oshp /
oshp-tracking

Code Issues 2 Pull requests **Discussions** Actions Security Insigh

Edit

✓ CSP Limits Recommendation #29

Closed | ✓ Answered by righettod | **riramar** asked this question in **Q&A**

riramar on Oct 18 Maintainer

I'm looking for the recommendation in case of too many subdomains in the CSP response header.
For example, when it's recommended to use *.example.com since the example.com subdomains allowed are too many.
I double checked here https://www.w3.org/TR/CSP3/ but couldn't find anything about it.

↑ 2 👍 1

✓ Answered by **righettod** last week

Based on the test performed, for me, modern browsers like Chromium based ones or FF supports sufficient size to specify a large CSP in case of need.

View full answer ↓

8 comments · 2 replies

Oldest Newest | Top

righettod on Oct 19 Maintainer

Nice question indeed 👍

If I have understood, your point is, for example regarding the following site with the following set of sub domains:

```
sub1.example.com
sub2.sub1.example.com
sub3.sub2.sub1.example.com
```

How to use CSP to only allow content from `sub3.sub2.sub1.example.com` ?

↑ 1 ☺ 👍 1 1 reply

riramar on Oct 20 Maintainer Author

> Nice question indeed 👍
>
> If I have understood, your point is, for example regarding the following site with the following set of sub domains:
>
> ```
> sub1.example.com
> sub2.sub1.example.com
> sub3.sub2.sub1.example.com
> ```
>
> How to use CSP to only allow content from `sub3.sub2.sub1.example.com` ?

Not exactly. I meant in case of the CSP header is too big that cause problems in certain web frameworks like:

```
Content-Security-Policy: default-src 'self'; img-src image1.example.com image2.example.com ...; media-src media1.example.com media2.example.com ...; script-src script1.example.com script2.example.com ...
```

AFAIK the HTTP RFC do not specify a limit and some frameworks can breaks when receiving a big header.

☺ 👍 1

Write a reply

riramar on Oct 21 Maintainer Author

BTW I posted the same question here https://lists.w3.org/Archives/Public/public-webappsec/2024Oct/0010.html to try get some info from the browser devs.

↑ 1 ☺ 0 replies

Write a reply

righettod on Oct 21 Maintainer

Thanks for the clarification, I will take a look as well and keep you posted with the results.

↑ 1 ☺ 👍 1 0 replies

Write a reply

righettod last week Maintainer edited ▾

@riramar Do you have received any feedback about your question?

🤔If I'm not wrong, in case of a large CSP policy sent by the app server or the WAF or the reverse proxy, it is the browser or any network device handling the HTTP response that will *cut* or *alter* the CSP received. At the framework level, it is just a string.

Do you have an example to allow me to better understand the issue, and its context, in order that I work on a proposal?

Thanks a lot in advance for your insights 😃

↑ 1 ☺ 0 replies

Write a reply

riramar last week Maintainer Author

Hi @righettod

I don't have a specific example for that. I found this paper from 2016 on Google which seems to point to the right direction.

https://research.google/pubs/csp-is-dead-long-live-csp-on-the-insecurity-of-whitelists-and-the-future-of-content-security-policy/
We expect that that the combination of a nonce-based approach and the 'strict-dynamic' keyword will allow developers and organizations to finally enjoy real security benefits offered by the Content Security Policy.

The entire paper PDF can be found here: https://dl.acm.org/doi/pdf/10.1145/[2976749.2978363](https://dl.acm.org/doi/pdf/10.1145/2976749.2978363)

Regards,
Ricardo Iramar

↑ 1 ☺ 👍 1 0 replies

Write a reply

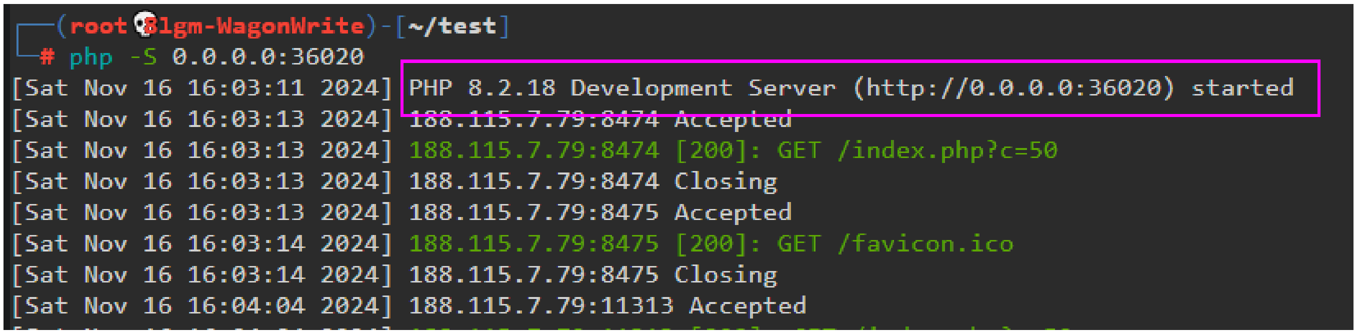
righettod last week Maintainer edited ▾

🧑‍💻I performed the following test.

📝Test page generating a large CSP based on a number of subdomains to add into the `img-src` directive:

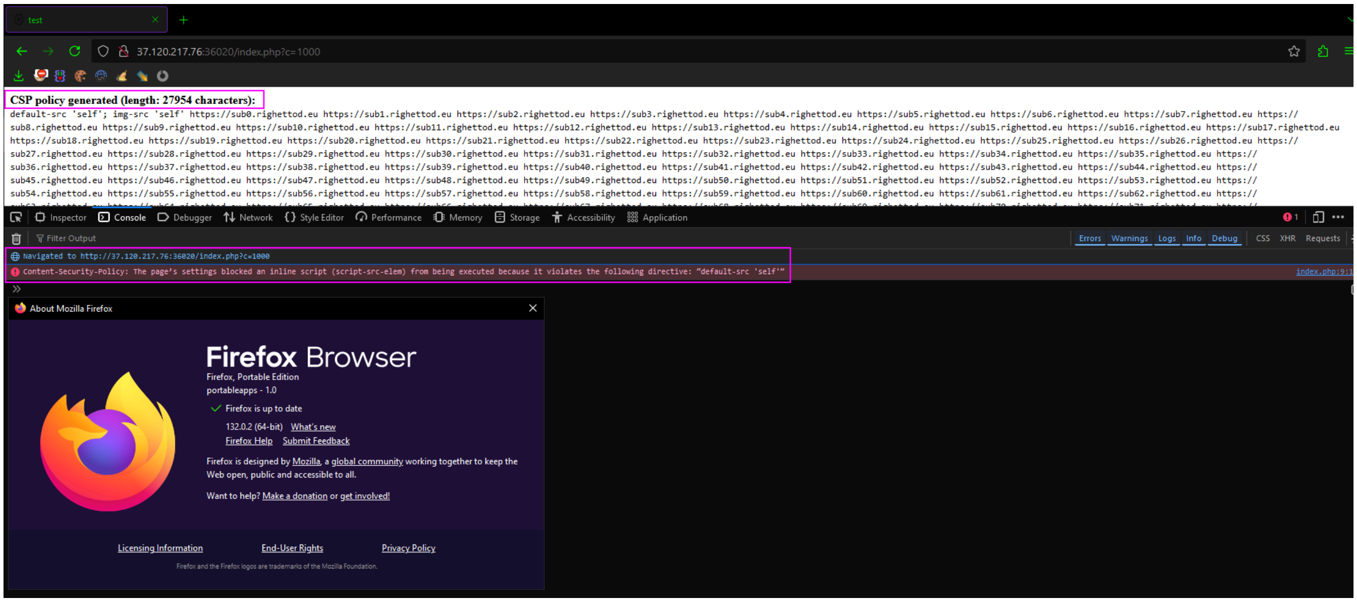
```
<?php
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);
$csp="default-src 'self'; img-src 'self'";
$cnt=intval($_GET["c"]);
for ($x = 0; $x <= $cnt; $x++) {
        $csp .= " https://sub$x.righettod.eu";
}
$csp .= ";";
header("Content-type: text/html; charset=utf-8");
header("Content-Security-Policy: $csp", True, 200);
?>
<!DOCTYPE html>
<html>
<head>
        <title>test</title>
</head>
<body>
        <b>CSP policy generated (length: <?php echo(strlen($csp)); ?> characters): </b><br>
        <code><?php echo($csp); ?><br>
        <script>alert("test xss");</script>
</body>
</html>
```

🌍Page exposed on Internet via a segfault instance:



```
┌──(root💀lgm-WagonWrite)-[~/test]
└─# php -S 0.0.0.0:36020
[Sat Nov 16 16:03:11 2024] PHP 8.2.18 Development Server (http://0.0.0.0:36020) started
[Sat Nov 16 16:03:13 2024] 188.115.7.79:8474 Accepted
[Sat Nov 16 16:03:13 2024] 188.115.7.79:8474 [200]: GET /index.php?c=50
[Sat Nov 16 16:03:13 2024] 188.115.7.79:8474 Closing
[Sat Nov 16 16:03:13 2024] 188.115.7.79:8475 Accepted
[Sat Nov 16 16:03:14 2024] 188.115.7.79:8475 [200]: GET /favicon.ico
[Sat Nov 16 16:03:14 2024] 188.115.7.79:8475 Closing
[Sat Nov 16 16:04:04 2024] 188.115.7.79:11313 Accepted
```

💻Test of generation of 1000 subdomains and loading of the page in the Firefox **132.0.2** (last release):



CSP policy generated (length: 27954 characters):

```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righettod.eu https://sub5.righettod.eu https://sub6.righettod.eu https://sub7.righettod.eu https://
sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https://sub14.righettod.eu https://sub15.righettod.eu https://sub16.righettod.eu https://sub17.righettod.eu
https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod.eu https://sub24.righettod.eu https://sub25.righettod.eu https://sub26.righettod.eu https://
sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu https://sub33.righettod.eu https://sub34.righettod.eu https://sub35.righettod.eu https://
sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu https://sub42.righettod.eu https://sub43.righettod.eu https://sub44.righettod.eu https://
sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu https://sub51.righettod.eu https://sub52.righettod.eu https://sub53.righettod.eu https://
sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu https://sub60.righettod.eu https://sub61.righettod.eu https://sub62.righettod.eu https://
```

```
Navigated to http://37.120.217.76:36020/index.php?c=1000
Content-Security-Policy: The page's settings blocked an inline script (script-src-elem) from being executed because it violates the following directive: "default-src 'self'"     index.php:9:1
```

About Mozilla Firefox

Firefox Browser
Firefox, Portable Edition
portableapps - 1.0

✓ Firefox is up to date

132.0.2 (64-bit) What's new
Firefox Help Submit Feedback

Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.

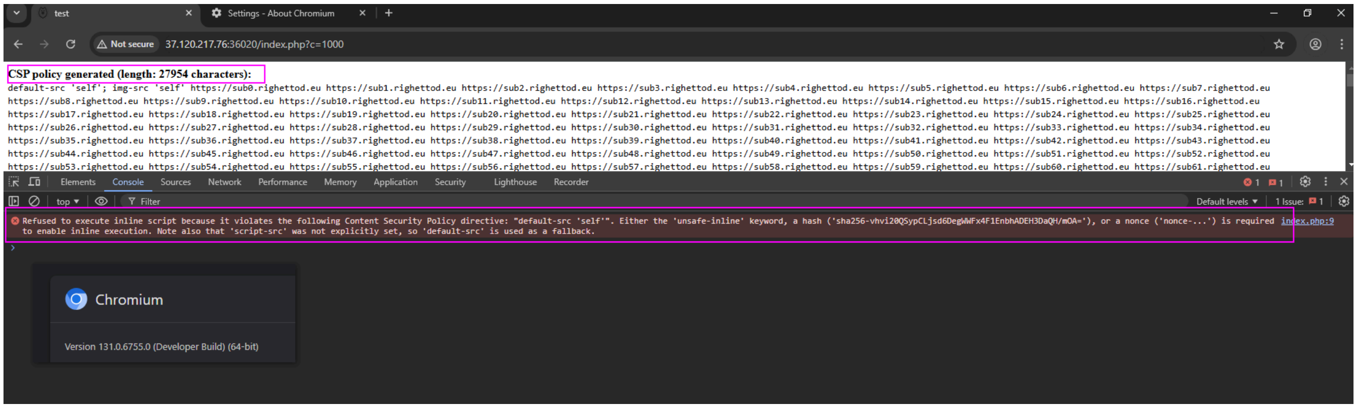
Want to help? Make a donation or get involved!

Licensing Information End-User Rights Privacy Policy

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.

✅ CSP correctly loaded and applied to block the inline JS code.

💻 Same test in Chromium **131.0.6755.0**:



CSP policy generated (length: 27954 characters):

```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righettod.eu https://sub5.righettod.eu https://sub6.righettod.eu https://sub7.righettod.eu
https://sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https://sub14.righettod.eu https://sub15.righettod.eu https://sub16.righettod.eu
https://sub17.righettod.eu https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod.eu https://sub24.righettod.eu https://sub25.righettod.eu
https://sub26.righettod.eu https://sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu https://sub33.righettod.eu https://sub34.righettod.eu
https://sub35.righettod.eu https://sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu https://sub42.righettod.eu https://sub43.righettod.eu
https://sub44.righettod.eu https://sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu https://sub51.righettod.eu https://sub52.righettod.eu
https://sub53.righettod.eu https://sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu https://sub60.righettod.eu https://sub61.righettod.eu
```

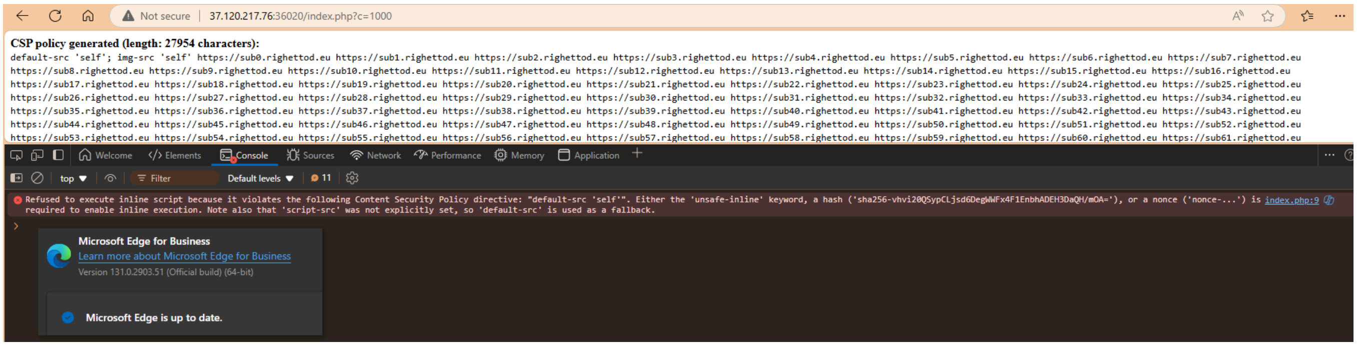
```
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-vhvi20QSypCLjsd6DegWWFx4F1EnbhADEH3DaQH/mOA='), or a nonce ('nonce-...') is required  index.php:9
to enable inline execution. Note also that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
```

Chromium

Version 131.0.6755.0 (Developer Build) (64-bit)

✅ CSP correctly loaded and applied to block the inline JS code.

💻 Same tes in Edge **131.0.2903.51** (last release):



CSP policy generated (length: 27954 characters):

```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righettod.eu https://sub5.righettod.eu https://sub6.righettod.eu https://sub7.righettod.eu
https://sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https://sub14.righettod.eu https://sub15.righettod.eu https://sub16.righettod.eu
https://sub17.righettod.eu https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod.eu https://sub24.righettod.eu https://sub25.righettod.eu
https://sub26.righettod.eu https://sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu https://sub33.righettod.eu https://sub34.righettod.eu
https://sub35.righettod.eu https://sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu https://sub42.righettod.eu https://sub43.righettod.eu
https://sub44.righettod.eu https://sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu https://sub51.righettod.eu https://sub52.righettod.eu
https://sub53.righettod.eu https://sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu https://sub60.righettod.eu https://sub61.righettod.eu
```

```
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-vhvi20QSypCLjsd6DegWWFx4F1EnbhADEH3DaQH/mOA='), or a nonce ('nonce-...') is  index.php:9
required to enable inline execution. Note also that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
```

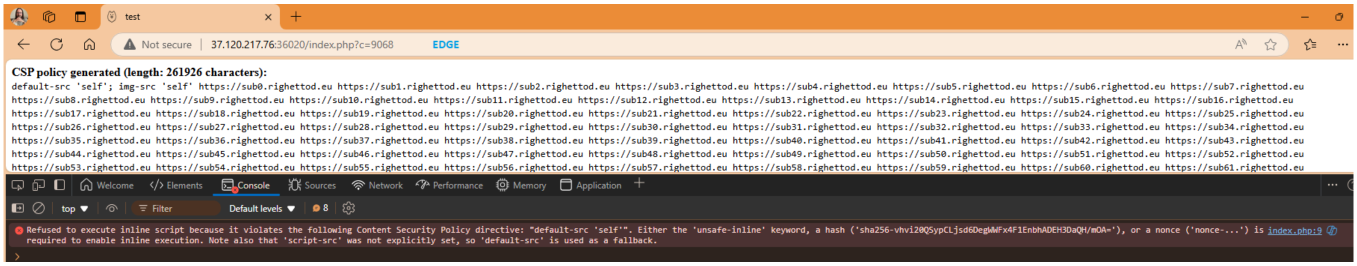
Microsoft Edge for Business
Learn more about Microsoft Edge for Business
Version 131.0.2903.51 (Official build) (64-bit)

Microsoft Edge is up to date.

✅ CSP correctly loaded and applied to block the inline JS code.

🧑‍💻 I tested to reach the limit.

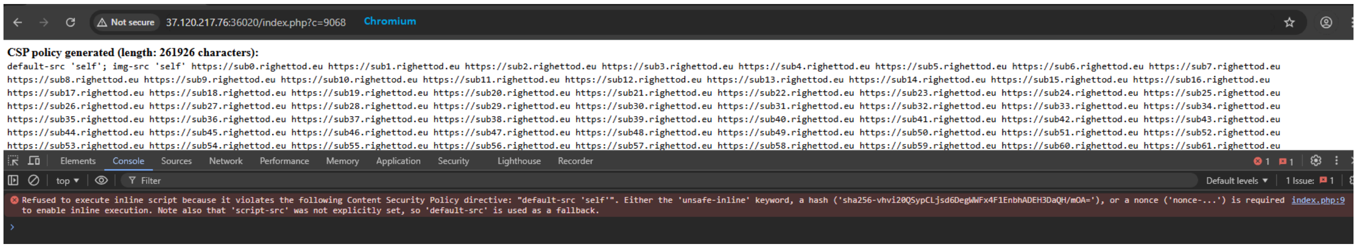
💻 For Edge and Chromium it was when CSP was above 261926 characters:



CSP policy generated (length: 261926 characters):

```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righettod.eu https://sub5.righettod.eu https://sub6.righettod.eu https://sub7.righettod.eu
https://sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https://sub14.righettod.eu https://sub15.righettod.eu https://sub16.righettod.eu
https://sub17.righettod.eu https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod.eu https://sub24.righettod.eu https://sub25.righettod.eu
https://sub26.righettod.eu https://sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu https://sub33.righettod.eu https://sub34.righettod.eu
https://sub35.righettod.eu https://sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu https://sub42.righettod.eu https://sub43.righettod.eu
https://sub44.righettod.eu https://sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu https://sub51.righettod.eu https://sub52.righettod.eu
https://sub53.righettod.eu https://sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu https://sub60.righettod.eu https://sub61.righettod.eu
```

```
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-vhvi20QSypCLjsd6DegWWFx4F1EnbhADEH3DaQH/mOA='), or a nonce ('nonce-...') is index.php:9
required to enable inline execution. Note also that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
```

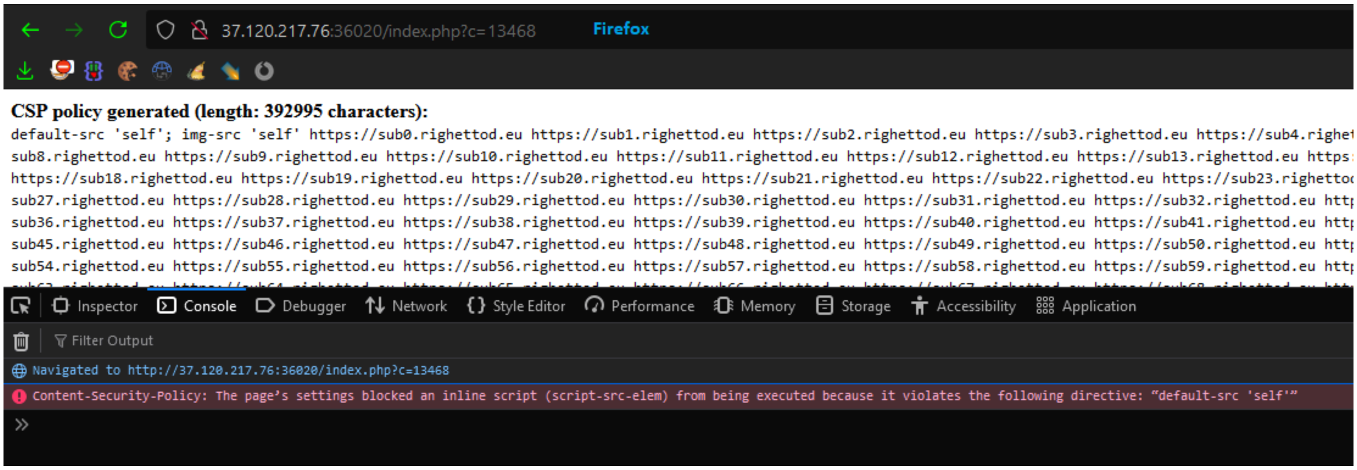


CSP policy generated (length: 261926 characters):

```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righettod.eu https://sub5.righettod.eu https://sub6.righettod.eu https://sub7.righettod.eu
https://sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https://sub14.righettod.eu https://sub15.righettod.eu https://sub16.righettod.eu
https://sub17.righettod.eu https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod.eu https://sub24.righettod.eu https://sub25.righettod.eu
https://sub26.righettod.eu https://sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu https://sub33.righettod.eu https://sub34.righettod.eu
https://sub35.righettod.eu https://sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu https://sub42.righettod.eu https://sub43.righettod.eu
https://sub44.righettod.eu https://sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu https://sub51.righettod.eu https://sub52.righettod.eu
https://sub53.righettod.eu https://sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu https://sub60.righettod.eu https://sub61.righettod.eu
```

```
Refused to execute inline script because it violates the following Content Security Policy directive: "default-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-vhvi20QSypCLjsd6DegWWFx4F1EnbhADEH3DaQH/mOA='), or a nonce ('nonce-...') is required index.php:9
to enable inline execution. Note also that 'script-src' was not explicitly set, so 'default-src' is used as a fallback.
```

💻For FF it was when CSP was above 392995 characters:

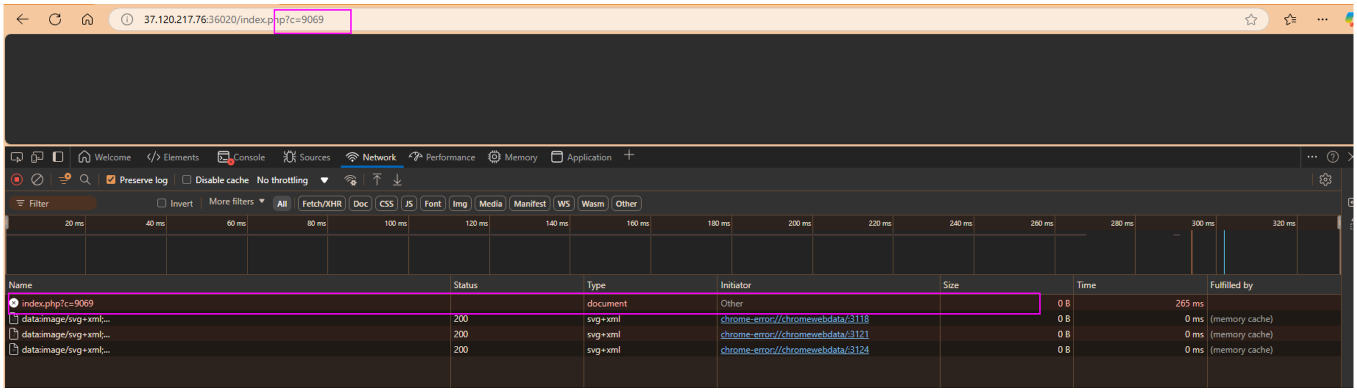


CSP policy generated (length: 392995 characters):

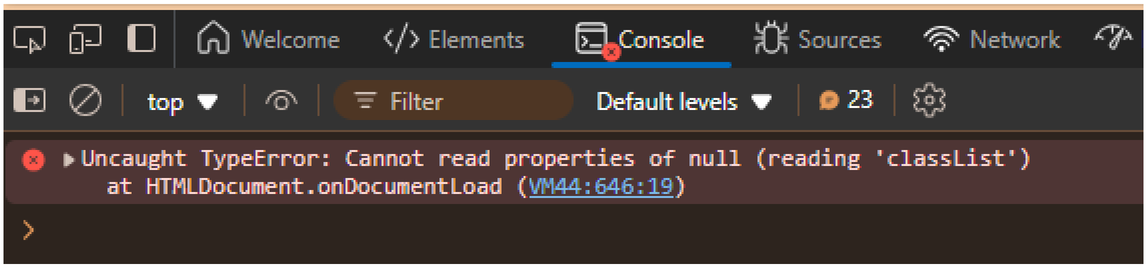
```
default-src 'self'; img-src 'self' https://sub0.righettod.eu https://sub1.righettod.eu https://sub2.righettod.eu https://sub3.righettod.eu https://sub4.righet
sub8.righettod.eu https://sub9.righettod.eu https://sub10.righettod.eu https://sub11.righettod.eu https://sub12.righettod.eu https://sub13.righettod.eu https:
https://sub18.righettod.eu https://sub19.righettod.eu https://sub20.righettod.eu https://sub21.righettod.eu https://sub22.righettod.eu https://sub23.righettod
sub27.righettod.eu https://sub28.righettod.eu https://sub29.righettod.eu https://sub30.righettod.eu https://sub31.righettod.eu https://sub32.righettod.eu http
sub36.righettod.eu https://sub37.righettod.eu https://sub38.righettod.eu https://sub39.righettod.eu https://sub40.righettod.eu https://sub41.righettod.eu http
sub45.righettod.eu https://sub46.righettod.eu https://sub47.righettod.eu https://sub48.righettod.eu https://sub49.righettod.eu https://sub50.righettod.eu http
sub54.righettod.eu https://sub55.righettod.eu https://sub56.righettod.eu https://sub57.righettod.eu https://sub58.righettod.eu https://sub59.righettod.eu http
```

```
Navigated to http://37.120.217.76:36020/index.php?c=13468
Content-Security-Policy: The page’s settings blocked an inline script (script-src-elem) from being executed because it violates the following directive: “default-src 'self'”
```

👀Above the limit specified, the error was the following on the browser side (response correctly generated and sent by the php server):



Name	Status	Type	Initiator	Size	Time	Fulfilled by
index.php?c=9069		document	Other	0 B	265 ms	
data:image/svg+xml;...	200	svg+xml	chrome-error://chromewebdata/:3118	0 B	0 ms	(memory cache)
data:image/svg+xml;...	200	svg+xml	chrome-error://chromewebdata/:3121	0 B	0 ms	(memory cache)
data:image/svg+xml;...	200	svg+xml	chrome-error://chromewebdata/:3124	0 B	0 ms	(memory cache)



```
Uncaught TypeError: Cannot read properties of null (reading 'classList')
    at HTMLDocument.onDocumentLoad (VM44:646:19)
```

↑ 1 ☺ 👍 1 0 replies

Write a reply

righettod last week Maintainer

Based on the test performed, for me, modern browsers like Chromium based ones or FF supports sufficient size to specify a large CSP in case of need.

✓ Unmark as answer ↑ 1 ☺ 👍 1 0 replies

Write a reply

Answer selected by **righettod**

riramar last week Maintainer Author

Agreed! I think in that case we can close this topic.
Thanks a lot for the tests.

↑ 1 ☺ 👍 1 1 reply 1 new

righettod last week Maintainer

Thanks to you for this very interesting question 💯

☺ 👍 1

Write a reply

Category

❓ Q&A

Labels

enhancement

2 participants

Events

✓ righettod Marked an Answer 1w

◉ riramar Closed as resolved 1w