# Testing for Weak Password Change or Reset Functionalities (Zayıf Şifre Değişikliği veya Sıfırlama İşlevsellikleri için Test)

## Summary (Özet)

Bir uygulamanın şifre değişikliği ve sıfırlama işlevi, kullanıcılar için self servis şifre değişikliği veya sıfırlama mekanizmasıdır. Bu self servis mekanizması, kullanıcıların bir yönetici müdahale etmeden şifrelerini hızlı bir şekilde değiştirmelerini veya sıfırlamalarını sağlar. Şifreler değiştirildiğinde, genellikle uygulama içinde değiştirilir. Şifreler sıfırlandığında, uygulama içinde yapılır veya kullanıcıya e-posta gönderilir. Bu, şifrelerin düz metinde veya şifresini çözebilir bir formatta sakladığını gösterebilir.

## Test Objectives (Test Hedefleri)

- Başvurunun hesap değiştirme işleminin bir hesabın şifresini değiştirmesine izin verme direncini belirleyin.
- Şifrelerin direncinin, tahmin veya atlamaya karşı işlevselliği sıfırlamanın düzeltildiğini belirleyin.

## How to Test (Nasıl Test Edilir)

Hem şifre değişikliği hem de şifre sıfırlaması için aşağıdakileri kontrol etmek önemlidir:

1. Kullanıcılar, yöneticiler dışında, kendi dışındaki hesaplar için şifreleri değiştirebilir veya sıfırlayabilirse.
2. Kullanıcılar, başka bir kullanıcının veya yöneticinin şifresini değiştirmek veya sıfırlamak için şifre değişikliğini manipüle edebilir veya sıfırlayabilirse.
3. Şifre değişikliği veya sıfırlama işlemi CSRF'ye karşı savunmasızsa.

**Test Password Reset (Test Şifresi Sıfırlama)**

Önceki kontrollere ek olarak aşağıdakileri doğrulamak önemlidir:

- Şifreyi sıfırlamak için hangi bilgiler gereklidir?

  İlk adım, gizli soruların gerekli olup olmadığını kontrol etmektir. Şifreyi (veya bir şifre sıfırlama bağlantısının) ilk önce gizli bir soru sormadan kullanıcı e-posta adresine gönderilmesi, uygulamanın yüksek bir güvenliğe ihtiyacı varsa uygun olmayan, bu e-posta adresinin güvenliğine% 100 güvenmek anlamına gelir.

  Öte yandan, gizli sorular kullanılırsa, bir sonraki adım güçlerini değerlendirmektir. Bu özel test, bu kılavuzun Zayıf Güvenlik sorusu / cevap paragrafı için Test paragrafında ayrıntılı olarak tartışılmaktadır.

- Sıfırlama şifreleri kullanıcıya nasıl iletilir?

  Buradaki en güvensiz senaryo, şifre sıfırlama aracının size şifreyi göstermesidir; Bu, saldırgana hesaba giriş yapma olanağı verir ve uygulama kurbandaki son gün hakkında bilgi vermedikçe, hesaplarının ele geçirildiğini bilmez.

  Daha az güvensiz bir senaryo, şifre sıfırlama aracının kullanıcıyı hemen şifrelerini değiştirmeye zorlamasıdır. İlk vaka kadar gizli olmasa da, saldırganın erişime izin verir ve gerçek kullanıcıyı
  kilitler.

  En iyi güvenlik, kullanıcının başlangıçta kayıtlı olduğu adrese veya başka bir e-posta adresine bir e-posta adresiyle bir e-posta yoluyla yapılırsa elde edilir; Bu, saldırganı yalnızca şifre
  sıfırlamanın hangi e-posta hesabına gönderildiğini tahmin etmemeye (uygulama bu bilgileri göstermediği sürece) değil, aynı zamanda geçici şifreyi veya şifre sıfırlama bağlantısı elde etmek için bu e-posta hesabını tehlikeye atmaya zorlar.

- Sıfırlama şifreleri rastgele oluşturulur mı?

  Buradaki en güvensiz senaryo, uygulamanın eski şifreyi net metinle göndermesi veya görselleştirmesidir, çünkü bu, şifrelerin kendi içinde bir güvenlik sorunu olan bir hashed formunda saklanmadığı anlamına gelir.

  En iyi güvenlik, şifreler türetilemeyen güvenli bir algoritma ile rastgele oluşturulursa elde edilir.

- Sıfırlama şifresi işlevselliği şifreyi değiştirmeden önce onay istiyor mu?

  Hizmet reddi saldırılarını sınırlamak için uygulama, kullanıcıya rastgele bir belirteçle bir bağlantı e-postayla e-postayla ve yalnızca kullanıcı bağlantıyı ziyaret ederse, sıfırlama prosedürü tamamlanır. Bu, sıfırlama onaylanana kadar mevcut şifrenin hala geçerli olmasını sağlar.

**Test Password Change (Şifre Değişikliğini Test Et)**

Önceki teste ek olarak doğrulama yapmak da önemlidir:

- Değişikliği tamamlamak için talep edilen eski şifre mi?

  Buradaki en güvensiz senaryo, uygulamanın mevcut şifreyi talep etmeden şifrenin değiştirilmesine izin vermesidir. Gerçekten de bir saldırgan geçerli bir oturumun kontrolünü ele geçirebilirse, kurbanın şifresini kolayca değiştirebilirler.Bu kılavuzun Zayıf şifre politikası paragrafı için Test ayrıca bakınız.

## Remediation (Düzeltme)

Şifre değişikliği veya sıfırlama işlevi hassas bir işlevdir ve kullanıcıların işlem sırasında kullanıcıya yeniden doğrulamalarını veya onay ekranlarını sunmalarını istemek gibi bir tür koruma gerektirir.

## References (Referanslar)

- OWASP Forgot Password Cheat Sheet