Making CSP work for you

Making CSP work for you

@mr_goodwin

Me (and why I'm here)

- I am Mark Goodwin
- I work for Mozilla on security (platform, Firefox & web)
- I want to improve web security
- CSP is underused :(

A plan for the talk

- Talk about... XSS
- ... CSP (what, why?)
- ... why CSP is awkward
- ... making it less awkward
- ... some common mistakes

Let's talk about XSS

- Reflected
- Stored
- DOM

Click!

Let's talk about CSP

- Content Security Policy
- It's a policy...
- ... to secure content

example

```
Content-Security-Policy:
default-src 'self'; object-src 'none';
report-uri: 'http://example.com/report
```


CSP in action

- Modern browsers applying CSP to browser UI
- FirefoxOS - uses CSP for all privileged apps

Awesome!... but...

- We have exiting content
- Defaults are restrictive
- Too relaxed - pointless
- CSP is awkward
- What can we do?

Fixing things (a bit)

- Newer library versions (e.g. jquery)
- Frameworks gaining support (e.g. Django)
- CSP has gained new features
- Better tools

CSP 1.1 features

- nonce-source
- hash-source
- can be used in creative ways (demo)
- There are still limitations

Better tools

- UserCSP
- Hash generation tools
- ... and many others

Common Mistakes

- Policy too relaxed
- Policy inconsistently applied
- Info leakage via report-uri

End!

- Questions?
- Contact:
  Twitter: @mr_goodwin
  irc: mgoodwin on
  irc.mozilla.org