Denetci.org

REFERANS İLKELERİ

Parola İlkeleri

Rİ-KIM-3

Sürüm 1.0 · 11.08.2026

www.denetci.org

Parola İlkeleri

Parolalar, bir kimlik hakkında güven oluşturmak için kullanılan ancak yalnızca gizli kaldıkları ölçüde değer taşıyan kimlik doğrulama unsurlarıdır. Bu ilkelerin amacı belirli uzunluklar, karakter kuralları veya değişim süreleri belirlemek değil; parola kullanılan sistemlerde tahmin, ele geçirme, yeniden kullanım ve kurtarma risklerinin insan davranışıyla birlikte ele alındığı güvenilir bir tasarım anlayışı oluşturmaktır.

İlke 1: Parola kullanımı kendi başına bir güvenlik hedefi olmamalıdır.

Bir sistemin amacı parola kullandırmak değil, kimliği yeterli güvenle doğrulamaktır. Daha uygun bir kimlik doğrulama yaklaşımı bulunduğunda yalnızca alışkanlık veya teknik miras nedeniyle parolaya bağımlılık sürdürülmemelidir.

İlke 2: Parolanın gücü görünürdeki karmaşıklığından çok tahmin edilebilirliğine dayanmalıdır.

Belirli karakter türlerini içeren bir parola yine de kolay tahmin edilen bir kalıba dayanabilir. Parola tasarımı biçimsel karmaşıklığı güvenliğin kendisi saymamalı; saldırganın gerçek tahmin ve kırma imkânını azaltmaya odaklanmalıdır.

İlke 3: Güvenli parola kullanımı insan kapasitesiyle çatışmamalıdır.

İnsanlardan çok sayıda karmaşık ve benzersiz değeri hatırlamalarını bekleyen bir sistem, kullanıcıları tekrar kullanıma, basit kalıplara veya güvensiz kayıt yöntemlerine yöneltebilir. Tasarım, güvenli davranışın gerçek kullanım içinde sürdürülebilir olmasını sağlamalıdır.

İlke 4: Parolanın başka yerlerde kullanılması bu sistemin güvenini belirlememelidir.

Aynı parolanın farklı hizmetlerde kullanılması, başka bir sistemdeki ihlalin etkisini yeni bir kimlik alanına taşıyabilir. Parola yaklaşımı, bağımsız sistemlerin güvenini mümkün olduğu ölçüde birbirine bağlamamalıdır.

İlke 5: Bilinen zayıflıklar biçimsel kurallardan daha anlamlı kabul edilmelidir.

Yaygın, tahmin edilebilir veya daha önce açığa çıkmış bir parola teknik kurallara uyuyor olsa bile güçlü sayılmamalıdır. Güvenlik değerlendirmesi, parolanın gerçek saldırı koşullarındaki değerini dikkate almalıdır.

İlke 6: Parola yöneticileri ve benzeri güvenli kullanım araçları gereksiz yere engellenmemelidir.

İnsan hafızasına olan bağımlılığı azaltan araçlar benzersiz ve güçlü parolaların kullanılmasını kolaylaştırabilir. Kullanıcı arayüzü, gerçek bir güvenlik gerekçesi olmadan bu yöntemleri zorlaştırmamalıdır.

İlke 7: Parola değişikliği takvime değil güven durumuna anlamlı biçimde bağlı olmalıdır.

Bir parolanın yalnızca belirli bir süre geçtiği için değiştirilmesi güvenliği her zaman artırmaz ve tahmin edilebilir varyasyonlara yol açabilir. Buna karşılık parolanın güvenini kaybettiğine ilişkin anlamlı bir neden bulunduğunda eski güven ilişkisi sürdürülememelidir.

İlke 8: Parolanın değiştirilmesi tek başına hesabın yeniden güvenli olduğu anlamına gelmemelidir.

Ele geçirilmiş bir parola kullanılarak daha önce oturum, belirteç veya başka kalıcı erişim elde edilmiş olabilir. Kimliğin güveni yeniden kurulurken paroladan doğan diğer aktif güven ilişkileri de gerektiğinde hesaba katılmalıdır.

İlke 9: Parola kurtarma yolu normal kimlik doğrulamanın daha zayıf alternatifi olmamalıdır.

Bir hesabın parolası bilinmeden değiştirilebiliyorsa kurtarma mekanizması fiilen başka bir kimlik doğrulama yöntemidir. Bu yol, koruduğu hesabın oluşturabileceği etkiyle uyumlu güven sağlamalıdır.

İlke 10: Biyografik veya kolay öğrenilebilir bilgi güçlü parola kurtarma sırrı sayılmamalıdır.

Bir kişinin geçmişi, ailesi veya benzeri bilgileri yalnızca kullanıcı tarafından bilinen sırlar değildir. Kimlik kurtarma, araştırılabilen veya başkaları tarafından bilinebilen bilgiyi güçlü güven kanıtı olarak kabul etmemelidir.

İlke 11: Parola tahmini saldırgan için sınırsız ve maliyetsiz bir işlem olmamalıdır.

Bir saldırganın çok sayıda parolayı veya çok sayıda hesabı otomatik biçimde deneyebilmesi parolanın gerçek gücünü azaltır. Savunma, yalnızca tek hesaptaki hata sayısına değil tahmin davranışının bütününe karşı anlam taşımalıdır.

İlke 12: Tahmin saldırısına karşı koruma meşru kullanıcıya karşı kolay bir saldırı aracına dönüşmemelidir.

Parola denemelerini sınırlayan mekanizmalar saldırganın hesapları kasıtlı olarak kullanılamaz hale getirmesine yol açabilir. Gizliliği koruma ile erişilebilirliği koruma arasındaki ilişki birlikte düşünülmelidir.

İlke 13: Yüksek etkili erişimin güveni yalnızca parolaya bağlı olmamalıdır.

Parola, ele geçirilebilen ve başka bir tarafa aktarılabilen bir bilgidir. Oluşturulabilecek etki arttıkça kimlik hakkında duyulan güvenin yalnızca tek bir bilgi unsuruna dayanması yetersiz kalabilir.

İlke 14: İlk veya geçici parola kalıcı güven ilişkisi oluşturmamalıdır.

Bir kimliğin kurulması veya kurtarılması sırasında verilen geçici değerler, olağan kullanıcı parolasıyla aynı güven ömrüne sahip olmamalıdır. Başlangıç kolaylığı, çok sayıda kullanıcı veya sistem arasında kalıcı ortak güven oluşturmamalıdır.

İlke 15: Parola yalnızca kullanıcı ile doğrulayan sistem tarafından bilinmesi gereken bir değer olarak ele alınmalıdır.

Destek personelinin, yöneticilerin veya başka tarafların kullanıcının gerçek parolasını bilmesi normal işletim gereksinimi haline gelmemelidir. Bir parolanın doğrulanabilmesi onun geri okunabilmesini gerektirmez.

İlke 16: Parolanın ele geçirilmesi saklandığı veriden doğrudan kolaylaştırılmamalıdır.

Parola doğrulama amacıyla tutulan bilgi, veri tabanı ele geçirildiğinde parolaların doğrudan öğrenilmesine veya çok düşük maliyetle denenmesine imkân vermemelidir. Saklama tasarımı çevrimdışı saldırıyı da güvenlik modelinin bir parçası olarak kabul etmelidir.

İlke 17: Parola yaşamı boyunca gereksiz gözlem ve kopyalara maruz bırakılmamalıdır.

Parola giriş, aktarım, doğrulama ve destek süreçlerinde loglara, adreslere, komutlara veya başka kalıcı ortamlara istemeden yayılabilir. Kimlik doğrulama tasarımı parolanın ihtiyaç duyulmayan yerlere taşınmasını doğal çalışma biçimi haline getirmemelidir.

İlke 18: Parola güvenliği gerçek kimlik doğrulama davranışı üzerinden doğrulanabilmelidir.

Bir parola politikasının bulunması veya kullanıcıların kurallara uyması tek başına güvence değildir. Kullanılan parolaların makul saldırılara karşı ne ölçüde dayanıklı olduğu, ele geçirilmiş bir parolanın nasıl etkisiz hale geldiği, kurtarma yollarının hangi güvene dayandığı ve saklanan doğrulama verisinin parola bilgisini ne ölçüde koruduğu gerektiğinde sınanabilmelidir.