There is a better way

Content Security Policy with React WebApp

Meetup OWASP

10 Septembre 2020

There is a better way

01

Content Security Policy

02

React

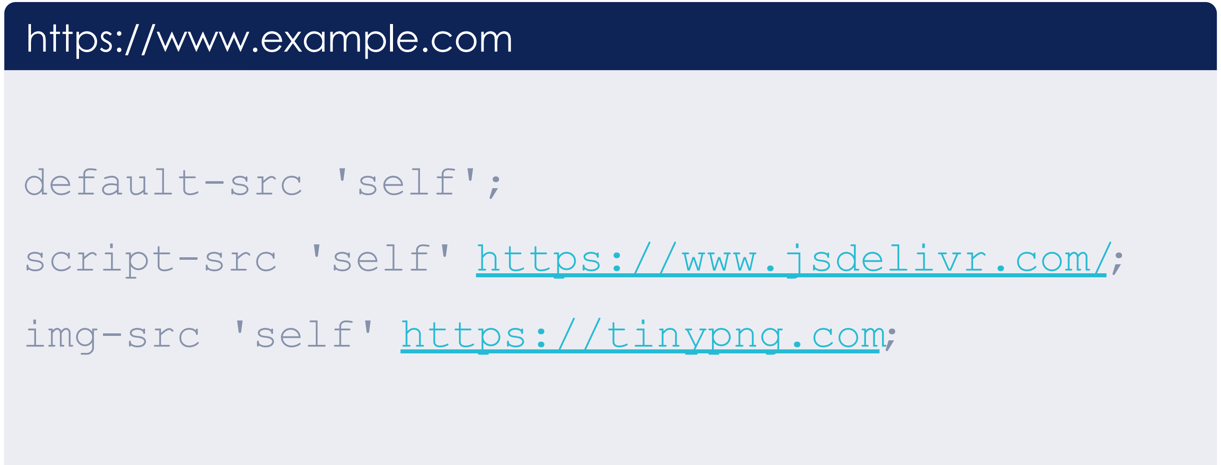
There is a better way

01

Content Security Policy

Content Security Policy

OBJECTIF:
La Content Security Policy est une entête HTTP permettant de définir les interactions entre les ressources d’une page web.



https://www.example.com

```
default-src 'self';
script-src 'self' https://www.jsdelivr.com/;
img-src 'self' https://tinypng.com;
```

Unsafe inline

https://www.example.com/index.html

```
<script>
    // JavaScript Code
</script>
```

Content Security Policy

```
script-src 'unsafe-inline';
```

Le **JavaScript Inline** est largement **exploité** par les attaques **XSS**.

Il ne faut pas autoriser **~~unsafe-inline~~**

There is a better way

There is a better way

02

React

React

OBJECTIF:
React est un framework Javascript pour construire des Single Page Application.

- Scaffold

```
npx create-react-app my-app
```

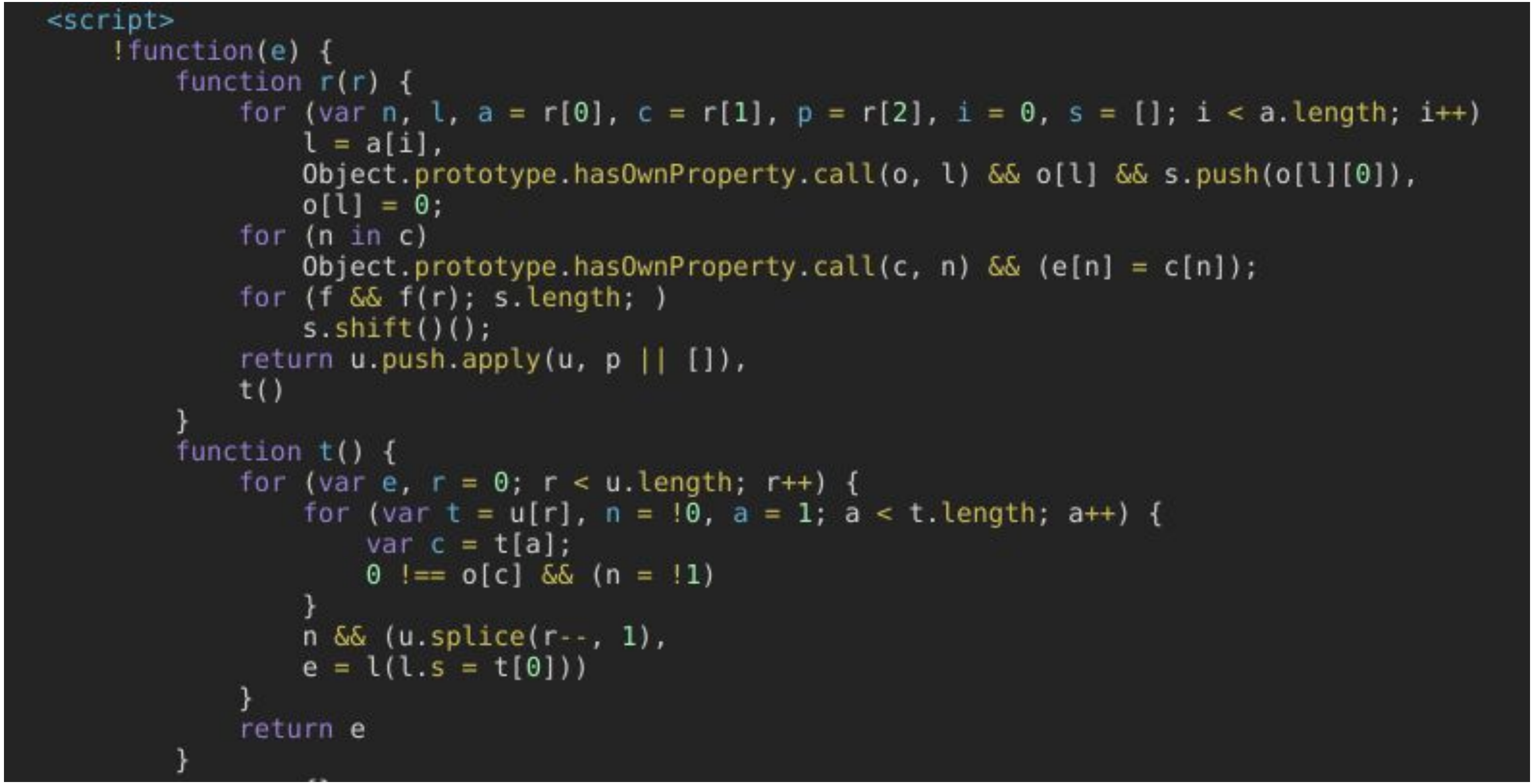
- Build

```
npm run build
```

- Serve

```
npx serve -s build
```

There is a better way

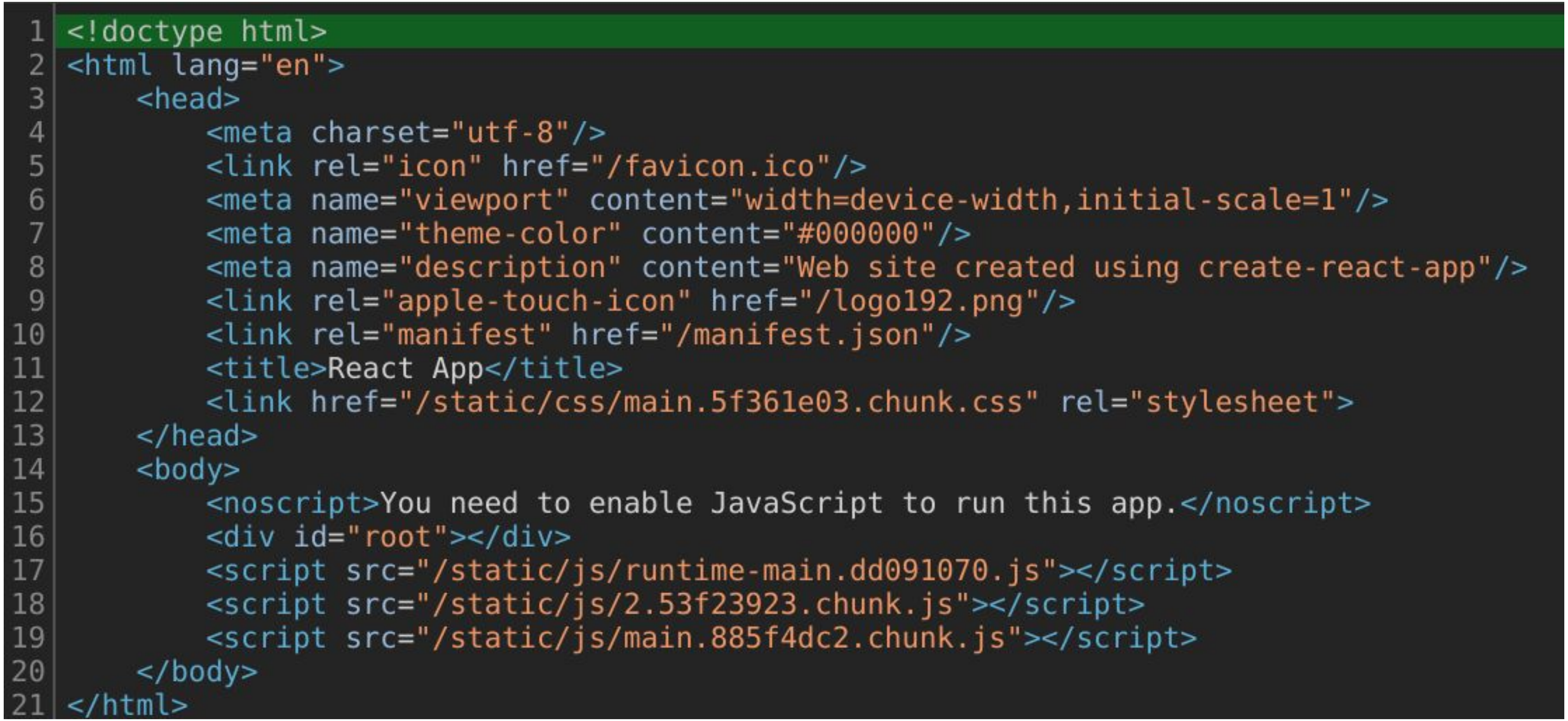


```
<script>
    !function(e) {
        function r(r) {
            for (var n, l, a = r[0], c = r[1], p = r[2], i = 0, s = []; i < a.length; i++)
                l = a[i],
                Object.prototype.hasOwnProperty.call(o, l) && o[l] && s.push(o[l][0]),
                o[l] = 0;
            for (n in c)
                Object.prototype.hasOwnProperty.call(c, n) && (e[n] = c[n]);
            for (f && f(r); s.length; )
                s.shift()();
            return u.push.apply(u, p || []),
            t()
        }
        function t() {
            for (var e, r = 0; r < u.length; r++) {
                for (var t = u[r], n = !0, a = 1; a < t.length; a++) {
                    var c = t[a];
                    0 !== o[c] && (n = !1)
                }
                n && (u.splice(r--, 1),
                e = l(l.s = t[0]))
            }
            return e
        }
```

… et voila du Inline JavaScript !

React without Inline Javascript

```
INLINE_RUNTIME_CHUNK=false react-scripts build
```



```html
<!doctype html>
<html lang="en">
    <head>
        <meta charset="utf-8"/>
        <link rel="icon" href="/favicon.ico"/>
        <meta name="viewport" content="width=device-width,initial-scale=1"/>
        <meta name="theme-color" content="#000000"/>
        <meta name="description" content="Web site created using create-react-app"/>
        <link rel="apple-touch-icon" href="/logo192.png"/>
        <link rel="manifest" href="/manifest.json"/>
        <title>React App</title>
        <link href="/static/css/main.5f361e03.chunk.css" rel="stylesheet">
    </head>
    <body>
        <noscript>You need to enable JavaScript to run this app.</noscript>
        <div id="root"></div>
        <script src="/static/js/runtime-main.dd091070.js"></script>
        <script src="/static/js/2.53f23923.chunk.js"></script>
        <script src="/static/js/main.885f4dc2.chunk.js"></script>
    </body>
</html>
```

Le JS inline à disparu !!!

React

Basic Content Security Policy

```
<meta
  http-equiv="Content-Security-Policy"
  content="
    connect-src 'self';
    default-src 'none';
    img-src 'self';
    manifest-src 'self';
    script-src-elem 'self';
    style-src-elem 'self';
">
```

There is a better way

There is a Better Way