1 Service Worker

Luan Herrera 在 2019 年提出了基于 service worker 以及 performance API，影响到 Chromium 的攻击[1]。

Performance API（性能接口）让开发者精确地测量网页在用户的设备上的性能。https://www.wbolt.com/performance-api.html https://blog.csdn.net/weixin_47450807/article/details/123951462https://blog.openreplay.com/how-to-evaluate-site-speed-with-the-performance-api。此攻击

攻击过程如下：

1. 安装拦截 range header（字节范围头）为 `bytes=0-` 的请求的 Service Worker。
2. 使用 `audio` 或 `video` 元素向目标资源发出请求，其请求中的字节范围头为 `bytes=0-`。
3. Service Worker 拦截以上的请求，并返回任意内容，长度为 `n` 的响应。Chromium 会再发出类似的请求，类以区别是 `bytes=0-` 变成了 `bytes=n-`。分两种情况：
   (a) 目标资源的大小小于 `n`，则请求失败，服务器返回 `4xx` 状态码，此事件不产生 `PerformanceEntry`
   (b) 目标资源的大小大于 `n`，则请求成功，服务器返回 `2xx` 状态码，此事件产生 `PerformanceEntry`
4. 使用 `performance.getEntries().length` 可以得知当前的请求是否产生了 `PerformanceEntry`，从而可以判断目标资源的大小是否小于 `n`。

（测试包含 service worker 的网站后，为了注销 service worker, 可能需要重启浏览器程序）。

参考文献

[1] HERRERA L. Issue 990849: Leaking size of cross-origin resource by using Range Requests and Service Workers[EB/OL]. (2019-08-06) [2022-08-15]. https://bugs.chromium.org/p/chromium/issues/detail?id=990849.