**1. Injection**

-when attacker is able to execute unintended commands on the system

Ex: SQL queries, PHP queries, LDAP queries and OS commands.

**Q: Where to inject?**

A: Wherever a user input is required or use can modify data. It can be a text box, username/password field, feedback fields, comment field, URL etc.

**Q: Why to inject?**

A: To check if the application is vulnerable.

--when we build a SQL statement by concatenating a string – we are inviting a SQL injection attack.

What can cause SQL Injection?

Building sql statement dynamically, by concatenating strings can cause sql injections

How to avoid sql injections?

2 Ways to avoid sql injection

Use Parameterized queries

or

Use Stored Procedures

1..Building SQL statment dynamically and concatinating the string

SqlCommand cmd = new SQLCommand("Select \* from tblProduct where Name = '"+ TextBox1.Text + "'", con)

--attack inviting string

'"+ TextBox1.Text + "'"

select \* from tblProduct where Name = 'Pens'

------------------------

in user input box user can enter

Pen --- no attack

in the given text box enter:

Pen'; delete from tblProduct --'

**youtube link:**

https://www.youtube.com/watch?v=4Q\_ZSEyLf4k

To avoid SQL injection this issue:

1. use parameterized query

2. use stored procedures

1.avoid SQL injuction

2.Avoids N/W traffic

3. we can reuse the stored procedures in different placess(code reusability)

4. improves performance - as adhoc queries has to create a execution plan every time before executing the actual command this can be avoided if we are using stored procedures

Stored procedure:

Create Proc spGetProductByName

@Name varchar(30)

as

Begin

select \* from tblProducts where Name = @Name

End

1. use parameterized query

- SqlCommand cmd = new SQLCommand("Select \* from tblProduct where Name = @Name",con);

cmd.Parameters.ADD(new SQLParameter("@Name",TextBox1.Text));

-- @Name -- is a parameter

2. use stored procedures

1.avoid SQL injuction

2.Avoids N/W traffic

3. we can reuse the stored procedures in different placess(code reusability)

4. improves performance - as adhoc queries has to create a execution plan every time before executing the actual command this can be avoided if we are using stored procedures

Stored procedure:

Create Proc spGetProductByName

@Name varchar(30)

as

Begin

select \* from tblProducts where Name = @Name

End

in C# code

--------------

SqlCommand cmd = new SQLCommand("spGetProductByName",con);

cmd.CommandType = CommandType.StoredProcedure;

cmd.Parameters.ADD(new SQLParameter("@Name",TextBox1.Text));

Hi Akila

This is madhan, I have joined Move Bangalore team.

Please let me know what should I start with.

Could you please help me in accessing “move.okta.com” and “Move Email”. Currently it is not accessible.

A string is a list of characters in order.

Python strings are immutable

An empty string is a string that has 0 characters.

Python recognize as strings everything that is delimited by quotation marks

(" " or ' ').

I was looking forward to talk to you regarding the project. Because of my Access issue I was not able to connect with you.

Akila if you don’t mind could you please share your personal number; so that I can call you at your time (8:30 to 9:30 AM PST)

If you are busy please let me know your free time today (18 Sep) so that I can connect with you.

Sorry Akila instead of mentioning today I have scheduled meeting for Tomorrow.

Good Morning.

Are you available for meeting?

Odibal

Hi Akila,

Good Evening.

I was looking forward to talk to you regarding the project. Because of my Access issue I was not able to connect with you.

Akila if you don’t mind could you please share your personal number; so that I can call you at your time (8:30 to 9:30 AM PST)

Python module re. -- under this module we have some useful methods like

Whitespace

String Manipulation

To manipulate strings, we can use some of Pythons built-in methods.

word = "Hello World"