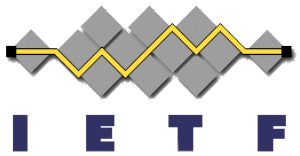
Frame-Options



(draft-gondrom-frame-options-01)

David Ross, Tobias Gondrom

July 2011

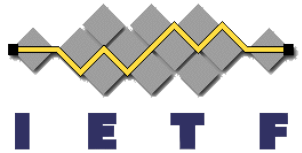
Frame-Options

1. History
2. Use Cases
3. Draft
4. TBD
5. Future steps

Frame-Options - History

- X-Frame-Options widely deployed/used to prevent XSS, CSRF
  - First draft as result from Beijing and OWASP Summit:
  - Running code and (some) consensus by implementers in using X-FRAME-OPTIONS
- HTTP-Header:
  - DENY: cannot be displayed in a frame, regardless of the site attempting to do so.
  - SAMEORIGIN: can only be displayed if the top-frame is of the same “origin” as the page itself.

Frame-Options – Example Use-Cases



- A.1. Shop
  - An Internet Marketplace/Shop link/button to "Buy this" Gadget, wants their affiliates to be able to stick the "Buy such-and-such from XYZ" IFRAMES into their pages.
- A.2. Confirm Purchase Page
  - Onlineshop "Confirm purchase" anti-CSRF page. The Confirm Purchase page must be shown to the end user without possibility of overlay or misuse by an attacker.

Frame-Options - draft

- Frame-Options
  - In EBNF:

Frame-Options = "Frame-Options" ":" "DENY"/ "SAMEORIGIN" / ("ALLOW-FROM" ":" Origin-List)

  - DENY: The page cannot be displayed in a frame, regardless of the site attempting to do so.
  - SAMEORIGIN: can only be displayed in a frame on the same origin as the page itself.
  - ALLOW-FROM: can only be displayed in a frame on the specified origin(s)

6. Frame-Options - TBD

- Allowed framing: only top-level or whole frame chain
- Origin: is not the same as in origin draft (scheme:URI:port)
- Allow-From: one or more origins (parsing)
- Behavior in case of a fail: “No-Frame page”
- Interdependencies with CSP (frame-ancestor)

Frame-Options - Allow-From

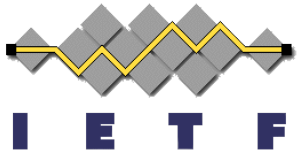
- Allow-From: from only one location
- Reasons:
  1. Privacy of other allowed framing sites
  2. Keep size of http header small
  3. Not to handle on web servers but in application
- Procedure:
- Origin of requesting page will be verified dynamically by the server and answer with matching Allow-From if authorized.

Frame-Options – future steps

- Other approaches:
  - CSP defining framed-by policy: CSP authors indicated to support Frame-Options instead of part of CSP
  - The "From-Origin" draft (aka "Cross-Origin Resource Embedding Exclusion") about half page document appeared a few weeks ago as an FPWD in the W3C Webapps WG: http://lists.w3.org/Archives/Public/public-webapps/2011JulSep/0088.html
    - Includes idea control of other embedded objects like fonts, images.

Frame-Options – future steps

- Do we want to work on this in websec?
- Review volunteers
  - Already received a number of reviews, but more never hurts



Thank you