Testing for Weak Password Policy (Zayıf Şifre Politikası için Test)

Summary (Özet)

En yaygın ve en kolay uygulanan kimlik doğrulama mekanizması statik bir şifredir. Şifre, krallığın anahtarlarını temsil eder, ancak genellikle kullanıcılar tarafından kullanılabilirlik adına altüst
edilir. Kullanıcı kimlik bilgilerini ortaya çıkaran son yüksek profilli saldırıların her birinde, en yaygın şifrelerin hala olduğu konusunda yakındır: `123456`, `password` ve `qwerty`. .

Test Objectives (Test Hedefleri)

- Şifrelerin uzunluğu, karmaşıklığı, yeniden kullanımı ve yaşlanma gereksinimlerini değerlendirerek mevcut şifre sözcülerini kullanarak mevcut şifre sözcüleri kullanılarak uygulamanın kaba kuvvet şifre tahminine karşı direnci belirleyin.

How to Test (Nasıl Test Edilir)

1. Hangi karakterlere şifre içinde kullanılmasına izin verilir ve yasaklanır? Kullanıcının alt ve üst harfler, rakamlar ve özel semboller gibi farklı karakter setlerinden karakterleri kullanması gerekiyor mu?
2. Bir kullanıcı şifresini ne sıklıkla değiştirebilir? Bir kullanıcı önceki bir değişiklikten sonra şifrelerini ne kadar hızlı değiştirebilir? Kullanıcılar, şifrelerini üst üste 5 kez değiştirerek
   şifre geçmişin gereksinimlerini atlayabilir, böylece son şifre değişikliğinden sonra ilk şifrelerini tekrar yapılandırmışlardır.
3. Bir kullanıcı ne zaman şifresini değiştirmeli?
   - Hem NIST hem de NCSC, PCI DSS gibi standartlarda gerekli olsa da, düzenli şifre süresinin uygulanmasına **karşı** öneride bulunur.

4. Bir kullanıcı ne sıklıkla şifreyi yeniden kullanabilir? Uygulama, kullanıcının önceki kullanılmış 8 şifresinin geçmişini koruyor mu?
5. Bir sonraki şifre son şifreden ne kadar farklı olmalı?
6. Kullanıcının kullanıcı adı veya diğer hesap bilgilerini (ilk veya soyadı gibi) şifrede kullanması engellenir mi?
7. Belirlenebilecek minimum ve maksimum şifre uzunlukları nelerdir ve hesap ve uygulamanın hassasiyeti için uygundurlar mı?
8. Mümkün mü, örneğin ortak şifreler mi `Password1` ya da `123456`?

Remediation (Düzeltme)

Kolay tahmin edilen parolaların yetkisiz erişimi kolaylaştırma riskini azaltmak için iki çözüm vardır: ek kimlik doğrulama kontrolleri (yani iki faktörlü kimlik doğrulama) uygulamak veya güçlü bir parola politikası uygulamak. Bunlardan en basit ve ucuz olanı parola uzunluğu, karmaşıklığı, yeniden kullanımı ve eskimesini sağlayan güçlü bir parola politikasının uygulamaya konmasıdır; ancak ideal olarak her ikisinin de uygulanması gerekir.

References (Referanslar)

- Brute Force Attacks