**1. Attack Type: AutocompleteAttributeCheck**

**2. Attack Type: FormReSubmission**

Add the following code to your web.config, clear the browser’s cache and try again.

<system.webServer>

<httpProtocol>

<customHeaders>

<add name="Cache-Control" value="no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0, s-maxage=0" />

</customHeaders>

</httpProtocol>

</system.webServer>

Reference: https://stackoverflow.com/questions/68088802/replacing-cache-control-using-web-config-with-new-value

**3. ViewStatate Encryption**

<System.Web>

<pages viewStateEncryptionMode="Always">

</System.Web >

**5. DirectoryIndexing**

In Core Application

Startup.cs

Change

EnableDirectoryBrowsing = true

To

EnableDirectoryBrowsing = true

app.UseFileServer(new FileServerOptions

{

EnableDefaultFiles = true,

EnableDirectoryBrowsing = false,

// FileProvider = new PhysicalFileProvider(Path.Combine(Directory.GetCurrentDirectory(), @"tempFiles")),

// RequestPath = new PathString("/AROULETTE")

});

6. Attack Type: CSPHeaders

Solution:

In Web.config

<system.webServer>

<httpProtocol>

**<customHeaders>**

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

**</customHeaders>**

</httpProtocol>

</system.webServer>

Reference: <https://content-security-policy.com/>

Note: Not working. Stuck on login

7. Attack Type: SecureAttribute

In startup.cs

public void ConfigureServices(IServiceCollection services)

{

services.AddSession(options =>

{

options.Cookie.SecurePolicy = CookieSecurePolicy.Always;

});

}

Reference: <https://stackoverflow.com/questions/48216598/netcore-session-secure-cookie>

8. Hide Server version

Open the web.config file for Secret Server (located in the root directory for the website).  
Just after the <system.web> tag add this: <httpRuntime enableVersionHeader="false" />

<https://www.ibm.com/support/pages/disabling-iis-web-banner-and-other-iis-headers>

9. XSS attach

<system.webServer>

<httpProtocol>

<customHeaders>  
 <add name="X-XSS-Protection" value="1; mode=block" />  
 </customHeaders>

</httpProtocol>

</system.webServer>