Personnalisation de la stratégie de sécurité du contenu pour Webbridge sur CMS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Configurations

Vérifier

Dépannage

Introduction

Ce document décrit la procédure de configuration et d'activation d'une stratégie de sécurité de contenu personnalisée pour webbridge sur Cisco Meeting Server (CMS) version 3.2.

Contribution d'Octavio Miralrio, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

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

Composants utilisés

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.

Configurer

Configurations

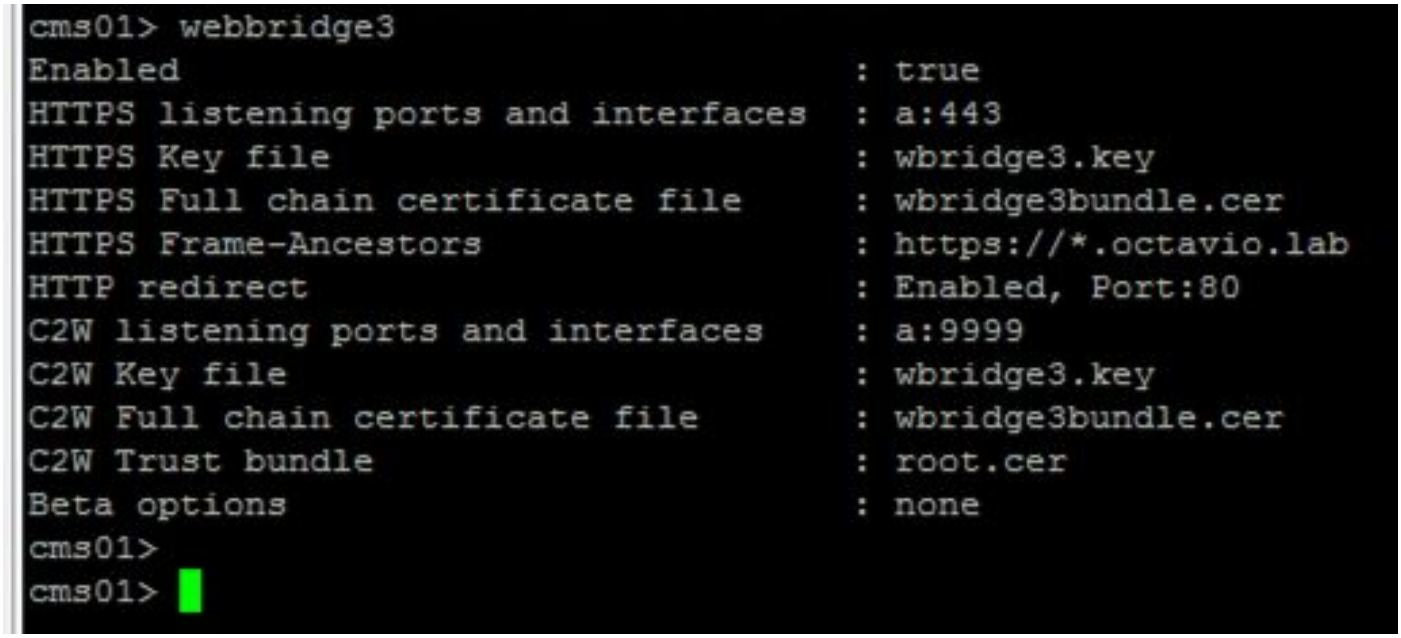
Pour les versions 3.2 et ultérieures de CMS, les administrateurs CMS peuvent intégrer l'application Web dans un autre site Web. Cela signifie que l'application Web est intégrée à une autre page Web.

Remarque : L'application Web peut exécuter des médias lorsqu'elle est intégrée aux navigateurs qui nécessitent HTTPS et non aux 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 illustré dans l'image :



L'application Web ne vérifie pas le contenu de l'en-tête, sauf 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 1000 caractères et les caractères autorisés sont a-z A-Z 0-9_ . / : ? # [ ] @ ! $ & ' ( ) * + - = ~ %.

Étape 2 : configuration de l'iFrame intégré dans une page Web

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

Remarque : HTTPS est requis pour exécuter les médias webapp. D'autres attributs pris en charge par iframe, tels que height et width, peuvent également être inclus.

La création du contenu iFrame appartient à 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

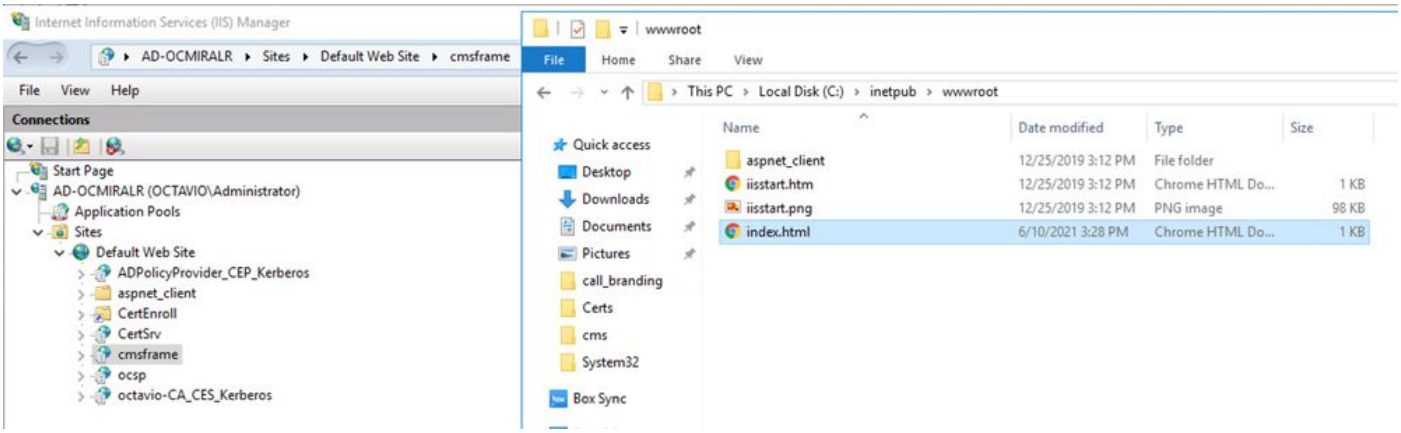
```
Welcome to the CMS Content Security Policy Demostration.


All this text is not part of the webbridge itself.


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

Étape 3. Déploiement sur le serveur Web

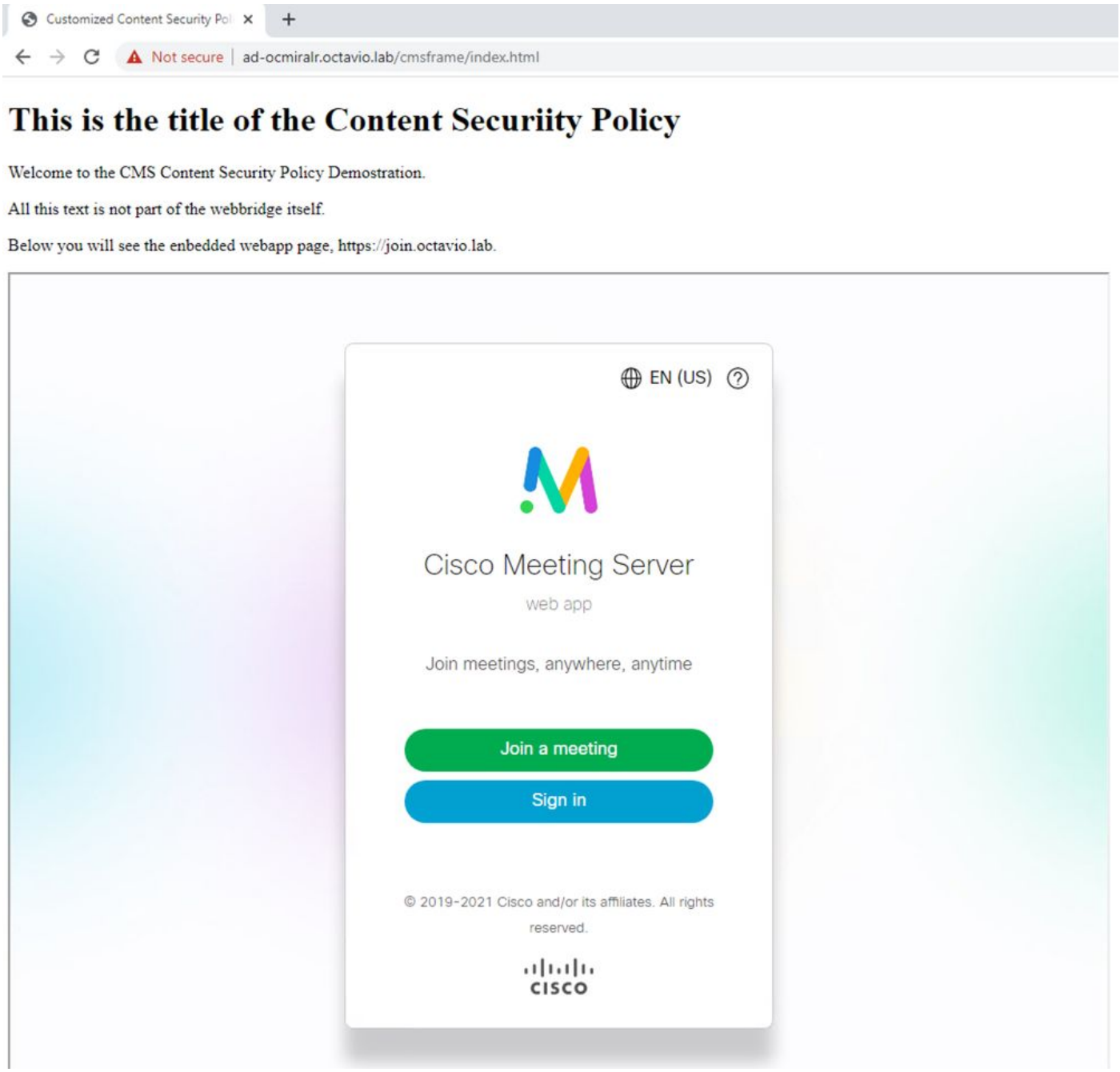
Une fois que le document HTML comporte un iframe incorporé, la page doit être chargée sur un serveur Web. Pour les besoins de ce document le fichier HTML est appelé index.html et stocké sur un serveur Web Windows, comme montré dans l'image :



Remarque : Les configurations supplémentaires du serveur Web et les options disponibles pour la page Web ne sont pas prises en compte dans ce document. L'administrateur du serveur Web doit terminer le déploiement de la page Web.

Vérifier

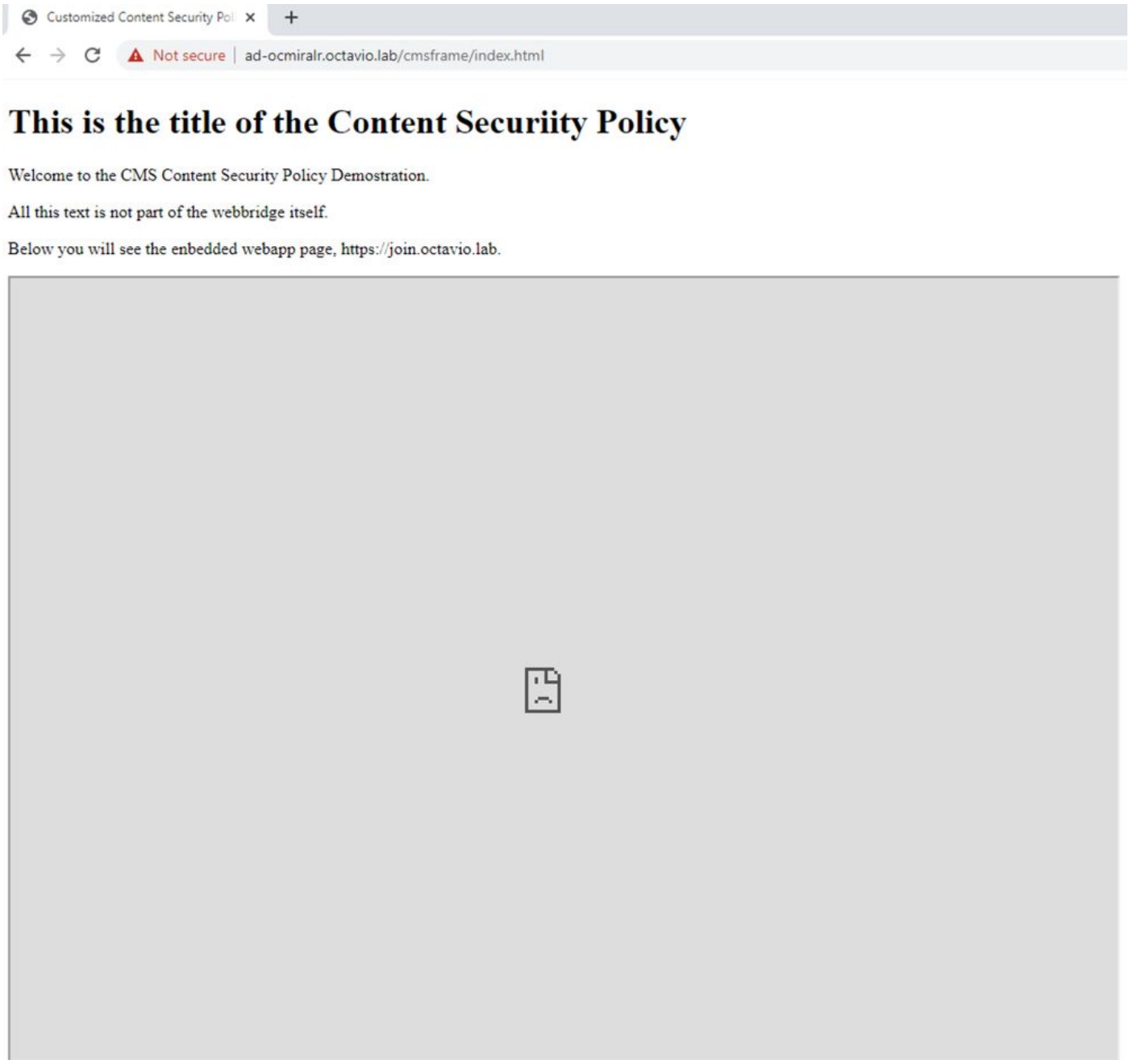
Afin de valider le bon fonctionnement de la configuration, ouvrez un navigateur Web et naviguez jusqu'à la page Web où l'iFrame a été configuré, pour ce document c'est https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Accédez à toutes les réunions disponibles sur le CMS et vérifiez que l'audio et la vidéo fonctionnent correctement.

Dépannage

1. La page Web est affichée, mais l'application Web n'est pas chargée.



Afin de résoudre ce type de problème, suivez les étapes suivantes :

Étape 1 : ouverture de l’interface de ligne de commande du CMS

Étape 2. Exécutez la commande suivante : webbridge.

Étape 3. À partir de la configuration du pont Web, assurez-vous que les Frame-Ancestors sont corrects. Il doit s’agir du src iframe configuré sur la page Web créée.

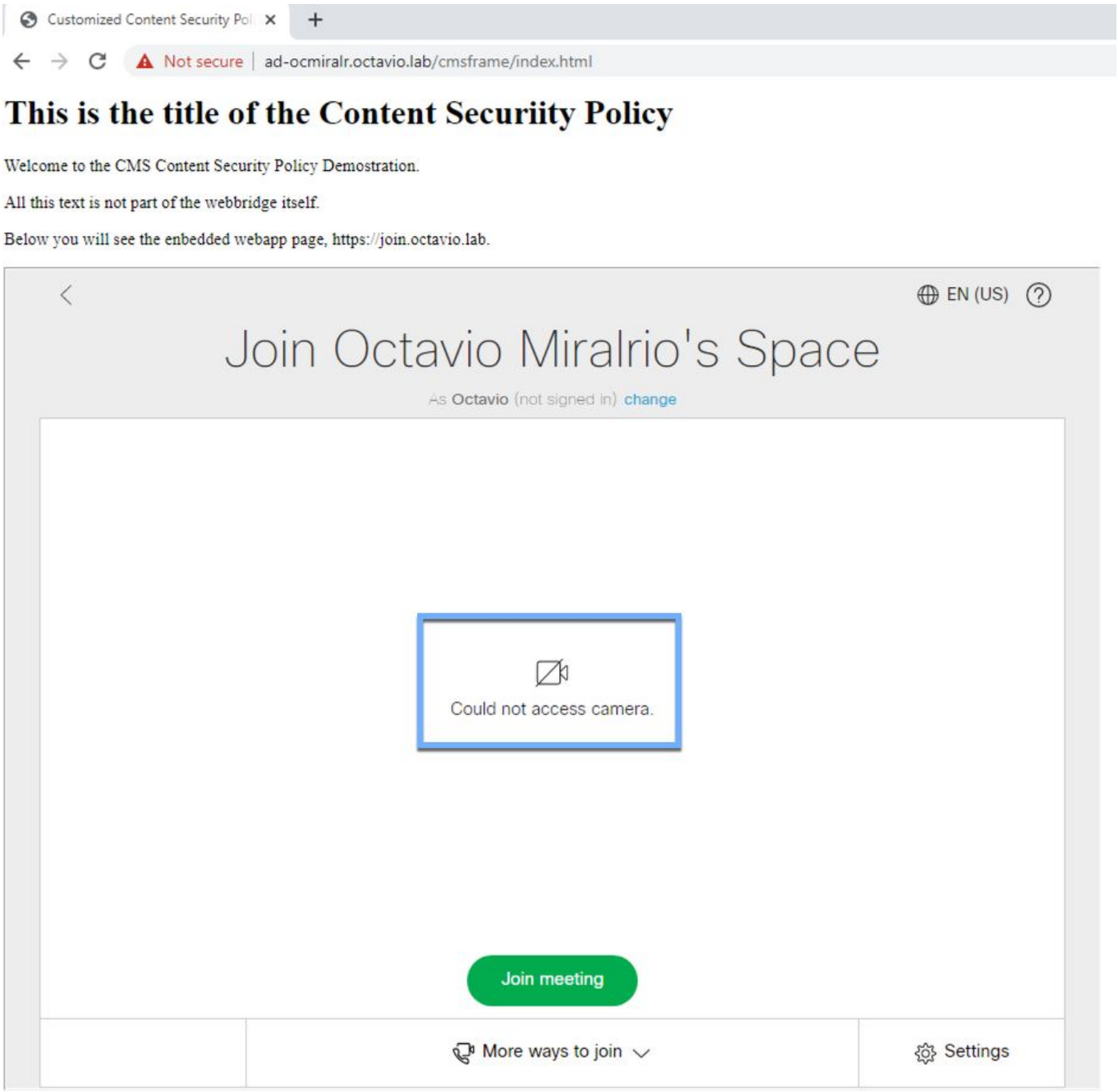
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Full chain certificate file          : wbridge3bundle.cer
HTTPS Frame-Ancestors                      : https://*.cms.lab
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>
```

Dans ce cas, les Frame-Ancestors configurés sur webbridge sont différents de celui configuré sur la page Web, comme illustré dans 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>
<p>Below you will see the embedded webapp 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 dans la configuration du pont Web ou dans le code de la page Web, le cas échéant.

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



Ce problème est causé par le fait que l'iframe n'est pas configuré correctement. Pour prendre en charge l'audio et la vidéo, l'iframe doit inclure les attributs allowusermedia allow="microphone; caméra ; display-capture".

Afin de résoudre ce problème, suivez les étapes suivantes :

Étape 1 : ouverture du serveur Web et recherche du fichier HTML de la page principale

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

Étape 3. Ajoutez les attributs de support à l'iframe, comme indiqué dans le code suivant :

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.