Comment personnaliser la stratégie de sécurité de contenu pour Webbridge sur CMS

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Configurations](#)
[Vérification](#)
[Dépannage](#)

Introduction

Ce document décrit la procédure à suivre pour configurer et activer une stratégie de sécurité de contenu personnalisée pour webbridge sur Cisco Meeting Server (CMS) version 3.2.

Contribué par Octavio Miralrio, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez ces sujets :

- Configuration générale CMS
- Protocole HTTPS (Hypertext Transfer Protocol Secure)
- HTML (Hypertext Markup Language)
- Serveur Web

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMS version 3.2
- Serveur Web Windows 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Configurations

Pour les versions 3.2 et ultérieures de CMS, les administrateurs CMS peuvent incorporer l'application Web à un autre site Web. Cela signifie que l'application Web est intégrée à une autre page Web.

> **Note**: L'application Web peut exécuter un support lorsqu'il est incorporé dans les navigateurs qui nécessitent HTTPS et non sur les navigateurs avec HTTP.

Étape 1. Ouvrez l'interface de ligne de commande (CLI) du CMS et exécutez la commande suivante :

```
webbridge3 https frame-ancestors
```

Le paramètre **<frame-ancestors space-Separated string>** doit être remplacé par l'URL (Uniform Resource Locator) de la trame dans laquelle l'application Web est incorporée, les caractères génériques sont pris en charge, par exemple **https://*.octavio.lab** comme l'illustre l'image :

```
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>
```

L'application Web ne vérifie pas le contenu de l'en-tête, à part que les caractères sont valides. Les administrateurs doivent s'assurer que l'en-tête de stratégie de sécurité du contenu contient des chaînes valides. La taille de la chaîne est limitée à 1 000 caractères et les caractères autorisés sont **a-z A-Z 0-9_ . / : ? # [ ] @ ! $ & ' ( ) * + - = ~ %**.

Étape 2. Configurez l'image intégrée dans une page Web.

L'étape suivante consiste à incorporer l'élément iframe dans une page Web. L'élément iframe est reconnu par la balise **<iframe>** dans un document HTML. Pour prendre en charge le support, les attributs suivants sont requis :

> **Note**: HTTPS est requis pour exécuter le média webapp. D'autres attributs pris en charge par iframe, tels que **la hauteur** et **la largeur**, peuvent également être inclus.

La création du contenu iFrame dépend de l'administrateur de la page Web, il peut être personnalisé selon les besoins, le suivant est un exemple d'iFrame créé à des fins de démonstration :

This is the title of the Content Securiity Policy

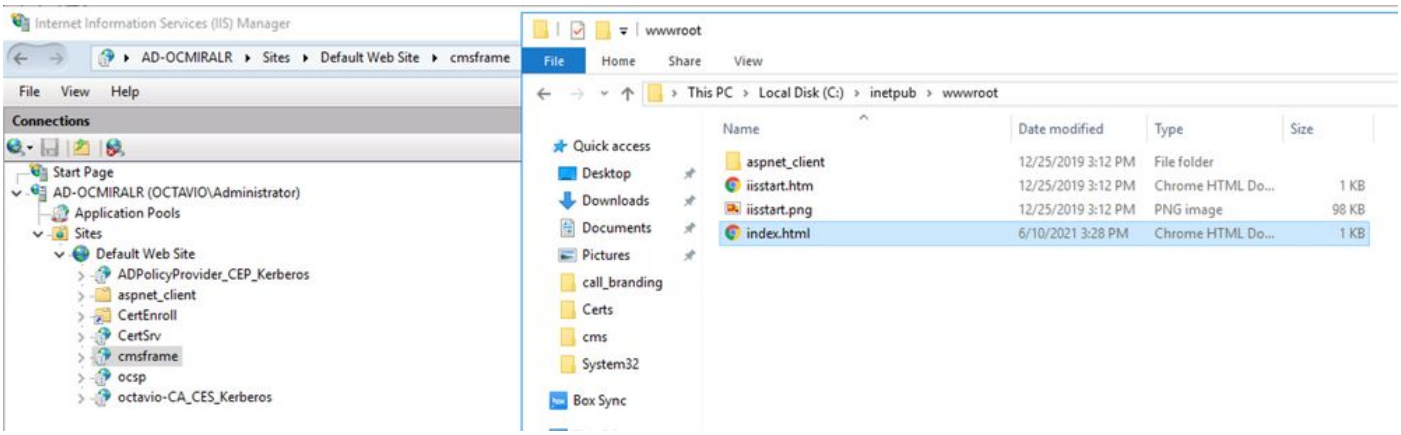
```
Welcome to the CMS Content Security Policy Demostration.

All this text is not part of the webbridge itself.

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

Étape 3. Déployer sur le serveur Web.

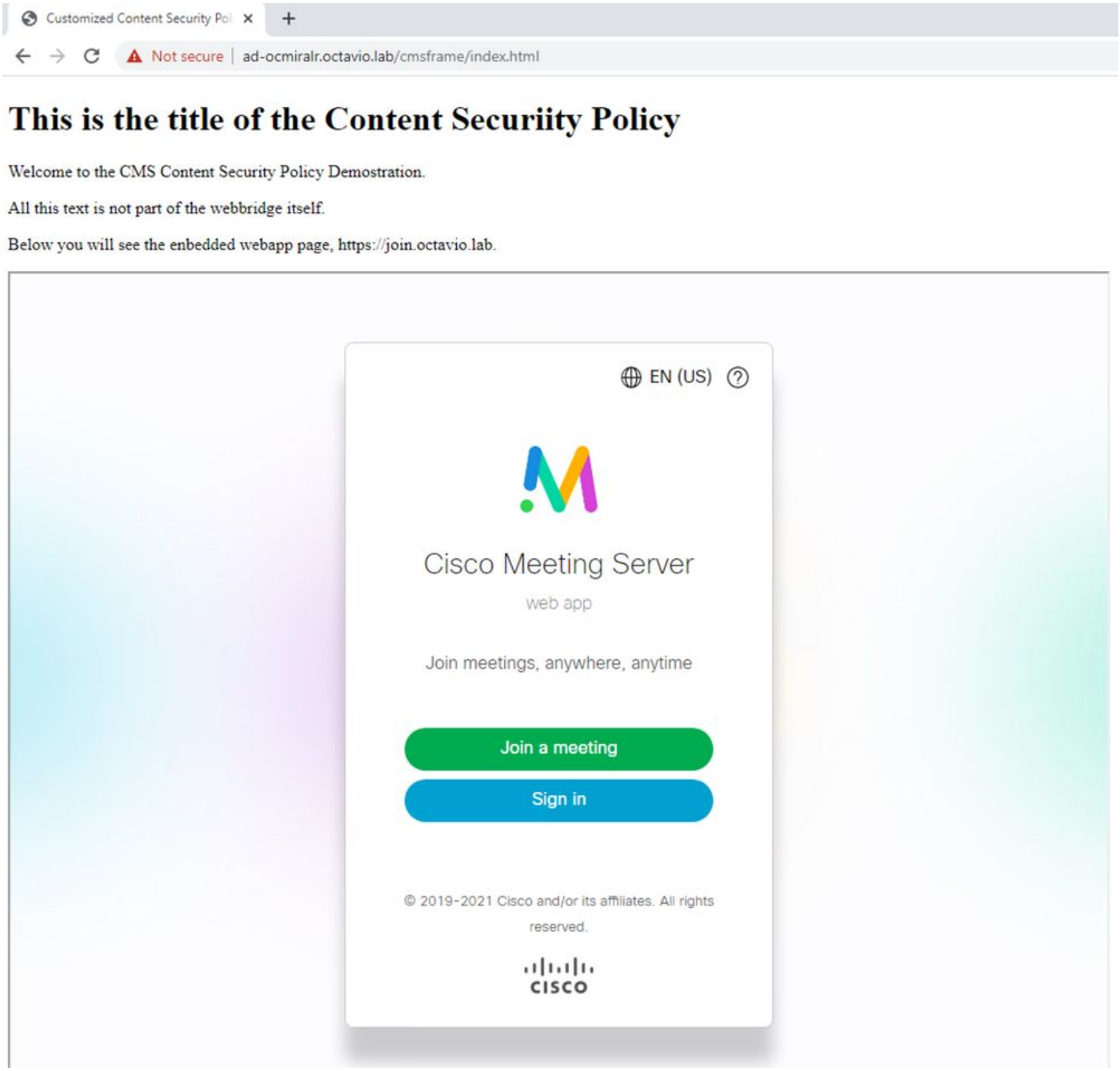
Une fois que le document HTML a une image incorporée, la page doit être chargée sur un serveur Web. Pour les besoins de ce document, le fichier HTML est appelé **index.html** et stocké sur un serveur Web Windows, comme illustré dans l'image :



> **Note**: Les configurations supplémentaires du serveur Web et les options disponibles pour la page Web ne sont pas incluses dans ce document. L'administrateur du serveur Web doit terminer le déploiement de la page Web.

Vérification

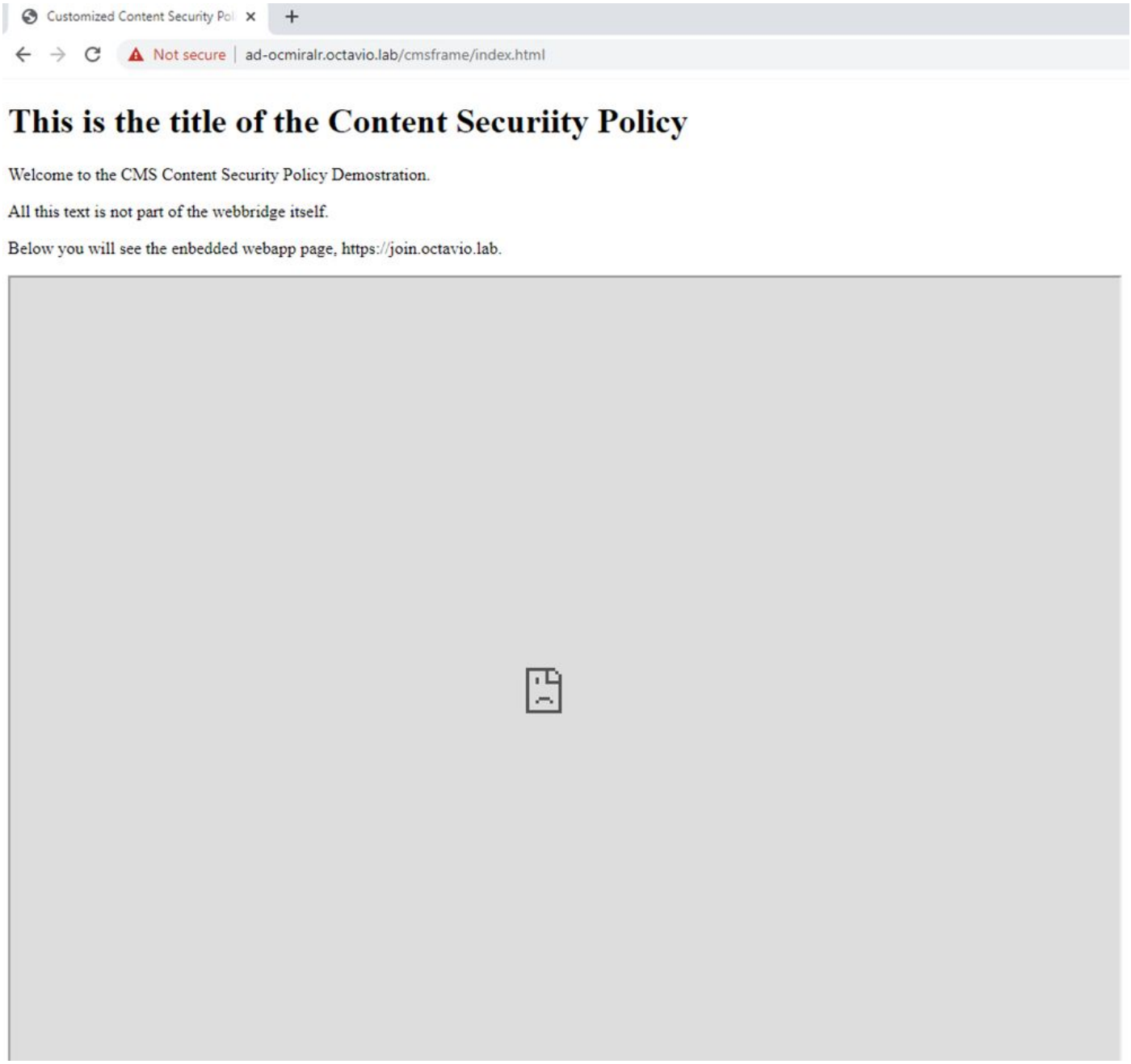
Afin de vérifier que la configuration fonctionne correctement, ouvrez un navigateur Web et accédez à la page Web sur laquelle l'iFrame a été configuré. Pour ce document, il s'agit de https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Accédez à toutes les téléconférences disponibles sur le CMS et validez le fonctionnement audio et vidéo.

Dépannage

1. La page Web s'affiche mais l'application Web n'est pas chargée.



Pour résoudre ce type de problème, procédez comme suit :

Étape 1. Ouvrez la CLI du CMS.

Étape 2. Exécutez la commande suivante : **webbridge**.

Étape 3. À partir de la configuration de webbridge, assurez-vous que **Frame-Ancestors** est correct, il doit s'agir de l'**iframe src** configuré sur la page Web créée.

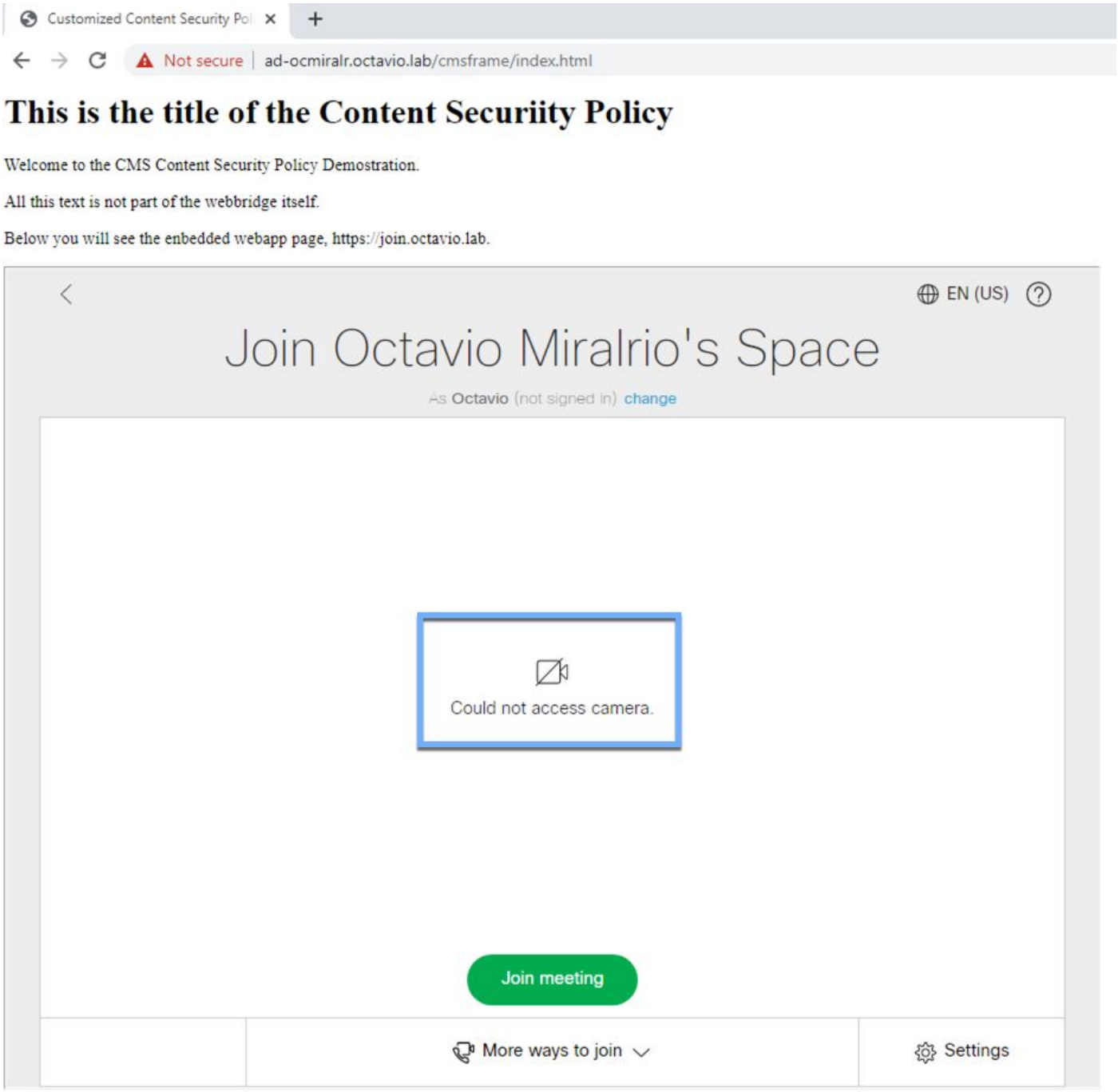
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Frame-Ancestors                      : https://*.cms.lab
C2W listening ports and interfaces         : a:9999
C2W Key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

Dans ce cas, les Frame-Ancestors configurés sur webbridge sont différents de ceux configurés sur la page Web, comme l'illustre l'image :

```
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>
```

Étape 4. Corrigez la valeur Frame-Ancestor sur la configuration du pont Web ou dans le code de page Web, si nécessaire.

2. L'application Web est chargée mais ne peut pas accéder à la caméra ou au microphone.



Ce problème est dû au fait que la trame n'est pas configurée correctement. Pour prendre en charge l'audio et la vidéo, la trame doit inclure les attributs **allowusermedia allow=« microphone; caméra ; display-capture »**.

Pour résoudre ce problème, procédez comme suit :

Étape 1. Ouvrez le serveur Web et localisez le fichier HTML de la page principale.

Étape 2. Utilisez un éditeur de texte pour modifier le fichier HTML.

Étape 3. Ajoutez les attributs de média à la trame, comme indiqué dans le code suivant :