HTTP hlavičky pro bezpečnější web

Petr Krčmář

13. dubna 2019

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ vpsFree.cz

HTTP hlavičky

- HTTP server posílá v odpovědi klientovi
- metadata pro zobrazení stránky
  - content-encoding, cache-control, date, expires, server…
- bezpečnostní kontext (security headders)
  - jak se má prohlížeč chovat k obsahu
  - umožňuje ovlivnit chování prohlížeče
  - dovoluje vypnout některé vlastnosti
  - nastavit přísnější politiku pro danou stránku
- obecně: rozšiřuje kontrolu ze serveru také na klienta

Nastavení ve web serveru

- web servery umožňují ovlivňovat v konfiguraci

Apache

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

Nginx

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

Lighttpd

```
setenv.add-response-header = ( "Strict-Transport-Security" => "max-age=31536000; includeSubdomains" )
```

ROOT.CZ vpsFree.cz

Jak je prohlédnout

- v prohlížeči v konzoli pro vývojáře: F12 → Network
- ve webovém testu SecurityHeaders.com
- pomocí konzolových nástrojů

```
$ curl -I https://www.example.com/
$ wget -S --spider https://www.example.com
```

Strict-Transport-Security (HSTS)

- zapíná povinné použití HTTPS s důvěryhodným certifikátem
- prohlížeč se naučí na stanovenou dobu
- nespoléhá se pak na přesměrování z 80 na 443
- možné stránku přidat do *preload listu*
- hlavička obsahuje:
  - čas platnosti v sekundách
  - volitelně: zda platí i pro subdomény
  - volitelně: zda je možné provést preload
- problém s certifikátem pak **nelze přeskočit**

```
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
```

ROOT.CZ vpsFree.cz

X-Frame-Options

- zakazuje vkládání stránky do jiných stránek
- brání *clickjackingu* – klikání přes průhlednou vrstvu
- možno zakázat úplně nebo povolit pro vybrané domény

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com
```

X-Content-Type-Options

- zabrání prohlížeči hádat MIME typ
- pokud neobdrží typ dokumentu, může prohlížeč hádat
- může dokonce změnit MIME, pokud se mu *nelíbí*
- každý prohlížeč k tomu přistupuje jinak
  - snadno může vzniknout nekonzistence
  - lze pak podvrhnout spustitelný kód
- touto hlavičkou říkáme, že autor ví, co dělá

```
X-Content-Type-Options: nosniff
```

ROOT.CZ vpsFree.cz

X-XSS-Protection

- zapíná ochranu proti XSS (cross-site scripting attacks)
- prohlížeč nabízí základní ochranu, kterou hlavička vynutí
- hlídá se, zda není kód součástí dotazu (XSS reflection)
- pokud prohlížeč detekuje XSS:
  - odstraní části stránky (výchozí)
  - odmítne stránku zobrazit (block)
- možno posílat JSON reporty na zvolenou adresu
- modernějším řešením je Content-Security-Policy

```
X-XSS-Protection: 0
X-XSS-Protection: 1
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=reporting-uri
```

Referrer-Policy

- ovlivňuje hlavičku Referrer při odkazování
- omezuje úniky údajů z webu v hlavičce
  - brání ve sběru analytickým nástrojům
  - URL se nelogují na cizích serverech
  - identita neuniká na sociální sítě
- hlavičku je možné:
  - zcela potlačit
  - potlačit při přechodu z HTTP na HTTP a naopak
  - omezit jen na doménu
  - posílat v plném rozsahu

```
Referrer-Policy: no-referrer
```

Referrer-Policy možnosti

unsafe-url posílá vždy kamkoliv vše (výchozí)
no-referrer neposílá nikdy nikam nic
no-referrer-when-downgrade neposílá při změně schématu
origin posílá jen doménu bez cesty
strict-origin posílá jen doménu ale ne při downgrade na HTTP
same-origin posílá jen na stejnou doménu
origin-when-cross-origin na stejnou doménu vše, jinam jen doména
strict-origin-when-cross-origin na stejnou vše, při downgrade nic

Feature-Policy

- umožňuje zapnout/vypnout vlastnosti prohlížeče
- týká se různých API pro mikrofon, lokalizaci...
- je možné:
  - zakázat (none)
  - povolit ze stejné domény (self)
  - povolit ze všech domén (*)
  - vyjmenovat zdroje
- porušení pravidel vyvolá hlášení v konzoli

```
Feature-Policy: microphone 'none'; geolocation 'none'
```

ROOT.CZ vpsFree.cz

Feature-Policy možnosti

accelerometer	akcelerometr v mobilních zařízeních
autoplay	automatické přehrávání médií
camera	použití nahrávání z kamery
fullscreen	roztažení na celou obrazovku
geolocation	použití lokalizace prohlížeče
microphone	použití nahrávání z mikrofonu
midi	použití WebMIDI API
payment	použití Payment Request API
vr	použití WebVR API

- existují další a stále přibývají

Content-Security-Policy

- politika pro načítání obsahu z různých zdrojů
- dovoluje web velmi přísně svázat
- velmi mocná a komplexní hlavička:
  - rozlišení podle typu obsahu
  - povolení zdroje podle domény
  - možnost omezit podle schématu (HTTPS)
  - inline objekty možné povolit podle haše/nonce
- nasazení na složitém webu nemusí být snadné
- brání mnoha různým typům problémů
- možné poslat JSON report v případě překročení

```
Content-Security-Policy: default-src https:;
Content-Security-Policy: upgrade-insecure-requests;
Content-Security-Policy: script-src 'self' www.google-analytics.com ajax.googleapis.com;
```

Content-Security-Policy politiky podle typu objektu

default-src	výchozí politika pro všechny
script-src	politika pro skripty
object-src	politika pro object a embed
style-src	politika pro styly
img-src	politika pro obrázky
media-src	politika pro video a audio
frame-src	politika pro vkládání iframes
font-src	politika pro fonty
form-action	politika pro odesílání formulářů
report-uri	adrese pro zasílání reportů

ROOT.CZ vpsFree.cz

Content-Security-Policy možné akce

none	tento objekt nelze načíst
self	pouze ze stejné domény
<domain>	povolení z konkrétní(ch) domén(y)
https:	pouze pomocí bezpečného HTTPS
data:	povoluje vkládat obsah do tagu pomocí Base64
unsafe-inline	dovoluje inline skripty
nonce-...	spustí jen skript se stejným tagem nonce
sha...	spustí jen inline skript s tímto hašem

Odkazy

- SecurityHeaders.com
- OWASP Secure Headers Project
- Mozilla Developer Network
- Root.cz: Bezpečnější web s hlavičkou Content Security Policy

ROOT.CZ vpsFree.cz

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz