* سامانه سمت
  1. آپدیت کتابخانه Jquery از نسخه 1.10.2 به 2.2.4
  2. غیر فعال کردن tls1.0 روی IIS:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

"DisabledByDefault"=dword:00000001

* 1. غیر فعال کردن 3DES cipher روی IIS:

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168]

"Enabled"=dword:00000000

* 1. عدم ارسال نسخه IIS به کلاینت:

$ Set-WebConfigurationProperty -pspath 'MACHINE/WEBROOT/APPHOST' -filter "system.webServer/security/requestFiltering" -name "removeServerHeader" -value "True"

یا

Web.config

<system.webServer>

<security>

<requestFiltering removeServerHeader="true" />

</security>

</system.webServer>

* 1. عدم ارسال نسخه ASP.NET به کلاینت:

Web.config

<system.webServer>

<httpProtocol>

<customHeaders>

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

<remove name="X-AspNet-Version" />

</customHeaders>

</httpProtocol>

</system.webServer>

<system.web>

<httpRuntime enableVersionHeader="false" />

</system.web>

* 1. اضافه کردن هدر X-Frame-Options

Web.config

<system.webServer>

<httpProtocol>

<customHeaders>

<add name="X-Frame-Options" value="SAMEORIGIN" />

</customHeaders>

</httpProtocol>

</system.webServer>

یا

Global.asax

protected void Application\_BeginRequest()

{

Response.AddHeader("X-Frame-Options", "SAMEORIGIN");

}

* 1. اضافه کردن هدر Content-Security-Policy

Web.config

<system.webServer>

<httpProtocol>

<customHeaders>

<add name="Content-Security-Policy" value="default-src 'self' www.gravatar.com fonts.googleapis.com fonts.gstatic.com cdn.goftino.com cdnjs.cloudflare.com ws.goftino.com www.goftino.com wss: 'unsafe-eval';script-src 'self' 'unsafe-inline' www.gravatar.com fonts.googleapis.com fonts.gstatic.com cdn.goftino.com cdnjs.cloudflare.com ws.goftino.com www.goftino.com wss: 'unsafe-eval';style-src 'self' 'unsafe-inline' www.gravatar.com fonts.googleapis.com fonts.gstatic.com cdn.goftino.com cdnjs.cloudflare.com ws.goftino.com www.goftino.com wss: 'unsafe-eval';img-src 'self' www.gravatar.com fonts.googleapis.com fonts.gstatic.com cdn.goftino.com cdnjs.cloudflare.com ws.goftino.com www.goftino.com wss: 'unsafe-eval';font-src 'self' www.gravatar.com fonts.googleapis.com fonts.gstatic.com cdn.goftino.com cdnjs.cloudflare.com ws.goftino.com www.goftino.com wss: 'unsafe-eval'" />

</customHeaders>

</httpProtocol>

</system.webServer>

* 1. امنیت Cookie ها

Web.config

<system.web>

<httpCookies httpOnlyCookies="true" requireSSL="true" />

</system.web>

یا

Global.asax

protected void Application\_EndRequest()

{

if (Response.Cookies.Count > 0)

{

foreach (string s in Response.Cookies.AllKeys)

{

if (s == FormsAuthentication.FormsCookieName || "asp.net\_sessionid".Equals(s, StringComparison.InvariantCultureIgnoreCase))

{

Response.Cookies[s].HttpOnly = true;

Response.Cookies[s].Secure = true;

}

}

}

}