Test Role Definitions (Test Rol Tanımları)

Summary (Özet)

Uygulamalar çeşitli işlev ve hizmet türlerine sahiptir ve bunlar kullanıcının ihtiyaçlarına göre erişim izni gerektirir. Bu kullanıcı şunlar olabilir:

- Uygulama işlevlerini yönettikleri bir yönetici.
- Başvuru işlemlerini inceleyen ve detaylı bir rapor verdikleri bir denetçi.
- Müşterilerin hesaplarındaki sorunları çözmelerine ve çözmelerine yardımcı oldukları bir destek mühendisi.
- Uygulama ile etkileşime girerek hizmetlerinden yararlandıkları bir müşteri.

Bu kullanımları ve bu uygulama için diğer kullanım durumlarını ele almak için, rol tanımları kurulumdur (daha yaygın olarak RBAC olarak bilinir). Bu rollere dayanarak, kullanıcı gerekli görevi yerine getirebilir.

Test Objectives (Test Hedefleri)

- Uygulamanın kullandığı rolleri tanımlayın ve belgeleyin.
- Başka bir rolü değiştirmeye, değiştirmeye veya erişmeye çalışın.
- Verilen izinlerin arkasındaki rollerin ve ihtiyaçların ayrıntılılığını gözden geçirin.

How to Test (Nasıl Test Edilir)

Roles Identification (**Roller Tanımlama**)

Test cihazı, aşağıdaki yöntemlerden herhangi biri üzerinden test edilen uygulama rollerini belirleyerek başlamalıdır:

- Uygulama belgeleri.
- Uygulamanın geliştiricileri veya yöneticileri tarafından rehberlik.
- Uygulama yorumları.
- Fuzz olası roller:

- çerez değişkeni (*örneğin*. `role=admin`, `isAdmin=True`)
- Hesap değişkeni (örneğin.*e.g.* `Role: manager`)
- Gizli dizinler veya dosyalar *(örneğin.* `/admin`, `/mod`, `/backups`)
- İyi bilinen kullanıcılara geçiş *(*örneğin. `admin`, `backups`, vb.)

Switching to Available Roles (**Mevcut rollere geçiş**)

Olası saldırı vektörlerini belirledikten sonra, testçinin mevcut rollere erişebildiklerini test etmesi ve doğrulaması gerekir.

> Bazı uygulamalar, kullanıcının oluşturma konusundaki rollerini titiz kontroller ve politikalar yoluyla veya kullanıcının rolünün arka uç tarafından oluşturulan bir imza ile uygun şekilde korunmasını sağlayarak tanımlar. Rollerin var olduğunu bulmak, onların bir güvenlik
> açığı olduğu anlamına gelmez.

Review Roles Permissions (Rezerv Rolleri İncelemeleri)

Sistemdeki rollere erişim kazandıktan sonra, testçi her bir role sağlanan izinleri anlamalıdır.

Bir destek mühendisi, bir kullanıcının yerine idari işlevler yürütmemeli, yedeklemeleri yönetememeli veya herhangi bir işlem yapabilmemelidir.

Bir yönetici sistemde tam yetkiye sahip olmamalıdır. Hassas yönetici işlevselliği, bir maker-kitre prensibinden yararlanmalı veya yöneticinin işlemi yürüttüğünden emin olmak için MFA'yı kullanmalıdır. Bu konuda açık bir örnek, 2020'deki Twitter olayıydı.

Tools (Araçlar)

Yukarıda belirtilen testler, sisteme erişmek için kullanılan hariç, herhangi bir aracın kullanılmadan yapılabilir.

İşleri daha kolay ve daha belgeli hale getirmek için, kişi kullanabilir:

- Burp'un Otoriter Uzantısı

- ZAP’in Erişim Kontrolü Test eklentisi

References (Referanslar)

- Kurumsal Güvenlik Yönetimi için Rol Mühendisliği, E Coyne & J Davis, 2007
- Rol mühendisliği ve RBAC standartları