Content Security Policy 1.0 is officially awesome.

By Mike West

Mike is a contributor to Web**Fundamentals**

It's official! The W3C has advanced the Content Security Policy 1.0 specification from Working Draft to Candidate Recommendation, and issued a call for implementations. Cross-site scripting attacks are one step closer to being (mostly) a thing of the past.

Chrome Canary and WebKit nightlies now support the unprefixed `Content-Security-Policy` header, and will be using the prefixed `X-WebKit-CSP` header to begin experimenting with some new behavior that's being specified as part of Content Security Policy 1.1. Instead of writing:

```
  X-WebKit-CSP: script-src 'self'; object-src 'none'
```

You'll write:

```
Content-Security-Policy: script-src 'self'; object-src 'none'
```

We expect other browser vendors to follow suit within the next few revisions, so it's a great idea to start sending the canonical header today.

Content Securawhat?

Content Security Policy! It helps you reduce the risk of cross-site scripting and other content injection attacks in your applications. It's a huge step forward in terms of the protection you can offer your users, and we highly recommend taking a hard look at implementing it. You can get all the details in the ever so cleverly named "An Introduction to Content Security Policy".

Last updated July 2, 2018.