Security Considerations for Optimistic ~~Use of HTTP Upgrade~~ *Protocol Transitions in HTTP/1.1*

Ben Schwartz, Meta Platforms, Inc.

HTTPBIS @ IETF 121

Changes since IETF 120 (draft 00→01)

- #2821 Add discussion of HTTP CONNECT (including new title)
  - CONNECT and Upgrade have very similar issues, and the document now covers both.
- #2845 Remove all mention of “Upgrade: HTTP/*.*”
  - Deleting that text was easier than trying to figure out whether this token is already deprecated.
- #2827 Recommend using “GET” for Upgrade if the method is not meaningful.
  - This is what we have decided every time to date, so we might as well write it down.
- #2828 Note that TLS is theoretically impossible to misparse as HTTP/1.1.
  - This is mostly a curiosity, but it informs the risk assessment.
- #2820 Mention “connect-ip”.
  - It is safe from these security issues as specified.

Notable new text: HTTP CONNECT

Clients that send HTTP CONNECT requests on behalf of untrusted TCP clients MUST wait for a 2xx (Successful) response before sending any TCP payload data.

To mitigate vulnerabilities from any clients that do not conform to this requirement, proxy servers MAY close the underlying connection when rejecting an HTTP CONNECT request, without processing any further data sent to the proxy server on that connection. Note that this behavior may impair performance, especially when returning a "407 (Proxy Authentication Required)" response.

0\r\n
\r\n