Summary

This article provides information on how to Protect your Website from ClickJacking.

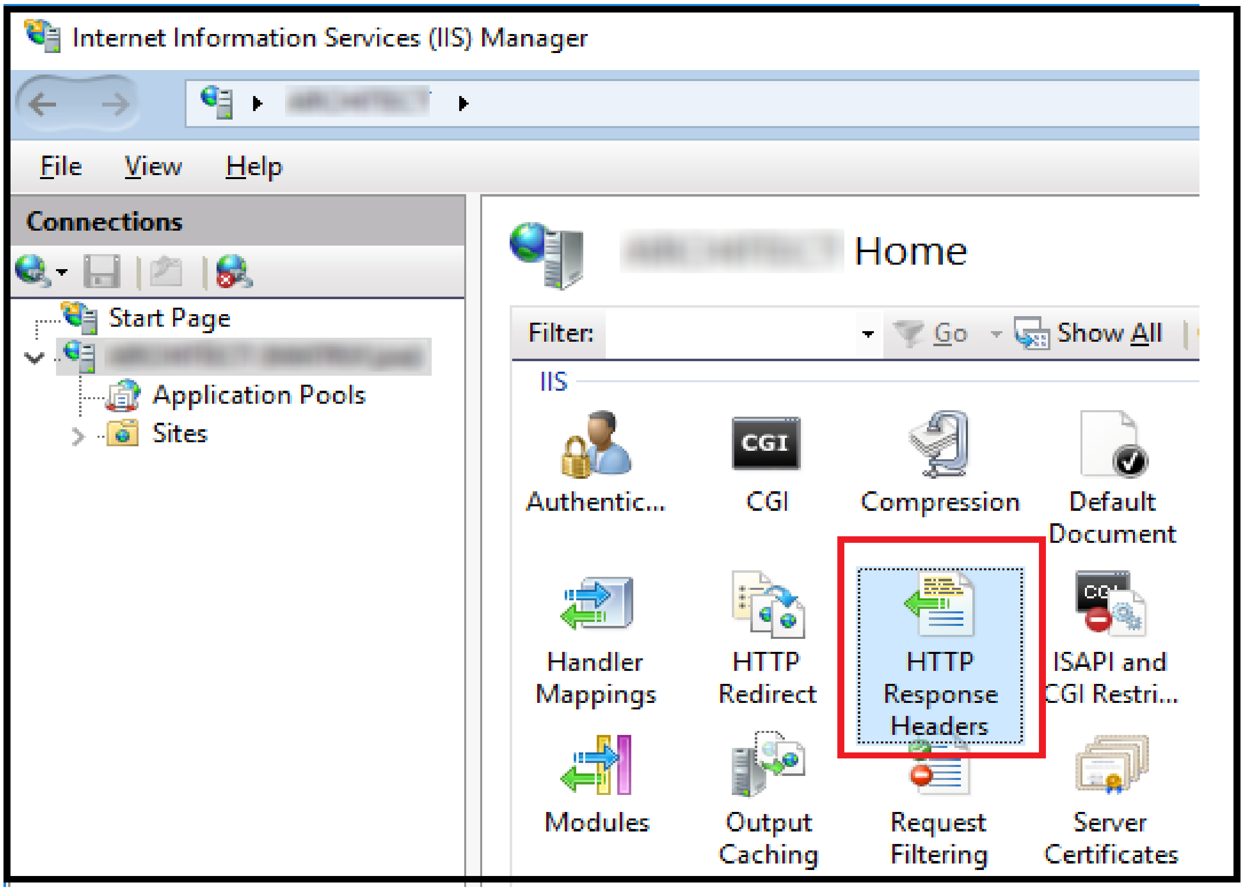
Applies To

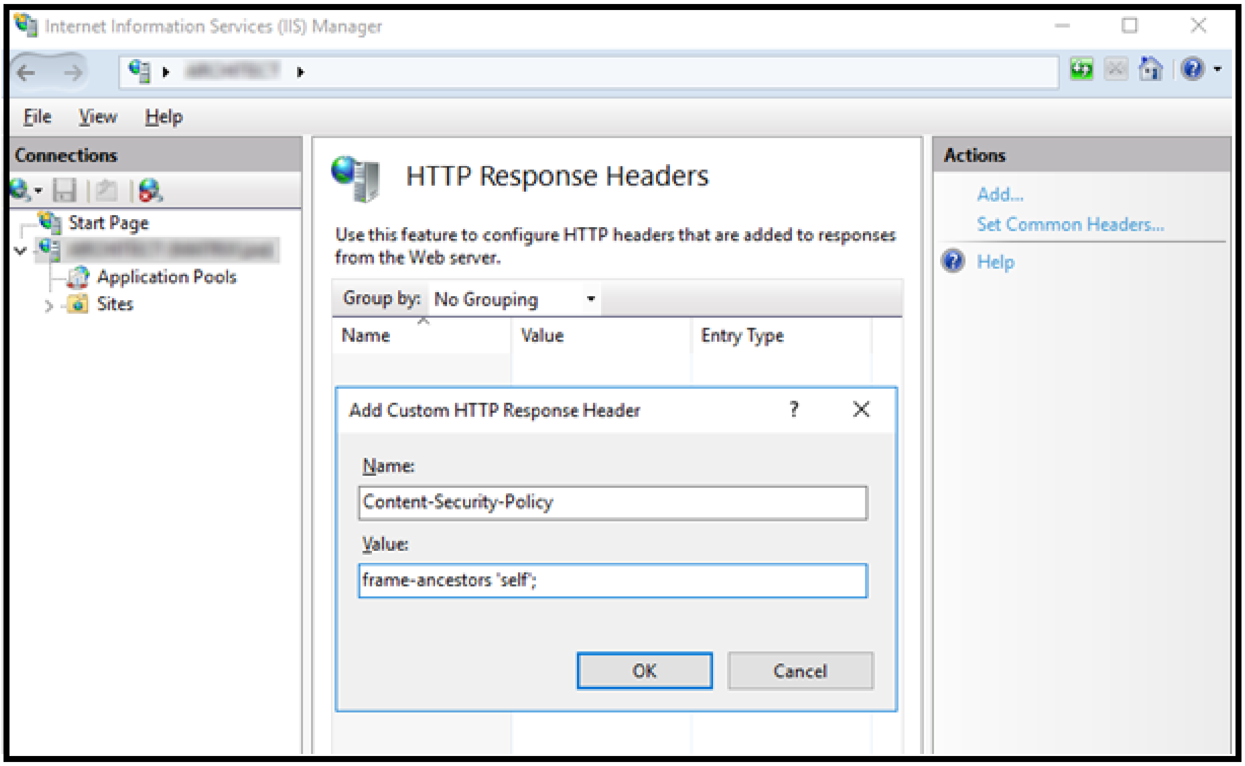
This article applies to MachPanel v6 and above.

Steps and Procedure

To protect website from clickjacking, it is required to append a **Content Security Policy** header to the HTTP response with frame-ancestors directive sent by web server.

Custom header can be added to a website in IIS as shown below.





Use this feature to configure HTTP headers that are added to responses from the Web server.

Name: Content-Security-Policy

Value: frame-ancestors 'self';

Inside ‘Value’ for ‘frame-ancestors’ multiple values can be specified separated by white space like below

Frame-ancestors ‘self’ ‘https://*.jquery.com’ ‘https://www.example.com’ ‘https://*.providesupprot.com’;

For Machpanel add as below

frame-ancestors ‘self’ ‘https://*.duosecurity.com’ ‘https://app.powerbi.com’

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Secu

https://content-security-policy.com/

https://portswigger.net/web-security/cross-site-scripting/content-security-po

MachPanel Knowledgebase
https://kb.machsol.com/Knowledgebase/55646/Protecting-Your-Website-From-Cli...