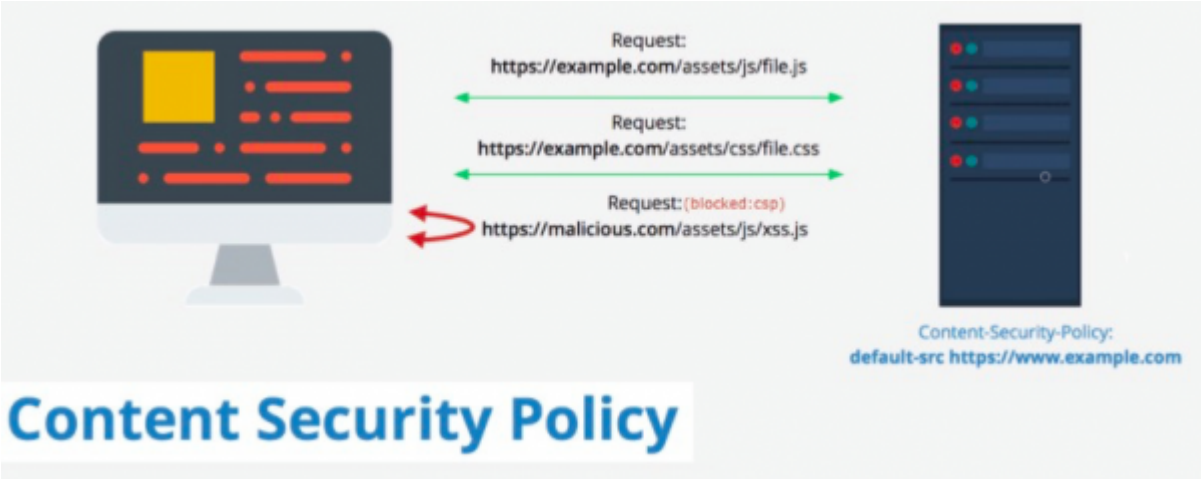
CSP(Content Security Policy)

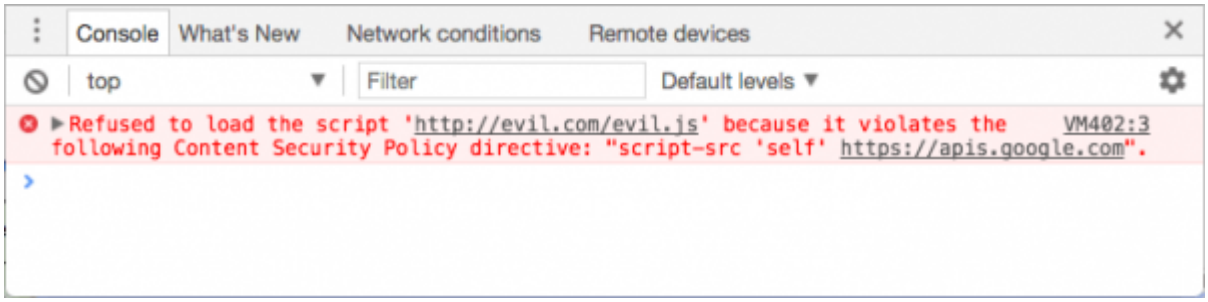
- description : CSP(Content Security Policy)로 콘텐츠 보안 정책 설정하기
- author : 와프
- email : iyyeo@repia.com
- lastupdate : 2021-10-08

개요



- 콘텐츠 보안 정책(CSP: Content Security Policy)이란 교차 사이트 스크립팅(XSS) 공격과 데이터 삽입 공격을 막기 위한 추가적인 브라우저 보안 계층입니다.

- 사용자들이 많이 사용하는 브라우저는 대부분 CSP를 지원하고 있습니다.



- CSP 헤더 혹은 태그를 전달받은 사용자의 브라우저는 다음과 같이 작동합니다.
  1. 유효한 도메인으로 지정한 도메인의 스크립트만 실행하여 XSS 위험성을 제거합니다.
  2. 허용 목록에 있는 도메인에서 수신한 스크립트만 실행하며, 그 외 스크립트는 무시합니다.
- CSP에서 설정한 내용을 위반하는 내용이 호출되면 브라우저는 그것을 차단하고 차단 내역을 알려줍니다.
- CSP는 콘텐츠를 다운로드하여 실행하는 도메인을 제한하지만 다른 보안 헤더들과 같이 사용하면서 더 높은 보안 강도를 추구할 수 있습니다. ☞ Strict-Transport-Security 헤더를 사용하여 암호화된 채널만 사용하도록 설정.

사용방법

- CSP를 사용하는 방법은 어렵지 않습니다. 웹 서버의 응답 헤더에 Content-Security-Policy 헤더를 추가하도록 설정하거나 HTML에 <meta> 태그를 사용하여 추가할 수 있습니다.

```
<헤더 방식>
Content-Security-Policy: 설정할 정책 내용

<태그 방식>
<meta http-equiv="Content-Security-Policy" content="default-src 'self'; img-
src https://*; child-src 'none';">
```

- CSP 문법은 다음과 같습니다. 웹 페이지가 사용하는 하위 도메인을 파악하고 웹 서버에 설정합니다. 추후 서드 파티 스크립트의 원치 않는 도메인 호출을 막을 수 있습니다.

```
#모든 콘텐츠는 현재 도메인에서만 제공되어야 한다.
Content-Security-Policy: default-src 'self'

#신뢰할 수 있는 특정 도메인과 그것의 모든 하위 도메인의 콘텐츠를 허용한다.
Content-Security-Policy: default-src 'self' *. trusted.com

#이미지는 모든 도메인, 미디어와 스크립트는 특정 도메인만 허용한다.
Content-Security-Policy: default-src 'self'; img-src *; media-src media1.com
media2.com; script-src userscripts.example.com

#콘텐츠 다운로드는 기본적으로 HTTPS를 사용하는 특정 도메인만 사용한다.
Content-Security-Policy: default-src https://onlinebanking.mybank.com
```

Tip

스크립트 리소스가 가장 명백한 보안 위험이지만, CSP는 페이지가 로드하도록 허용되는 리소스를 상당히 세분화하여 제어할 수 있는 다양하고 충분한 정책 지시문을 제공합니다. 다음은 나머지 리소스 지시문입니다.

- `base-uri`는 페이지의 <base> 요소에 나타날 수 있는 URL을 제한합니다.
- `child-src`는 작업자와 삽입된 프레임 콘텐츠에 대한 URL을 나열합니다. 예: child-src https://youtube.com을 사용하면 다른 출처가 아니라 YouTube에서 가져온 동영상을 삽입할 수 있습니다. 지원 중단된 frame-src 지시문 대신 이 지시문을 사용하세요.
- `connect-src`는 (XHR, WebSockets 및 EventSource를 통해) 연결할 수 있는 출처를 제한합니다.
- `font-src`는 웹 글꼴을 제공할 수 있는 출처를 지정합니다. font-src https://themes.googleusercontent.com을 통해 Google의 웹 글꼴을 사용할 수 있습니다.
- `form-action`은 <form> 태그에서의 제출을 위해 유효한 엔드포인트를 나열합니다.
- `frame-ancestors`는 현재 페이지를 삽입할 수 있는 소스를 지정합니다. 이 지시문은 <frame>, <iframe>, <embed> 및 <applet> 태그에 적용됩니다. 이 지시문은 <meta> 태그에서 사용할 수 없고 HTML 이외의 리소스에만 적용됩니다.
- `frame-src`는 지원 중단되었습니다. child-src 를 대신 사용하세요.
- `img-src`는 이미지를 로드할 수 있는 출처를 정의합니다.
- `media-src`는 동영상과 오디오를 제공하도록 허용되는 출처를 제한합니다.
- `object-src`는 플래시와 기타 플러그인에 대한 제어를 허용합니다.
- `plugin-types`는 페이지가 호출할 수 있는 플러그인의 종류를 제한합니다.
- `report-uri`은 콘텐츠 보안 정책 위반 시 브라우저가 보고서를 보낼 URL을 지정합니다. <meta> 태그에서는 이 지시문을 사용할 수 없습니다.
- `style-src`는 script-src에서 스타일시트에 해당합니다.
- `upgrade-insecure-requests`는 사용자 에이전트에 URL 구성표를 다시 작성하여 HTTP를 HTTPS로 변경하도록 지시합니다. 이 지시문은 다시 작성해야 할 이전 URL이 많은 웹사이트를 위한 것입니다.

Troubleshooting

Ref

- 콘텐츠 보안 정책
- CSP로 웹사이트의 콘텐츠 보안 정책 설정하기

와프, csp, cdn, 보안정책, security

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=wiki:javascript:csp&rev=1647230908

Last update: **2022/03/14 13:08**