Testing for Insecure Direct Object References (Güvensiz Doğrudan Nesne Referansları için Test)

Summary (Özet)

Güvensiz Doğrudan Nesne Referansları (IDOR), bir uygulama kullanıcı tarafından sağlanan girdiye dayalı nesnelere doğrudan erişim sağladığında ortaya çıkar. Bu güvenlik açığının bir sonucu olarak saldırganlar, örneğin veritabanı kayıtları veya dosyaları gibi sistemdeki yetkilendirme ve erişim kaynaklarını doğrudan atlayabilir. Güvensiz Doğrudan Nesne Referansları, saldırganların doğrudan bir nesneye işaret etmek için kullanılan bir parametrenin değerini değiştirerek yetkilendirmeyi ve erişim kaynaklarını doğrudan atlamasına izin verir. Bu kaynaklar, diğer kullanıcılara, sistemdeki dosyalara ve daha fazlasına ait veritabanı girişi olabilir. Bu, uygulamanın kullanıcıya verilen girdiyi almasından ve yeterli yetkilendirme kontrolleri yapmadan bir nesneyi almak için kullanmasından kaynaklanır.

Test Objectives (Test Hedefleri)

- Nesne referanslarının gerçekleşebileceği noktaları belirleyin.
- Erişim kontrol önlemlerini ve IDOR'a karşı savunmasız olup olmadıklarını değerlendirin.

How to Test (Nasıl Test Edilir)

Bu güvenlik açığını test etmek için testçinin önce, kullanıcı girişinin doğrudan nesneleri referans almak için kullanıldığı uygulamadaki tüm yerleri haritalaması gerekir. Örneğin, bir veritabanı
satırına, bir dosyaya, uygulama sayfalarına ve daha fazlasına erişmek için kullanıcı girişinin kullanıldığı konumlar. Daha sonra test cihazı, nesneleri referans almak için kullanılan parametrenin değerini değiştirmeli ve diğer kullanıcılara ait nesneleri

almanın veya başka bir şekilde yetkilendirmeyi atlamanın mümkün olup olmadığını değerlendirmelidir.

Doğrudan nesne referanslarını test etmenin en iyi yolu, farklı sahip olunan nesneleri ve işlevleri kapsayacak en az iki (genellikle daha fazla) kullanıcıya sahip olmaktır. Örneğin, her biri farklı nesnelere (satın alma bilgileri, özel mesajlar vb. gibi) ve (ilgiliyse) farklı ayrıcalıklara (örneğin yönetici kullanıcıları) erişime sahip iki kullanıcı, uygulama işlevselliğine doğrudan referanslar olup olmadığını görmek için. Birden fazla kullanıcıya sahip olarak test cihazı, diğer kullanıcıya ait nesnelere erişmeye çalışabileceği için farklı nesne isimlerini tahmin etmede değerli test süresi kaydeder.

Aşağıda, bu güvenlik açığı ve her biri için test edilmesi gereken yöntemler için birkaç tipik senaryo vardır:

The Value of a Parameter Is Used Directly to Retrieve a Database Record (Bir Parametrenin Değeri Doğrudan Bir Veritabanı Kaydı Almak İçin Kullanılır)

Örnek istek:

```
http://foo.bar/somepage?invoice=12345
```

Bu durumda fatura *invoice*parametresinin değeri veri tabanındaki fatura tablosunda indeks olarak kullanılır. Uygulama bu parametrenin değerini alır ve veritabanına bir sorguda kullanır. Uygulama daha sonra fatura bilgilerini kullanıcıya iade eder.

Faturanın değeri doğrudan sorguya girdiğinden, parametrenin değerini değiştirerek, faturanın ait olduğu kullanıcıdan bağımsız olarak herhangi bir fatura nesnesini geri almak mümkündür. Bu durumu test etmek için test cihazı, farklı bir test kullanıcısına ait bir faturanın tanımlayıcısını (bu bilgiyi uygulama iş mantığına göre görüntülememesi gerektiğini varsaymadığını) ve daha sonra yetkisiz nesnelere erişmenin mümkün olup olmadığını kontrol etmelidir.

The Value of a Parameter Is Used Directly to Perform an Operation in the System (Bir Parametrenin Değeri Sistemde Bir Operasyon Gerçekleştirmek İçin Doğrudan Kullanılır)

Örnek istek:

```
http://foo.bar/changepassword?user=someuser
```

Bu durumda, değerinin `user` Parametre, hangi kullanıcıya şifreyi değiştirmesi gerektiğini söylemek için kullanılır. Çoğu durumda bu adım bir büyücünün parçası veya çok adımlı bir operasyon olacaktır. İlk adımda uygulama, kullanıcının şifresinin hangisinin değiştirileceğini belirten bir talep alacak ve bir sonraki adımda kullanıcı yeni bir şifre sağlayacaktır (mevcut olanı istemeden).

The (İngilizce) `user` Parametre, şifre değiştirme işleminin yapılacağı kullanıcının nesnesine doğrudan atıfta bulunmak için kullanılır. Bu durumu test etmek için test cihazı, şu anda giriş yapandan farklı bir test kullanıcı adı sağlamaya çalışmalı ve başka bir kullanıcının şifresini değiştirmenin mümkün olup olmadığını kontrol etmelidir.

The Value of a Parameter Is Used Directly to Retrieve a File System Resource (Bir Parametrenin Değeri Doğrudan Bir Dosya Sistemi Kaynağını almak için kullanılır)

Örnek istek:

```
http://foo.bar/showImage?img=img00011
```

Bu durumda, değerinin `file` Parametre, uygulamaya kullanıcının hangi dosyayı almayı planladığını söylemek için kullanılır. Saldırgan, farklı bir dosyanın adını veya tanımlayıcısını
(örneğin dosya =image00012.jpg) sağlayarak, diğer kullanıcılara ait nesneleri geri alabilecektir.

Bu davayı test etmek için, test cihazı kullanıcının erişememesi ve bunun değeri olarak kullanarak erişmesi ve erişmeye çalışması gereken bir referans almalıdır. `file` Parametre. Not: Bu güvenlik açığı genellikle bir dizin / yol geçişi güvenlik açığı ile birlikte kullanılır (bkz. Path Traversal Testi)

The Value of a Parameter Is Used Directly to Access Application Functionality (Bir Parametrenin Değeri Doğrudan Uygulama İşlevselliğine Erişmek İçin Kullanılır)

Örnek istek:

`http://foo.bar/accessPage?menuitem=12`

Bu durumda, değerinin `menuitem` Parametre, uygulamaya kullanıcının hangi menü öğesine (ve dolayısıyla hangi uygulama işlevselliğine) erişmeye çalıştığını söylemek için kullanılır. Kullanıcının kısıtlanması gerektiğini ve bu nedenle yalnızca menü öğelerine 1, 2 ve 3'e erişmek için bağlantılara sahip olduğunu varsayalım. Değeri değiştirerek `menuitem` Parametre, yetkilendirmeyi atlamak ve ek uygulama işlevselliğine erişmek mümkündür. Bu durumu test etmek için test cihazı, uygulama
işlevselliğinin bir menü öğesine atıfta bulunarak belirlendiği bir konumu tanımlar, verilen test kullanıcısının erişebileceği menü öğelerinin değerlerini haritalandırır ve ardından diğer menü öğelerini işler.

Yukarıdaki örneklerde tek bir parametrenin değiştirilmesi yeterlidir. Bununla birlikte, bazen nesne referansı birden fazla parametre arasında bölünebilir ve test buna göre ayarlanmalıdır.

References (Referanslar)

En iyi 10 2013-A4-Güvensiz Doğrudan Nesne Referansları