Denetci.org

REFERANS İLKELERİ

Web Uygulaması Güvenliği İlkeleri

Rİ-YAZ-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

Web Uygulaması Güvenliği İlkeleri

Web uygulaması güvenliği, tarayıcı, kullanıcı, sunucu, uygulama bileşenleri ve dış içerikler arasındaki güven ilişkilerinin güvenli biçimde kurulmasını ele alır. Amaç belirli web zafiyetleri için bir kontrol listesi oluşturmak değil; tarayıcıdaki kodun, kullanıcı girdisinin ve görünür uygulama akışının değiştirilebileceği kabulü altında güvenlik kararlarının doğru tarafta ve doğru bağlamda alınmasını sağlamaktır.

İlke 1: Tarayıcı güvenilir bir yürütme ortamı olarak kabul edilmemelidir.

Tarayıcıdaki kod, durum, form alanları ve istekler kullanıcı veya saldırgan tarafından değiştirilebilir. Uygulamanın önemli güvenlik kararları istemci tarafının amaçlanan biçimde çalışacağı varsayımına bırakılmamalıdır.

İlke 2: Kullanıcı arayüzünün gösterdiği sınırlar gerçek güvenlik sınırı sayılmamalıdır.

Bir işlevin gizlenmesi, bir düğmenin gösterilmemesi veya belirli bir akışta sunulmaması o işlemi erişilemez hale getirmez. Sunucu, önemli işlemlerin kendi kimlik, yetki ve durum koşullarını bağımsız biçimde korumalıdır.

İlke 3: İstemciden gelen bütün bilgi değiştirilebilir dış girdi olarak görülmelidir.

Formlar, başlıklar, cookie'ler, adresler ve tarayıcının oluşturduğu diğer değerler uygulamanın beklediğinden farklı hale getirilebilir. Görünür arayüzde uygulanmış kısıtlar sunucu tarafındaki güvenin yerine geçmemelidir.

İlke 4: Girdinin geçerli olması yalnızca teknik biçiminin doğru olmasına bağlı olmamalıdır.

Bir değer doğru türde veya doğru biçimde olabilir ancak iş bağlamında anlamsız, izin verilmeyen veya beklenmeyen bir etki oluşturabilir. Uygulama girdiyi kullanılacağı gerçek bağlam içinde anlamlandırabilmelidir.

İlke 5: Veri ile çalıştırılabilir davranış arasındaki sınır korunmalıdır.

Kullanıcı veya dış kaynaklardan alınan veri, gösterildiği ya da işlendiği bağlama göre tarayıcı, sorgu motoru, işletim sistemi veya başka yorumlayıcılar tarafından komut gibi değerlendirilebilir. Veri olarak alınan içerik uygulamanın sahip olduğu yürütme yetkisini kendiliğinden devralmamalıdır.

İlke 6: Dış girdinin işleneceği bağlam güvenliğin bir parçasıdır.

Aynı içerik HTML, betik, adres, sorgu veya dosya bağlamında farklı davranış oluşturabilir. Güvenlik, veriyi yalnızca kaynağına göre değil hangi yorumlayıcı veya bileşen tarafından nasıl kullanılacağına göre ele almalıdır.

İlke 7: Dosya kabul etmek dosyanın içeriğine güvenmek anlamına gelmemelidir.

Dosya adı, uzantısı veya beyan edilen türü içeriğin güvenli olduğunu göstermez. Yüklenen veya dışarıdan alınan dosyaların oluşturabileceği davranış, daha sonra hangi bileşenler tarafından işleneceğiyle birlikte değerlendirilmelidir.

İlke 8: Kullanıcının sağladığı içerik uygulamanın yürütme alanına gereksiz biçimde dönüşmemelidir.

Yüklenen dosya, oluşturulan metin veya başka kullanıcı içeriği yalnızca uygulama tarafından saklandığı için uygulamanın kendi koduyla aynı çalıştırma veya güven düzeyine sahip olmamalıdır.

İlke 9: Kimlik doğrulama sonrasında oluşan oturum bağımsız bir güven unsuru olarak korunmalıdır.

Kullanıcı doğrulandıktan sonra oturum bilgisi onun adına işlem yapma gücünü taşır. Bu bilginin ele geçirilmesi parolanın bilinmesine gerek kalmadan kimliğin kullanılmasına yol açabilir.

İlke 10: Oturumun güveni ihtiyaç duyulan süre ve bağlamı aşmamalıdır.

Geçmişte kurulmuş bir oturumun koşulları değişebilir veya oturum başka tarafa geçebilir. Erişim ve özellikle yüksek etkili işlemler, ilk giriş anında oluşmuş güvene sınırsız süreyle bağlı kalmamalıdır.

İlke 11: Oturumun sona erdirilmesi gerçek erişimi sona erdirebilmelidir.

Kullanıcı arayüzünde çıkış yapılmış görünmesi yeterli değildir. Oturumu temsil eden kullanılabilir güven unsurlarının ilgili erişimi sürdürmemesi gerekir.

İlke 12: Oturum ve kimlik bilgileri uygulamanın olağan veri yüzeylerine gereksiz biçimde yayılmamalıdır.

Adresler, tarayıcı depoları, günlükler, analitik sistemleri ve üçüncü taraf bileşenler hassas güven unsurlarının beklenmeyen kopyalarını oluşturabilir. Uygulamanın tasarımı bu değerleri ihtiyaç dışındaki alanlara taşımamalıdır.

İlke 13: Yetkilendirme her önemli işlemde gerçek kaynak ve etki bağlamını korumalıdır.

Bir kullanıcının uygulamaya girebilmesi veya belirli bir role sahip olması bütün kaynaklara ve işlemlere erişmesini gerektirmez. Yetki, hangi veri veya nesnenin hangi işlemle etkilenebildiğine kadar anlamını korumalıdır.

İlke 14: Kaynağın adresini veya tanımlayıcısını bilmek erişim hakkı oluşturmamalıdır.

Karmaşık veya tahmin edilmesi zor tanımlayıcılar keşfi zorlaştırabilir; ancak gerçek yetkilendirmenin yerine geçmez. Bir kullanıcının başka bir kaynağa erişimi, tanımlayıcıyı elde edip edememesine bağlı olmamalıdır.

İlke 15: Uygulamanın iş kuralları yalnızca kullanıcı arayüzündeki sıraya dayanmamalıdır.

Tarayıcıdaki adımlar atlanabilir, tekrar edilebilir veya farklı sırada çağrılabilir. Kritik durum değişiklikleri uygulamanın kendi tarafında geçerli durum ve yetki koşullarıyla korunmalıdır.

İlke 16: Tekrar, eşzamanlılık ve otomasyon iş güvenliği sınırlarını aşmamalıdır.

Bir işlem tek başına geçerli olsa bile çok sayıda, aynı anda veya beklenmeyen sırada gerçekleştirilmesi farklı bir etki oluşturabilir. Uygulamanın güvenilirliği kullanıcıların yalnızca ekranda öngörülen hız ve sırayla hareket edeceği varsayımına dayanmamalıdır.

İlke 17: Tarayıcının otomatik davranışları kullanıcının iradesiyle aynı şey olarak kabul edilmemelidir.

Tarayıcı bazı kimlik ve oturum bilgilerini kullanıcının ayrıca karar vermesine gerek olmadan isteklere ekleyebilir veya farklı kaynaklar arasında davranış gösterebilir. Durum değiştiren önemli işlemler yalnızca isteğin geçerli bir tarayıcı oturumundan gelmesine dayanarak meşru kabul edilmemelidir.

İlke 18: Tarayıcı güvenlik mekanizmaları sunucu tarafındaki güven kararlarının yerine geçmemelidir.

Kaynak politikaları, güvenlik başlıkları ve benzeri tarayıcı özellikleri önemli savunma katmanları sağlayabilir. Ancak istemci dışındaki saldırganların doğrudan sunucuya ulaşabileceği ve bazı tarayıcı korumalarının yanlış yapılandırılabileceği kabul edilmelidir.

İlke 19: Üçüncü taraf istemci kodu uygulamanın güven sınırının parçasıdır.

Harici betikler, SDK'lar, analiz ve benzeri bileşenler kullanıcı tarayıcısında uygulamanın verilerine veya davranışına erişebilir. Bir bileşenin başka sağlayıcı tarafından geliştirilmesi onun uygulama üzerindeki gerçek etkisini azaltmaz.

İlke 20: Hata ve tanılama davranışı gereksiz bir bilgi kanalı oluşturmamalıdır.

Hatalar kullanıcıya gerekli bilgiyi sağlayabilir; ancak iç yapı, hassas veri, kimliklerin varlığı veya başka saldırıya yardımcı ayrıntıları gereksiz biçimde açığa çıkarmamalıdır. İşletim için gerekli tanı bilgisi ile dış kullanıcıya verilmesi gereken bilgi ayrıştırılabilmelidir.

İlke 21: Web uygulaması güvencesi yalnızca normal kullanıcı akışının testine dayanmamalıdır.

Gerçek saldırgan arayüzü kullanmak, adımları sırayla izlemek veya uygulamanın oluşturduğu isteklerle sınırlı kalmak zorunda değildir. Güvence; doğrudan ve değiştirilmiş istekler karşısında kimlik, yetki, veri, iş mantığı ve oturum sınırlarının fiilen korunup korunmadığı üzerinden doğrulanabilmelidir.