Implementing the prerendering content restrictions

Authors: falken@chromium.org
July 2021

Summary

- Tracker: Task tracker
- Bug: https://crbug.com/1158250
- POC: falken@chromium.org
- Channel: #mparch on chromium.slack.com.

Background

The Prerender2 feature introduces prerendering of pages to Chromium. A prerendered pages is loaded and executed in the background. Various web APIs are more restricted in prerendered pages. Examples of restrictions are to throw an error, delay until the prerendered page is activated, or cancel prerendering.

This task is to ensure that the proper restrictions are applied on prerendered content. This involves writing code and end-to-end tests.

See the explainer of desired behavior and the draft specification.

The first step is to take care of web-exposed APIs. Future work can be to work on internal restrictions (navigation throttles and other cancellation reasons).

Mojo capability control

Prerendering automatically defers many APIs by controlling when to bind interfaces requested by the renderer over BrowserInterfaceBroker. See [public] BrowserInterfaceBroker Mojo Interface Control. Due to this mechanism, Chromium often already has the desired behavior, and we just need to add a test to verify it.

What to do

Step 1: Choose an Available entry from the task list.

Step 2: Mark it as Started and add yourself as Owner.

Step 3: Check whether Chromium already matches the behavior in “Decision for Same-origin-triggered Prerender”. See the comment in the spreadsheet for details.

You may need to write a test first, or your own local testing. Enable Prerendering via chrome://flags (#enable-prerender2) or the command line (--enable-features=”Prerender2”). You can trigger prerendering via <link rel=”prerender”>.

Step 4: Write code to make Chromium match the behavior in “Decision for Same-origin-triggered Prerender”, if needed. Once Chromium matches the behavior, write a test. Prefer a test in third_party/blink/web_tests/external/wpt_internal/prerender when possible, or else a browser_test in prerender_browsertest.cc.

Step 5: Submit the CL. You can use https://crbug.com/1158250 as the umbrella bug. If desired, you can also file a new blocking bug for the feature. This can be appropriate for features that require multiple CLs or discussion on the crbug.

Step 6: Update the Methodology, Test Status, Mojo interface, Comments fields on the task list as appropriate.

Step 7: Once the CL is landed and Chromium matches the behavior with a Test, mark the row as Done.

Guide for writing and reviewing CLs

- See the Prerender WPT Style Guide.
- Ensure the CL matches the “Decision for Same-origin-triggered Prerender” column of the spreadsheet.
- Ensure the “Explainer/Spec Status” column of the spreadsheet matches the Decision column.
- Add “Bug: 1158250” or a bug marked as a blocking bug of 1158250, to the commit description.

Reference CLs

- https://chromium-review.googlesource.com/c/chromium/src/+/2730378
    - Broadcast Channel is granted to prerendered pages, so the CL adds a test for that.
- https://chromium-review.googlesource.com/c/chromium/src/+/2717126

    - Local Storage is granted to prerendered pages. Since it is an interface on BrowserInterfaceBroker, the CL needs to update the capability control to grant the interface as well as adding a test.
- https://chromium-review.googlesource.com/c/chromium/src/+/2717845
    - Local File System hangs for prerendered pages.