CSP(Content Security Policy)

- description : CSP(Content Security Policy)
- author :
- email : iyyeo@repia.com
- lastupdate : 2021-10-08

- (CSP: Content Security Policy) (XSS)

- CSP

- CSP
    1. XSS
    2. ,
- CSP

- CSP
    . ☞ Strict-Transport-Security

- CSP Content-Security-Policy
  HTML <meta>

```
<       >
Content-Security-Policy:

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

- CSP .

.   .

```
#                                                   .
Content-Security-Policy: default-src 'self'

#                                                          .
Content-Security-Policy: default-src 'self' *. trusted.com

#                   ,                                    .
Content-Security-Policy: default-src 'self'; img-src *; media-src media1.com
media2.com; script-src userscripts.example.com

#                               HTTPS                        .
Content-Security-Policy: default-src https://onlinebanking.mybank.com
```

Tip

, CSP
.
.

- `base-uri`   `<base>`   URL   .
- `child-src`   URL   . : `child-src`
  https://youtube.com   YouTube
  .   `frame-src`   .
- `connect-src` (XHR, WebSockets   EventSource   )   .
- `font-src`   . `font-src`
  https://themes.googleusercontent.com   Google   .
- `form-action`   `<form>`   .
- `frame-ancestors`   .   `<frame>`,
  `<iframe>`, `<embed>`   `<applet>`   .   `<meta>`
      HTML   .
- `frame-src`   . `child-src`   .
- `img-src`   .
- `media-src`   .
- `object-src`   .
- `plugin-types`   .
- `report-uri`   URL   . `<meta>`
  .
- `style-src`   `script-src`   .
- `upgrade-insecure-requests`   URL   HTTP
  HTTPS   .   URL
  .

Troubleshooting

Ref

- - [CSP](#)

  , [csp](#), [cdn](#), , [security](#)

From:
http://rwiki.repia.com/ - . - 2023.12

Permanent link:
http://rwiki.repia.com/doku.php?id=wiki:javascript:csp&rev=1647230908

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