

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Content Security Policy

Developer and IT Training

u2u

Content Security Policy

26°C Mostly sunny

Search

3:14 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Content Security Policy

- Introduction
- The CSP header
- Running inline scripts
- The frame-ancestors directive
- Developing with CSP

26°C
Mostly sunny

Search

3:14 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

What is the Content Security Policy header?

- Gives you fine grained control over what kind of content your site is allowed to run
- Will stop vulnerabilities like
 - Cross Site Scripting
 - Click Jacking
 - ...

GitHub's CSP journey

ptomey3 April 12, 2016

We shipped [subresource integrity](#) a few months back to reduce the risk of a compromised CDN serving malicious JavaScript. That is a big win, but does not address related content injection issues that may exist on GitHub.com itself. We have been tackling this side of the problem over the past few years and thought it would be fun, and hopefully useful, to share what we have been up to.

<https://githubengineering.com/githubs-csp-journey/>

26°C Mostly sunny

Search

3:14 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Content Security Policy

Developer and IT Training

U2U

Demo

Make your website do the harlem shake

26°C Mostly sunny

Search

3:14 PM 12/29/2023

The screenshot shows a web browser window with the address bar displaying 'online.u2u.be/courses/25896/modules/4/24846'. The page title is 'The CSP Header'. The U2U logo is in the top right corner. A sidebar on the left contains a navigation menu with items like 'Content Security Policy', 'Introduction', 'The CSP Header', 'Blocking inline scripts', 'The Same-Origin Policy', and 'Developing with CSP'. The main content area has a red horizontal line under the title. Below the title, there is a list of bullet points. The second bullet point contains a code snippet for a Content-Security-Policy header. The third bullet point includes a red URL. The Windows taskbar at the bottom shows the date as 12/29/2023 and the time as 3:14 PM.

The CSP Header

- The header is quite simple, for example:

Content-Security-Policy: script-src 'self'

- The script-src is one of many **content sources** you can control with this header
 - In this case the page can only run script from the page itself
- A list of everything you can control can be found at <https://scotthelme.co.uk/csp-cheat-sheet/>

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Content-Sources

- Your page is built from many sources
 - Your CSS comes from your own server
 - Your JavaScript comes from a CDN server
 - Your videos come from YouTube, etc...
- Content source keywords
 - *
 - 'none'
 - 'self'
- Content source hosts (these include the scheme)
 - <https://youtube.com>
 - https://*.othersite.com
 - https:

26°C Mostly sunny

Search

3:14 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Content Security Policy

CSP Header example

CONTENT-SECURITY-POLICY:

```
default-src *;  
script-src 'self' assets-cdn.github.com jobs.github.com  
          ssl.google-analytics.com secure.gaug.es;  
style-src 'self' assets-cdn.github.com 'unsafe-inline';  
object-src 'self' assets-cdn.github.com;
```

26°C
Mostly sunny

Search

3:14 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Running inline scripts

- Setting `script-src 'self'` will block inline scripts
 - But what if you still want to execute your own inline scripts?

✖ Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self' <https://ajax.aspnetcdn.com>". Either the 'unsafe-inline' keyword, a hash ('sha256-9FLqevjfnI80Rt3z09prhe9sCFtWYVSaHXIcLZKWC+s='), or a nonce ('nonce-...') is required to enable inline execution.

- Copy the generated hash and add it as a content source

26°C Mostly sunny

Search

3:14 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

frame-ancestors

- Defines valid parents that may embed the page in a frame or iframe
- Great way to protect against click-jacking

❌ Refused to display 'http://localhost:5000/' in a frame about:blank:1 because an ancestor violates the following Content Security Policy directive: "frame-ancestors 'none'".

26°C Mostly sunny

Search

3:14 PM 12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Developer and IT Training

U2U

Demo

Click Jacking

26°C Mostly sunny

Search

3:14 PM 12/29/2023

The screenshot shows a web browser window displaying a course page on 'U2U Online'. The browser's address bar shows the URL 'online.u2u.be/courses/25896/modules/4/24846'. The page has a dark blue sidebar on the left with a navigation menu. The main content area has a white background with the title 'Developing with CSP' in a large, dark font, followed by a red horizontal line. Below the title is a list of four bullet points. The U2U logo is in the top right corner of the content area. The Windows taskbar is visible at the bottom of the screen.

U2U Online

online.u2u.be/courses/25896/modules/4/24846

Developing with CSP

- Start by using the Content-Security-Policy-Report-Only header
- Start by adding the default-src 'self' and adjust your CSP based on violations being reported
- Build the CSP to support the site as it is (allow unsafe-script for example)
- Configure the report-uri directive and monitor until your CSP is accurate

U2U

26°C Mostly sunny

Search

3:14 PM 12/29/2023