Test for Process Timing (İşlem Zamanlamasını Test Edin)

Summary (Özet)

Saldırganların bir görevi tamamlamak veya yanıt vermek için gereken süreyi izleyerek bir uygulama hakkında bilgi toplayabilmeleri mümkündür. Ek olarak, saldırganlar aktif oturumları açık tutarak ve işlemlerini "beklenen" zaman diliminde göndermeyerek tasarlanmış iş süreci
akışlarını manipüle edebilir ve bozabilirler.

İşlem zamanlama mantığı güvenlik açıkları, bu manuel yanlış kullanım durumlarının uygulama / sisteme özgü yürütme ve işlem zamanlaması göz önünde bulundurularak oluşturulması gerektiği konusunda benzersizdir.

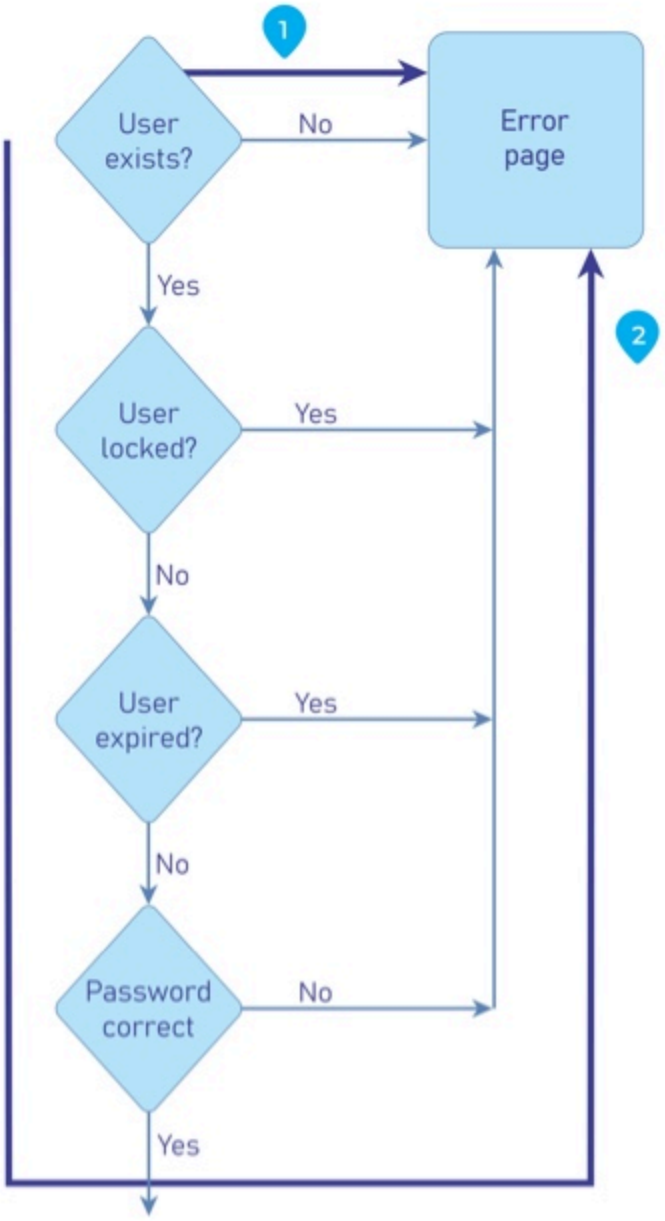
İşleme zamanlaması, uygulama / sistem arka plan süreçlerinde neler yapıldığına dair bilgi verebilir / sızdırabilir. Bir uygulama, kullanıcıların zaman değişikliklerini işleyerek bir sonraki sonucun ne
olacağını tahmin etmelerini sağlarsa, kullanıcılar buna göre ayarlayabilecek ve beklentiye ve "sistemi oynat" temelinde davranışı değiştirebilecektir.

Example 1 (Örnek 1)

Video kumar / slot makineleri, büyük bir ödemeden hemen önce bir işlemi işlemek için daha uzun sürebilir. Bu, zeki kumarbazların uzun süreç süresini görene kadar minimum miktarlarda kumar oynamalarına izin verecektir ve bu da maksimum bahis yapmalarını sağlayacaktır.

Example 2 (Örnek 2)

Süreçlerde birçok sistem günlüğü kullanıcı adı ve şifreyi sorar. Yakından bakarsanız, geçersiz bir kullanıcı adı ve geçersiz kullanıcı şifresi girmenin, bir hatayı iade etmek için geçerli bir kullanıcı adı
ve geçersiz kullanıcı şifresi girmekten daha fazla zaman aldığını görebilirsiniz. Bu, saldırganın geçerli bir kullanıcı adı olup olmadığını bilmesini ve GUI mesajına güvenmeleri gerekip gerekmediğini bilmesini sağlayabilir.



Şekil 4.10.4-1: Giriş Formunun Örnek Kontrol Akışı

Example 3 (Örnek 3)

Çoğu Arena veya seyahat acentesi, kullanıcıların bilet satın almalarına ve koltuk rezerve almalarına izin veren biletleme uygulamalarına sahiptir. Kullanıcı talep ettiğinde, bilet koltukları kilitlenir veya ödemeyi bekletilir. Ya bir saldırgan koltukları rezerve etmeye devam ederse, ancak kontrol etmezse? Koltuklar serbest

bırakılacak mı, yoksa bilet satılacak mı? Bazı bilet satıcıları artık kullanıcıların bir işlemi tamamlaması için yalnızca 5 dakika izin verir veya işlem geçersizdir.

Example 4 (Örnek 4)

Değerli bir metaller e-ticaret sitesinin, kullanıcıların oturum açtıklarında piyasa fiyatına dayalı bir fiyat teklifi ile alışveriş yapmalarına izin verdiğini varsayalım. Ya bir saldırgan bir sipariş verirse, ancak işlemi günün ilerleyen saatlerine kadar tamamlamazsa, ancak yalnızca metallerin fiyatının yükselmesine kadar işlemi tamamlayamazsa? Saldırgan ilk düşük fiyatı alacak mı?

Test Objectives (Test Hedefleri)

- Zamanla etkilenebilecek sistem işlevselliği için proje dokümantasyonunu gözden geçirin.
- Yanlış kullanım davalarını geliştirin ve uygulayın.

How To Test (Nasıl Test Edilir)

Test cihazı, hangi süreçlerin zamana bağlı olduğunu, bir görevin tamamlanması için bir pencere olup olmadığını veya belirli kontrollerin baypas etmesine izin verebilecek iki süreç arasında yürütme süresi olup olmadığını belirlemelidir.

Bunu takiben, yukarıdaki keşfedilen süreçleri kötüye kullanacak talepleri otomatikleştirmek en iyisidir, çünkü araçlar zamanlamayı analiz etmek için daha uygundur ve manuel testten daha hassastır. Bu mümkün değilse, manuel testler hala kullanılabilir.

Test cihazı, işlemin nasıl aktığına dair bir diyagram çizmelidir ve talepleri savunmasız süreçlerde başlatmak için ellerden önce hazırlamalıdır. Bir kez yapıldıktan sonra, süreç yürütmedeki
farklılıkları belirlemek için ve süreç kararlaştırılan iş mantığına karşı yanlış davranıyorsa, yakın analiz yapılmalıdır.

Related Test Cases (İlgili Test Vakaları)

- Çerezler özellikleri için test
- Test Oturum Zaman Kesintisi

Remediation (Düzeltme)

İşlem süresi göz önünde bulundurularak uygulamalar geliştirin. Saldırganlar, farklı işlem sürelerini ve sonuçları bilmekten bir tür avantaj elde edebilirse, sonuçlar ne olursa olsun aynı zaman diliminde
sağlanır.Ek olarak, uygulama / sistem, saldırganların işlemleri “kabul edilebilir” bir süre boyunca uzatmalarına izin vermemek için mekanizmaya sahip olmalıdır. Bu, bazı bilet satıcılarının şimdi kullandığı gibi belirli bir süre geçtikten sonra işlemleri iptal ederek veya sıfırlayarak yapılabilir.