Testing for Weak Security Question Answer (Zayıf Güvenlik Sorusu Cevabı için Test)

Summary (Özet)

Genellikle “gizli” sorular ve cevaplar olarak adlandırılır, güvenlik soruları ve cevapları genellikle unutulmuş şifreleri kurtarmak için kullanılır (zayıf şifre değişikliği veya sıfırlama işlevleri için test yapın veya şifrenin üstünde ekstra güvenlik olarak bakın.

Genellikle hesap oluşturma üzerine oluşturulurlar ve kullanıcının önceden oluşturulmuş bazı sorulardan seçim yapmasını ve uygun bir cevap vermesini gerektirir. Kullanıcının kendi sorularını oluşturmasına ve çiftleri cevaplamasına izin verebilirler. Her iki yöntem de güvensizliklere eğilimlidir. Yani, güvenlik soruları yalnızca kullanıcı tarafından bilinen ve başkaları tarafından tahmin edilemeyen veya keşfedilemeyen cevaplar üretmelidir. Bu göründüğünden daha zor. Güvenlik soruları ve cevaplar cevabın gizliliğine dayanır. Cevaplar sadece hesap sahibi tarafından bilinmesi için sorular ve cevaplar seçilmelidir. Bununla birlikte, birçok cevap kamuya açık olarak bilinmese de, web sitelerinin uyguladığı soruların çoğu sahte-özel olan cevapları teşvik eder.

Pre-generated Questions (Önceden oluşturulmuş sorular)

Önceden oluşturulmuş soruların çoğunluğu doğada oldukça basittir ve güvensiz cevaplara yol açabilir. Örneğin:

- Cevaplar, örneğin kullanıcının aile üyeleri veya yakın arkadaşları tarafından bilinebilir. “Annenin kızlık soyadı nedir?”, “Doğum tarihiniz nedir?”
- Cevaplar kolayca tahmin edilebilir olabilir, örneğin. “En sevdiğin renk nedir?”, “En sevdiğiniz beyzbol takımı nedir?”
- Cevaplar kabaca zor olabilir, örneğin. “En sevdiğiniz lise öğretmeninin ilk adı nedir?” – cevap muhtemelen popüler ilk isimlerin bazı kolayca indirilebilir

listelerindedir ve bu nedenle basit bir kaba kuvvet saldırısı yazılabilir.

- Cevaplar kamuya açık bir şekilde keşfedilebilir olabilir, örneğin. “En sevdiğiniz film nedir?” –cevap, kullanıcının sosyal medya profil sayfasında kolayca bulunabilir.

Self-generated Questions (Kendi kendine üretilen sorular)

Kullanıcıların kendi sorularını üretmeleri ile ilgili sorun, çok güvensiz sorular üretmelerine veya hatta ilk etapta bir güvenlik sorusuna sahip olmanın tüm noktasını atlamalarına izin vermesidir. İşte bu noktayı gösteren bazı gerçek dünya örnekleri:

- 1+1 nedir?”
- “A kullanıcının nedir?”
- “Benim şifrem S3cur“Ol!”

Test Objectives (Test Hedefleri)

- Karmaşıklığı ve soruların ne kadar düz olduğunu belirleyin.
- Olası kullanıcı cevaplarını ve kaba kuvvet yeteneklerini değerlendirin

How to Test (Nasıl Test Edilir)

Testing for Weak Pre-generated Questions (Zayıf önceden oluşturulmuş sorular için test)

Yeni bir hesap oluşturarak veya “şişilikimi hatırlamıyorum” sürecini izleyerek güvenlik sorularının bir listesini elde etmeye çalışın. Sorulan güvenlik soruları türü hakkında iyi bir fikir edinmek için mümkün olduğunca çok soru üretmeye çalışın. Güvenlik sorularından herhangi biri yukarıda açıklanan kategorilerde düşerse, saldırıya uğramaya karşı savunmasızdırlar (tahmin edilir, kaba kuvvetlendirilmiş, sosyal medyada mevcuttur vb.).

Testing for Weak Self-Generated Questions (Zayıf Öz Türlü Sorular Testi)

Yeni bir hesap oluşturarak veya mevcut hesabınızın şifre kurtarma özelliklerini kullanarak güvenlik soruları oluşturmaya çalışın. Sistem, kullanıcının kendi güvenlik sorularını oluşturmasına izin veriyorsa, güvensiz soruların oluşturulmasına karşı savunmasızdır. Sistem, unutulmuş şifre işlevselliği sırasında kendiliğinden

oluşturulmuş güvenlik sorularını kullanırsa ve kullanıcı adları numaralandırılabilirse (Hesap Yumarlaması ve Tahmin Edilebilir Kullanıcı Hesabı Testi bölümüne bakın, test cihazının bir dizi kendi ürettiği soruyu numaralandırması kolay olmalıdır. Bu yöntemi kullanarak kendi ürettiği birkaç şüpheliyi bulması beklenmelidir.

Testing for Brute-forcible Answers (Brute-zor Cevaplar için Test)

Zayıflama için Test kilitleme mekanizmasında açıklanan yöntemleri kullanın, bir dizi yanlış sağlanan güvenlik cevabının bir lokavt mekanizmasını tetikleyip tetiklemediğini belirlemek için kullanın.

Güvenlik sorularını sömürmeye çalışırken dikkate alınması gereken ilk şey, cevaplanması gereken soruların sayısıdır. Uygulamaların çoğunluğu yalnızca kullanıcının tek bir soruyu cevaplaması gerekirken, bazı kritik uygulamalar kullanıcının iki veya daha fazla soruyu yanıtlamasını gerektirebilir.

Bir sonraki adım, güvenlik sorularının gücünü değerlendirmektir. Cevaplar basit bir Google araması veya sosyal mühendislik saldırısıyla elde edilebilir mi? Bir penetrasyon testçisi olarak, burada bir güvenlik sorusu şemasının adım adım bir yürüyüşü var:

- Uygulama, son kullanıcının cevaplanması gereken soruyu seçmesine izin veriyor mu? Eğer öyleyse, şu sorulara odaklanın:
    - Bir “kamuoyu” cevabı; örneğin, basit bir arama motoru sorgusu ile bulunabilecek bir şey.
    - “İlk okul” veya yukarı bakılabilecek diğer gerçekler gibi gerçek bir cevap.
    - “İlk arabanızın hangi modeliydi” gibi birkaç olası cevap. Bu sorular saldırgana olası cevapların kısa bir listesini sunacak ve istatistiklere dayanarak saldırganın cevapları en azından muhtemele göre sıralayabilir.
- Mümkünse kaç tahmininiz olduğunu belirleyin.
    - Şifre sıfırlama sınırsız girişimlere izin veriyor mu?
    - X yanlış cevaplarından sonra lokavt dönemi var mı? Bir lokavt sisteminin kendi içinde bir güvenlik sorunu olabileceğini unutmayın, çünkü bir

saldırgan tarafından meşru kullanıcılara karşı bir Hizmet İnkarı başlatmak için istismar edilebilir.

- Yukarıdaki noktalardan analize dayanarak uygun soruyu seçin ve en olası cevapları belirlemek için araştırma yapın.

Zayıf bir güvenlik soru şemasını başarılı bir şekilde sömürmenin ve atlamanın anahtarı, cevapları kolayca bulma imkanı veren bir soru veya dizi soru bulmaktır. Her zaman, cevaplardan herhangi birinden tamamen emin değilseniz, doğru cevabı tahmin etmek için en büyük istatistiksel şansı verebilecek sorular arayın. Sonunda, bir güvenlik soru planı sadece en zayıf soru kadar güçlüdür.

References (Referanslar)

- The Curse of the Secret Question
- The OWASP Security Questions Cheat Sheet