Testing for Session Puzzling (Oturum Bulmacası için Test)

Summary (Özet)

Oturum Değişken Aşırı Yükleme (Oturum Bulmaca olarak da bilinir), bir saldırganın aşağıdakiler de dahil olmak üzere çeşitli kötü niyetli eylemler gerçekleştirmesini sağlayabilecek bir uygulama seviyesi güvenlik açığıdır:

- Verimli kimlik doğrulama uygulama mekanizmalarını atın ve meşru kullanıcıları taklit edin.
- Kötü niyetli bir kullanıcı hesabının ayrıcalıklarını, aksi takdirde kusursuz olarak kabul edilecek bir ortamda yükseltin.
- Çok fazlı süreçlerde eleme aşamalarını atlayın, süreç yaygın olarak önerilen tüm kod seviyesi kısıtlamalarını içerse bile.
- Sunucu tarafı değerlerini tahmin edilemeyen veya algılanamayan dolaylı yöntemlerle manipüle edin.
- Daha önce ulaşılamayan veya hatta güvenli kabul edilen yerlerde geleneksel saldırıları gerçekleştirin.

Bu güvenlik açığı, bir uygulama aynı oturum değişkenini birden fazla amaç için kullandığında ortaya çıkar. Bir saldırgan, geliştiriciler tarafından beklenmeyen bir siparişte sayfalara potansiyel olarak
erişebilir, böylece oturum değişkeni bir bağlamda ayarlanır ve daha sonra başka bir bağlamda kullanılır.

Örneğin, bir saldırgan, genellikle başarılı bir kimlik doğrulama işleminden sonra oturumda saklanan kimlikle ilgili değerler içeren oturum değişkenlerinin varlığını doğrulayarak kimlik doğrulamasını
uygulayan uygulamaların kimlik doğrulama uygulamalarını atlamak için oturum değişken aşırı yüklemesini kullanabilir. Bu, bir saldırganın ilk olarak uygulamada oturum bağlamı belirleyen bir yere eriştiği ve daha sonra bu bağlamı inceleyen ayrıcalıklı yerlere eriştiği anlamına gelir.

Örneğin - bir kimlik doğrulama bypass saldırı vektörü, oturumu sabit değerlere veya kullanıcı kaynaklı girdilere göre aynı oturumla dolduran halka açık bir giriş noktasına (örneğin bir şifre kurtarma sayfası) erişerek gerçekleştirilebilir.

Test Objectives (Test Hedefleri)

- Tüm oturum değişkenlerini belirleyin.
- Oturum üretiminin mantıksal akışını kırın.

How to Test (Nasıl Test Edilir)

Black-Box Testing (Siyah-Kutu Testi)

Bu güvenlik açığı, uygulama tarafından kullanılan ve hangi bağlamda geçerli oldukları tüm oturum değişkenlerini numaralandırarak tespit edilebilir ve kullanılabilir. Özellikle bu, bir dizi giriş noktasına erişerek ve ardından çıkış noktalarını inceleyerek mümkündür. Kara kutu testi durumunda bu prosedür zordur ve her farklı dizi farklı bir sonuca yol açabileceğinden biraz şans gerektirir.

Examples (Örnekler)

Çok basit bir örnek, giriş noktasında, kullanıcıdan kullanıcı adı veya e-posta adresi gibi bazı tanımlayıcı bilgiler sağlamasını talep edebilecek şifre sıfırlama işlevi olabilir. Bu sayfa daha sonra oturumu doğrudan istemci tarafından alınan veya alınan girdiye göre sorgulardan veya hesaplamalardan elde edilen bu tanımlayıcı değerler ile doldurabilir. Bu noktada, uygulamada bu oturum nesnesine dayalı özel verileri gösteren bazı sayfalar olabilir. Bu şekilde saldırgan kimlik doğrulama işlemini atlayabilir.

Gray-Box Testing (Gri-Kutu Testi)

Bu güvenlik açıklarını tespit etmenin en etkili yolu bir kaynak kodu incelemesidir.

Remediation (Düzeltme)

Oturum değişkenleri sadece tek bir tutarlı amaç için kullanılmalıdır.

Referances (Referanslar)

- Oturum Puslu

- Oturum Bulmaca ve Oturum Yarışı Koşulları