常用的 CSP 指令如下

2020年4月24日　　下午 01:33

- default-src
  預設所有類型的載入都使用這個規則。
  - connect-src
    載入 Ajax、Web Socket 套用的規則。
  - font-src
    載入字型套用的規則。
  - frame-src
    載入 IFrame 套用的規則。
  - img-src
    載入圖片套用的規則。
  - media-src
    載入影音標籤套用的規則。如：<audio>、<video>等。
  - object-src
    載入非影音標籤物件套用的規則。如：<object>、<embed>及<applet>等。
  - script-src
    載入 JavaScript 套用的規則。
  - style-src
    載入 Stylesheets (CSS) 套用的規則。
  - report-uri
    當瀏覽器發現 CSP 安全性問題時，就會提報錯誤給 report-uri 指定的網址。
    若使用 Content-Security-Policy-Report-Only 就需要搭配 report-uri。
    強烈建議使用回報功能，當被 XSS 攻擊時才會知道。

其他 CSP 指令可以參考 W3C 的 CSP 規範。

每個 CSP 指令可以限制一個或多個能發出 Request 的位置，設定參數如下：

- `*`
  允許對任何位置發出 Request。
  如：`default-src *;`，允許載入來自任何地方、任何類型的資源。
- `'none'`
  不允許對任何位置發出 Request。
  如：`media-src 'none';`，不允許載入影音標籤。
- `'self'`
  只允許同網域的位置發出 Request。
  如：`script-src 'self';`，只允許載入同網域的 `*.js`。
- URL
  指定允許發出 Request 的位置，可搭配 `*` 使用。
  如：`img-src http://cdn.johnwu.cc https:;`，只允許
  從 http://cdn.johnwu.cc 或其他 HTTPS 的位置載入 `*.css`。