Testing for Weaker Authentication in Alternative Channel (Alternatif Kanalda Daha Zayıf Kimlik Doğrulama Testi)

Summary (Özet)

Birincil kimlik doğrulama mekanizmaları herhangi bir güvenlik açığı içermese bile, aynı kullanıcı hesapları için alternatif meşru kimlik doğrulama kullanıcı kanallarında güvenlik açıklarının mevcut olması olabilir. Alternatif kanalları tanımlamak ve test kapsamına tabi olarak güvenlik açıklarını tanımlamak için testler yapılmalıdır.

Alternatif kullanıcı etkileşim kanalları, birincil kanalı aşmak veya daha sonra birincil kanala karşı bir saldırıya yardımcı olmak için kullanılabilecek bilgileri ortaya çıkarmak için kullanılabilir. Bu
kanallardan bazıları farklı ana bilgisayarları veya yollar kullanarak ayrı web uygulamaları olabilir. Örneğin:

- Standart web sitesi
- Mobil veya özel cihaz, optimize edilmiş web sitesi
- Erişilebilirlik optimize edilmiş web sitesi
- Alternatif ülke ve dil web siteleri
- Aynı kullanıcı hesaplarını kullanan paralel web siteleri (örneğin, kullanıcı hesaplarının paylaşıldığı bir ortak web sitesi olan aynı
  kuruluşun işlevsel olarak farklı bir web sitesi sunan başka bir web
  sitesi)
- Standart web sitesinin geliştirme, test, UAT ve evreleme sürümleri

Ancak diğer uygulama veya iş süreçleri de olabilir:

- Mobil cihaz uygulaması
- Masaüstü uygulaması
- Çağrı merkezi operatörleri
- Etkileşimli sesli yanıt veya telefon ağacı sistemleri

Bu testin odak noktasının alternatif kanallarda olduğunu unutmayın; bazı kimlik doğrulama alternatifleri aynı web sitesi üzerinden sunulan farklı içerik olarak görünebilir ve neredeyse kesinlikle test için kapsam olabilir. Bunlar burada daha fazla tartışılmamıştır ve bilgi toplama ve birincil kimlik doğrulama testi sırasında tanımlanmalıydı.

Örneğin:

- İşlevselliği değiştiren ilerici zenginleştirme ve zarif bozulma
- Site çerezleri olmadan kullanım
- JavaScript olmadan site kullanımı
- Flash ve Java gibi eklentiler olmadan site kullanımı

Testin kapsamı alternatif kanalların test edilmesine izin vermese bile varlıkları belgelenmelidir. Bunlar, kimlik doğrulama mekanizmalarındaki güvence derecesini zayıflatabilir ve ek testlerin
öncüsü olabilir.

Exapmle (Örnek)

Birincil web sitesi `http://www.example.com` ve kimlik doğrulama işlevleri her zaman TLS kullanan sayfalarda gerçekleşir `https://www.example.com/myaccount/` . .

Bununla birlikte, TLS'yi hiç kullanmayan ve daha zayıf bir şifre kurtarma mekanizmasına sahip ayrı bir mobil-iyimleşmiş web sitesi vardır. `http://m.example.com/myaccount/` . .

Test Objectives (Test Hedefleri)

- Alternatif kimlik doğrulama kanallarını tanımlayın.
- Kullanılan güvenlik önlemlerini ve alternatif kanallarda herhangi bir baypas varsa değerlendirin.

How to Test (Nasıl Test Edilir)

Understand the Primary Mechanism (Birincil Mekanizmayı Anlayın)

Web sitesinin birincil kimlik doğrulama işlevlerini tam olarak test edin. Bu, hesapların nasıl düzenlendiğini, oluşturulduğunu veya değiştirildiğini ve şifrelerin nasıl kurtarıldığını, sıfırlandığını veya değiştirildiğini belirlemelidir. Ek olarak, yükseltilmiş ayrıcalık kimlik doğrulaması ve kimlik doğrulama koruma önlemleri hakkında bilgi bilinmektedir. Bu öncüller, herhangi bir alternatif kanalla karşılaştırabilmek için gereklidir.

Identify Other Channels (Diğer Kanalları Tanımlayın)

Diğer kanallar aşağıdaki yöntemleri kullanarak bulunabilir:

- Site içeriğini, özellikle ana sayfa, bizimle iletişime geçin, yardım sayfaları, makaleleri ve SSS'leri, T & C'leri, gizlilik bildirimleri, robots.txt dosyası ve herhangi bir sitemap.xml dosyası ile iletişime geçin.
- HTTP proxy günlüklerini arama, önceki bilgi toplama ve test sırasında kaydedilen, “mobil”, “android”, böğürtlen, “ipid”, “iphone”, “iphone”, “e-okuma”, “telsiz”, URL yollarında ve vücut içeriğinde “single işaret” gibi dizeler için kayıtlar.
- Aynı kuruluştan farklı web siteleri bulmak için arama motorlarını kullanın veya benzer ana sayfa içeriğine sahip olan veya aynı kimlik doğrulama mekanizmalarına sahip aynı alan adını kullanarak kullanın.

Her olası kanal için, kullanıcı hesaplarının bunlar arasında paylaşılıp paylaşılmadığını veya aynı veya benzer işlevselliğe erişim sağlayıp sağlamadığını onaylayın.

Enumerate Authentication Functionality (Kimlik Doğrulama İşlevselliğini Numaralandır)

Kullanıcı hesaplarının veya işlevselliğinin paylaşıldığı her alternatif kanal için, birincil kanalın tüm kimlik doğrulama işlevlerinin mevcut olup olmadığını ve ekstra bir şey varsa belirleyin. Aşağıdaki gibi bir ızgara oluşturmak yararlı olabilir:

Birincil	Mobil	Çağrı Merkezi	Partner Web Sitesi
Kayıt Ol	Evet	- -	- -
Giriş yapın	Evet	Evet	Evet (SSO)

Çıkış yap	- -	- -	- -
Şifre sıfırlama	Evet	Evet	- -
- -	Şifreyi değiştirin	- -	- -

Bu örnekte, mobilin ekstra bir işlevi “politika değiştirme” özelliğine sahiptir, ancak “log out” sunmaz. Çağrı merkezini arayarak sınırlı sayıda görev de mümkündür. Çağrı merkezleri ilginç olabilir, çünkü kimlik onay kontrolleri web sitesininkinden daha zayıf olabilir ve bu kanalın bir kullanıcının hesabına karşı bir saldırıya yardımcı olmak için kullanılmasına izin verir.

Bunları numaralandırırken, oturum yönetiminin nasıl üstlenildiğini not etmeye değer, herhangi bir kanalda örtüşme durumunda (örneğin, aynı ana alan adına kapsanan çerezler, kanallar arasında izin verilen eşzamanlı oturumlar, ancak aynı kanalda değil).

Review and Test (İnceleme ve Test)

Test raporunda alternatif kanallardan, “yalnızca bilgi” veya “kapsam dışı” olarak işaretlenmiş olsalar bile belirtilmelidir. Bazı durumlarda test kapsamı alternatif kanalı içerebilir (örneğin, hedef ana bilgisayar adındaki başka bir yol olduğu için) veya tüm kanalların sahipleriyle tartıştıktan sonra kapsamaya eklenebilir. Teste izin verilir ve yetkilendirilmişse, bu kılavuzdaki diğer tüm kimlik doğrulama testleri daha sonra gerçekleştirilmeli ve birincil kanala kıyasla karşılaştırılmalıdır.

Related Test Cases (İlgili Test Vakaları)

Diğer tüm kimlik doğrulama testleri için test durumları kullanılmalıdır.

Remediation (Düzeltme)

Tutarlı bir kimlik doğrulama politikasının tüm kanallarda uygulanmasını sağlayın, böylece eşit derecede güvenlidirler.