BEGINNER'S GUIDE TO **WEB SECURITY**

Gokulakrishnan Kalaikovan

Table of Contents

Table of Contents

Content Security Policy (CSP)

05. Content Security Policy (CSP)

What is Content Security Policy?

The content security policy, also known as CSP, is an HTTP response header that adds more security to the web applications from attacks like Cross Site Scripting, Data Injection, etc. To configure this, we need to add this header to the response for each request in the web server. We can also enable it on the client-side by adding HTML meta tag element in the web page.

CSP HTTP Header

```
Example: Content-Security-Policy: default-src 'self'; report-uri <url-to-report>
```

With the above header, we are asking the web browser to load content from its origin. For example, if a script tag is loaded from a CDN, a violation report will be sent to the specified URL.

HTML Meta Tag

```
Example: <meta http-equiv="Content-Security-Policy" content="default-src 'self'">
```

Using the above meta tag, we ask the web browser to accept resources like script tags, and stylesheet only from its origin (excluding its sub-domains). There are limitations to the number of CSP headers we can add via meta tags. A full list of the supported meta tags can be found here.

Report only mode in CSP

CSP HTTP headers also support report only mode, but it is supported only via HTTP headers. If the report only mode is enabled, the web browser will not enforce the policy; rather, it will send the violation as a report to the specified URL when such violation occurs.

Let's say we are serving our application from https://example.com, and we have set the HTTP header like the following.

```
Example: Content-Security-Policy: default-src "none"; script-src cdn.com, report-uri "https://reports.example.com"
```

05. Content Security Policy (CSP) > Report Only Mode in CSP

HTML:

```
<!DOCTYPE html>
<html>
   <head>
     <title>Sign Up</title>
     <script src="./main.js"></script>
   </head>
   <body>
       <!-- Content -->
   </body>
</html>
```

Do you think the above webpage will download and execute the main.js script file? The answer is no.

As per our CSP HTTP response header, we are configuring that there is no default source for any resources, and the only source for the script tags is from cdn.com. But in the above example, the webpage is trying to load the main.js script file from its own origin.

Hence it cannot load the file, and a violation will be thrown. The above violation will be sent to https://reports.example.com URL as per our header as POST request along with blocker-uri, violated directive, and original-policy details.

Example: Violation report

```
  {
    "csp-report": {
      "document-uri": “http://example.com/index.html",
      "referrer": "",
      "blocked-uri": “http://example.com/main.js",
      "violated-directive": "script-src cdn.com",
      "original-policy":
        "default-src 'none'; script-src cdn.com; report-uri report.com"
     }
}
```

05. Content Security Policy (CSP) > Browser Support

As of today, the content security policy headers is supported in most of the web browsers. Except for IE 10 and IE 11, which has only partial support.

Browser Support for CSP

CSP Policy Level 1:

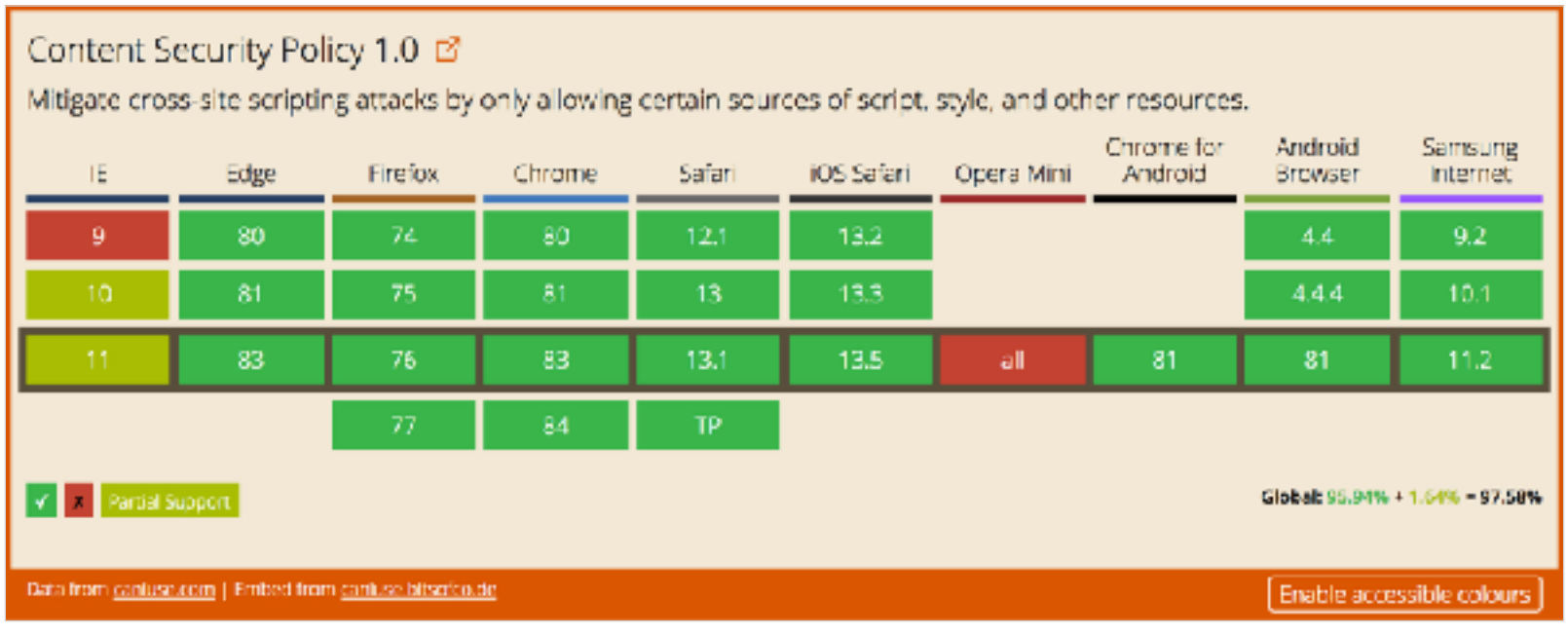

Figure 13: Content Security Policy Level 1 (2012)

CSP Policy Level 2:

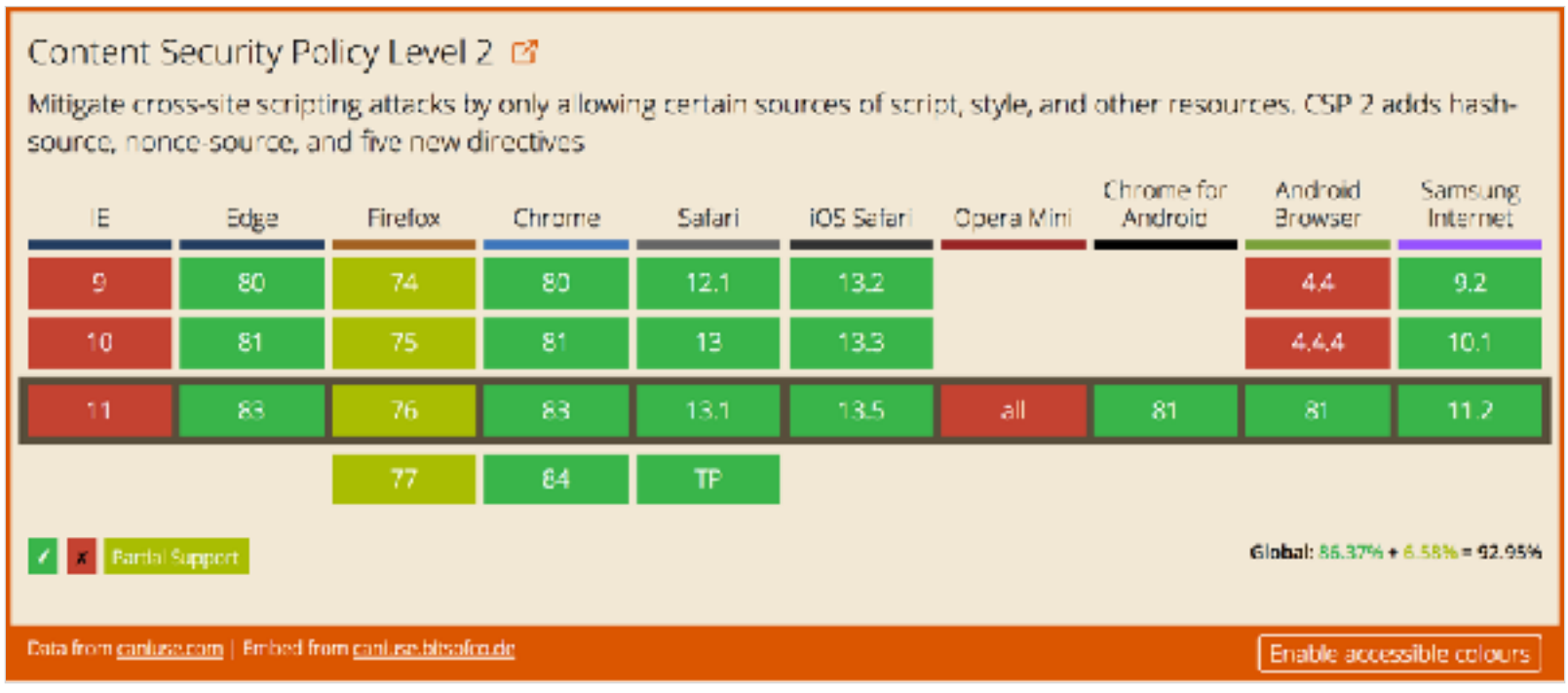

Figure 14: Content Security Policy 2 (2016)

Thanks for taking time to read this free chapter. If you like it, go to the website and purchase it.

And share it with your friends and colleagues.