Securing Web RA

To secure Web RA recommendations of OWASP are implemented.

1. Content Security Policy (CSP) Not Implemented Implemented content security policy by adding these in config file

<add name="Content-Security-Policy" value="object-src 'none'; default-src 'self' https://client.go-sign-desktop.com:8782/gosign-desktop https://netdna.bootstrapcdn.com; connect-src 'self' https://client.go-sign-desktop.com:8782 ; child-src 'self' https://www.google.com/; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/; style-src 'self' 'unsafe-inline'; img-src 'self' * data: blob:;" />

2. Version Disclosure

Add following tag inside rewrite tags:
<outboundRules>

<rule name="Remove Server header">
<match serverVariable="RESPONSE_Server" pattern=".+" />
<action type="Rewrite" value="" />
</rule>

</outboundRules>

3. Missing X-Frame-Options Header

Add following header in config file:
<add name="X-Frame-Options" value="DENY" />

4. Missing Invalid CYPHER

To fix this issue enable CYPHER from windows register. For more information follow this link

https://support.microsoft.com/en-ie/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc

5. Request Max-Length Issue

To fix max length issue add following tag in web.config in <system.webServer> tag:

<security>
<requestFiltering>
<requestLimits maxQueryString="8192" />
</requestFiltering>
</security>

6. Cookie not marked as HttpOnly

All cookies in Web RA are marked as secure except cookie used in anti-forgery token validation. To understand anti-forgery token validation, follow below link.

http://help.ascertia.com/webRA/#.insecure_cookie