Content Security Policy (CSP)

CSP je bezpečnostní standard implementovaný v moderních webových prohlížečích. Umožňuje majitelům webových stránek deklarovat, které zdroje (např. skripty, styly, obrázky) jsou považovány za důvěryhodné a odkud se smí do prohlížeče načítat. Tím se drasticky snižuje možnost útočníka spustit na webu škodlivý kód, i kdyby se mu ho podařilo do stránky „podstrčit“.

Jak CSP funguje?

CSP funguje na principu „povolujících seznamů“ (whitelisting). Server pošle prohlížeči v hlavičce HTTP odpovědi instrukce, které definují pravidla pro danou stránku. Pokud se prohlížeč pokusí načíst skript z adresy, která není na seznamu, zablokuje jej a nahlásí chybu v konzoli.

Příklad HTTP hlavičky:

```
Content-Security-Policy: default-src 'self'; img-src *; script-src trusted.com
```

* **default-src 'self'**: Všechno se smí načítat pouze z vlastní domény. * **img-src** *: Obrázky se smí načítat odkudkoliv. * **script-src trusted.com**: Skripty se smí načítat pouze z domény `trusted.com`.

Proti čemu CSP chrání?

- **Cross-Site Scripting (XSS):** Zabraňuje spuštění vloženého skriptu (inline script), který útočník poslal v komentáři nebo URL parametru.
- **Clickjacking:** Pomocí direktivy `frame-ancestors` určuje, zda a kde může být stránka vložena do rámce (iframe).
- **Packet Sniffing:** Vynucuje šifrované spojení (HTTPS) pomocí direktivy `upgrade-insecure-requests`.

Hlavní direktivy CSP

Direktiva	Význam
script-src	Definuje povolené zdroje pro JavaScript.
style-src	Definuje povolené zdroje pro CSS soubory.
img-src	Definuje, odkud se smí stahovat obrázky.

Direktiva	Význam
connect-src	Omezuje cíle, na které může web posílat data (např. přes Fetch nebo WebSocket).
frame-ancestors	Určuje, které weby smí tuto stránku vložit do `<iframe>`.

Režim hlášení (Report-Only)

Zavádění CSP na existující velký web je náročné, protože přísná pravidla mohou web „rozbít“. Proto existuje režim **Content-Security-Policy-Report-Only**. V tomto režimu prohlížeč:

```
1. Nic neblokuje.
2. Všechna porušení pravidel pouze nahlásí na zadanou URL (JSON report).
```

Vývojáři tak mohou vyladit pravidla bez rizika pro uživatele.

Proč není CSP všemocné?

- **Složitost:** Nesprávně nastavené CSP může být buď příliš přísné (nefunkční web), nebo příliš volné (neúčinné).
- **Zastaralé prohlížeče:** Velmi staré prohlížeče (např. Internet Explorer) CSP nepodporují nebo jej ignorují.
- **Inline skripty:** Mnoho webů používá kód přímo v HTML (inline). Aby CSP fungovalo správně, musí být tyto skripty přesunuty do souborů nebo označeny speciálním kódem (**Nonce**).

Související pojmy: OWASP, XSS, HTTP, HTTPS, ModSecurity, WAF, Clickjacking.