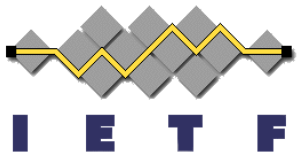
# Frame-Options




**(draft-gondrom-frame-options-02**
**draft-gondrom-x-frame-options-00)**

**David Ross, Tobias Gondrom**
**March 2012**

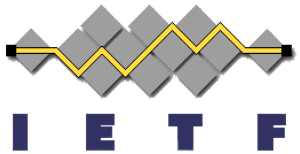
# Frame-Options

1. Background (History, Use Cases)
2. Draft
3. 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 - Drafts

- Two drafts (following discussion at websec at IETF81):
  - draft-gondrom-frame-options-02
    (std moving forward with improvements and clarification, also working complementing with CSP)
  - draft-gondrom-x-frame-options-00
    (informational, documenting the current status of use of X-Frame-Options header)

# Frame-Options

- 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

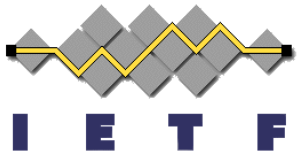
- Updates:
  - allow framing clarified to “AllAncestors”
  - Interdependencies with CSP: no more overlap (frame-ancestor was dropped from CSP will be delivered by Frame-Options)
- TBD:
  - Origin: is not the same as in origin draft (scheme:URI:port)
  - Allow-From: one or more origins (parsing)
  - Behavior in case of a fail: “No-Frame page”

# Frame-Options – Discuss 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

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




# Thank you