Test Ability to Forge Requests (İstekleri Taklit Edebilme Yeteneğini Test Edin)

Summary (Özet)

Talepleri taklit etmek, saldırganların arka uç işleme için doğrudan bilgi göndermek için ön uç GUI başvurusunu aşmak için kullandıkları bir yöntemdir. Saldırganın amacı, uygulama iş mantığı tarafından desteklenmeyen, korunmayan veya beklenen veri değerleriyle yakalanan bir vekil aracılığıyla HTTP POST/GET taleplerini göndermektir. Sahte isteklerin bazı örnekleri, tahmin edilebilir veya öngörülebilir parametrelerden yararlanmayı veya geliştirme sırasında çok yararlı olan
ancak bilgi sızdıran veya iş mantığını atlayabilecek özel ekranların veya pencerelerin sunulması gibi “gizli” özellikleri ve işlevselliği ortaya çıkarmaktır.

İstekler oluşturma yeteneği ile ilgili güvenlik açıkları her uygulamaya özgüdür ve iş mantığı veri doğrulamasından farklıdır, çünkü odak noktası iş mantığı iş akışını kırmaktır.

Uygulamalar, sistemin saldırganların iş mantığını, işlenmesinden veya akışını kullanma fırsatını kullanabilecek sahte talepleri kabul etmesini önlemek için mantık kontrollerine sahip olmalıdır. Sahtecilik talebi yeni bir şey değildir; saldırgan, HTTP POST / GET taleplerini uygulamaya göndermek için bir araya gelen bir proxy kullanır. Sahtecilik talebiyle saldırganlar, uygulamanın bir sürecin veya görevin gerçekleştiğini veya gerçekleşmediğini düşünmesini sağlamak için parametreleri bularak, tahmin ederek ve manipüle ederek iş mantığını veya sürecini atlatabilirler.

Ayrıca, sahte talepler, başlangıçta geliştiriciler ve testçiler tarafından bazen “Paskalya yumurtası”
olarak adlandırılan geliştiriciler ve testçiler tarafından kullanılan “gizli” özellikler veya işlevler çağırarak programatik veya iş mantığı akışının sübvanse edilmesine izin verebilir. “Bir Paskalya yumurtası, içinde kasıtlı bir şaka, gizli mesaj veya bilgisayar programı, film, kitap veya bulmaca gibi bir eserde yer alır. Oyun

tasarımcısı Warren Robinett'e göre, terim Atari'de, Robinett tarafından zaten yaygın olarak dağıtılmış olan Adventure'da gizlenmiş gizli bir mesajın varlığına karşı uyarılan personel tarafından icat edildi. İsmin geleneksel bir Paskalya yumurtası avı fikrini çağrıştırdığı söyleniyor" dedi.

Example 1 (Örnek 1)

Bir e-ticaret tiyatro sitesinin kullanıcıların biletlerini seçmelerine, tüm satışta bir kez% 10 Kıdemli indirim uygulamasına, alt totuğu görüntülemesine ve satışı ihale etmesine izin verdiğini varsayalım. Bir saldırgan bir vekil aracılığıyla, uygulamanın bir indirimin alınıp alınmadığını belirlemek için iş mantığı tarafından kullanılan gizli bir alana (1 veya 0 veya 0) sahip olduğunu görebilirse. Saldırgan daha sonra aynı indirimden birden çok kez yararlanmak için 1 veya “istek alınmadı” değerini birden çok kez sunabiliyor.

Example 2 (Örnek 2)

Bir çevrimiçi video oyununun, korsanlar hazinesi ve korsanları bulmak ve tamamlanan her seviye için puan için puanlar için jetonlar ödediğini varsayalım. Bu belirteçler daha sonra ödüller için değiştirilebilir. Ek olarak, her seviyenin puanları seviyeye eşit çarpan bir değere sahiptir. Bir saldırgan bir vekil aracılığıyla, uygulamanın oyunun en yüksek seviyelerine hızlı bir şekilde ulaşmak için geliştirme ve test sırasında kullanılan gizli bir alana sahip olduğunu ve hızlı bir şekilde
kazanılmamış puanları biriktirdiklerini görebilseydi.

Ayrıca, bir saldırgan bir vekil aracılığıyla, uygulamanın geliştirme ve test sırasında kullanılan gizli bir alana sahip olduğunu, diğer çevrimiçi oyuncuların veya gizli hazinenin saldırganla ilgili olduğu
yerde belirtilen bir kütüğü etkinleştirmesini sağlayabilirse, hızlı bir şekilde bu yerlere gidebilir ve puanlar alabilirlerdi.

Test Objectives (Test Hedefleri)

- Alanların tahmin edilebilir, öngörülebilir veya gizli işlevselliğini arayan proje belgelerini gözden geçirin.
- Normal iş mantığı iş akışını atlamak için mantıksal olarak geçerli veriler ekleyin.

How To Test (Nasıl Test Edilir)

Through Identifying Guessable Values (Tahmini Değerleri Belirleyici Olarak Belirleyici)

- Bir vekaleten kullanmak, HTTP POST / GET'in, değerlerin düzenli bir aralıkta arttığının veya kolayca tahmin edilebilir olduğuna dair bazı göstergeler aradığını gözlemleyin.
- Bazı değerlerin tahmin edilebilir olduğu tespit edilirse, bu değer değiştirilebilir ve beklenmedik bir görünürlük kazanılabilir.

Through Identifying Hidden Options (Gizli Seçenekleri Tanımlayarak)

- Kesişen bir vekil kullanarak, HTTP POST / GET'i, açılabilir veya etkinleştirilebilen debug gibi gizli özelliklerin bazı göstergelerini arayın.
- Bulunan varsa, farklı bir uygulama yanıtı veya davranışı elde etmek için bu değerleri tahmin etmeye ve değiştirmeye çalışın.

Related Test Cases (İlgili Test Vakaları)

- Testing for Exposed Session Variables
- Testing for Cross Site Request Forgery (CSRF)
- Testing for Account Enumeration and Guessable User Account

Remediation (Düzeltme)

Uygulama, saldırganların programatik veya iş mantığı akışını altüst etmek için parametreleri tahmin etmelerini ve manipüle etmesini veya hata ayıklama gibi gizli / belgesiz işlevsellikten yararlanmasını
önleyecek iş mantığı ile yeterince akıllı olmalı ve iş mantığı ile tasarlanmalıdır.

Tools (Araçlar)

- OWASP Zed Attack Proxy (ZAP)
- Burp Suite

References (Referanslar)

- Cross Site Request Forgery - Legitimizing Forged Requests

- Easter egg
- Top 10 Software Easter Eggs