CSP WILDCARD DIRECTIVES + CSP STYLE-SRC unsafe-inline

RISK : Medium

Parameter: Content Security Policy

ATTACK : frame-ancestors 'self' teams.microsoft.com

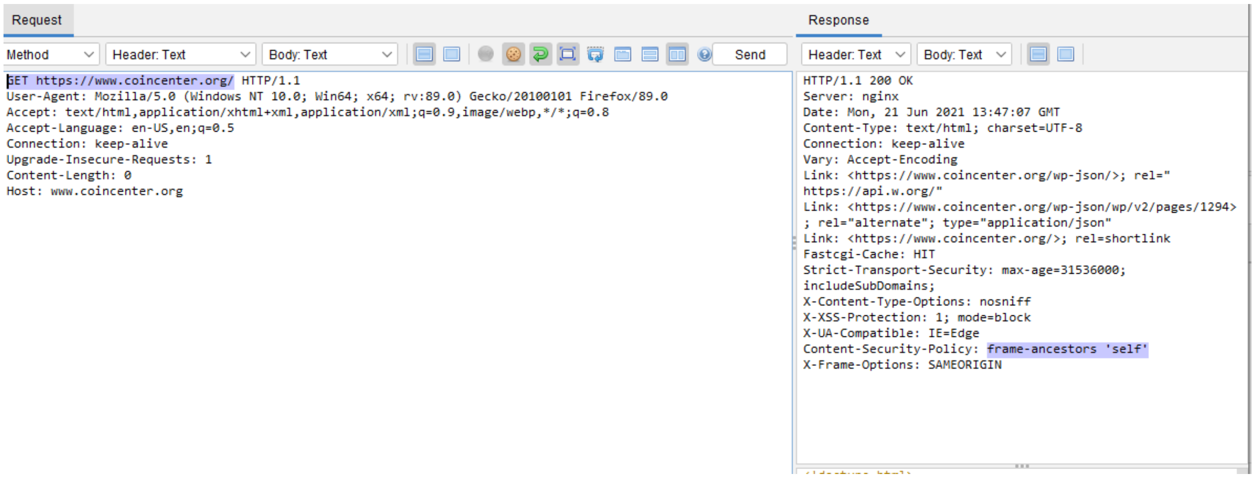
Description:

The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:

script-src, script-src-elem, script-src-attr, style-src, style-src-elem, style-src-attr, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src, form-action

the directive(s): form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

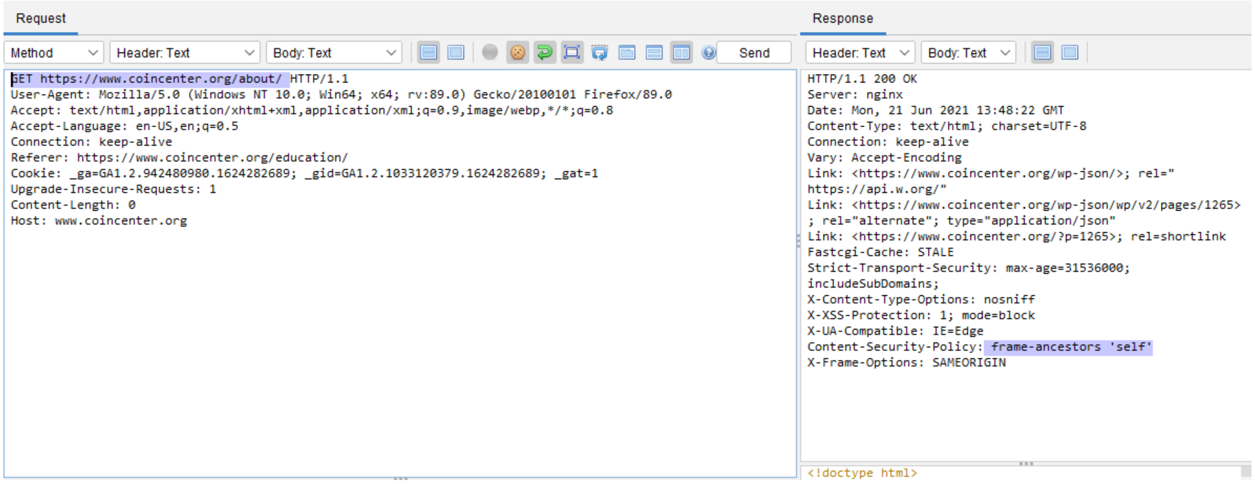
- GET: https://www.coincenter.org/



```
GET https://www.coincenter.org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Length: 0
Host: www.coincenter.org
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Jun 2021 13:47:07 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Link: <https://www.coincenter.org/wp-json/>; rel="
https://api.w.org/"
Link: <https://www.coincenter.org/wp-json/wp/v2/pages/1294>
; rel="alternate"; type="application/json"
Link: <https://www.coincenter.org/>; rel=shortlink
Fastcgi-Cache: HIT
Strict-Transport-Security: max-age=31536000;
includeSubDomains;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-UA-Compatible: IE=Edge
Content-Security-Policy: frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
```

- GET: https://www.coincenter.org/about/

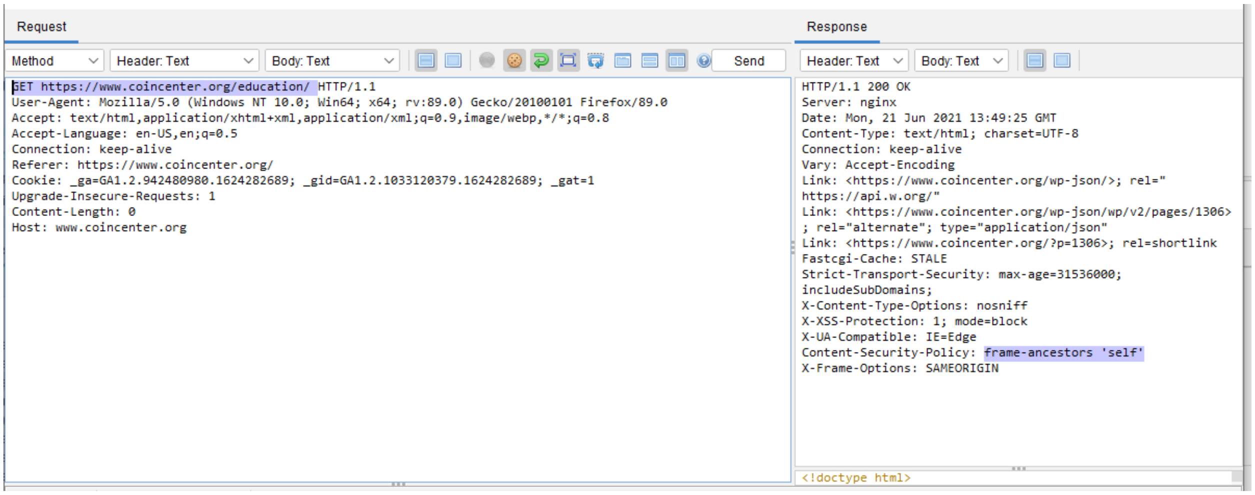


```
GET https://www.coincenter.org/about/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://www.coincenter.org/education/
Cookie: _ga=GA1.2.942480980.1624282689; _gid=GA1.2.1033120379.1624282689; _gat=1
Upgrade-Insecure-Requests: 1
Content-Length: 0
Host: www.coincenter.org
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Jun 2021 13:48:22 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Link: <https://www.coincenter.org/wp-json/>; rel="
https://api.w.org/"
Link: <https://www.coincenter.org/wp-json/wp/v2/pages/1265>
; rel="alternate"; type="application/json"
Link: <https://www.coincenter.org/?p=1265>; rel=shortlink
Fastcgi-Cache: STALE
Strict-Transport-Security: max-age=31536000;
includeSubDomains;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-UA-Compatible: IE=Edge
Content-Security-Policy: frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN

<!doctype html>
```

- GET: https://www.coincenter.org/education/



```
GET https://www.coincenter.org/education/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://www.coincenter.org/
Cookie: _ga=GA1.2.942480980.1624282689; _gid=GA1.2.1033120379.1624282689; _gat=1
Upgrade-Insecure-Requests: 1
Content-Length: 0
Host: www.coincenter.org
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Jun 2021 13:49:25 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Link: <https://www.coincenter.org/wp-json/>; rel="
https://api.w.org/"
Link: <https://www.coincenter.org/wp-json/wp/v2/pages/1306>
; rel="alternate"; type="application/json"
Link: <https://www.coincenter.org/?p=1306>; rel=shortlink
Fastcgi-Cache: STALE
Strict-Transport-Security: max-age=31536000;
includeSubDomains;
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-UA-Compatible: IE=Edge
Content-Security-Policy: frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN

<!doctype html>
```

Solution:

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

References :

http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/

http://caniuse.com/#search=content+security+policy http://content-

security-policy.com/ https://github.com/shapesecurity/salvation

https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources