Testing for Vulnerable Remember Password (Savunmasız için Test Parolayı Hatırla)

Summary (Özet)

Kimlik bilgileri en çok kullanılan kimlik doğrulama teknolojisidir. Kullanıcı-süpürme çiftlerinin bu kadar geniş kullanımı nedeniyle, kullanıcılar artık çok sayıda kullanılmış uygulamada kimlik bilgilerini düzgün bir şekilde kaldıramazlar.

Kullanıcılara kimlik bilgilerine yardımcı olmak için, birden fazla teknoloji ortaya çıktı:

- Uygulamalar, kullanıcının kimlik bilgilerini tekrar sormadan, kullanıcının uzun süre kimlik doğrulamasını sağlayan *bir* işlevselliği *hatırlamayı* sağlar.
- Kullanıcının kimlik bilgilerini güvenli bir şekilde saklamasına ve daha sonra herhangi bir kullanıcı müdahalesi olmadan kullanıcı formlarına enjekte etmesine izin veren tarayıcı şifresi yöneticileri de dahil olmak üzere şifre Yöneticileri.

Test Objectives (Test Hedefleri)

- Oluşturulan oturumun güvenli bir şekilde yönetildiğini doğrulayın ve kullanıcının kimlik bilgilerini tehlikeye atmayın.

How to Test (Nasıl Test Edilir)

Bu yöntemler daha iyi bir kullanıcı deneyimi sağladıkça ve kullanıcının kimlik bilgileriyle ilgili her şeyi unutmasına izin verdikçe, saldırı yüzey alanını arttırırlar. Bazı uygulamalar:

- Kimlik bilgilerini tarayıcının depolama mekanizmalarında kodlanmış bir şekilde saklayın, bu da web depolama test senaryosunu takip ederek ve oturum analizi senaryolarından geçerek doğrulanabilir. Kimlik bilgileri istemci tarafı

uygulamasında hiçbir şekilde saklanmamalı ve sunucu tarafı tarafından oluşturulan belirteçlerle yerine getirilmelidir.

- Kullanıcının kimlik bilgilerini otomatik olarak aşağıdakiler tarafından sulandırılabilen bilgileri:
  - Jacking saldırıları.
  - CSRF saldırıları.
- Tokenler, bazı belirteçlerin asla sona ermediği ve bu jetonların çalınması durumunda kullanıcıları tehlikeye attığı token-can-ötesi süresi açısından analiz edilmelidir. Oturum zaman aşımı test senaryosunu takip ettiğinizden emin olun.

Remediation (Düzeltme)

- Oturum yönetimi iyi uygulamalarını takip edin.
- Hiçbir kimlik bilgisinin net metinde saklanmadığından veya tarayıcı depolama mekanizmalarında kodlanmış veya şifrelenmiş formlarda kolayca geri alındığından emin olun; sunucu tarafında saklanmalı ve iyi şifre depolama uygulamalarını takip etmelidirler.