Anpassung der Inhaltssicherheitsrichtlinie für Webbridge in CMS

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfiguration](#)
[Konfigurationen](#)
[Überprüfung](#)
[Fehlerbehebung](#)

Einführung

In diesem Dokument wird das Verfahren zum Konfigurieren und Aktivieren einer benutzerdefinierten Inhaltssicherheitsrichtlinie für Webbridge auf Cisco Meeting Server (CMS) Version 3.2 beschrieben.

Mitwirkend von Octavio Miralrio, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Allgemeine CMS-Konfiguration
- Hypertext Transfer Protocol Secure (HTTPS)
- Hypertext Markup Language (HTML)
- Webserver

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CMS Version 3.2
- Windows-Webserver 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Konfigurationen

Für CMS Version 3.2 und höher können die CMS-Administratoren die Web-App in eine andere Website einbetten. Das bedeutet, dass die Web-App in eine andere Webseite eingebettet ist.

> **Hinweis:** Eine Web-App kann Medien ausführen, wenn sie in Browser eingebettet ist, die HTTPS und nicht in Browsern mit HTTP erfordern.

Schritt 1: Öffnen Sie die Befehlszeilenschnittstelle (CLI) des CMS, und führen Sie den folgenden Befehl aus:

```
webbridge3 https frame-ancestors
```

Der **<frame-ancestors space-Separated String>**-Parameter muss durch den Frame Uniform Resource Locator (URL) ersetzt werden, in dem die Web-App eingebettet ist. Platzhalter werden unterstützt, z. B. **https://*.octavio.lab**, wie im Bild gezeigt:

```
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>
```

Die Web-App überprüft den Headerinhalt nur, wenn die Zeichen gültig sind. Die Administratoren müssen sicherstellen, dass der Header der Inhaltssicherheitsrichtlinie gültige Zeichenfolgen enthält. Die Zeichenfolgengröße ist auf 1000 Zeichen beschränkt, und zulässige Zeichen sind **a-z A-Z 0-9_ . /: ? # [ ] @ ! $ & ' ( ) * + - = ~ %**.

Schritt 2: Konfigurieren Sie den eingebetteten iFrame in einer Webseite.

Im nächsten Schritt wird das iframe-Element in eine Webseite eingebettet. Das iframe-Element wird vom **<iframe>**-Tag in einem HTML-Dokument erkannt. Zur Unterstützung von Medien sind folgende Attribute erforderlich:

> **Hinweis:** Zum Ausführen von Webanwendungsmedien ist HTTPS erforderlich. Andere

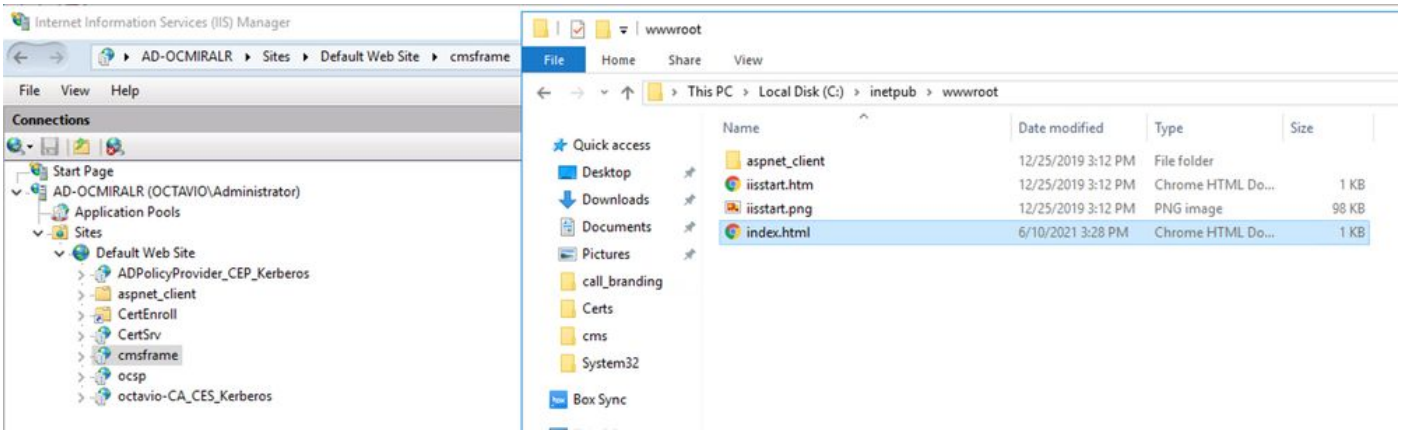
Attribute, die von iframe unterstützt werden, wie **Höhe** und **Breite** können ebenfalls einbezogen werden.

Die Erstellung des iFrame-Inhalts obliegt dem Webseitenadministrator. Er kann nach Bedarf angepasst werden. Das nächste Beispiel ist ein iFrame, der zu Demonstrationszwecken erstellt wurde:

```
# 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.
```

Schritt 3: Bereitstellung auf Webserver

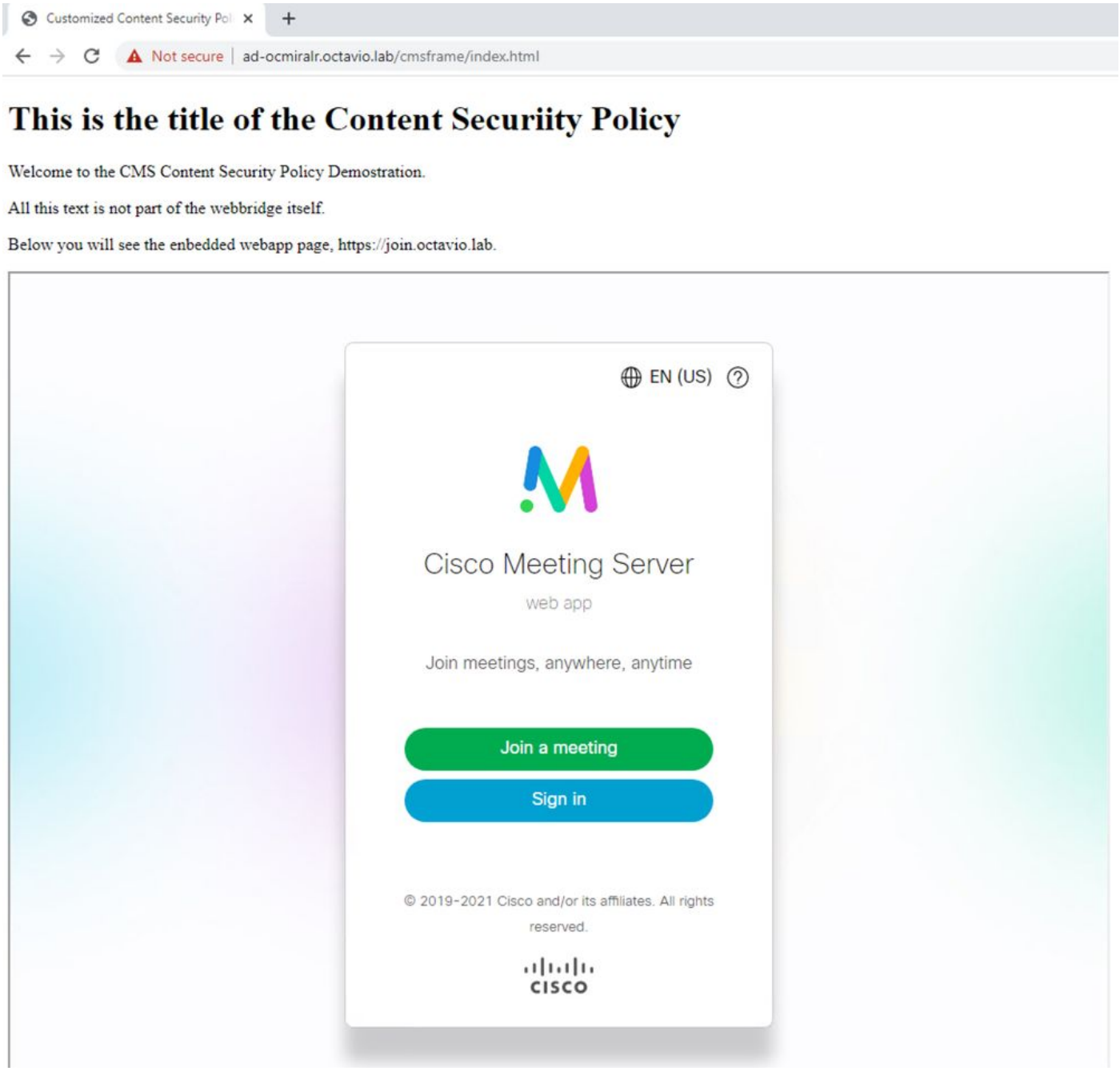
Sobald das HTML-Dokument über einen eingebetteten Frame verfügt, muss die Seite auf einen Webserver geladen werden. Für dieses Dokument wird die HTML-Datei **index.html** genannt und auf einem Windows-Webserver gespeichert, wie im Bild gezeigt:



Hinweis: Die zusätzlichen Konfigurationen des Webservers und die für die Webseite verfügbaren Optionen sind nicht Bestandteil des vorliegenden Dokuments. Der Webserver-Administrator muss die Bereitstellung der Webseite abschließen.

Überprüfung

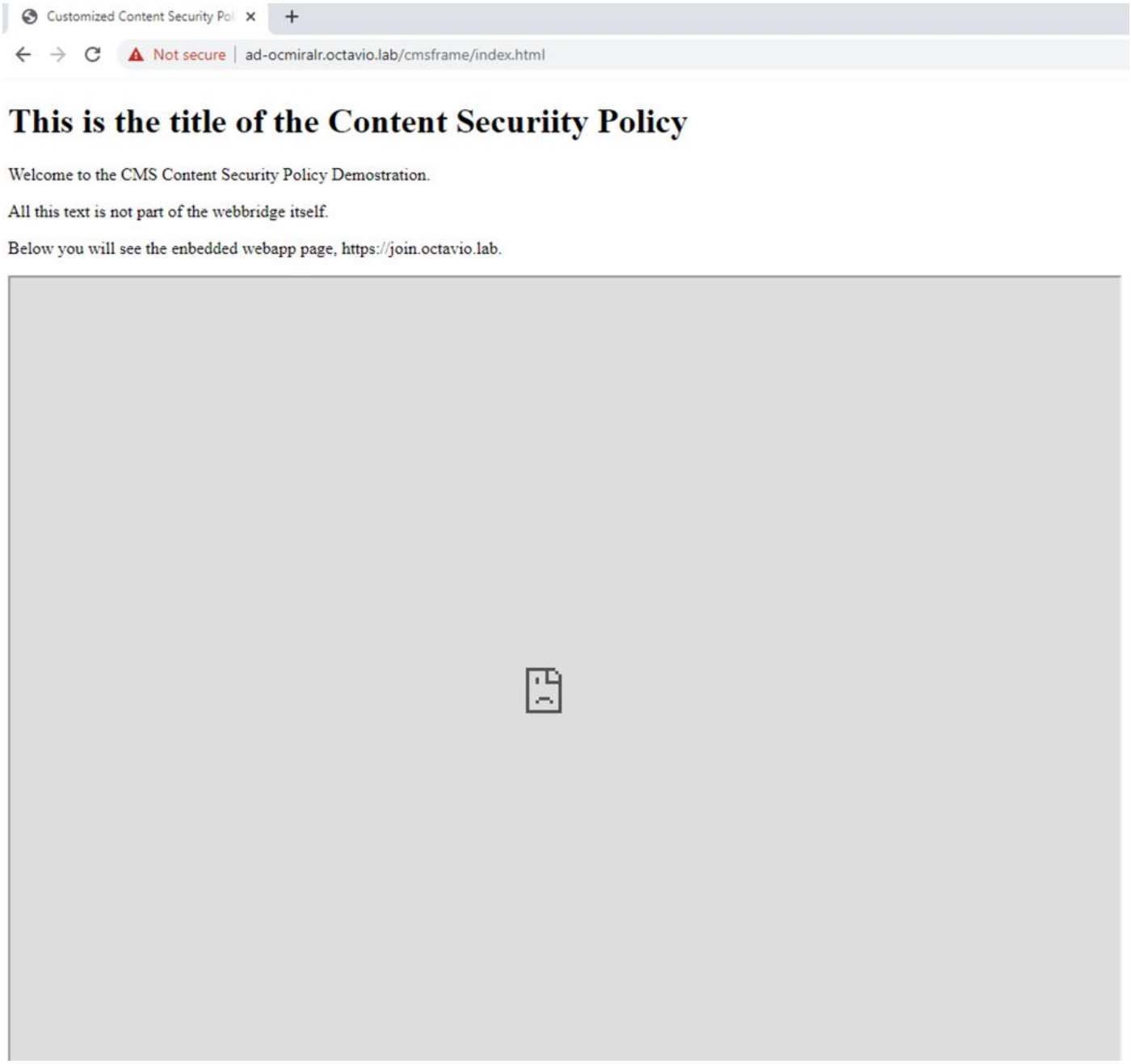
Um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert, öffnen Sie einen Webbrowser, und navigieren Sie zur Webseite, auf der der iFrame konfiguriert wurde. Für dieses Dokument ist es https://ad-ocmiralr.octavio.lab/cmsframe/index.html.



Greifen Sie auf alle verfügbaren Meetings im CMS zu, und prüfen Sie, ob Audio und Video einwandfrei funktionieren.

Fehlerbehebung

1. Die Webseite wird angezeigt, aber die Web-App wird nicht geladen.



Um dieses Problem zu beheben, gehen Sie wie folgt vor:

Schritt 1: Öffnen Sie die CLI des CMS.

Schritt 2: Führen Sie den folgenden Befehl aus: **webbridge**.

Schritt 3: Stellen Sie in der Webbridge-Konfiguration sicher, dass die **Frame-Ancestors** korrekt sind. Dies muss der **iframe src** sein, der auf der erstellten Webseite konfiguriert wurde.

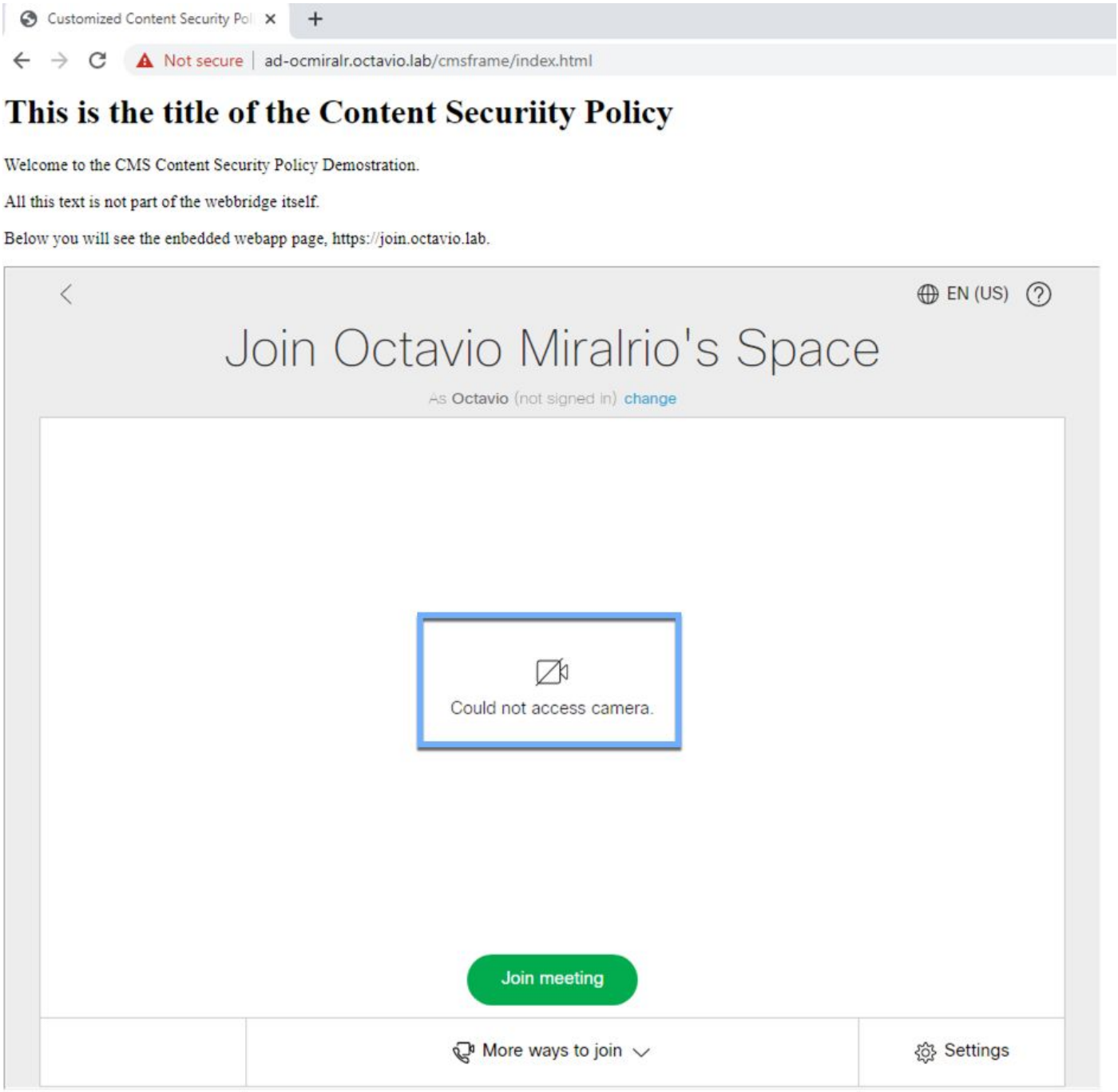
```
cms01> webbridge3
Enabled                                    : true
HTTPS listening ports and interfaces       : a:443
HTTPS Key file                             : wbridge3.key
HTTPS Frame-Ancestors                      : https://*.cms.lab
C2W listening ports and interfaces         : a:9999
C2W Key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

In diesem Fall unterscheiden sich die konfigurierten Frame-Ancestors auf webbridge von denen auf der Webseite, wie im Bild gezeigt:

```
<!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>
```

Schritt 4: Korrigieren Sie den Frame-Ancestor-Wert entweder in der Webbridge-Konfiguration oder im Webseitencode nach Bedarf.

2. Die Web-App ist geladen, kann aber nicht auf die Kamera oder das Mikrofon zugreifen.



Dieses Problem wird verursacht, weil der iFrame nicht richtig konfiguriert ist. Zur Unterstützung von Audio und Video muss der iframe die Attribute **allowusermedia allow="microone** enthalten**. Kamera; Display-Capture"**.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

Schritt 1: Öffnen Sie den Webserver, und suchen Sie die HTML-Datei der Hauptseite.

Schritt 2: Bearbeiten Sie die HTML-Datei mit einem Text-Editor.

Schritt 3: Fügen Sie dem iFrame die Medienattribute hinzu, wie im nächsten Code gezeigt: