





COMPLETE CODE

Web.config

<?xml version="1.0" encoding="utf-8"?>

<!--

For more information on how to configure your ASP.NET application, please visit

https://go.microsoft.com/fwlink/?LinkId=301880

-->

<configuration>

<appSettings>

<add key="webpages:Version" value="3.0.0.0" />

<add key="webpages:Enabled" value="false" />

<add key="ClientValidationEnabled" value="true" />

<add key="UnobtrusiveJavaScriptEnabled" value="true" />

</appSettings>

<system.web>

<compilation debug="true" targetFramework="4.7.2" />

<httpRuntime enableVersionHeader="false" />

</system.web>

<system.webServer>

<httpProtocol>

<customHeaders>

<remove name ="X-Powered-By"/>

<add name="Content-Security-Policy" value="default-src 'self';" />

</customHeaders>

</httpProtocol>

</system.webServer>

<runtime>

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

<dependentAssembly>

<assemblyIdentity name="Antlr3.Runtime" publicKeyToken="eb42632606e9261f" />

<bindingRedirect oldVersion="0.0.0.0-3.5.0.2" newVersion="3.5.0.2" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Microsoft.Web.Infrastructure" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="0.0.0.0-2.0.0.0" newVersion="2.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" />

<bindingRedirect oldVersion="0.0.0.0-13.0.0.0" newVersion="13.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.Optimization" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-1.1.0.0" newVersion="1.1.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="WebGrease" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-1.6.5135.21930" newVersion="1.6.5135.21930" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.Helpers" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.WebPages" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.Mvc" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-5.2.9.0" newVersion="5.2.9.0" />

</dependentAssembly>

</assemblyBinding>

</runtime>

<system.codedom>

<compilers>

<compiler language="c#;cs;csharp" extension=".cs" type="Microsoft.CodeDom.Providers.DotNetCompilerPlatform.CSharpCodeProvider, Microsoft.CodeDom.Providers.DotNetCompilerPlatform, Version=2.0.1.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" warningLevel="4" compilerOptions="/langversion:default /nowarn:1659;1699;1701" />

<compiler language="vb;vbs;visualbasic;vbscript" extension=".vb" type="Microsoft.CodeDom.Providers.DotNetCompilerPlatform.VBCodeProvider, Microsoft.CodeDom.Providers.DotNetCompilerPlatform, Version=2.0.1.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" warningLevel="4" compilerOptions="/langversion:default /nowarn:41008 /define:\_MYTYPE=\&quot;Web\&quot; /optionInfer+" />

</compilers>

</system.codedom>

</configuration>

GLOBAL.ASAX.CS

using System;

using System.Collections.Generic;

using System.Linq;

using System.Web;

using System.Web.Mvc;

using System.Web.Optimization;

using System.Web.Routing;

namespace appSecDay1

{

public class MvcApplication : System.Web.HttpApplication

{

protected void Application\_Start()

{

AreaRegistration.RegisterAllAreas();

FilterConfig.RegisterGlobalFilters(GlobalFilters.Filters);

RouteConfig.RegisterRoutes(RouteTable.Routes);

BundleConfig.RegisterBundles(BundleTable.Bundles);

MvcHandler.DisableMvcResponseHeader = true;

}

}

}

REFLECTION

I set up my ASP.NET MVC app to remove the X-AspNet-Version, X-AspNetMvc-Version, and X-Powered-By headers by tweaking the web.config file and adding some code changes. In web.config, I used the <customHeaders> section under <system.webServer> to strip those headers from the HTTP response, set enableVersionHeader="false" in <httpRuntime>, and added MvcHandler.DisableMvcResponseHeader = true; in Global.asax so the X-AspNetMvc-Version header would not appear at all. I also added a Content Security Policy (CSP) in the same <customHeaders> block: <add name="Content-Security-Policy" value="default-src 'self';" />. This restricts scripts, styles, and images so they can only load from the same origin, which helps prevent XSS attacks. I encountered a few problems, such as making sure there was only one <system.webServer> section to avoid conflicts, and I got an internal server error because I had a duplicate <httpRuntime targetFramework="4.7.2" /> line, which stopped the app from running until I removed it. After testing everything in the browser developer tools, I learned how these headers can reveal framework details and how adding a proper CSP can greatly improve security against client-side attacks.