Security Misconfiguration

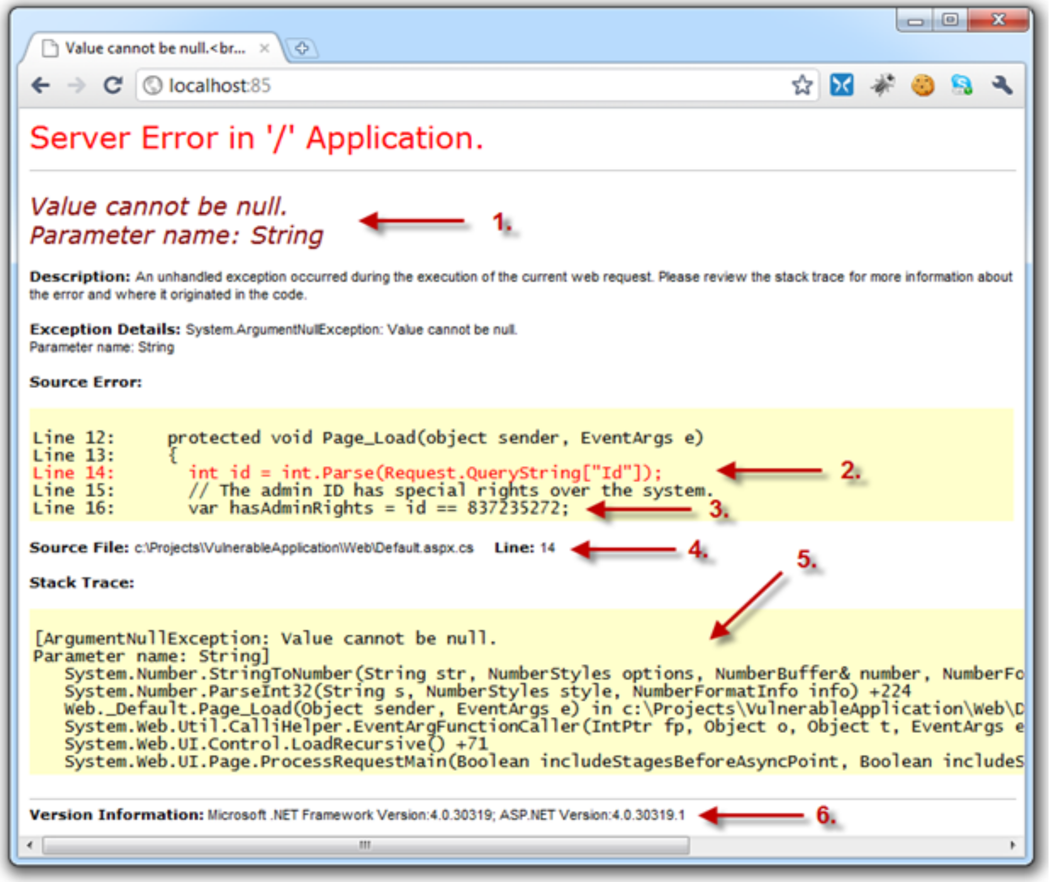
What is security misconfiguration?

- Security misconfiguration is very large concept
- It can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code.
- Leaving settings to default (accounts,sample applications)
- Running unnecessary servers or interpreters (ftp etc)
- Lack of updates being applied
- Server misconfigurations that allows directory listing and directory traversal attacks

- Administrative or debugging functions that are enabled or accessible
- Misconfigured SSL certificates and encryption settings
- Session cookie is not randomized enough
- Session cookie does not expire

Example

- Error messages



Server Error in '/' Application.

Value cannot be null.
Parameter name: String

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.ArgumentNullException: Value cannot be null.
Parameter name: String

Source Error:

```
Line 12:     protected void Page_Load(object sender, EventArgs e)
Line 13:     {
Line 14:       int id = int.Parse(Request.QueryString["Id"]);
Line 15:       // The admin ID has special rights over the system.
Line 16:       var hasAdminRights = id == 837235272;
```

Source File: c:\Projects\VulnerableApplication\Web\Default.aspx.cs   **Line:** 14

Stack Trace:

```
[ArgumentNullException: Value cannot be null.
Parameter name: String]
   System.Number.StringToNumber(String str, NumberStyles options, NumberBuffer& number, NumberFo
   System.Number.ParseInt32(String s, NumberStyles style, NumberFormatInfo info) +224
   Web._Default.Page_Load(Object sender, EventArgs e) in c:\Projects\VulnerableApplication\Web\D
   System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e
   System.Web.UI.Control.LoadRecursive() +71
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeS
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.1

How to test?

- Look for custom error messages.
- Look for debugger session being allowed.