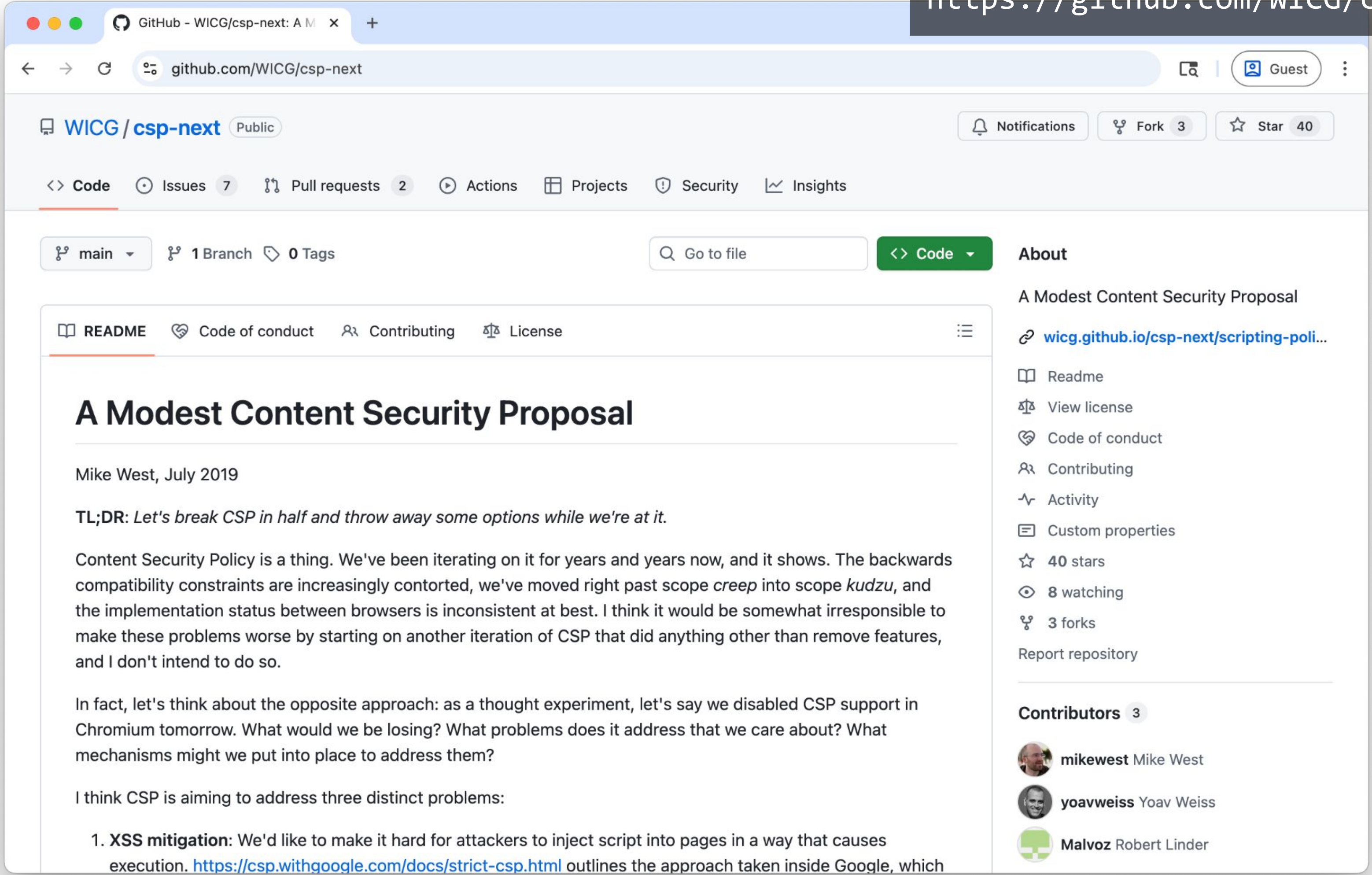
Exfiltration Mitigation

Mike West - TPAC 2025

TL;DR: Developer have a reasonable desire to mitigate the risk of data leakage.

We should provide them with a tool focused on addressing *that* threat.

https://github.com/WICG/csp-next



A Modest Content Security Proposal

Mike West, July 2019

TL;DR: *Let's break CSP in half and throw away some options while we're at it.*

Content Security Policy is a thing. We've been iterating on it for years and years now, and it shows. The backwards compatibility constraints are increasingly contorted, we've moved right past scope *creep* into scope *kudzu*, and the implementation status between browsers is inconsistent at best. I think it would be somewhat irresponsible to make these problems worse by starting on another iteration of CSP that did anything other than remove features, and I don't intend to do so.

In fact, let's think about the opposite approach: as a thought experiment, let's say we disabled CSP support in Chromium tomorrow. What would we be losing? What problems does it address that we care about? What mechanisms might we put into place to address them?

I think CSP is aiming to address three distinct problems:

1. **XSS mitigation**: We'd like to make it hard for attackers to inject script into pages in a way that causes execution. https://csp.withgoogle.com/docs/strict-csp.html outlines the approach taken inside Google, which

About

A Modest Content Security Proposal

wicg.github.io/csp-next/scripting-poli...

- Readme
- View license
- Code of conduct
- Contributing
- Activity
- Custom properties
- 40 stars
- 8 watching
- 3 forks

Report repository

Contributors 3

mikewest	Mike West
yoavweiss	Yoav Weiss
Malvoz	Robert Linder

https://github.com/mikewest/anti-exfil

Regarding exfiltration:

- CSP's model is too granular.
- CSP's syntax is not granular enough.
- CSP's coverage is incomplete.

```
default-src blob: 'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net *.whatsapp.com whatsapp.com
*.whatsapp.net whatsapp.net *.facebook.net facebook.net;

script-src *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'nonce-1HuSTfsU' blob: 'self'
connect.facebook.net 'wasm-unsafe-eval' *.whatsapp.com whatsapp.com *.whatsapp.net whatsapp.net
facebook.net;

style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' *.whatsapp.com whatsapp.com *.whatsapp.net
whatsapp.net *.facebook.net facebook.net;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net
wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob:
*.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com *.whatsapp.com
whatsapp.com *.whatsapp.net whatsapp.net facebook.net;

font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com *.whatsapp.com whatsapp.com *.whatsapp.net
whatsapp.net *.facebook.net facebook.net;

img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com
fbcdn.net connect.facebook.net blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com
*.whatsapp.com whatsapp.com whatsapp.net *.facebook.net facebook.net https://trustly.one/
https://*.trustly.one/ https://paywithmybank.com/ https://*.paywithmybank.com/;

media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data:
*.whatsapp.com whatsapp.com *.whatsapp.net whatsapp.net *.facebook.net facebook.net;

child-src data: blob: 'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net *.whatsapp.com whatsapp.com
*.whatsapp.net whatsapp.net *.facebook.net facebook.net;frame-src *.facebook.com *.fbsbx.com fbsbx.com
data: www.instagram.com *.fbcdn.net accounts.meta.com *.accounts.meta.com *.whatsapp.com whatsapp.com
```

```
default-src blob: 'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net *.whatsapp.com whatsapp.com
*.whatsapp.net whatsapp.net *.facebook.net facebook.net;

script-src *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'nonce-1HuSTfsU' blob: 'self'
connect.facebook.net 'wasm-unsafe-eval' *.whatsapp.com whatsapp.com *.whatsapp.net whatsapp.net
facebook.net;

style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' *.whatsapp.com whatsapp.com *.whatsapp.net
whatsapp.net *.facebook.net facebook.net;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net
wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob:
*.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com *.whatsapp.com
whatsapp.com *.whatsapp.net whatsapp.net facebook.net;

font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com *.whatsapp.com whatsapp.com *.whatsapp.net
whatsapp.net *.facebook.net facebook.net;

img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com
fbcdn.net connect.facebook.net blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com
*.whatsapp.com whatsapp.com whatsapp.net *.facebook.net facebook.net https://trustly.one/
https://*.trustly.one/ https://paywithmybank.com/ https://*.paywithmybank.com/;

media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data:
*.whatsapp.com whatsapp.com *.whatsapp.net whatsapp.net *.facebook.net facebook.net;

child-src data: blob: 'self' https://*.fbsbx.com *.facebook.com *.fbcdn.net *.whatsapp.com whatsapp.com
*.whatsapp.net whatsapp.net *.facebook.net facebook.net;frame-src *.facebook.com *.fbsbx.com fbsbx.com
data: www.instagram.com *.fbcdn.net accounts.meta.com *.accounts.meta.com *.whatsapp.com whatsapp.com
```

https://github.com/mikewest/anti-exfil

```
Connection-Allowlist:
  ("https://{*.}?fbcdn.net" "https://{*.}?facebook.net"
   "https://{*.}?fb.com" "https://{*.}?fbsbx.com"
   "https://{*.}?whatsapp.com" ...); report-to=group
```

Open Questions

1. Is it actually worth building something like this when CSP is *right there* (mikewest/anti-exfil#2)?

2. How do we deal with redirects?

3. What inheritance model makes sense (mikewest/anti-exfil#1)?

4. How much of URLPattern's syntax is necessary (see compression dictionaries, Service Worker's static routing, etc)?