

draft-ietf-websec-strict-transport-sec

Jeff “=JeffH” Hodges

IETF-82

Taipei, Taiwan

Recent Progress

- draft-ietf-websec-strict-transport-sec-02 published on 5-Aug-2011
 - Addressed 12 tracker tickets + other minor items
 - Received feedback from various folks on -02 (thanks!)
 - Incorp'd feedback on..
 - STS header ABNF
 - Effective Request URI
 - Referencing IDNA2008
- ..into -03 (published on 31-Oct-2011)

Detailed Status

- Newly submitted tickets (tying up loose ends)..
 - Already addressed in -03..
 - #26: reference IDNA2008 as well as IDNA2003
 - #27: header ABNF is a hybrid of RFC2616 and httpbis
 - To be addressed in -04..
 - #28: spec unclear about the denotation of "HSTS policy"
 - #29: disambiguate "mixed content" term & provide reference
 - #30: add an informational reference to RFC 4732
 - #31: mention case insensitivity for directive names

Overall Status

- Present spec implemented in Firefox and Chrome
 - more coming?
- 80+ web apps issue STS policy
 - per www.shodanhq.com
- LockCA / LockCert / LockFoo directive thoughts subsumed by cert pinning spec effort (IMHO)
 - draft-evans-palmer-key-pinning-00

To Do

- Near-term ToDo's:
 - Put issues in the Tracker – largely done
 - Update spec per remaining tracker tickets
 - Essentially remaining tickets are all clarifications
 - Issue -04 spec in a few weeks
- Further-term steps:
 - Go to WG Last Call ?
 - With -04 spec?