Testing for XPath Injection (XPath Enjeksiyonu için Test)

Summary (Özet)

XPath, öncelikle bir XML belgesinin parçalarını ele almak için tasarlanmış ve geliştirilmiş bir dildir. XPath enjeksiyon testinde, XPath syntakx'i uygulama tarafından yorumlanan bir talebe enjekte
etmenin mümkün olup olmadığını test ederek, bir saldırganın kullanıcı kontrollü XPath sorgularını yürütmesine izin verir. Başarılı bir şekilde yararlanıldığında, bu güvenlik açığı, bir saldırganın kimlik doğrulama mekanizmalarını atlamasına veya uygun yetkilendirme olmadan bilgiye erişmesine izin verebilir.

Web uygulamaları, operasyonları için ihtiyaç duydukları verileri depolamak ve erişmek için veritabanlarını yoğun bir şekilde kullanır. Tarihsel olarak, ilişkisel veri tabanları veri depolama için en yaygın teknoloji olmuştur, ancak son yıllarda XML dilini kullanarak verileri düzenleyen veritabanları için artan bir popülerliğe tanık oluyoruz. Tıpkı ilişkisel veritabanlarına SQL dili ile erişildiği gibi, XML veritabanları da XPath'i standart sorgu dili olarak kullanır.

Çünkü, kavramsal bir bakış açısıyla, XPath amacında ve uygulamalarında SQL'e çok benzer, ilginç bir sonuç, XPath enjeksiyon saldırılarının SQL Injection saldırılarıyla aynı mantığı izlemesidir. Bazı yönlerden, XPath standart SQL'den daha da güçlüdür, çünkü tüm gücü zaten özelliklerinde
bulunurken, bir SQL Enjeksiyon saldırısında kullanılabilecek tekniklerin çok sayıdaı, hedef veritabanı tarafından kullanılan SQL lehçesinin özelliklerine bağlıdır. Bu, XPath enjeksiyon saldırılarının çok daha uyarlanabilir ve her yerde olabileceği anlamına gelir. Bir XPath enjeksiyon saldırısının bir başka avantajı, SQL'in aksine, sorgumuz XML belgesinin her bölümüne erişebileceğinden hiçbir ACL'nin uygulanmamasıdır.

Test Objectives (Test Hedefleri)

- XPATH enjeksiyon noktalarını belirleyin.

How To Test (Nasıl Test Edilir)

XPath saldırı deseni ilk olarak Amit Klein tarafından yayınlandı ve normal SQL Injection'a çok benziyor. Sorunu ilk kavrayışı elde etmek için, kullanıcının kullanıcı adını ve şifresini girmesi gereken bir uygulamaya kimlik doğrulamayı yöneten bir giriş sayfası hayal edelim. Veritabanımızın aşağıdaki XML dosyasıyla temsil edildiğini varsayalım:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
   <user>
      <username>gandalf</username>
      <password>!c3</password>
      <account>admin</account>
   </user>
   <user>
      <username>Stefan0</username>
      <password>w1s3c</password>
      <account>guest</account>
   </user>
   <user>
      <username>tony</username>
      <password>Un6R34kb!e</password>
      <account>guest</account>
   </user>
</users>
```

Kullanıcı adı olan hesabı döndüren bir XPath sorgusu `gandalf` ve şifre `!c3` Aşağıdakiler şöyledir:

```
string(//user[username/text()='gandalf' and password/text()='!c3']/account/text())
```

Uygulama kullanıcı girişini düzgün bir şekilde filtrelemezse test cihazı XPath kodunu enjekte edebilir ve sorgu sonucuna müdahale edebilir. Örneğin, test cihazı aşağıdaki değerleri girebilir:

```
Username: ' or '1' = '1
Password: ' or '1' = '1
```

Oldukça tanıdık geliyor, değil mi? Bu parametreleri kullanarak, sorgu gelir:

```
string(//user[username/text()='' or '1' = '1' and password/text()='' or '1' = '1']/account/text())
```

Ortak bir SQL Enjeksiyon saldırısında olduğu gibi, her zaman doğru değerlendiren bir sorgu oluşturduk, bu da uygulamanın bir kullanıcı adı veya şifre sağlanmamış olsa bile kullanıcıyı doğrulayacağı anlamına geliyor. Ve yaygın bir SQL Enjeksiyon saldırısında olduğu gibi, XPath
enjeksiyonu ile ilk adım tek bir alıntı eklemektir (
`'`) test edilmek üzere sahada, sorguda bir sözdizimi hatası getirilmesi ve uygulamanın bir hata mesajı iade edip etmediğini kontrol etmek.

XML verileri dahili ayrıntıları hakkında bilgi yoksa ve uygulama, iç mantığını yeniden yapılandırmamıza yardımcı olan yararlı hata mesajları sağlamazsa, amacı tüm veri yapısını yeniden yapılandırmak olan bir Kör XPath Enjeksiyonu saldırısı gerçekleştirmek mümkündür. Teknik, çıkarım tabanlı SQL Injection'a benzer, çünkü yaklaşım, bir miktar bilgi döndüren bir sorgu oluşturan kod enjekte etmektir. Blind XPath Injection, referanslı makalede Amit Klein tarafından daha ayrıntılı olarak açıklanmaktadır.

References (Referanslar)

Whitepapers (Beyaz kağıtlar)

- Amit Klein: “Blind XPath Injection”
- XPath 1.0 specifications