Denetci.org

REFERANS İLKELERİ

API Güvenliği İlkeleri

Rİ-YAZ-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

API Güvenliği İlkeleri

API güvenliği, sistemlerin birbirlerine hangi kimlik, veri, işlem ve yetki sınırları içinde hizmet sunduğunu ele alır. Amaç belirli bir API teknolojisi, ağ geçidi veya kimlik doğrulama yöntemi belirlemek değil; istemcinin değiştirilebilir ve ele geçirilebilir olduğu kabulü altında API'nin kendi güvenlik sınırlarını bağımsız biçimde koruyabilmesini sağlamaktır.

İlke 1: Bir API'nin erişilebilir olması kullanımının güvenilir olduğu anlamına gelmemelidir.

Bir istemcinin API'ye bağlanabilmesi veya doğru biçimde istek gönderebilmesi, kimliğinin, amacının veya yapmak istediği işlemin güvenilir olduğunu göstermez. Bağlantı ile güven kararı birbirinden ayrılmalıdır.

İlke 2: API adına işlem yaptığı tarafı gerektiği ölçüde ayırt edebilmelidir.

İnsan kullanıcılar, uygulamalar, hizmetler ve otomasyonlar farklı sorumluluk ve güven ilişkileri oluşturabilir. Bir işlemin hangi taraf adına gerçekleştiği önemliyse bu bilgi teknik bağlantının arkasında kaybolmamalıdır.

İlke 3: Kimliğin doğrulanması işlemin yetkili olduğunu göstermemelidir.

Geçerli bir kimlik yalnızca tarafın kim olduğuna ilişkin güven sağlar. Hangi işlemi, hangi kaynak üzerinde ve hangi kapsamda yapabileceği ayrıca belirlenmelidir.

İlke 4: Bir kaynağın tanımlayıcısını bilmek erişim hakkı oluşturmamalıdır.

Kayıt numarası, adres, isim veya başka bir teknik tanımlayıcının tahmin edilemez olması gerçek erişim kontrolünün yerine geçmez. API, her önemli kaynağın erişimini gerçek kimlik ve yetki bağlamında değerlendirebilmelidir.

İlke 5: Yetki yalnızca uç nokta veya işlev düzeyinde kalmamalıdır.

Bir tarafın belirli bir işlemi çağırabilmesi, bu işlem üzerinden erişilebilen bütün kayıtları, alanları veya özellikleri kullanabilmesi anlamına gelmez. Yetki, işlemin gerçek veri ve durum etkisine kadar anlamını korumalıdır.

İlke 6: İstemcinin gönderebildiği veri ile değiştirmeye yetkili olduğu durum aynı şey olmamalıdır.

Bir alanın teknik olarak istek içerisinde gönderilebilmesi sistemin o alan üzerinde istemciye karar yetkisi verdiği anlamına gelmez. API, istemcinin değiştirebileceği sistem durumunu açık biçimde sınırlandırmalıdır.

İlke 7: API amaç için gerekli olandan fazla veri açığa çıkarmamalıdır.

Bir teknik nesnenin içinde bulunması bütün alanların istemciye aktarılması için yeterli gerekçe değildir. Veri paylaşımı istemcinin gerçek işlevi ve erişim hakkıyla sınırlı olmalıdır.

İlke 8: Kimliği doğrulanmış istemciden gelen veri yine de dış girdidir.

Geçerli kullanıcı veya hizmetler de hata yapabilir, ele geçirilebilir veya beklenmeyen değerler gönderebilir. API'nin kendi veri, sorgu, dosya, ağ ve iş mantığı sınırları istemcinin iyi davranacağı varsayımına bırakılmamalıdır.

İlke 9: API'nin sahip olduğu yetkiler istemci girdisi aracılığıyla görünmez biçimde devredilmemelidir.

Bir API uzak sistemlere, dosyalara veya başka hizmetlere erişebiliyorsa istemcinin verdiği hedef bu erişimi sınırsız biçimde yönlendirememelidir. Sunucunun teknik gücü, istemcinin fiilî gücü haline gelmemelidir.

İlke 10: İş mantığı yalnızca tek bir isteğin teknik geçerliliğine dayanarak korunmamalıdır.

Tek başına meşru olan bir işlem çok sık, otomatik, farklı sırada veya alışılmadık ölçekte kullanıldığında farklı sonuç oluşturabilir. API, iş kurallarını istemcinin normal arayüz akışını takip edeceği varsayımına bağlamamalıdır.

İlke 11: Bir isteğin oluşturabileceği etki yalnızca boyutuyla veya sayısıyla değerlendirilmemelidir.

Küçük bir istek yoğun hesaplama, büyük veri aktarımı veya başka sistemlerde önemli işlemler başlatabilir. Kaynak kullanımı ve hizmet üzerindeki etki istemcinin oluşturabileceği gerçek maliyet üzerinden düşünülmelidir.

İlke 12: Ortak kaynaklar tek bir istemcinin davranışına sınırsız bağımlı olmamalıdır.

Hatalı, ele geçirilmiş veya aşırı kullanan bir istemci diğer tarafların hizmete erişimini ölçüsüz biçimde etkileyememelidir. Kullanılabilirlik de API'nin güven sınırlarından biridir.

İlke 13: Tekrar ve eşzamanlılık işlem anlamını değiştirebildiğinde açık biçimde ele alınmalıdır.

Aynı isteğin yeniden gönderilmesi veya iki işlemin aynı anda gerçekleşmesi, ödeme, kota, durum değişikliği veya başka iş kurallarında beklenmeyen sonuç doğurabilir. API'nin güvenilirliği isteklerin her zaman bir kez ve sırayla geleceği varsayımına dayanmamalıdır.

İlke 14: Geçmişte geçerli bir istek veya yetki bilgisi sınırsız süreyle yeniden kullanılabilir olmamalıdır.

Bazı işlemlerde zaman ve işlem bağlamı güvenin parçasıdır. Daha önce geçerli olmuş bir belirteç, imza veya istek sonraki bir zamanda aynı etkiyi otomatik olarak oluşturmamalıdır.

İlke 15: API kimlik bilgileri sağladıkları gerçek erişim kadar kritik kabul edilmelidir.

Anahtar, belirteç veya başka bir teknik kimlik bilgisi ele geçirildiğinde hangi veri ve işlemlere ulaşılabildiği onun güvenlik değerini belirler. Bu unsurların kapsamı ve yaşamı ihtiyaç duyulan güven ilişkisinden gereksiz biçimde daha geniş olmamalıdır.

İlke 16: API güvenliği tek bir merkezi aracının kusursuzluğuna bağlı olmamalıdır.

Ağ geçitleri veya merkezi güvenlik katmanları ortak kontroller sağlayabilir; ancak kaynağın veya işlemin anlamını en iyi bilen bileşenin gerekli güvenlik kararlarını bütünüyle kaybetmesine yol açmamalıdır. Tek bir merkezi hata bütün API güven sınırlarını ortadan kaldırmamalıdır.

İlke 17: İç API'ler de gerçek güven sınırları içinde çalışmalıdır.

Bir API'nin yalnızca kuruluş ağı veya diğer arka uç hizmetleri tarafından kullanılması istemcilerinin hata yapmayacağı veya ele geçirilmeyeceği anlamına gelmez. İç konum, kimlik ve yetki ihtiyacını otomatik olarak ortadan kaldırmamalıdır.

İlke 18: API tüketmek de API sunmak kadar bir güven ilişkisi oluşturur.

Başka bir hizmetten alınan veri yalnızca güvenilir bir sağlayıcıdan geldiği için doğru veya güvenli kabul edilmemelidir. Dış veya iç API'lerin hatalı ya da saldırgan tarafından etkilenmiş davranışı, tüketen sistemin güven sınırlarını aşamamalıdır.

İlke 19: API sürümleri ve değişiklikleri geçmiş güvenlik sınırlarını görünmez biçimde sürdürmemelidir.

Yeni bir sürümde daha güçlü güvenlik oluşturulması, eski ve daha zayıf arayüz erişilebilir kaldığı sürece gerçek güvenlik düzeyini değiştirmeyebilir. Yeni alanlar ve işlevler de mevcut veri veya yetki sınırlarını fark edilmeden genişletmemelidir.

İlke 20: API güvencesi gerçek istek ve etki davranışı üzerinden doğrulanabilmelidir.

API belgeleri, sözleşmeler, ağ geçitleri veya güvenlik testleri tek başına güvence oluşturmaz. Gerçekte hangi istemcilerin hangi veri ve işlemlere erişebildiği, beklenmeyen isteklerin ne sonuç doğurduğu, tek bir istemcinin ne kadar etki oluşturabildiği ve eski ya da alternatif erişim yollarının güvenlik sınırlarını aşıp aşmadığı gerektiğinde gösterilebilmelidir.