğine zorlanmamalı; kullanılan güvence sistemin oluşturabileceği gerçek sonuçlarla orantılı olmalıdır.

İlke 6: Güvenlik yalnızca tek bir saldırgan bakış açısından sınanmamalıdır.

Dış saldırgan, sıradan kullanıcı, ayrıcalıklı kullanıcı, ele geçirilmiş hizmet veya tedarik zinciri gibi farklı konumlar farklı güven sınırlarını ortaya çıkarabilir. Bir perspektifte dirençli olan sistem başka bir güven konumunda farklı zayıflıklar taşıyabilir.

İlke 7: Kimlik doğrulama ile yetkilendirme ayrı güven iddiaları olarak sınanmalıdır.

Bir kimliğin doğru biçimde doğrulanması onun hangi kaynaklarda hangi işlemleri yapabileceğini göstermez. Test, geçerli kimliklerin de gereksiz veya beklenmeyen yetkilere ulaşabileceği ihtimalini değerlendirebilmelidir.

İlke 8: Test yalnızca sistemin izin vermesi gereken davranışları doğrulamamalıdır.

Olumlu senaryolar işlevin çalıştığını gösterir; güvenlik ise izin verilmemesi gereken davranışların da gerçekten engellendiğine dayanır. Yanlış kimlik, yanlış durum, yanlış sıra ve başka beklenmeyen koşullar güvenlik doğrulamasının doğal parçasıdır.

İlke 9: Normal istemci davranışı testin sınırı olmamalıdır.

Gerçek saldırgan kullanıcı arayüzünü, belgelenmiş API kullanımını veya amaçlanan işlem sırasını takip etmek zorunda değildir. Test, güvenlik sınırlarını doğrudan ve değiştirilmiş davranış karşısında da değerlendirebilmelidir.

İlke 10: İş mantığı ve durum geçişleri teknik girdi hataları kadar güvenlik açısından önemlidir.

Tek tek geçerli işlemler birleştiğinde, tekrarlandığında veya farklı sırada kullanıldığında yetkisiz sonuç oluşturabilir. Güvenlik testi yalnızca bilinen teknik zafiyet kalıplarını aramakla sınırlı kalmamalıdır.

İlke 11: Eşzamanlılık, tekrar ve zamanlama anlamlı olduğunda doğrulamanın parçası olmalıdır.

Sistemlerin güvenliği işlemlerin her zaman bir kez ve sıralı gerçekleşeceği varsayımına dayanabilir. Bu varsayım bozulduğunda yetki, kota, veri bütünlüğü veya başka güvenlik özellikleri değişebiliyorsa ilgili davranış sınanabilmelidir.

İlke 12: Test ortamı ve test yetkileri yeni bir güvenlik riski oluşturmamalıdır.

Test hesapları, özel araçlar, ayrıcalıklı erişimler ve kullanılan veriler test amacıyla gerekli olabilir. Bu imkânlar testin kendisini kalıcı veya gereksiz geniş bir erişim yoluna dönüştürmemelidir.

İlke 13: Üretim üzerinde doğrulama yapılması gerçek işletim etkisini dikkate almalıdır.

Bazı güvenlik özellikleri ancak çalışan ortamda anlamlı biçimde doğrulanabilir. Bununla birlikte test faaliyeti veri kaybı, kesinti veya gerçek kullanıcılar üzerinde ölçüsüz etki oluşturmamalıdır; doğrulamanın kendisi kontrolsüz bir saldırıya dönüşmemelidir.

İlke 14: Otomatik araçların sonuçları güvenlik kanıtının tamamı olarak görülmemelidir.

Araçlar geniş alanları tutarlı biçimde inceleyebilir; fakat iş bağlamını, karmaşık yetki ilişkilerini veya aracın modellemediği saldırıları kaçırabilir. Otomatik sonuçlar yorumlanması gereken kanıt girdileridir, güvenliğin nihai hükmü değildir.

İlke 15: Tek bir test yöntemi bütün güvenlik iddiaları için yeterli kabul edilmemelidir.

Kaynak kod, çalışan davranış, yapılandırma, mimari ve dış etkileşimler farklı kanıt yöntemleri gerektirebilir. Yöntem, alışkanlık veya araç mevcudiyetine göre değil sınanmak istenen iddiaya göre seçilmelidir.

İlke 16: Yapılandırma ve mimari iddiaları gerçek davranışla karşılaştırılabilmelidir.

Bir ağın ayrılmış görünmesi veya bir ayarın beklenen değerde olması fiilî erişimin de aynı olduğunu göstermeyebilir. Doğrulama, amaçlanan yapı ile çalışan sistem arasında güvenlik açısından anlamlı farklar bulunup bulunmadığını sınamalıdır.

İlke 17: Güvenlik mekanizmalarının hata davranışı da doğrulanmalıdır.

Kimlik sağlayıcı, ağ sınırı, güvenlik servisi veya başka bağımlılık kullanılamaz hale geldiğinde sistem farklı davranabilir. Normal koşullarda çalışan bir kontrolün başarısızlık anında güven sınırlarını genişletip genişletmediği de güvenlik iddiasının parçasıdır.

İlke 18: Bir saldırının engellenmesi tek başarılı güvenlik sonucu değildir.

Bazı saldırılar bütünüyle engellenemeyebilir. Etkinin sınırlandırılması, olayın görünür hale gelmesi ve sistemin güvenilir duruma dönebilmesi de doğrulanabilir güvenlik özellikleridir.

İlke 19: Saldırı simülasyonu gerçek savunma kapasitesini sınamalıdır.

Bir saldırı tekniğinin uygulanabilmiş olması tek başına kuruluşun savunmasının başarısız olduğunu; uygulanamamış olması da başarılı olduğunu göstermeyebilir. Simülasyon, önleme, tespit, anlamlandırma ve müdahalenin birlikte nasıl çalıştığını değerlendirebilmelidir.

İlke 20: Test senaryoları yalnızca geçmişte bilinen saldırılara bağlı kalmamalıdır.

Geçmiş zafiyetler değerli örneklerdir; ancak yeni sistem özellikleri ve güven ilişkileri daha önce kataloglanmamış hata biçimleri oluşturabilir. Doğrulama, sistemin kendi güven varsayımlarından da senaryo üretebilmelidir.

İlke 21: Bulgunun önemi yalnızca teknik sınıfına veya aracın verdiği puana bağlı olmamalıdır.

Aynı teknik zayıflık farklı sistemlerde çok farklı sonuçlar doğurabilir. Ciddiyet; erişilebilirlik, gerekli koşullar, etkilenen varlıklar, oluşturulabilecek sonuç ve mevcut savunmalarla birlikte anlaşılmalıdır.

İlke 22: Test kanıtı yeniden değerlendirilebilir olmalı ancak gereksiz zarar üretmemelidir.

Bir bulgunun neye dayandığı başka bir yetkin tarafça anlaşılabilmelidir. Bunun için gerçek verinin gereksiz kopyalanması, sistemin bozulması veya zayıflığın ihtiyaç dışı biçimde yayılması gerekmemelidir.

İlke 23: Test sonucu desteklediği kesinlik sınırını aşmamalıdır.

Bir zafiyet bulunamamış olması zafiyet olmadığı anlamına gelmez; bulunan bir davranışın da her koşulda aynı etkiyi oluşturacağı varsayılamaz. Güvence, kullanılan yöntemin kapsamı ve sınırlılıkları açıkça bilinerek yorumlanmalıdır.

İlke 24: Başarılı bir test sonucu kalıcı güven damgası oluşturmamalıdır.

Sistem, bağımlılıkları, kullanımı ve tehdit ortamı değişebilir. Geçmişte test edilmiş olmak gelecekteki farklı bir sistem durumu için otomatik güvence sağlamamalıdır.

İlke 25: Yeniden doğrulama yalnızca takvimsel bir faaliyet olmamalıdır.

Önemli değişiklikler, yeni saldırı bilgileri, güvenlik olayları veya önceki varsayımları etkileyen başka gelişmeler güvenlik iddialarının yeniden sınanmasını gerektirebilir. Test ihtiyacı yalnızca geçen zamana göre belirlenmemelidir.

İlke 26: Bir düzeltmenin doğrulanması eski saldırı adımının artık çalışmamasından ibaret olmamalıdır.

Düzeltme sorunun kaynağını ortadan kaldırmamış, saldırıyı başka yola taşımış veya yeni bir zayıflık oluşturmuş olabilir. Yeniden test, düzeltilmek istenen güvenlik iddiasının gerçekten sağlanıp sağlanmadığını değerlendirmelidir.

İlke 27: Tekrarlanan bulgular daha temel bir sistem sorununa işaret edebilmelidir.

Aynı hata sınıfının farklı yerlerde sürekli ortaya çıkması yalnızca ayrı ayrı geliştirici hataları olmayabilir. Mimari, ortak bileşen, geliştirme yaklaşımı veya güvenlik varsayımında yapısal bir neden bulunup bulunmadığı sorgulanmalıdır.

İlke 28: Doğrulama yeterince bağımsız muhakemeye sahip olmalıdır.

Sistemi tasarlayan taraf kendi varsayımlarını fark etmeden doğrulamaya taşıyabilir. Bağımsız bakış bu kör noktaları azaltabilir; ancak bağımsızlık sistemi ve iş bağlamını anlamamayı gerektirmez.

İlke 29: Güvenlik doğrulamasının güvencesi gerçek iddiaların kanıtla sınanmasına dayanmalıdır.

Test raporu, tarama sonucu, sertifika veya tamamlanmış faaliyet listesi tek başına güvence oluşturmaz. Güvence; sistem hakkında önemli güvenlik iddialarının uygun yöntemlerle sınanmış, sonuçlarının sınırları anlaşılmış ve elde edilen kanıtın gerçek sistem davranışıyla ilişkilendirilebilir olmasıyla oluşmalıdır.