Testing for the Circumvention of Work Flows (İş Akışlarının Atlatılmasını Test Edin)

Summary (Özet)

İş akışı güvenlik açıkları, saldırganın bir uygulamayı / sistemi, tasarlanmış / amaçlanan iş akışını atlatmalarını (takip etmemesine) izin verecek şekilde kötüye kullanmasına izin veren herhangi bir güvenlik açığını içerir.

Vikipedi'de iş akışı tanımı :

> Bir iş akışı, her adımın gecikme veya boşluk olmadan takip ettiği ve sonraki adım başlamadan hemen önce sona erdiği bir dizi bağlantılı adımdan oluşur. Bir kişi veya grubun çalışması, bir personel organizasyonu veya bir veya daha basit veya daha karmaşık mekanizmalar olarak ilan edilen bir dizi operasyonun tasviridir. İş akışı, gerçek çalışmanın herhangi bir soyutlanması olarak görülebilir.

Uygulamanın iş mantığı, kullanıcının doğru / özel sıradaki belirli adımları tamamlamasını ve iş akışının doğru bir şekilde tamamlanmadan sonlandırılmasını gerektirmelidir, tüm eylemler ve yumurtlayan eylemler “geri çekilir” veya iptal edilir.
İş akışlarının atlatılması veya doğru
iş mantığı iş akışını atlamasıyla ilgili güvenlik açıkları, çok uygulama / sistem spesifik ve dikkatli manuel yanlış kullanım durumları gereksinimleri ve kullanım durumları kullanılarak geliştirilmelidir.

Uygulama iş süreci, kullanıcının işlemlerinin / eylemlerinin doğru / kabul edilebilir düzende devam etmesini sağlamak için kontrollere sahip olmalıdır ve bir işlem bir tür eylemi tetiklerse, işlem başarılı bir şekilde tamamlanmadığı takdirde bu eylem “geri çekilir” ve kaldırılacaktır.

Example 1 (Örnek 1)

Birçoğumuz marketlerden ve benzin istasyonlarından satın alımlar için “kulüp / saadet noktaları” alıyoruz. Bir kullanıcının hesaplarına bağlı bir işlem başlatabildiğini ve daha sonra kulüp / pastorallik
hesaplarına puanlar eklendikten sonra işlemden iptal edildiğini veya öğeleri “sepet” ve ihalelerinden kaldırdığını varsayalım. Bu durumda sistem, ihale edilene kadar hesaba puan / kredi uygulamamalıdır veya puan / krediler, nokta / kredi artışı son ihaleye uymazsa “geri çekilmelidir”. Bunu göz önünde bulundurarak, bir saldırgan işlem başlatabilir ve aslında hiçbir şey satın almadan nokta seviyelerini oluşturmak için iptal edebilir.

Example 2 (Örnek 2)

Bir elektronik bülten panosu sistemi, ilk yayınların, gönderinin karşılaştırıldığı bir listeye dayanarak küfür içermemesini sağlamak için tasarlanabilir. Bir inkar listesindeki bir kelime girilen metinde
bulunursa, gönderim yayınlanmaz. Ancak, bir gönderim yayınlandıktan sonra, gönderim içeriğine, düzenlemeye ve değiştirebileceği, gönderim içeriğine, düzenlemeyi düzenleyebilir ve değiştirebilir, çünkü düzenlemede yayın yapılmada asla bir daha asla karşılaştırılamaz. Bunu akılda tutarak, saldırganlar ilk boş veya minimum bir tartışma açabilir ve daha sonra bir güncelleme olarak istedikleri her şeyi ekleyebilirler.

Test Objectives (Test Hedefleri)

- Uygulama sürecindeki adımları atlamak veya geçiş yöntemleri için proje belgelerini, amaçlanan iş mantığı akışından farklı bir düzende gözden geçirin.
- Bir yanlış kullanım vakası geliştirin ve tespit edilen her mantık akışını aşmaya çalışın.

How To Test (Nasıl Test Edilir)

Testing Method 1 (Test Yöntemi 1)

- Kullanıcı hesabına kredileri / noktaları tetikleyen noktaları geçen bir işlemden sonra bir işlem başlatın.
- İşlemden vazgeçin veya son ihaleyi azaltın, böylece nokta değerlerin azaltılması ve uygun puanların / kredilerin kaydedilmesini sağlamak için puan /

kredi sistemini kontrol etmeniz gerekir.

Testing Method 2 (Test Yöntemi 2)

- Bir içerik yönetimi veya bülteni panosu sisteminde geçerli ilk metin veya değerleri girin ve kaydedin.
- Ardından, kullanıcının yanlış bilgileri kaydetmesine izin verilmemesini sağlamak için mevcut verileri geçersiz bir durumda veya geçersiz değerlere bırakacak verileri eklemeye, düzenlemeyi ve kaldırmaya çalışın. Bazı “geçersiz” veriler veya bilgiler belirli kelimeler (küfürlülük) veya belirli konular (siyasi meseleler gibi) olabilir.

Related Test Cases (İlgili Test Vakaları)

- Test Dizini Traversal / Dosya Dahil
- Onaylama Yetkileme Şeması için Test
- Bypass Oturum Yönetimi Şeması için Test
- İş Mantık Verileri Test
- İstekleri Teçhitler Önünde Bulundurmak İçin Test Yeteneği
- Test Bütünlüğü Kontrolleri
- Süreç Zamanlaması için Test
- Test Sayısı Bir Fonksiyon Kullanılabilir Sınırlar
- Uygulama Yanlış Kullanıma Karşı Test Savunmaları
- Beklenmedik Dosya Türlerinin Yüklenmesini Test Edin
- Kötü Niyetli Dosyaların Yüklenmesini Test Edin

Remediation (Düzeltme)

Uygulamanın öz farkındalığı olması ve kullanıcıların iş akışı sürecindeki her adımı doğru sırayla tamamlamalarını ve saldırganların iş akışındaki herhangi bir adımı / atmasını / atmasını / veya
tekrarlamasını önlediğinden emin olmak için kendi kendine uyarlıdır. İş akışı güvenlik açıkları için test, doğru sırayla doğru adımları tamamlamazken iş sürecini

başarıyla tamamlamak amacıyla iş mantığı kötüye kullanımı / kötüye kullanım durumlarının geliştirilmesini içerir.

Referances (Referanslar)

- OWASP İtismarı Kase Hile Sayfası
- CWE-840: İş Mantık Hataları