Content Security Policy

Nový přístup v boji proti XSS

2011

.cCuMiNn.

Cross Site Scripting (XSS)

- XSS je všudypřítomné
  - výskyt cca v 80% webových aplikací
- Webový browser nevidí rozdíl mezi
  - legitimním skriptem
  - injektovaným skriptem
- Ochrana na straně uživatele
  - blokování JavaScriptu
  - NoScript
  - IE XSS filter

Content Security Policy

- Nový přístup v boji proti XSS
- Jsou zakázány veškeré skripty
- Je zakázáno veškeré načítání obsahu z externích zdrojů
- Vývojáři mohou určit, které zdroje jsou bezpečné, a ze kterých může být externí obsah načítán

Defaultní pravidla CSP

- Zákazáno
  - přímo vložené skripty `<script>`
  - javascript: URIs `<a href="javascript:bad_stuff()">`
  - ovladače událostí `<a onclick="bad_stuff()">`
  - funkce eval() `eval("evil string...")`
  - setTimeout() a setInterval() `setTimeout("evil string...", 1000)`
  - konstruktor new function `var f = new Function("evil string...")`
  - data: URIs `<a href="data:text/html,<script>alert(...">`
  - XBL bindings pro jiné protokoly než chrome: a resource: `-moz-binding` pro navázání CSS

Defaultní pravidla CSP

- Povoleno
  - skripty z def.zdrojů <script src="..."><script>
  - posluchače událostí addEventListener("click", function(), false);
  - setTimeout() a setInterval() setTimeout("function()", 1000)
  - funkční operátory var f = function() {code}
function f() {code}
  - data: URIs pro explicitně povolený druh obsahu

Režimy CSP

– Bezpečnostní politika
  - HTTP hlavičkou

    X-Content-Security-Policy:
  - Prvkem <meta>

    <meta http-equiv="X-Content-Security-Policy">

– Report zpráv s pokusy o narušení
  - HTTP hlavičkou

    X-Content-Security-Policy-Report-Only:
  - Prvkem <meta>

    <meta http-equiv="X-Content-Security-Policy-Report-Only">

Direktivy CSP

- default-src definice defaultně povolených zdrojů
- script-src definice zdrojů pro scripty <script>
- img-src definice zdrojů pro obrázky <img>
- media-src definice zdrojů pro media <video>, <audio>
- object-src definice zdrojů pro objekty <object>, <embed>, <applet>
- frame-src definice zdrojů pro plovoucí rámy <iframe>
- font-src definice zdrojů pro fonty v CSS @font-face
- xhr-src definice zdrojů pro XMLHttpRequest
- style-src definice zdrojů pro stylopisy <link rel="stylesheet">
- frame-ancestors definice zdrojů pro <iframe>, <frame> a <object>
- report-uri definice adres pro zasílání reportů
- policy-uri definice adresy s definicí CSP
- options modifikace některých základních restrikcí CSP

Directiva options

Modifikace základních restrikcí CSP

disable-xss-protection

- povolení přímo vložených scriptů <script>
- povolení javascript: URIs

eval-script

- povolení funkce eval()
- povolení stringů u funkcí setTimeout() a setInterval()
- povolení konstruktoru new Function

Formát zápisu povolených zdrojů

- Uvedením zdroje
  - protokol (volitelně) http://, https://, ftp://
  - hostname www.host.cz
    .host.cz *.host.cz
  - port (volitelně) .host.cz:443
- klíčové slovo
  - stejný host, protokol a port ‘self‘
  - zákaz všech zdrojů ‘none‘
- data: img-src data:

Příklady použití CSP

- Povolení načítání dat pouze ze stejného zdroje, jako pochází chráněný dokument

  X-Content-Security-Policy: default-src 'self'

- Defaultně povolen stejný zdroj dat, obrázky odkudkoliv, objekty a skripty z vyjmenovaných zdrojů

  X-Content-Security-Policy: default-src 'self'; img-src *; \
  object-src media.example.com .host.com; \
  script-src trustedscripts.example.com

Reporty při pokusu o narušení

- Jsou definovány jako JSON objekt
- Jsou odesílány metodou POST
- Jsou odesílány na URI definované v request-uri
- Direktivy reportu
  - request: request line z HTTP požadavku
  - request-headers: hlavičky HTTP požadavku
  - blocked-uri: zablokované URI
  - violated-directive: direktiva způsobující blokování
  - original-policy: zdroj bezpečnostní politiky

Ukázka reportu


```
{
  "csp-report":  {
      "request": "GET http://example.org/page.html HTTP/1.1",
      "request-headers": "Host: example.org
                          User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0b12pre)
                                      Gecko/20110222 Firefox/4.0b12pre
                          Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                          Accept-Language: en-us,en;q=0.5
                          Accept-Encoding: gzip, deflate
                          Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
                          Keep-Alive: 115
                          Proxy-Connection: keep-alive
                          Cache-Control: max-age=0",
      "blocked-uri": "http://evil.example.com/image.png",
      "violated-directive": "default-src http://example.org"
    }
}
```

Závěr

- Ve stádiu draftu
- Funkční jen v prohlížečích, které CSP podporují
- V současné chvíli podpora jen ve Firefoxu 4
- Snaha o standardizaci
- Nutná implementace do webových aplikací
- Hackeři mají ještě pár let ring volný
- V případě širšího nasazení dokáže vymýtit XSS