W3C WebAppSec WG update

websec WG
tlr@w3.org

Chartering status

- Proposed co-chairs: Rescorla, Hill
- Charter under review by W3C Advisory Committee until 19 August
- Relevant requirements work in draft-hodges-websec-framework-reqs

Deliverables

- CORS & UMP: Policy-expression for cross-origin XMLHttpRequest
- CSP: “content restrictions for a web resource”
- Secure Cross-Domain Framing

Cross-Origin Authorizations

- CORS, UMP (W3C Webapps, W3C Webappsec)
  - “you can access my data if your origin is foo.com”
  - use case: XMLHttpRequest
- X-Frame-Options (websec)
  - “you can frame me if your origin is bar.com, or if you’re same-origin”
  - use case: frame protection

Cross-Origin Authorizations

- Timing-Allow-Origin (W3C Web Performance WG)
  - “you can access timing information about me if you’re coming from baz.com”
  - use case: mitigate timing attacks
- From-Origin (W3C Webapps WG)
  - “you can embed me if you’re coming from bar.net”
  - use case: limit embedding of resources (fonts, …)
- CSP Secure Cross-Domain Framing (W3C Webappsec WG)
  - “you frame me if you’re coming from baz.org and fulfill the following conditions”
  - use case: unified syntax with other policy expression, ability to articulateadditional conditions

major need for coordination!

CSP

- experimental implementations in Mozilla, Chrome
- experimental deployment: twitter

Next Steps

- Expecting to have WG operational in early September.
- To keep up with updates in detail, subscribe to public-web-security@w3.org.