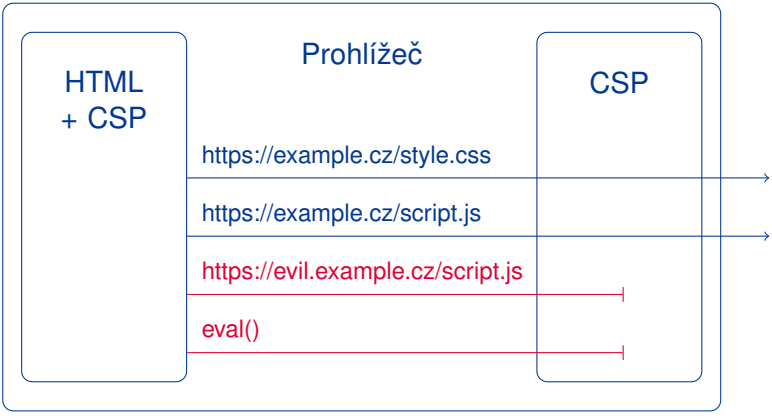
Content Security Policy

Vlastimil Zíma • vlastimil.zima@nic.cz • 24. listopadu 2017

Content Security Policy

- Obrana před XSS apod.
- Vázaný na HTML stránku
-  `https://content-security-policy.com/`
- Level 2, ve vývoji Level 3

Jak to funguje



Základní direktivy

- `script-src` – JS
- `style-src` – CSS
- `object-src` – `<object>` apod.
- `img-src` – obrázky
- `media-src` – audio, video apod.
- `child-src`
  - `frame-src` – `<frame>`, `<iframe>`
  - `worker-src` – `Worker` apod.
- `font-src` – fonty
- `connect-src` – AJAX apod.
- `default-src`

Hodnoty direktiv

- Speciální hodnoty
  - `'self'`
  - `'none'`
  - `*`
  - `'unsafe-inline'` – `<style>`, `style=`, `<script>`, `on*=` apod.
  - `'unsafe-eval'` – `eval`, `setTimeout` a `setInterval`
- Schémata
  - `https:`
  - `data:`
- Zdroje
  - `example.cz`
  - `https://example.cz`
  - `*.example.cz`
  - `example.cz:8000`
- Výjimky pro inline
  - `'nonce-vybrana-hodnota'`
  - `'sha256-base64-hodnota'`

Hlášení

- `report-uri`
- Závislé na prohlížeči
- Zobrazují se v konzoli

```
{"csp-report" : {
    "document-uri" : "https://example.cz/",
    "referrer" : "",
    "blocked-uri" : "https://evil.example.cz/",
    "violated-directive" : "default-src 'self'",
    "original-policy" : "default-src 'self'; report-uri https://example.cz/report/",
    "status-code" : 200,
    "effective-directive" : "style-src",
    "source-file" : "https://example.cz/",
    "line-number" : 31,
    "column-number" : 21
}}
```

Kam s ním

- HTTP hlavička
- HTML `meta` – Level 2+

- `Content-Security-Policy`
- `Content-Security-Policy-Report-Only`
- `X-Content-Security-Policy`
- `X-Content-Security-Policy-Report-Only`

Jak na to

1. `default-src 'none'`
2. Otestovat
3. Opravit kód / CSP

Jak na to

1. `default-src 'none'`
2. Otestovat
3. Opravit kód / CSP

- `eval`, `setTimeout` a `setInterval`
- `<script>`, `on*=` apod.
- `<style>`, `style=` apod.
- `data:` URI

Prokletí sociálních sítí

- Chybí návody
- Pokus-omyl

Prokletí sociálních sítí

- Chybí návody
- Pokus-omyl

Twitter widget

- `<meta name="twitter:widgets:csp" content="on" />`
- `script-src https://platform.twitter.com https://cdn.syndication.twimg.com`
- `style-src https://platform.twitter.com`
- `connect-src https://syndication.twitter.com`

Prokletí sociálních sítí

- Chybí návody
- Pokus-omyl

Facebook +1

- `script-src https://connect.facebook.net`

Prokletí sociálních sítí

- Chybí návody
- Pokus-omyl

Google

- `script-src https://*.googleapis.com` – mapy, překlady, CDN
- `script-src https://*.google.com` – Google+, mapy, reCAPTCHA
- `script-src https://www.gstatic.com` – reCAPTCHA
- `style-src https://fonts.googleapis.com` – fonty v mapách
- `font-src https://fonts.googleapis.com` – fonty v mapách

Naše direktivy

- https://www.nic.cz/, https://www.mojeid.cz/, ...

```
default-src 'self';
script-src 'self' 'unsafe-eval' 'unsafe-inline' https://test-ipv6.nic.cz https://*.test-ipv6.nic.cz
  https://piwik.nic.cz/piwik.js https://platform.twitter.com https://cdn.syndication.twimg.com
  https://s.ytimg.com https://*.googleapis.com https://*.google.com https://connect.facebook.net
  https://*.mapy.cz;
style-src 'self' 'unsafe-inline' https://www.rhybar.cz https://platform.twitter.com https://*.nic.cz
  https://fonts.googleapis.com https://api.mapy.cz;
img-src * data:;
media-src *;
child-src *;
frame-src *;
worker-src 'none';
font-src 'self' https://fonts.gstatic.com;
connect-src 'self' https://*.test-ipv6.nic.cz https://*.labs.nic.cz https://piwik.nic.cz/piwik.php
  https://www.nic.cz/files/CORS/projects-bar/ https://mojeid.cz https://syndication.twitter.com;
report-uri https://csp.nic.cz/report/
```

Naše direktivy

- https://mojeid.cz/

```
default-src 'self';
script-src 'self' https://piwik.nic.cz/piwik.js;
object-src 'none';
img-src * data:;
media-src 'none';
child-src 'none';
frame-src 'none';
connect-src 'self' https://piwik.nic.cz/piwik.php https://www.nic.cz/files/CORS/projects-bar/;
report-uri https://csp.nic.cz/report/
```

Naše CSP

- HTTP server – HTTP hlavičky
- `https://csp.nic.cz/report/`
- `https://github.com/adamalton/django-csp-reports`

Statistiky

- 40 000 zobrazení/den

Statistiky

- 40 000 zobrazení/den
- 110 000 hlášení/den

Statistiky

- 40 000 zobrazení/den
- 110 000 hlášení/den
- 70 % `script-src` se `self` URI

  `"script-sample":"onfocusin attribute on DIV element"`

Statistiky

- 40 000 zobrazení/den
- 110 000 hlášení/den
- 70 % `script-src` se `self` URI

  `"script-sample":"onfocusin attribute on DIV element"`
- 15 % prázdná URI

  ```
  "source-file":"https://mojeid.cz/password_reset/",
  "line-number":19,
  "column-number":26
  ```

Statistiky

- 40 000 zobrazení/den
- 110 000 hlášení/den
- 70 % `script-src` se `self` URI

  `"script-sample":"onfocusin attribute on DIV element"`
- 15 % prázdná URI

  ```
  "source-file":"https://mojeid.cz/password_reset/",
  "line-number":19,
  "column-number":26
  ```
- 10 % `font-src` se `https://sxt.cdn.skype.com/`, `https://fonts.gstatic.com/`, ... URI

Děkuji za pozornost

Vlastimil Zíma • vlastimil.zima@nic.cz