Content Security Policy aanpassen voor Webbridge op CMS

Inhoud

Inleiding

Dit document beschrijft de procedure om een aangepast content security beleid voor webbridge te configureren en in te schakelen op versie 3.2 van Cisco Meeting Server (CMS).

Bijgedragen door Octavio Miralrio, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco adviseert dat u kennis over deze onderwerpen hebt:

- CMS-algemene configuratie
- Hypertext Transfer Protocol Secure (HTTPS)
- Hypertext Markup Language (HTML)
- Webserver

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CMS versie 3.2
- Windows-webserver 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Configuraties

Met betrekking tot CMS versie 3.2 en nieuwer kunnen de CMS-beheerders de webapp insluiten met een andere website. Dat betekent dat de web app ingebed is in een andere webpagina.

> **Opmerking:** Web app kan media uitvoeren wanneer er HTTPS nodig is en niet op browsers met HTTP.

Stap 1. Open de Opdracht Line Interface (CLI) van CMS en voer de volgende opdracht uit:

```
webbridge3 https frame-ancestors
```

De **<frame-voorouders een spatie-gescheiden string>** moet worden vervangen door de frame Uniform Resource Locator (URL) waar de web app ingesloten is, worden wildcards ondersteund, bijvoorbeeld **https://*.octavio.lab** zoals in de afbeelding:

```
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>
```

De web app controleert de header niet behalve dat de tekens geldig zijn. De beheerders moeten ervoor zorgen dat de kop van het inhoudsbeveiligingsbeleid geldige strings bevat. De string size is beperkt tot 1000 karakters en toegestane tekens zijn **a-z A-Z 0-9_. / : ? # [ ] @ ! $ & ' ( ) * + - = ~ %**.

Stap 2. Het ingesloten frame binnen een webpagina configureren.

De volgende stap is het insluiten van een frame-element in een webpagina. Het frame-element wordt herkend met de tag **<iframe>** in een HTML-document. Om media te ondersteunen zijn de volgende eigenschappen vereist:

> **Opmerking:** HTTPS moet een webapp-media gebruiken. Andere eigenschappen die door een kader zoals **hoogte** en **breedte** worden ondersteund kunnen ook worden opgenomen.

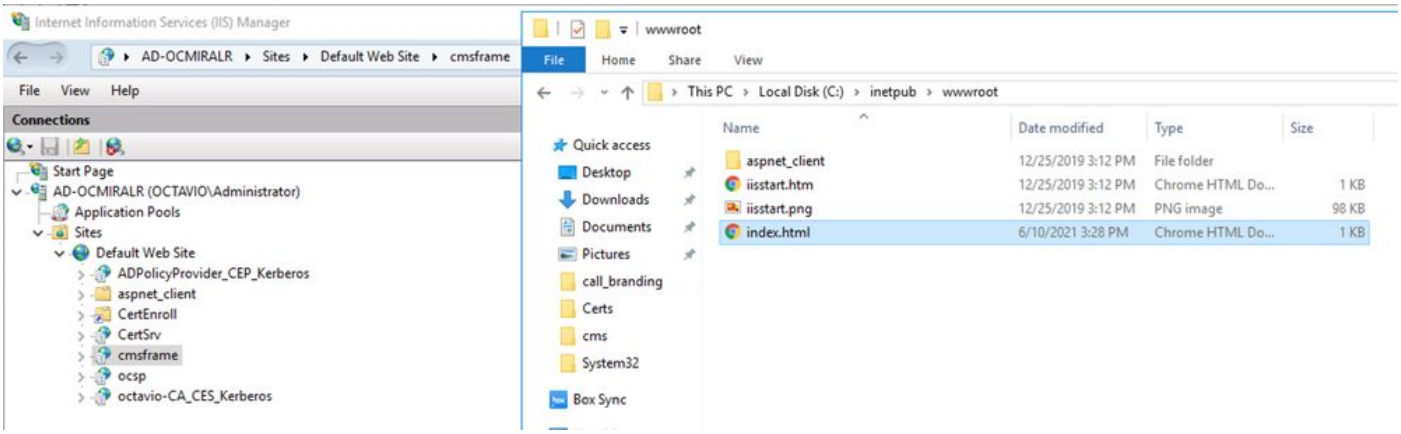
De iFrame-inhoud wordt gemaakt door de beheerder van de webpagina. Indien nodig kan de

inhoud aangepast worden, is het volgende voorbeeld van een iFrame gemaakt voor demonstratiedoeleinden:

```
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.
```

Stap 3. Stel de informatie op de webserver in.

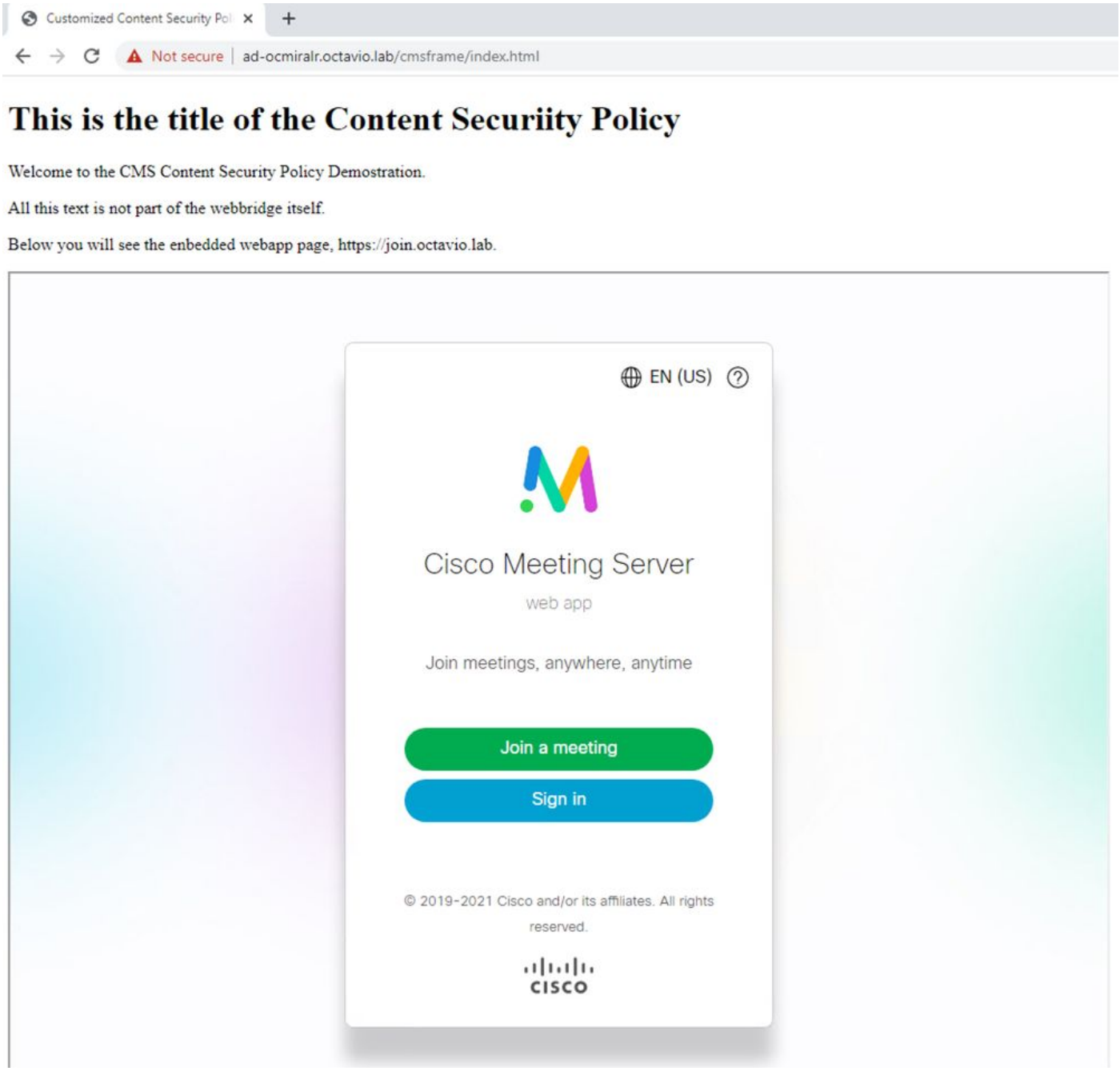
Zodra het HTML-document een ingesloten frame heeft, moet de pagina op een webserver worden geladen. In dit document wordt het HTML-bestand **index.html** genoemd en opgeslagen op een Windows-webserver, zoals in de afbeelding:



> **Opmerking:** De extra configuraties van de webserver en de opties voor de webpagina zijn buiten het bereik van dit document. De beheerder van de webserver moet de plaatsing van de webpagina voltooien.

Verifiëren

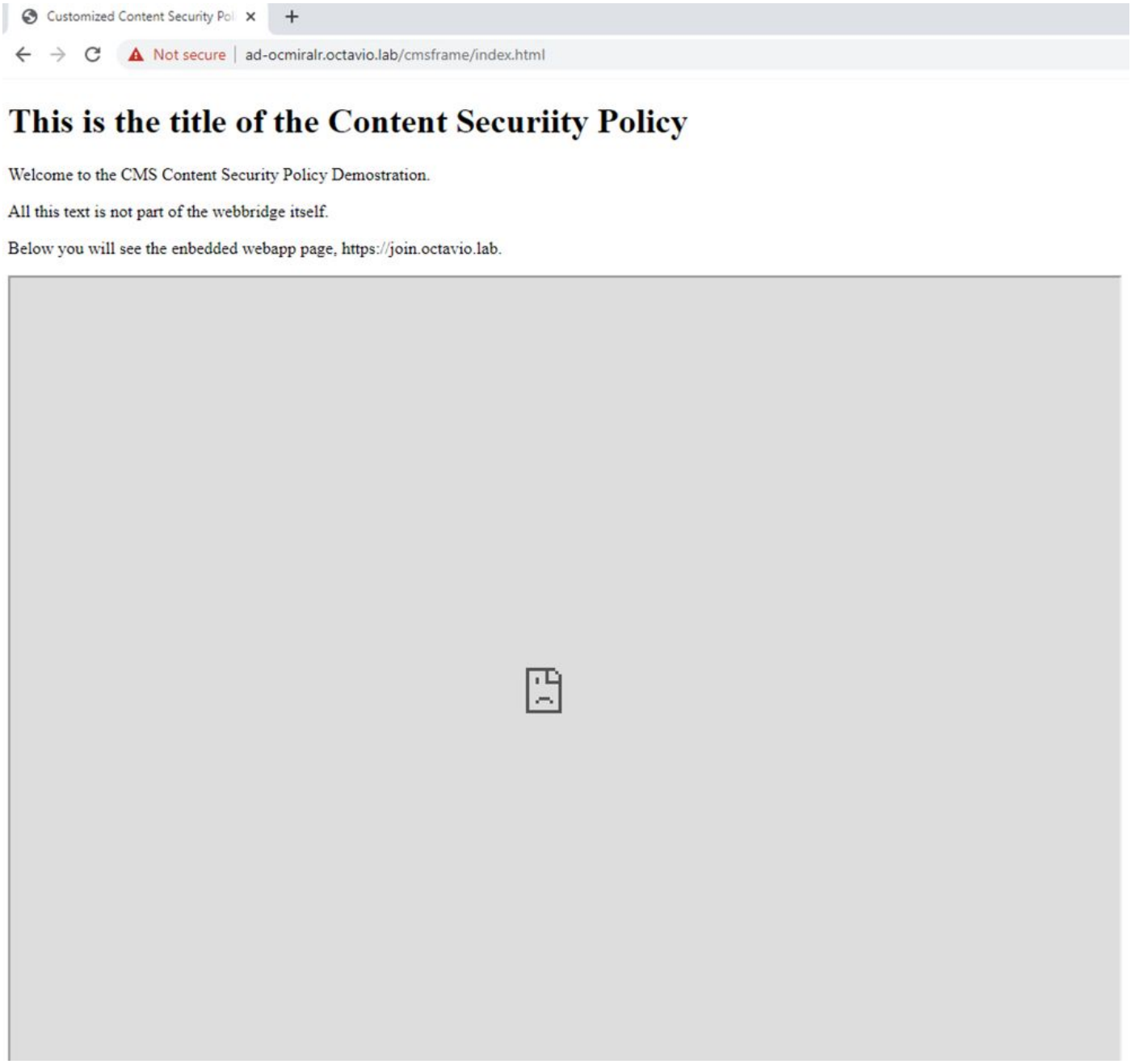
Om de configuratie correct te laten werken, opent u een webbrowser en navigeer naar de webpagina waar iFrame is geconfigureerd, voor dit document is het https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Toegang tot elke beschikbare vergadering op het CMS en validatie van audio en video werkt prima.

Problemen oplossen

1. De webpagina is afgebeeld, maar de webapp is niet geladen.



Om dit soort problemen op te lossen, volgt u de volgende stappen:

Stap 1. Open de CLI van het CMS.

Stap 2. Start de volgende opdracht: **Webbridge**.

Stap 3. Vanuit de configuratie van de webbridge dient te worden gewaarborgd dat de **Frame-Ancestors** correct zijn, dat wil zeggen dat het de **iframe src** is die op de gemaakte webpagina is geconfigureerd.

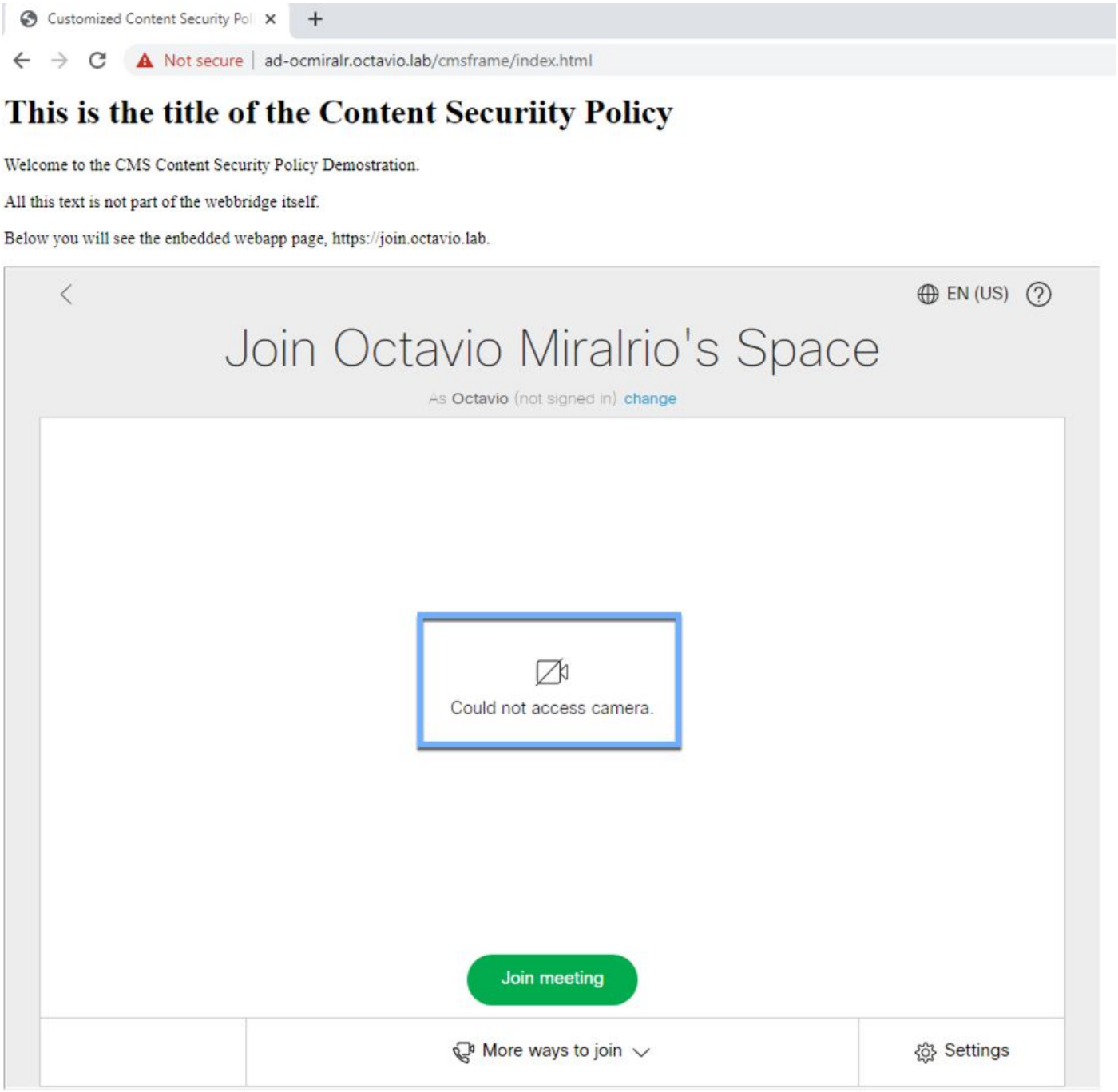
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Frame-Ancestors                      : https://*.cms.lab
C2W listening ports and interfaces         : a:9999
C2W Key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

In dit geval verschillen de geconfigureerde Frame-Ancestors op webbridge van het type dat op de webpagina is geconfigureerd, zoals in de afbeelding:

```
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>
```

Stap 4. Correcte de waarde van de reeds bestaande Frame-tumor in de configuratie van de webbrug of in de code van de webpagina naar wens.

2. De web app is geladen, maar heeft geen toegang tot camera of microfoon.



Deze kwestie wordt veroorzaakt omdat het frame niet correct is geconfigureerd, Om audio en video te ondersteunen moet het frame de eigenschappen **allowuser media allow="microphone** bevatten**; camera; weergave"**.

U volgt de volgende stappen om dit probleem op te lossen:

Stap 1. Open de webserver en bevestig het hoofdpagina-HTML-bestand.

Stap 2. Gebruik een teksteditor om het HTML-bestand te bewerken.

Stap 3. Voeg de mediaeigenschappen aan het frame toe, zoals in de volgende code: