Testing for Weak Lock Out Mechanism (Zayıf Kilitleme Mekanizması için Test)

Summary (Özet)

Kaba kuvvet saldırılarını hafifletmek için hesap kilitleme mekanizmaları kullanılır. Lokavt mekanizması kullanılarak yenilebilecek bazı saldırılar:

- Şifre veya kullanıcı adı tahmin saldırısına giriş.
- Herhangi bir 2FA işlevselliği veya Güvenlik Soruları hakkında kod tahmin.

Hesap kilitleme mekanizmaları, hesapları yetkisiz erişimden korumak ve kullanıcıları yetkili erişimin reddedilmesinden korumak arasında bir denge gerektirir. Hesaplar genellikle 3 ila 5 başarısız girişimden sonra kilitlenir ve yalnızca önceden belirlenmiş bir süre sonra, bir self servis kilidi açma mekanizması veya bir yöneticinin müdahalesi yoluyla kilidi açılabilir.

Kaba kuvvet saldırıları yapmak kolay olmasına rağmen, saldırganın kullanıcı hesabına tam erişime sahip olacağı ve bununla birlikte eriştikleri tüm işlevsellik ve hizmetlere sahip olacağı için başarılı
bir saldırının sonucu tehlikelidir.

Test Objectives (Test Hedefleri)

- Hesap lokavt mekanizmasının kaba kuvvet şifre tahminini hafifletme yeteneğini değerlendirin.
- Kilit açma mekanizmasının izinsiz hesap kilidine karşı direncini değerlendirin.

How to Test (Nasıl Test Edilir)

Lockout Mechanism (Kilitleme Mekanizması)

Lokavt mekanizmalarının gücünü test etmek için, istekli olduğunuz veya kilitlemeyi göze alabileceğiniz bir hesaba erişmeniz gerekecektir.Web uygulamasına giriş yapabileceğiniz tek bir hesabınız varsa, bu testi kilitlenerek test zamanını

kaybetmekten kaçınmak için test planınızın
sonunda yapın.

Hesap kilitleme mekanizmasının kaba kuvvet şifre tahminini hafifletme yeteneğini değerlendirmek için, hesabın kilitlendiğini doğrulamak için doğru şifreyi kullanmadan önce, yanlış şifreyi birkaç kez kullanarak geçersiz bir giriş yapmaya çalışın. Bir örnek test aşağıdaki gibidir:

1. Yanlış bir şifre ile 3 kez giriş yapmaya çalışın.
2. Doğru şifreyle başarılı bir şekilde giriş yapın, böylece lokavt mekanizmasının 3 yanlış kimlik doğrulama girişiminden sonra tetiklemediğini gösterir.
3. Yanlış bir şifreyle 4 kez giriş yapmaya çalışın.
4. Doğru şifreyi başarıyla oturum açın, böylece lokavt mekanizmasının 4 yanlış kimlik doğrulama girişiminden sonra tetiklemediğini gösterir.
5. Yanlış bir şifreyle 5 kez giriş yapmaya çalışın.
6. Doğru şifreyle giriş yapmaya çalışın. Uygulama “Hesabınız kilitlenir” i geri döndürür ve böylece 5 yanlış kimlik doğrulama girişiminden sonra hesabın kilitlendiğini onaylar.
7. 5 dakika sonra doğru şifreyle giriş yapmaya çalışın. Uygulama “Hesabınız kilitlenir” olarak geri döner ve böylece lokavt mekanizmasının 5 dakika sonra otomatik olarak kilidini açmadığını
gösterir.
8. 10 dakika sonra doğru şifreyle giriş yapmaya çalışın. Uygulama, “Hesabınız kilitlenir” olarak geri döner ve böylece lokavt mekanizmasının 10 dakika sonra otomatik olarak kilidini açmadığını
gösterir.
9. 15 dakika sonra doğru şifreyle başarılı bir şekilde giriş yapın. böylece lokavt mekanizmasının 10 ila 15 dakikalık bir süre sonra otomatik olarak kilidini açtığını gösterir.

Bir CAPTCHA, kaba kuvvet saldırılarını engelleyebilir, ancak kendi zayıflıklarıyla gelebilir ve bir lokavt mekanizmasının yerini almamalıdır. Bir CAPTCHA mekanizması yanlış uygulanırsa atlanabilir. CAPTCHA kusurları şunları içerir:

1. Aritimetik veya sınırlı soru seti gibi kolayca yenilmiş meydan okuma.

2. CAPTCHA, yanıt başarısı yerine HTTP yanıt kodu için kontrol eder.
3. CAPTCHA sunucu tarafı mantığı başarılı bir çözüme varsayılandır.
4. CAPTCHA meydan okuma sonucu asla sunucu tarafının doğrulanmamasıdır.
5. CAPTCHA giriş alanı veya parametre manuel olarak işlenir ve yanlış doğrulanır veya kaçılır.

CAPTCHA etkinliğini değerlendirmek için:

1. CAPTCHA zorluklarını değerlendirin ve zorluklara bağlı olarak çözümleri otomatikleştirmeye çalışın.
2. CAPTCHA'yı normal UI mekanizması (lar) üzerinden çözmeden talepte bulunmaya çalışın.
3. Kasıtlı CAPTCHA meydan okuma başarısızlığı ile talepte bulunma girişimi.
4. Bir test proxy (doğrudan sunucu tarafıyla gönderilen talep) kullanırken CAPTCHA'yı çözmeden talep göndermeye çalışın (doğrudan sunucu tarafıyla gönderilen talep) kullanırken (bazen bazı varsayılan değerlerin istemci tarafı kodu, vb.)
5. CAPTCHA veri giriş noktalarını (mazsak) ortak enjeksiyon yükleri veya özel karakter dizileri ile karıştırmaya çalışın.
6. CAPTCHA'nın çözümünün görüntünün alt metni, dosya adı(lar) veya ilişkili bir gizli alanda bir değer olup olmadığını kontrol edin.
7. Daha önce tanımlanmış bilinen iyi yanıtları yeniden gönderme girişimi.
8. Temizleme çerezlerinin CAPTCHA'nın atlanmasına neden olup olmadığını kontrol edin (örneğin, CAPTCHA sadece bir dizi başarısızlıktan sonra gösterilirse).
9. CAPTCHA çok adımlı bir sürecin parçasıysa, CAPTCHA'ya basitçe erişmeye veya tamamlamaya çalışın (örneğin, CAPTCHA bir oturum açma işleminin ilk adımıysa, ikinci adımı [kullanıcı adı ve şifre] göndermeyi deneyin).
10. CAPTCHA'nın uygulanmayabileceği alternatif yöntemleri kontrol edin, örneğin mobil uygulama erişimini kolaylaştırmak için bir API uç noktası gibi.

Bu işlemi bir lokavt mekanizması gerektirebilecek her olası işlevselliğe tekrarlayın.

Unlock Mechanism (Kilit Açma Mekanizması)

Kilit açma mekanizmasının yetkisiz hesap kilidine karşı direncini değerlendirmek için, kilidin açma mekanizmasını başlatın ve zayıflıkları arayın. Tipik kilit açma mekanizmaları gizli sorular veya e-postayla açık bir kilit açma bağlantısı içerebilir. Unca kilidi bağlantısı, bir saldırganın bağlantıyı tahmin etmesini veya tekrarlamasını ve partiler halinde kaba kuvvet saldırıları gerçekleştirmesini önlemek için benzersiz bir kerelik bağlantı olmalıdır.

Bir kilidin açma mekanizmasının yalnızca hesapların kilidini açmak için kullanılması gerektiğini unutmayın. Bir şifre kurtarma mekanizması ile aynı değildir, ancak aynı güvenlik uygulamalarını takip edebilir.

Remediation (Düzeltme)

Risk seviyesine bağlı olarak hesap kilidi açma mekanizmalarını uygulayın. En düşükten en yüksek güvenceye kadar:

1. Zamana dayalı lokavt ve kilidini açın.
2. Self servis kilidi açılır (kayıtlı e-posta adresine e-posta kilidini açar)
3. Manuel yönetici kilidini açar.
4. Manuel yönetici, olumlu kullanıcı kimliği ile kilidini açar.

Bir hesap kilitleme mekanizması uygularken göz önünde bulundurulması gereken faktörler:

1. Uygulamaya karşı kaba kuvvet şifre tahmin etme riski nedir?
2. Bir CAPTCHA bu riski azaltmak için yeterli mi?
3. Bir istemci tarafı kilitleme mekanizması (örneğin, JavaScript) kullanılır mı? (Eğer öyleyse, test etmek için istemci tarafı kodunu devre dışı bırakın.)
4. Lokavttan önceki girişimlerde başarısız gün sayısı. Lokavt eşiği düşük ise, geçerli kullanıcılar çok sık kilitlenebilir. Lokavt eşiği yüksekse, bir saldırganın kilitlenmeden önce hesabı kabartma için yapabileceği daha fazla girişimde bulunabilir. Uygulamanın amacına bağlı olarak, 5 ila 10 başarısız girişim aralığı tipik kilitleme eşiğidir.
5. Hesapların kilidi nasıl açılacak?

a. Bir yönetici tarafından manuel olarak: bu en güvenli lokavt yöntemidir, ancak kullanıcılara rahatsızlık verebilir ve yöneticinin “değerli” zamanını alabilir.
    i. Yönetimin, hesabının kilitlenmesi durumunda bir kurtarma yöntemine de sahip olması gerektiğini unutmayın.
    ii. Bu kilit açma mekanizması, bir saldırganın amacı web uygulamasının tüm kullanıcılarının hesaplarını kilitlemekse, hizmet reddi saldırısına yol açabilir.
b. Bir süre sonra: Lokavt süresi nedir? Bu, uygulamanın korunması için yeterli mi? Örneğin, 5 ila 30 dakikalık bir kilitleme süresi, kaba kuvvet saldırılarını hafifletmek ve geçerli kullanıcıları rahatsız etmek arasında iyi bir uzlaşma olabilir.
c. Bir self servis mekanizması aracılığıyla: Daha önce de belirtildiği gibi, bu self servis mekanizması, saldırganın hesapların kilidini kendisinin kilidini açabilmesini önlemek için yeterince güvenli olmalıdır.

References (Referanslar)

- See the OWASP article on Brute Force Attacks.
- Forgot Password CS.