Cómo personalizar la política de seguridad de contenido para Webbridge en CMS

Contenido

Introducción

Este documento describe el procedimiento para configurar y habilitar una política de seguridad de contenido personalizada para webbridge en Cisco Meeting Server (CMS) versión 3.2.

Colaborado por Octavio Miralrio, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- configuración general de CMS
- Protocolo de transferencia de hipertexto seguro (HTTPS)
- Lenguaje de marcado de hipertexto (HTML)
- Servidor Web

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CMS versión 3.2
- Windows Web Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuraciones

Desde la versión 3.2 y posteriores de CMS, los administradores de CMS pueden incrustar la aplicación web con otro sitio web. Esto significa que la aplicación web está integrada en otra página web.

> **Nota:** La aplicación web puede ejecutar medios cuando se incrusta en los exploradores que requieren HTTPS y no en exploradores con HTTP.

Paso 1. Abra la interfaz de línea de comandos (CLI) del CMS y ejecute el siguiente comando:

```
webbridge3 https frame-ancestors
```

El parámetro **<frame-ancestors space-Separated string>** debe reemplazarse por la trama Uniform Resource Locator (URL) donde se incrusta la aplicación web, se admiten comodines, por ejemplo **https://*.octavio.lab** como se muestra en la imagen:

```
cms01> webbridge3
Enabled                                 : true
HTTPS listening ports and interfaces    : a:443
HTTPS Key file                          : wbridge3.key
HTTPS Full chain certificate file       : wbridge3bundle.cer
HTTPS Frame-Ancestors                   : https://*.octavio.lab
HTTP redirect                           : Enabled, Port:80
C2W listening ports and interfaces      : a:9999
C2W Key file                            : wbridge3.key
C2W Full chain certificate file         : wbridge3bundle.cer
C2W Trust bundle                        : root.cer
Beta options                            : none
cms01>
cms01>
```

La aplicación web no verifica el contenido del encabezado además de que los caracteres son válidos. Los administradores deben asegurarse de que el encabezado de la directiva de seguridad de contenido contiene cadenas válidas. El tamaño de la cadena está limitado a 1000 caracteres y los caracteres permitidos son **a-z A-Z 0-9_ . /: ? # [ ] @ $ & ' ( ) * + - = ~ %**.

Paso 2. Configure el iFrame incrustado en una página web.

El paso siguiente es incrustar el elemento iframe en una página web. La etiqueta **<iframe>** reconoce el elemento iframe en un documento HTML. Para admitir medios, se requieren los siguientes atributos:

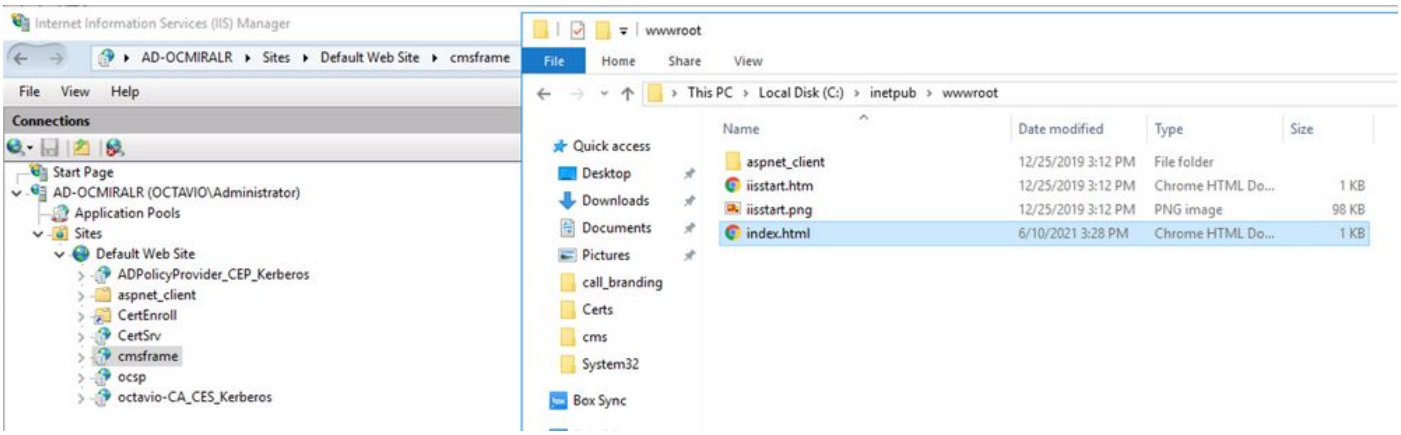
> **Nota:** Se necesita HTTPS para ejecutar medios de aplicación web. También se pueden incluir otros atributos que son soportados por iframe como **height** y **width**.

La creación del contenido de iFrame corresponde al administrador de la página web, se puede personalizar según sea necesario; el siguiente es un ejemplo de un iFrame creado con fines de demostración:

```
This is the title of the Content Securiity Policy

Welcome to the CMS Content Security Policy Demostration.

All this text is not part of the webbridge itself.

Below you will see the enbedded webapp page, https://join.octavio.lab.
```

Paso 3. Implementación en servidor web.

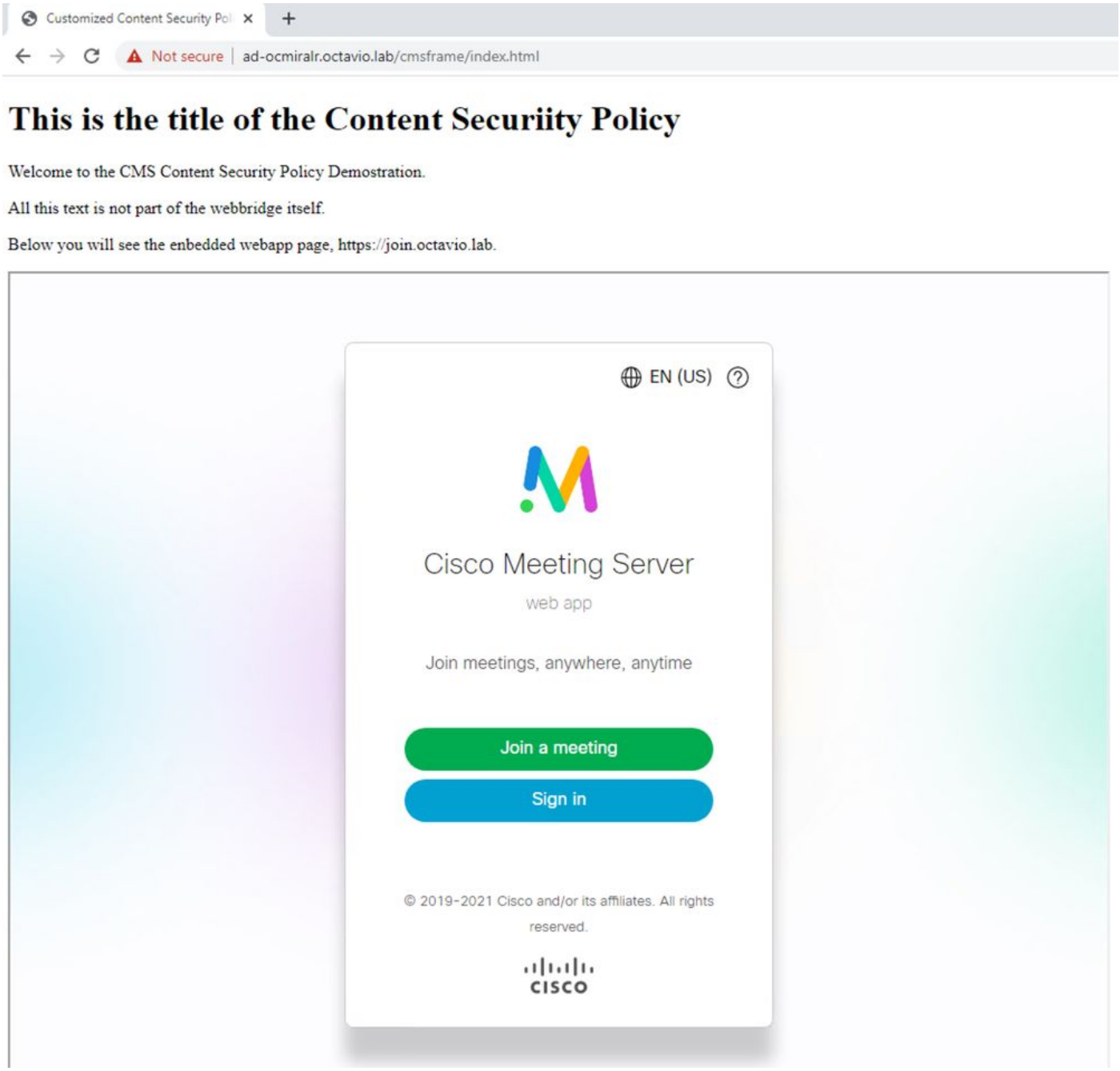
Una vez que el documento HTML tiene un marco de trabajo integrado, la página se debe cargar en un servidor web. A los efectos de este documento, el archivo HTML se denomina **index.html** y se almacena en un servidor Web de Windows, como se muestra en la imagen:



> **Nota:** Las configuraciones adicionales del servidor web y las opciones disponibles para la página web están fuera del alcance de este documento. El administrador del servidor web debe completar la implementación de la página web.

Verificación

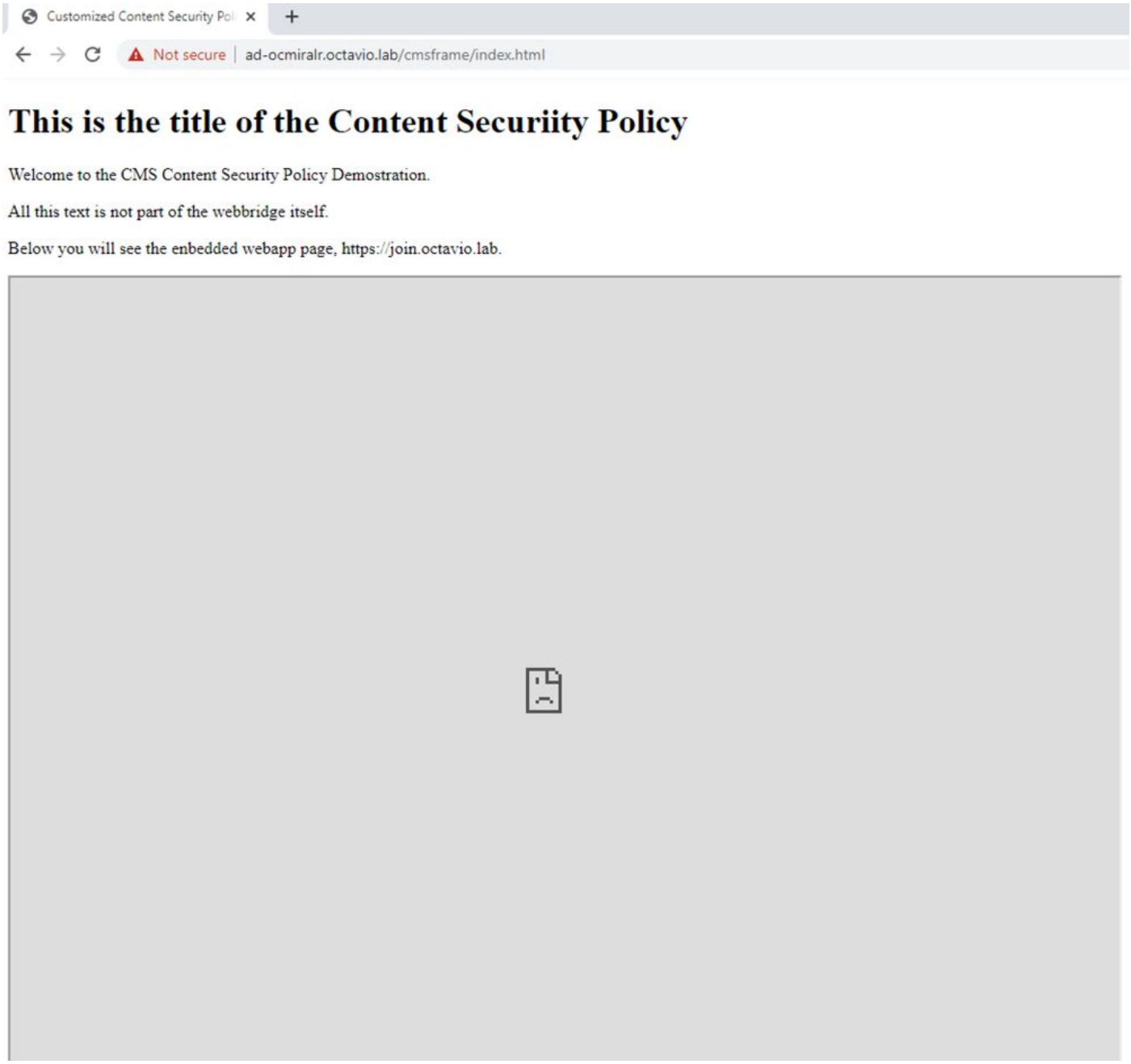
Para validar que la configuración funciona correctamente, abra un navegador web y navegue a la página web donde se configuró el iFrame, para este documento es https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Acceda a cualquier reunión disponible en CMS y valide que el audio y el vídeo funcionan correctamente.

Troubleshoot

1. Se muestra la página web pero la aplicación web no está cargada.



Para resolver este tipo de problema, siga los siguientes pasos:

Paso 1. Abra la CLI del CMS.

Paso 2. Ejecute el siguiente comando: **webbridge**.

Paso 3. Desde la configuración de webbridge, asegúrese de que los **Frame-Ancestors** sean correctos, debe ser el **iframe src** configurado en la página web creada.

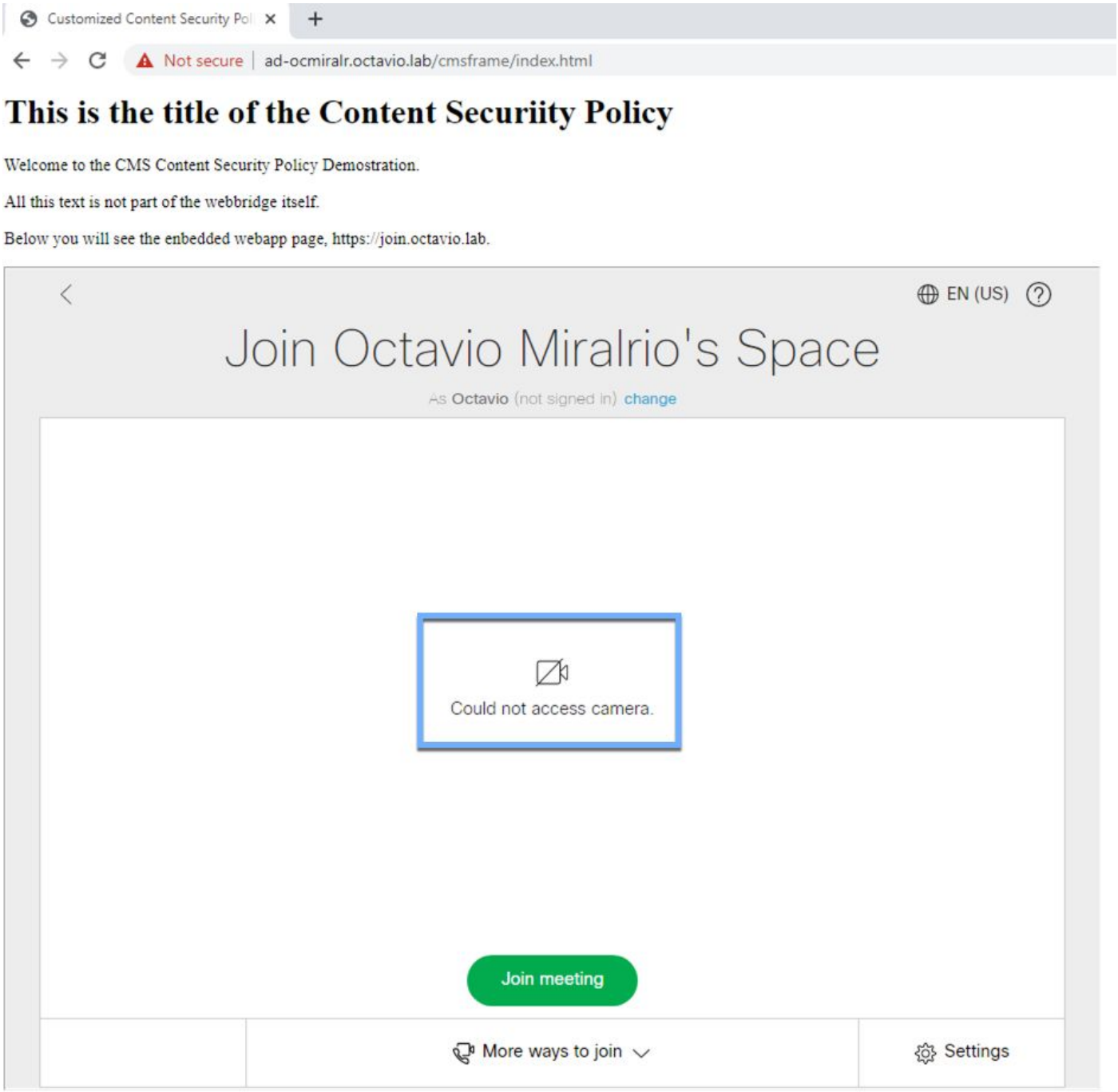
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Frame-Ancestors                      : https://*.cms.lab
C2W listening ports and interfaces         : a:9999
C2W Key file                               : wbridge3.key
C2W Full chain certificate file            : wbridge3bundle.cer
C2W Trust bundle                           : root.cer
Beta options                               : none
cms01>
```

En este caso, los Frame-Ancestors configurados en webbridge son diferentes de los configurados en la página web, como se muestra en la imagen:

```
index.html
<!DOCTYPE html>
<html lang="en">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<html>
<head>
<title>Customized Content Security Policy</title>
</head>
<body>
<h1>This is the title of the Content Securiity Policy</h1>
<p>Welcome to the CMS Content Security Policy Demostration.</p>
<p>All this text is not part of the webbridge itself.</p>
page, https://join.octavio.lab.</p>
<iframe src="https://join.octavio.lab" width="1024" height="768" title="CMS 3.2 Customizable CSP" allowusermedia allow="microphone; camera; display-capture"></iframe>
</body>
</html>
```

Paso 4. Corrija el valor de Frame-Ancestor en la configuración de webbridge o en el código de la página web según sea necesario.

2. La aplicación web está cargada pero no puede acceder a la cámara o al micrófono.



Este problema se debe a que el iframe no está configurado correctamente. Para soportar audio y video, el iframe debe incluir los atributos **allowusermedia allow="micrófono; cámara; display-capture"**.

Para resolver este problema, siga los siguientes pasos:

Paso 1. Abra el servidor web y busque el archivo HTML de la página principal.

Paso 2. Utilice un editor de texto para editar el archivo HTML.

Paso 3. Agregue los atributos de medios a la trama, como se muestra en el código siguiente: