Come personalizzare i criteri di sicurezza del contenuto per Webbridge su CMS

Sommario

Introduzione

In questo documento viene descritta la procedura per configurare e abilitare un criterio di protezione del contenuto personalizzato per webbridge su Cisco Meeting Server (CMS) versione 3.2.

Contributo di Octavio Miralrio, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione generale CMS
- HTTPS (Hypertext Transfer Protocol Secure)
- HTML (Hypertext Markup Language)
- server Web

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMS versione 3.2
- Windows Web server 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazioni

A partire dalla versione 3.2 di CMS e successive, gli amministratori CMS possono incorporare l'app Web in un altro sito Web. Ciò significa che l'app Web è incorporata in un'altra pagina Web.

> **Nota:** L'app Web può eseguire file multimediali se incorporata nei browser che richiedono HTTPS e non nei browser con HTTP.

Passaggio 1. Aprire l'interfaccia della riga di comando (CLI) del CMS ed eseguire il comando successivo:

```
webbridge3 https frame-ancestors
```

Il parametro **<frame-ancestors-space-separated string>** deve essere sostituito con l'URL (Uniform Resource Locator) del frame in cui è incorporata l'app Web. Sono supportati i caratteri jolly, ad esempio **https://*.octavio.lab** come mostrato nell'immagine:

```
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'app Web non controlla il contenuto dell'intestazione oltre al fatto che i caratteri sono validi. Gli amministratori devono assicurarsi che l'intestazione del criterio di protezione del contenuto contenga stringhe valide. La dimensione della stringa è limitata a 1000 caratteri e i caratteri consentiti sono **a-z A-Z 0-9_ . / : ? # [ ] @ ! $ & ' ( ) * + - = ~ %**.

Passaggio 2. Configurare l'iFrame incorporato in una pagina Web.

Il passaggio successivo consiste nell'incorporare l'elemento iframe in una pagina Web. L'elemento iframe viene riconosciuto dal tag **<iframe>** in un documento HTML. Per supportare i supporti, sono necessari i seguenti attributi:

> **Nota:** HTTPS è necessario per eseguire il supporto webapp. Possono essere inclusi anche

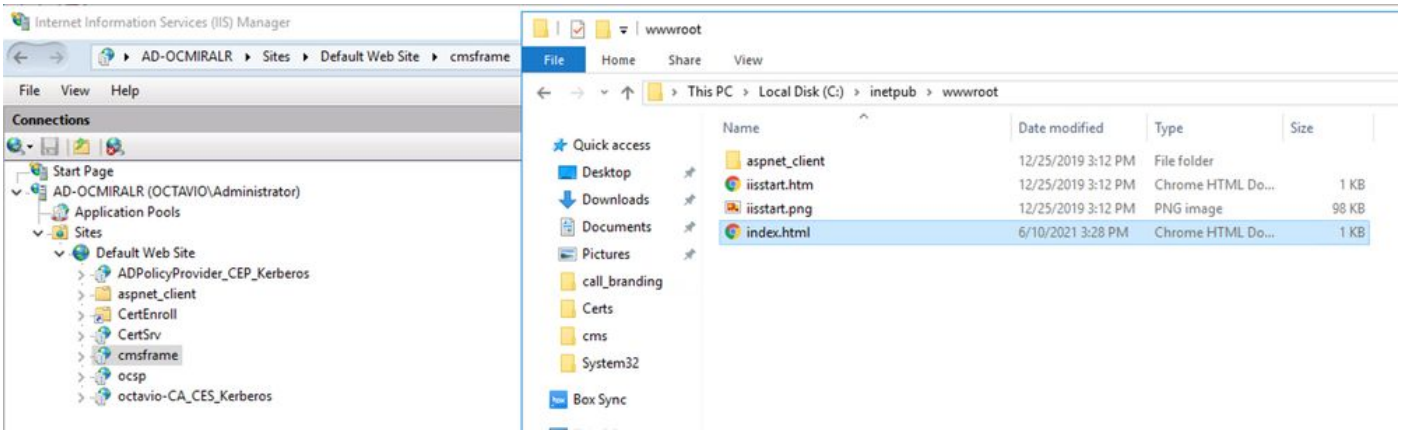
altri attributi supportati dall'iframe, quali **height** e **width**.

La creazione del contenuto iFrame è affidata all'amministratore della pagina Web, può essere personalizzata in base alle esigenze, il seguente è un esempio di iFrame creato a scopo dimostrativo:

```
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.
```

Passaggio 3. Eseguire la distribuzione sul server Web.

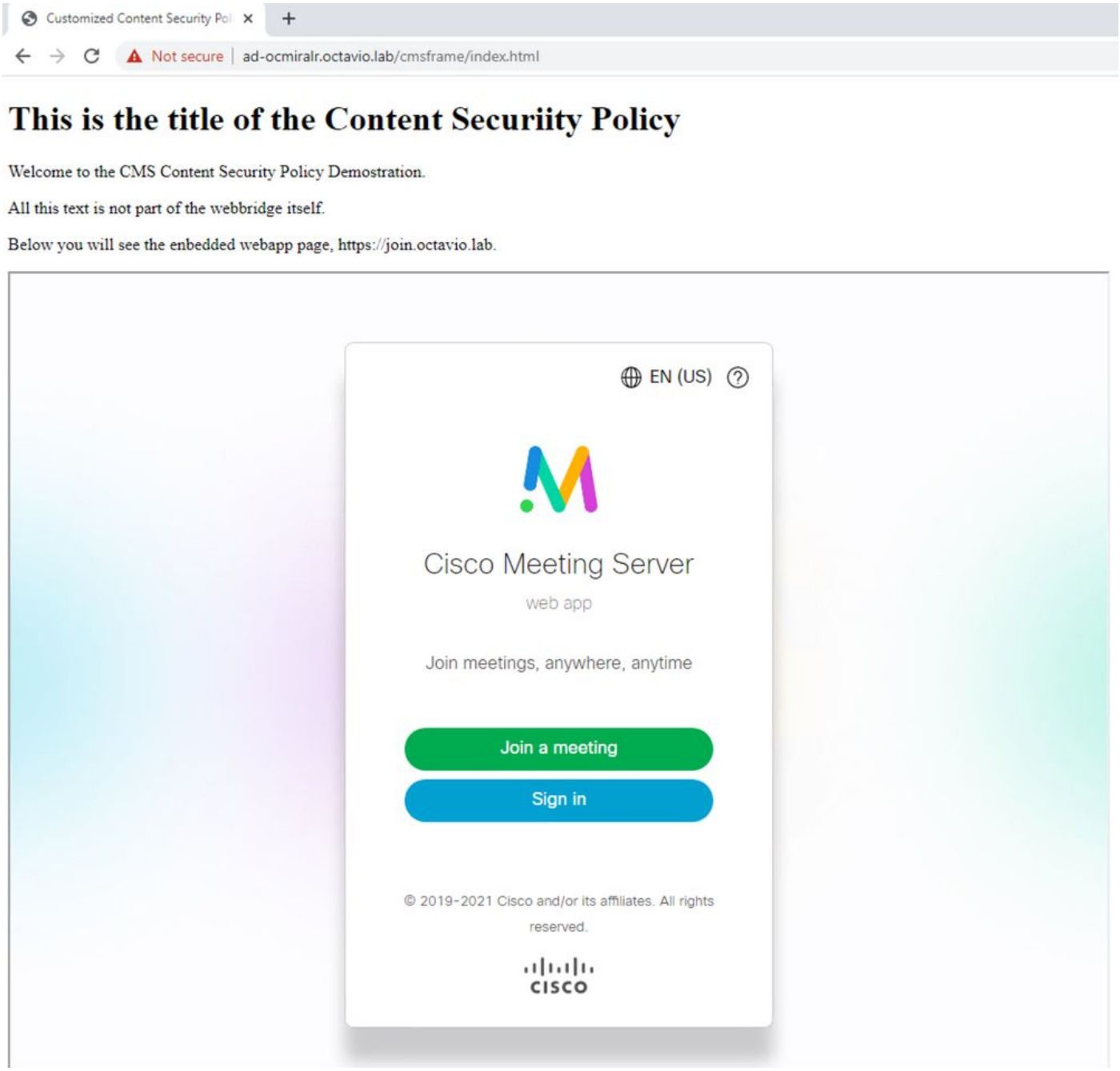
Quando il documento HTML ha un iframe incorporato, la pagina deve essere caricata su un server Web. Ai fini del presente documento, il file HTML è denominato **index.html** e viene memorizzato su un server Web Windows, come mostrato nell'immagine:



Nota: Le configurazioni aggiuntive del server Web e le opzioni disponibili per la pagina Web non rientrano nell'ambito di questo documento. L'amministratore del server Web deve completare la distribuzione della pagina Web.

Verifica

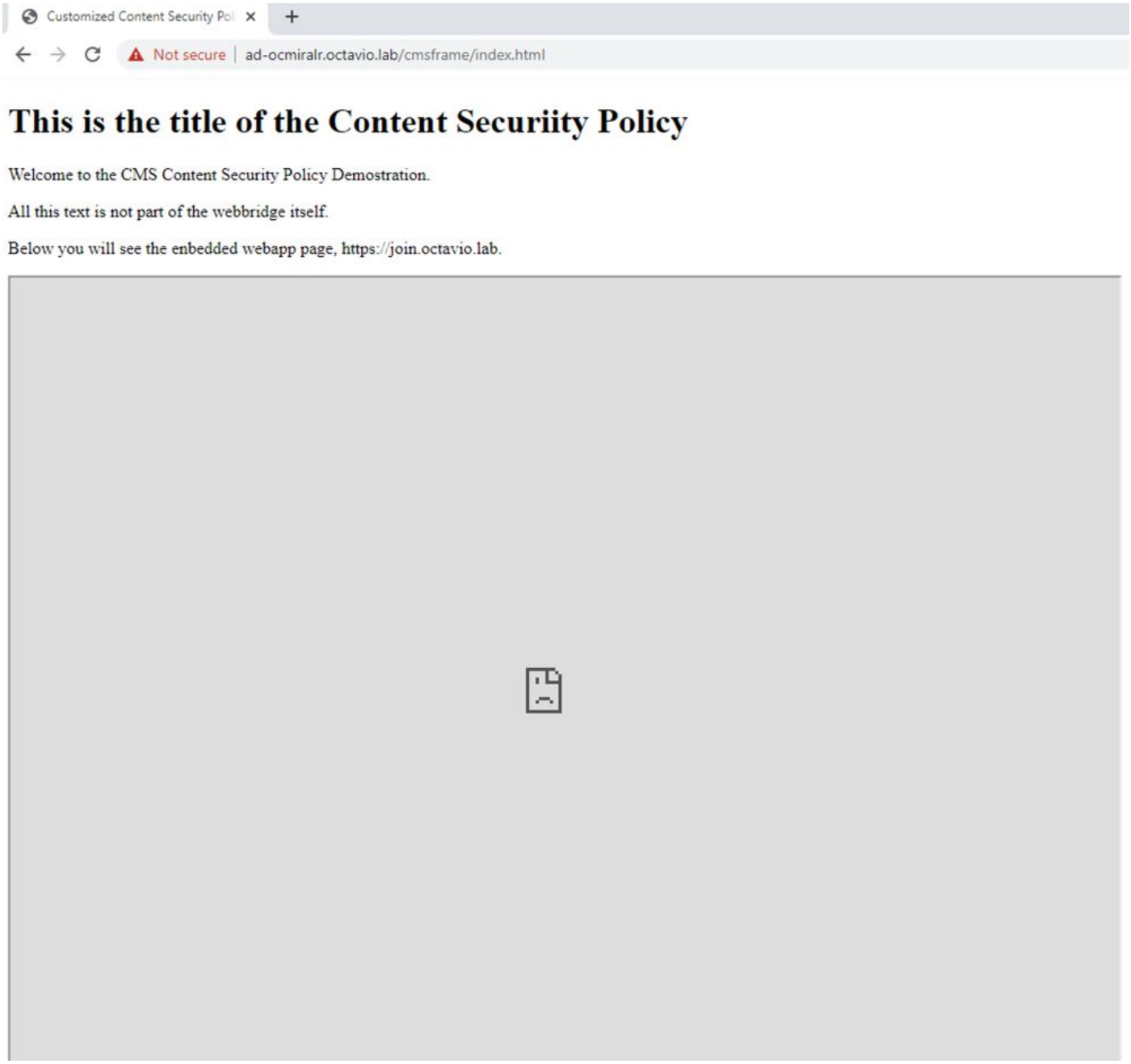
Per verificare il corretto funzionamento della configurazione, aprire un browser Web e accedere alla pagina Web in cui è stato configurato l'iFrame. Per questo documento, il percorso è https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Accedere a qualsiasi riunione disponibile nel CMS e verificare che audio e video funzionino correttamente.

Risoluzione dei problemi

1. La pagina Web è visualizzata ma l'app Web non è caricata.



Per risolvere questo tipo di problema, procedere come segue:

Passaggio 1. Aprire la CLI del CMS.

Passaggio 2. Eseguire il comando successivo: **webbridge**.

Passaggio 3. Dalla configurazione di webbridge verificare che i **Frame-Ancestor** siano corretti, deve essere **iframe src** configurato nella pagina Web creata.

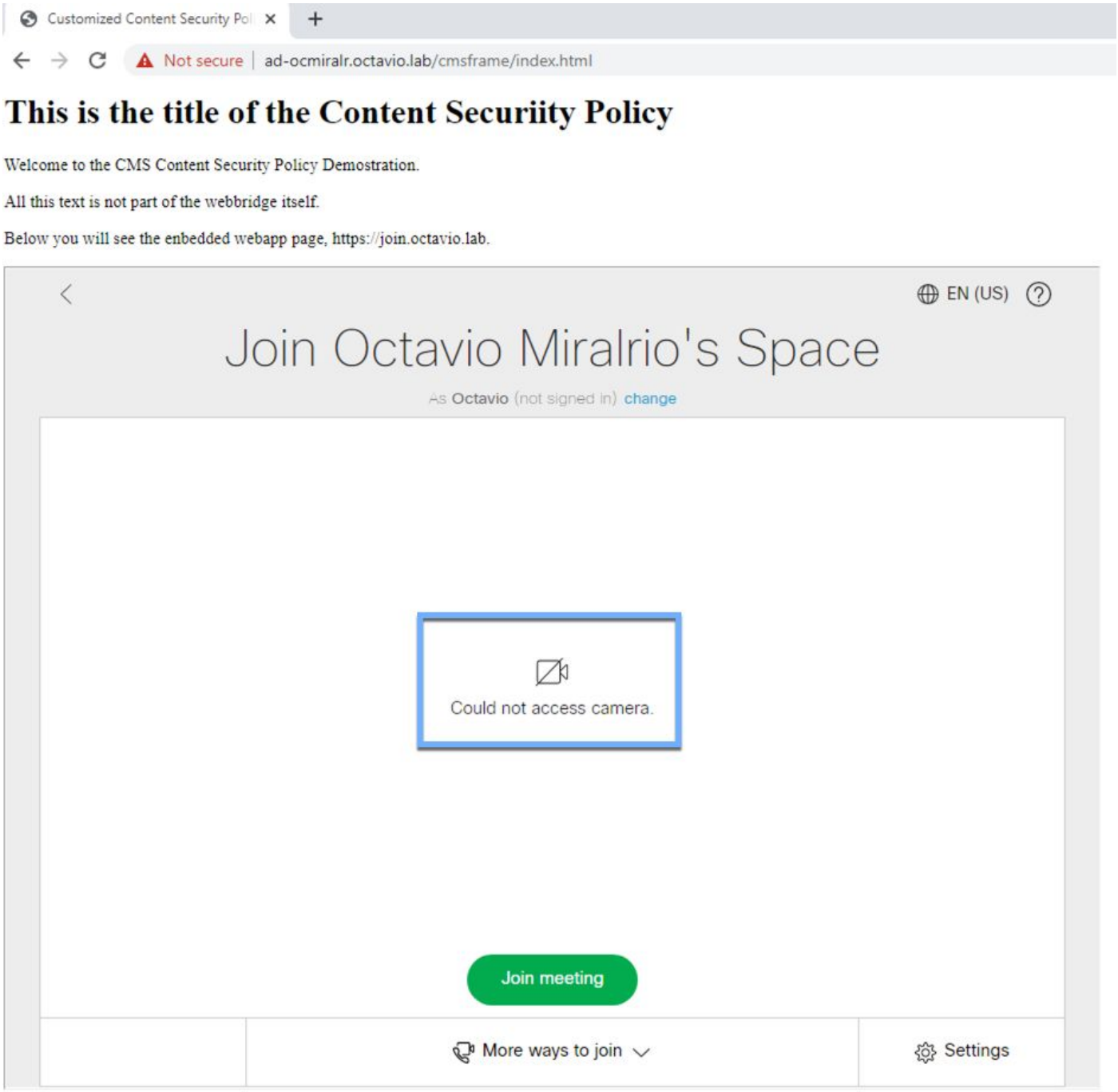
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Frame-Ancestors                      : https://*.cms.lab
C2W listening ports and interfaces         : a:9999
C2W Key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

In questo caso i Frame Predecessori configurati su webbridge sono diversi da quelli configurati sulla pagina Web, come mostrato nell'immagine:

```
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>
```

Passaggio 4. Correggere il valore Frame-Ancestor nella configurazione webbridge o nel codice della pagina Web, come richiesto.

2. L'app Web è caricata ma non è possibile accedere alla fotocamera o al microfono.



Questo problema è causato dal fatto che l'iframe non è configurato correttamente. Per supportare audio e video, l'iframe deve includere gli attributi **allowusermedia allow="microphone; telecamera; display-capture"**.

Per risolvere questo problema, procedere come segue:

Passaggio 1. Aprire il server Web e individuare il file HTML della pagina principale.

Passaggio 2. Utilizzare un editor di testo per modificare il file HTML.

Passaggio 3. Aggiungere gli attributi multimediali all'iframe, come mostrato nel codice seguente: