Fetch Streaming Upload Security Privacy Questionnaire

2. Questions to Consider

2.1. What information might this feature expose to Web sites or other parties, and for what purposes is that exposure necessary?

The feature provides an additional way to upload data to an HTTP server. No additional exposure is introduced.

2.2. Is this specification exposing the minimum amount of information necessary to power the feature?

Same above. Regarding the amount of information, there is little difference between this feature and traditional uploading feature (uploading strings/arraybuffers/blobs with fetch()).

2.3. How does this specification deal with personal information or personally-identifiable information or information derived thereof?

This feature doesn't interpret data it uploads. It is up to the application how to handle the data.

This feature is usable only on HTTP/2 and HTTP/3, which means the data is always protected by encryption.

2.4. How does this specification deal with sensitive information?

This feature doesn't interpret data it uploads. It is up to the application how to handle the data.

This feature is usable only on HTTP/2 and HTTP/3, which means the data is always protected by encryption.

2.5. Does this specification introduce new state for an origin that persists across browsing sessions?

No.

2.6. What information from the underlying platform, e.g. configuration data, is exposed by this specification to an origin?

No configuration data is explicitly exposed. Some network conditions can be obtained as side channel information. For example, a malicious developer can use this API to check whether a user is behind a proxy that only speaks HTTP/1.1.

2.7. Does this specification allow an origin access to sensors on a user's device

No.

2.8. What data does this specification expose to an origin? Please also document what data is identical to data exposed by other features, in the same or different contexts.

No additional data is exposed compared to other uploading features with fetch() and XMLHttpRequest.

2.9. Does this specification enable new script execution/loading mechanisms?

No.

2.10. Does this specification allow an origin to access other devices?

No.

2.11. Does this specification allow an origin some measure of control over a user agent's native UI?

No.

2.12. What temporary identifiers might this this specification create or expose to the web?

None.

2.13. How does this specification distinguish between behavior in first-party and third-party contexts?

The specification makes no distinction between any parties that can run script in the context of the document's origin.

2.14. How does this specification work in the context of a user agent's Private \ Browsing or "incognito" mode?

Behaviour is unchanged.

2.15. Does this specification have a "Security Considerations" and "Privacy Considerations" section?

No.

2.16. Does this specification allow downgrading default security characteristics?

No.

2.17. What should this questionnaire have asked?

None known.