Cookies: HTTP State Management Mechanism
draft-ietf-httpbis-rfc6265bis-08

June 15, 2021

Recent changes: -08 draft version

- Align on HTML terminology for origins
  - Replaced "globally unique identifier" with "opaque origin". (#1416)
- Control characters in `set-cookie-strings`
  - Explicitly specified handling of control characters in `set-cookie-strings` (consistent with current behavior of Chrome). (#1420)
- Cookie retrieval algorithm
  - Refactored retrieval algorithm to support cookie retrieval by non-HTTP APIs, allowing more complete specification of `SameSite` behavior consistent with Firefox and Chrome. (#1428)
- Lax-allowing-unsafe `SameSite` enforcement mode
  - Defined optional "Lax+POST" behavior (implemented by Chrome and Firefox). (#1435)
- User agent cookie policy
  - Defined a user agent's cookie policy and clarified ways in which cookies can be ignored according to the cookie policy. (#1013)
- Editorial fixes
  - #1425, #1469, #1505, #1516, #1527, etc.

Draft issues status

21 open issues:

- Defer/close: "6265bis-defer" label (not in scope, lacks consensus, needs work)
  - #1526, #1430, #1289, #1042, #762, #718, #525, #494, #441
- Investigate interop, define in spec (likely valid issues)
  - #1531, #1517, #1508, #1502, #1418, #1399, #1385, #1340, #1332, #1288, #1210, #1073

Open draft issues by topic

"Investigate interop, define in spec (likely valid issues)" bucket:

- `Cookie` and `Set-Cookie` headers (syntax, parsing, serialization)
  - #1531, #1517, #1502, #1399, #1210, #1073
- Cookie size limits
  - #1340
- Blocking/ignoring cookies; pre-existing invalid cookies
  - #1508, #1418, #1385
- `Domain` attribute
  - #1332
- `SameSite` attribute
  - #1288

Cookie truncation (#1531)

- Recent PR (#1420) specified control character handling while parsing a provided cookie:
  - Truncate at the first CR, LF, or NUL byte.
  - Reject the cookie if there are any other control characters present.
- Truncating in this way may enable an attack:
  - A site may use

    ```
    document.cookie = "before" + attackerControlled + "after";
    ```
  - Attacker can manipulate the cookie value.
- Considering rejecting all cookies containing any control character (rather than truncating).
  - Investigating web compatibility.

Cookie size limits (#1340)

- Current spec text:
  - "General-use user agents SHOULD provide … [the capability of storing] at least 4096 bytes per cookie (as measured by the sum of the length of the cookie's name, value, and attributes)."
- User agents enforce limits differently, providing a fingerprinting mechanism.
  - Chrome: Max 4096 bytes for whole cookie string.
  - Curl: Max 5000 bytes for whole cookie string, max 4096 bytes for name + value.
  - Firefox: Max 4096 bytes for name + value, max 1024 bytes for path.
  - Safari: Max 5000 bytes for whole cookie string.
- Considering standardizing limits:
  - 4096 bytes for name+value, 1024 bytes for each attribute value.
  - Investigating web compatibility.