Parameterized Query

SqlCommand command = new SqlCommand("Insert into Employee (id, name , address, salary) values(7,'Farhan','Delhi', 90000)", connection);

Right now. Our query is having hard coded values , we need to change them to parameterized queries

using System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Data.SqlClient;

namespace AdoNetDemos

{

enum choice { Insert=1 , Update, Delete, GetRecords};

class InsertDemo

{

static SqlConnection connection=null;

static void Main()

{

int Choice;

string ch = "y";

while (ch == "y")

{

MainMenu();

Console.WriteLine("Enter Your Choice");

Choice = Byte.Parse(Console.ReadLine());

switch (Choice)

{

case (int)choice.Insert:

{

InsertRecord();

break;

}

case (int)choice.Update:

{

UpdateRecord();

break;

}

case (int)choice.Delete:

{

DeleteRecord();

break;

}

case (int)choice.GetRecords:

{

GetRecords();

break;

}

default:

{

Console.WriteLine("Invalid Choice");

break;

}

}

Console.WriteLine("Do you want to repeat the process");

ch = Console.ReadLine();

}

}

static void MainMenu()

{

Console.WriteLine("1. Insert Record");

Console.WriteLine("2. Update Record");

Console.WriteLine("3. Delete Record");

Console.WriteLine("4. Display All Records");

}

static SqlConnection GetConnnection()

{

connection = new SqlConnection("data source=LAPTOP-53S2KQS8;" +

"initial catalog=PracticeDb;integrated security=true");

return connection;

}

static void InsertRecord()

{

connection = GetConnnection();

Console.WriteLine("Enter ID");

int id = Byte.Parse(Console.ReadLine());

Console.WriteLine("Enter Name");

string name = Console.ReadLine();

Console.WriteLine("Enter Address");

string address = Console.ReadLine();

Console.WriteLine("Enter Salary");

int salary = int.Parse(Console.ReadLine());

SqlCommand command = new SqlCommand("Insert into Employee (id, name , address, salary) values(@id, @name,@address,@salary)", connection);

command.Parameters.AddWithValue("@id", id);

command.Parameters.AddWithValue("@name", name);

command.Parameters.AddWithValue("@address", address);

command.Parameters.AddWithValue("@salary", salary);

connection.Open();

int count = command.ExecuteNonQuery();

Console.WriteLine("No of Records inserted are "+ count);

connection.Close();

}

static void UpdateRecord()

{

connection = GetConnnection();

Console.WriteLine("Enter ID whose Record you want to modisy");

int id = Byte.Parse(Console.ReadLine());

Console.WriteLine("Enter New Address");

string address = Console.ReadLine();

Console.WriteLine("Enter Revised Salary");

int salary = int.Parse(Console.ReadLine());

SqlCommand command = new SqlCommand("Update Employee" +

"set address =@adress, salary = @salary where is=@id", connection);

command.Parameters.AddWithValue("@id", id);

command.Parameters.AddWithValue("@address", address);

command.Parameters.AddWithValue("@salary", salary);

connection.Open();

int count = command.ExecuteNonQuery();

Console.WriteLine("No of Records updated are " + count);

connection.Close();

}

static void DeleteRecord()

{

connection = GetConnnection();

Console.WriteLine("Enter ID whose Record you want to delete");

int id = Byte.Parse(Console.ReadLine());

SqlCommand command = new SqlCommand("Delete Employee" +

"where id=@id", connection);

command.Parameters.AddWithValue("@id", id);

connection.Open();

int count = command.ExecuteNonQuery();

Console.WriteLine("No of Records deleted are " + count);

connection.Close();

}

static void GetRecords()

{

connection = GetConnnection();

SqlCommand command = new SqlCommand("Select \* from Employee",

connection);

connection.Open();

SqlDataReader reader = command.ExecuteReader();

if(reader.HasRows)

{

while(reader.Read())

{

Console.WriteLine(reader["id"].ToString()+ " " + reader["name"]);

}

}

reader.Close();

connection.Close();

}

}

}