

# SQL Server Tutorial

## Part 142 - Dynamic SQL in Stored Procedure

Venkat

PRAGIM Technologies

[kudvenkat@gmail.com](mailto:kudvenkat@gmail.com)

<http://csharp-video-tutorials.blogspot.com>

PragimTech.com | facebook.com/pragimtech | twitter.com/kudvenkat | 91 99456 99393

# In this session we will learn

- Using Dynamic SQL in a stored procedure and it's implications from SQL Injection perspective

**Link to Dot Net Basics, ASP.NET, C#, ADO.NET and SQL Server video series**

<http://www.youtube.com/user/kudvenkat/playlists>

## **Suggested Videos**

**Part 139 - Implement search web page using ASP .NET and Stored Procedure**

**Part 140 - Implement search web page using ASP.NET and Dynamic SQL**

**Part 141 - Prevent sql injection with dynamic sql**

# Dynamic SQL in Stored Procedure

If you are in need of the DVD with all the videos and PPT's, please visit  
<http://pragimtech.com/order.aspx>

**Whether you are creating Dynamic SQL** in a client application (like a web application) or in a stored procedure always use parameters instead of concatenating strings. Using parameters to create dynamic SQL statements prevents SQL injection

# Dynamic SQL in Stored Procedure


```
-- Stored procedure with Dynamic SQL that is prone to SQL Injection
Create Procedure spSearchEmployeesBadDynamicSQL
@FirstName nvarchar(100) = NULL,
@LastName nvarchar(100) = NULL,
@Gender nvarchar(50) = NULL,
@Salary int = NULL
As
Begin

    Declare @sql nvarchar(max)

    Set @sql = 'Select * from Employees where 1 = 1'

    if(@FirstName is not null)
        Set @sql = @sql + ' and FirstName=''' + @FirstName + ''''
    if(@LastName is not null)
        Set @sql = @sql + ' and LastName=''' + @LastName + ''''
    if(@Gender is not null)
        Set @sql = @sql + ' and Gender=''' + @Gender + ''''
    if(@Salary is not null)
        Set @sql = @sql + ' and Salary=''' + @Salary + ''''

    Execute sp_executesql @sql
End
Go
```



# Additional Resources

## PRAGIM Home Page:

[www.PragimTech.com](http://www.PragimTech.com)

## Resources:

C#, ADO.NET, ASP.NET, SQL Server & MVC youtube Playlists

<http://www.youtube.com/user/kudvenkat/playlists>

Code samples and text version of all the videos on my blog

<http://www.csharp-video-tutorials.blogspot.com>

To receive email alerts when new videos are uploaded, please subscribe to my YOUTUBE channel

[www.YouTube.com/kudvenkat](http://www.YouTube.com/kudvenkat)

<https://twitter.com/kudvenkat>

# Dynamic SQL in Stored Procedure

```
-- Stored procedure with Dynamic SQL that prevents SQL Injection
Create Procedure spSearchEmployeesGoodDynamicSQL
@FirstName nvarchar(100) = NULL,
@LastName nvarchar(100) = NULL,
@Gender nvarchar(50) = NULL,
@Salary int = NULL
As
Begin

    Declare @sql nvarchar(max)
    Declare @sqlParams nvarchar(max)

    Set @sql = 'Select * from Employees where 1 = 1'

    if(@FirstName is not null)
        Set @sql = @sql + ' and FirstName=@FN'
    if(@LastName is not null)
        Set @sql = @sql + ' and LastName=@LN'
    if(@Gender is not null)
        Set @sql = @sql + ' and Gender=@Gen'
    if(@Salary is not null)
        Set @sql = @sql + ' and Salary=@Sal'

    Execute sp_executesql @sql,
    N'@FN nvarchar(50), @LN nvarchar(50), @Gen nvarchar(50), @sal int',
    @FN=@FirstName, @LN=@LastName, @Gen=@Gender, @Sal=@Salary

End
Go
```

