www.PragimTech.com

Pragim@PragimTech.com

SQL Server Tutorial

Part 141 - Prevent SQL Injection with Dynamic SQL

Venkat
PRAGIM Technologies
kudvenkat@gmail.com
http://csharp-video-tutorials.blogspot.com

In this session we will learn

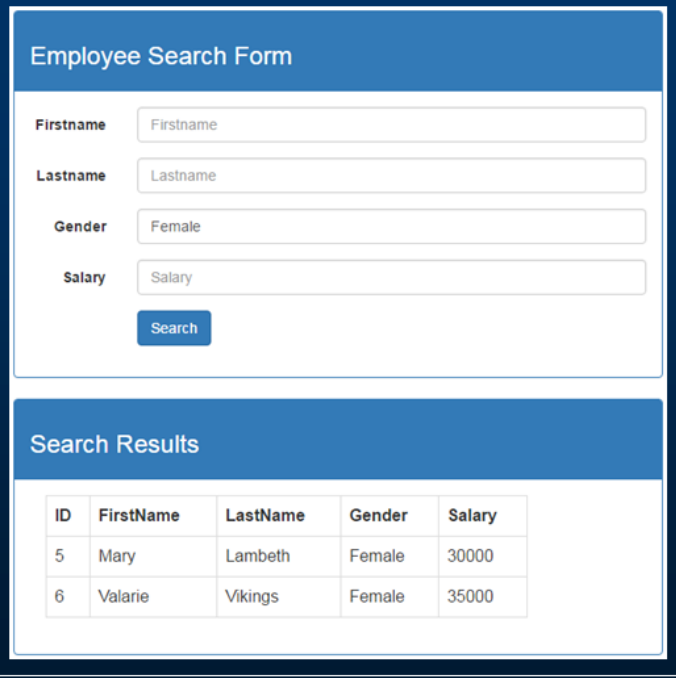
- How to prevent SQL injection when using dynamic SQL

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 138 - Dynamic SQL in SQL Server
Part 139 - Implement search web page using ASP .NET and Stored Procedure
Part 140 - Implement search web page using ASP.NET and Dynamic SQL

Prevent SQL Injection with Dynamic SQL

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



Prevent SQL Injection with Dynamic SQL

- Dynamic SQL provides great flexibility when implementing complicated logic with lot of permutations and combinations

- Always use parameters to build dynamic sql statements, which prevents SQL Injection

```
if (inputFirstname.Value.Trim() != "")
{
    sbCommand.Append(" AND FirstName=@FirstName");
    SqlParameter param = new SqlParameter("@FirstName", inputFirstname.Value);
    cmd.Parameters.Add(param);
}
```

- Never rely on concatenating user input values to build dynamic sql statements. It open doors for SQL Injection

```
if (inputFirstname.Value.Trim() != "")
{
    sbCommand.Append(" AND FirstName = '" + inputFirstname.Value + "'");
}
```

Prevent SQL Injection with Dynamic SQL

- Stored procedures are also prone to SQL Injection, if you are building dynamic sql statements in stored procedures by concatenating user input values instead of using parameters
  Example in next video

- Using parameters to build dynamic sql statements not only prevents SQL injection, but also increases performance by reusing the cached query plans.
  Example in a later video

Prevent SQL Injection with Dynamic SQL

```
protected void btnSearch_Click(object sender, EventArgs e)
{
    string strConnection = ConfigurationManager
        .ConnectionStrings["connectionStr"].ConnectionString;

    using (SqlConnection con = new SqlConnection(strConnection))
    {
        SqlCommand cmd = new SqlCommand();
        cmd.Connection = con;

        StringBuilder sbCommand = new StringBuilder("Select * from Employees where 1=1");

        if (inputFirstname.Value.Trim() != "")
        {
            sbCommand.Append(" AND FirstName = '" + inputFirstname.Value + "'");
        }

        if (inputLastname.Value.Trim() != "")
        {
            sbCommand.Append(" AND LastName = '" + inputLastname.Value + "'");
        }

        Other Parameters

        cmd.CommandText = sbCommand.ToString();
        cmd.CommandType = CommandType.Text;

        con.Open();
        SqlDataReader rdr = cmd.ExecuteReader();
        gvSearchResults.DataSource = rdr;
        gvSearchResults.DataBind();
    }
}
```

Additional Resources

PRAGIM Home Page:

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

https://twitter.com/kudvenkat