Testing for LDAP Injection (LDAP Enjeksiyonu için Test)

Summary (Özet)

Hafif Dizin Erişim Protokolü (LDAP), kullanıcılar, konakçılar ve diğer birçok nesne hakkında bilgi depolamak için kullanılır. LDAP enjeksiyonu, bir LDAP yapısında temsil edilen kullanıcılar ve konakçılar hakkında hassas bilgilerin açıklanmasına, değiştirilmesine veya eklenmesine izin
verebilecek bir sunucu tarafı saldırısıdır. Bu, daha sonra dahili aramaya, eklemeye ve işlevleri değiştirmek için geçiş yapan giriş parametrelerini manipüle ederek yapılır.

Bir web uygulaması, kullanıcıların kurumsal bir yapı içinde diğer kullanıcıların bilgilerini doğrulamasına veya aramasına izin vermek için LDAP'ı kullanabilir. LDAP enjeksiyon saldırılarının amacı, LDAP arama filtreleri metakaraktörlerini uygulama tarafından yürütülecek bir
sorguya enjekte etmektir.

Rfc2254, LDAPv3'te bir arama filtresinin nasıl oluşturulacağına dair bir dilbilgisi tanımlar ve RFc1960 (LDAPv2) uzatır.

Polonya notasyonu prefix notation olarak da bilinen Polonya notasyonunda bir LDAP arama filtresi inşa edilmiştir.

Bu, böyle bir arama filtresinde sahte bir kod koşulunun olduğu anlamına gelir:

`find("cn=John & userPassword=mypass")`

Şu şekilde temsil edilecektir:

`find("(&(cn=John)(userPassword=mypass))")`

Bir LDAP arama filtresindeki boolean koşulları ve grup agregasyonları aşağıdaki metakaraktörlerin kullanılmasıyla uygulanabilir:

Metachar	Meaning
&	Boolean AND
|	Boolean OR

!	Boolean NOT
=	Equals
~=	Approx
>=	Greater than
<=	Less than
*	Any character
()	Grouping parenthesis

Bir arama filtresinin nasıl oluşturulacağına dair daha eksiksiz örnekler ilgili RFC'de bulunabilir.

Bir LDAP enjeksiyonu kırılganlığının başarılı bir şekilde sömürülmesi, test cihazının şunları yapmasına izin verebilir:

- Yetkisiz içeriğe erişin
- Başvuru kısıtlamalarından kaçının
- İzinsiz bilgileri toplayın
- LDAP ağaç yapısı içindeki nesneleri ekleyin veya değiştirin.

Test Objectives (Test Hedefleri)

- LDAP enjeksiyon noktalarını belirleyin.
- Enjeksiyonun ciddiyetini değerlendirin.

How to Test (Nasıl Test Edilir)

Example 1: Search Filters (Örnek 1: Arama Filtreleri)

Aşağıdaki gibi bir arama filtresi kullanarak bir web uygulamasına sahip olduğumuzu varsayalım:

`searchfilter="(cn="+user+")"`

Bu şekilde bir HTTP isteği ile anlık olarak adlandırılır:

`http://www.example.com/ldapsearch?user=John`

Eğer değer varsa `John` Bir ile değiştirilir `*`, isteği göndererek:

`http://www.example.com/ldapsearch?user=*`

Filtre şöyle görünecektir:

`searchfilter="(cn=*)"`

Her nesneyi bir 'cn' özelliğiyle eşleştiren her şeye eşittir.

Uygulama LDAP enjeksiyonuna karşı savunmasızsa, uygulamanın yürütme akışına ve LDAP bağlantılı kullanıcının izinlerine bağlı olarak kullanıcının niteliklerinin bir kısmını veya tamamını gösterecektir.

Bir testçi, parametreye yerleştirerek bir deneme-yanılma yaklaşımı kullanabilir `(`, `|`, `&`, `*` ve diğer karakterler, hataların uygulanmasını kontrol etmek için.

Example 2: Login (Örnek 2: Giriş)

Bir web uygulaması, oturum açma işlemi sırasında kullanıcı kimlik bilgilerini kontrol etmek için LDAP kullanırsa ve LDAP enjeksiyonuna karşı savunmasızsa, her zaman gerçek bir LDAP sorgusu enjekte ederek kimlik doğrulama kontrolünü atlamak mümkündür (S SQL ve XPATH enjeksiyonuna benzer şekilde).

Bir web uygulamasının LDAP kullanıcı / paskalif çifti ile eşleşmek için bir filtre kullandığını varsayalım.

`searchlogin= "(&(uid="+user+")(userPassword={MD5}"+base64(pack("H*",md5(pass)))+"))";`

Aşağıdaki değerleri kullanarak:

```
user=*)(uid=*))(|(uid=*
pass=password
```

Arama filtresi aşağıdaki sonuçlarla sonuçlanacaktır:

`searchlogin="(&(uid=*)(uid=*))(|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))";`

Doğru ve her zaman doğru olan. Bu şekilde, test cihazı LDAP ağacındaki ilk kullanıcı olarak oturum açma statüsü kazanacak.

Tools (Araçlar)

- Softerra LDAP Browser

References (Referanslar)

- LDAP Injection Prevention Cheat Sheet

Whitepapers (Beyaz Kağıtlar)

- Sacha Faust: LDAP Injection: Are Your Applications Vulnerable?
- IBM paper: Understanding LDAP
- RFC 1960: A String Representation of LDAP Search Filters
- LDAP injection