Ghosts in the Browser::

Backdooring with Service Workers

Emmanuel Law (@libnex)

Claudio Contin (@claudiocontin)

Who We Are

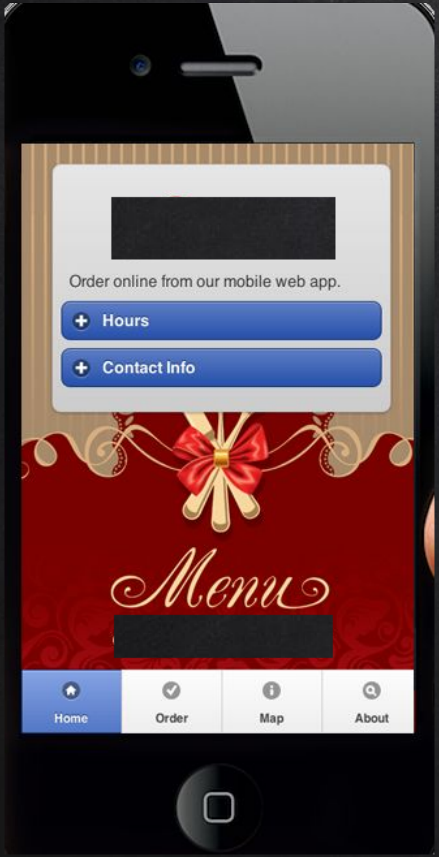
- Claudio Contin – Security Consultant @ ZX SECURITY

- Emmanuel Law (@libnex)

Views presented are of our own and do not reflect that of our employers.

Problem with Exploiting XSS

- ✘ HTTP-Only Flags
- ✘ Cookies have limited server-side lifespan
- ✘ Transient payload
- ✘ IP restrictions

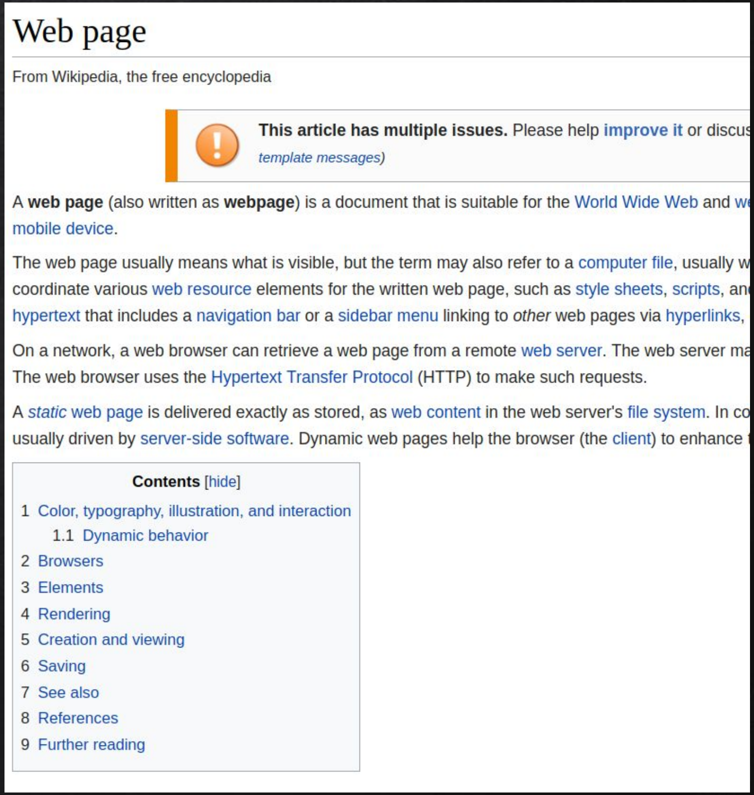


[redacted]

Order online from our mobile web app.

[redacted]

VS



Web page

From Wikipedia, the free encyclopedia

This article has multiple issues. Please help **improve it** or discus

template messages)

A **web page** (also written as **webpage**) is a document that is suitable for the World Wide Web and we

mobile device.

The web page usually means what is visible, but the term may also refer to a computer file, usually w

coordinate various web resource elements for the written web page, such as style sheets, scripts, an

hypertext that includes a navigation bar or a sidebar menu linking to *other* web pages via hyperlinks,

On a network, a web browser can retrieve a web page from a remote web server. The web server ma

The web browser uses the Hypertext Transfer Protocol (HTTP) to make such requests.

A *static* web page is delivered exactly as stored, as web content in the web server's file system. In co

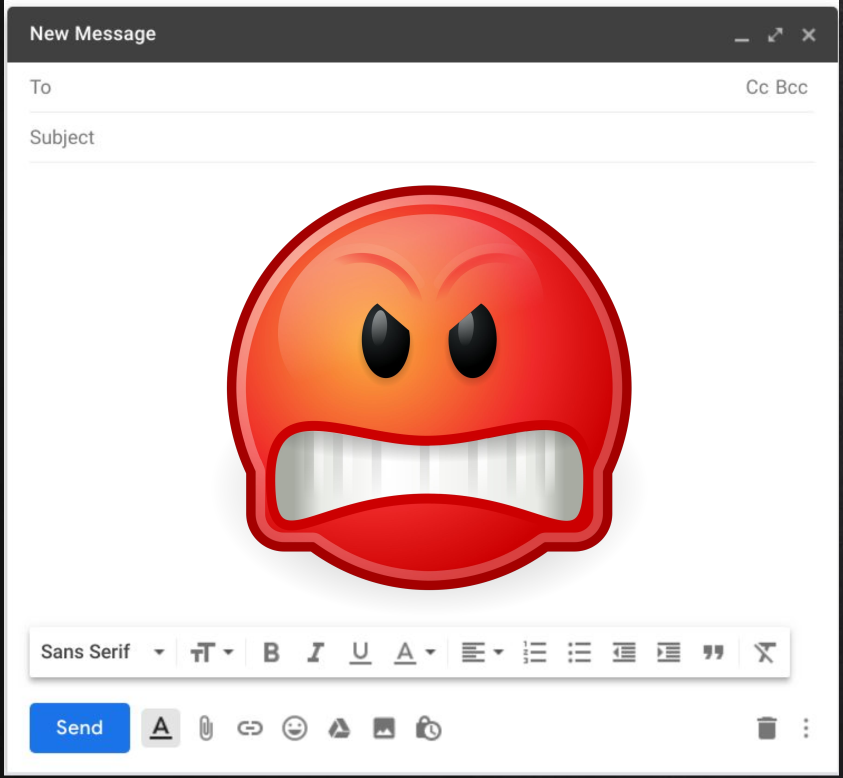
usually driven by server-side software. Dynamic web pages help the browser (the client) to enhance

Contents [hide]

“The introduction of the Service Worker API is one of the most significant improvements to the web in recent history”*

* *https://blog.chromium.org/2018/05/the-state-of-web-at-google-io-2018.html*

Service Workers

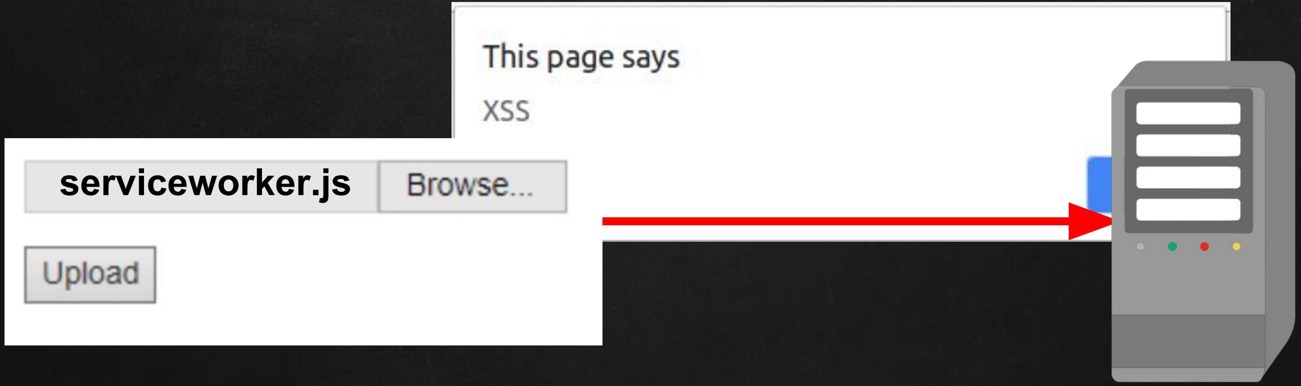


Install a Service Worker

```
navigator.serviceWorker.register('/sw.js')
```

Need Ability To Run JS

Need To Point To a JS File



This page says

XSS

serviceworker.js

Primitives

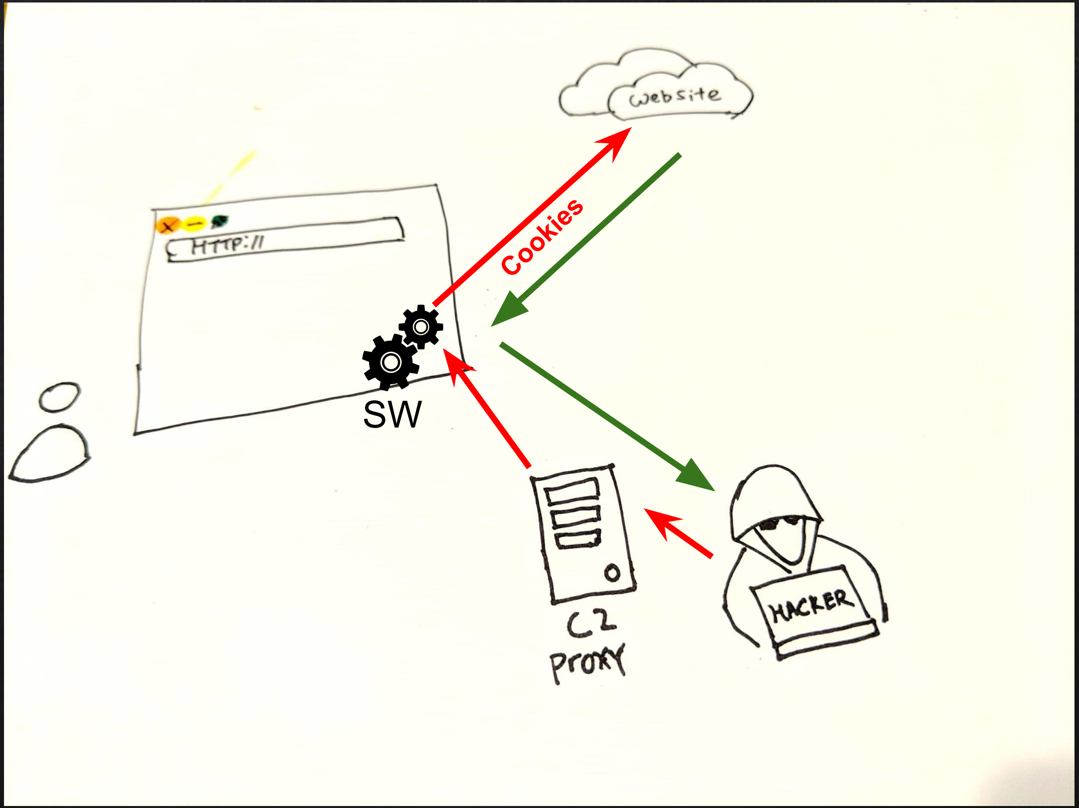
Fetch():

- ✖ Ability to make HTTP requests
- ✖ XMLHttpRequest deprecated in 2015
- ✖ Service Workers only have Fetch API available
- ✖ Bounded to Same Origin Policy rules

Background Sync

- ✘ Typically used to provide offline capabilities
- ✘ 2 Step process:
  - ○ Registering a Sync: `registration.sync.register('mysync');`
  - ○ Listen for Sync Event: `addEventListener('sync', _CALLBACK_);`

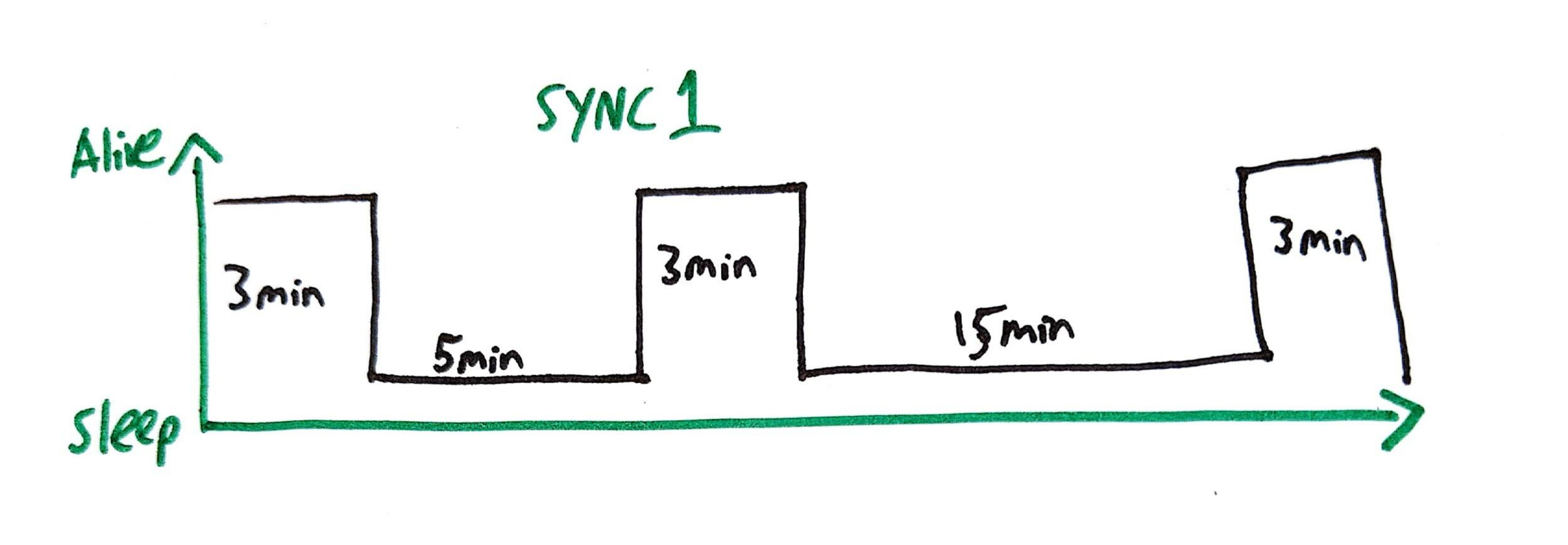
Ghosting through Background Sync

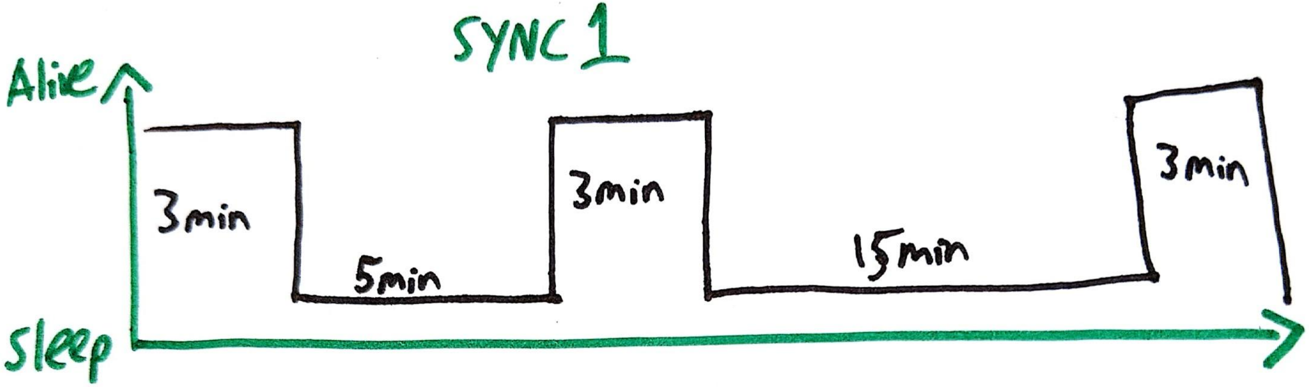


Problem with Background Sync

- ✘ Background Sync Events (Once Off)

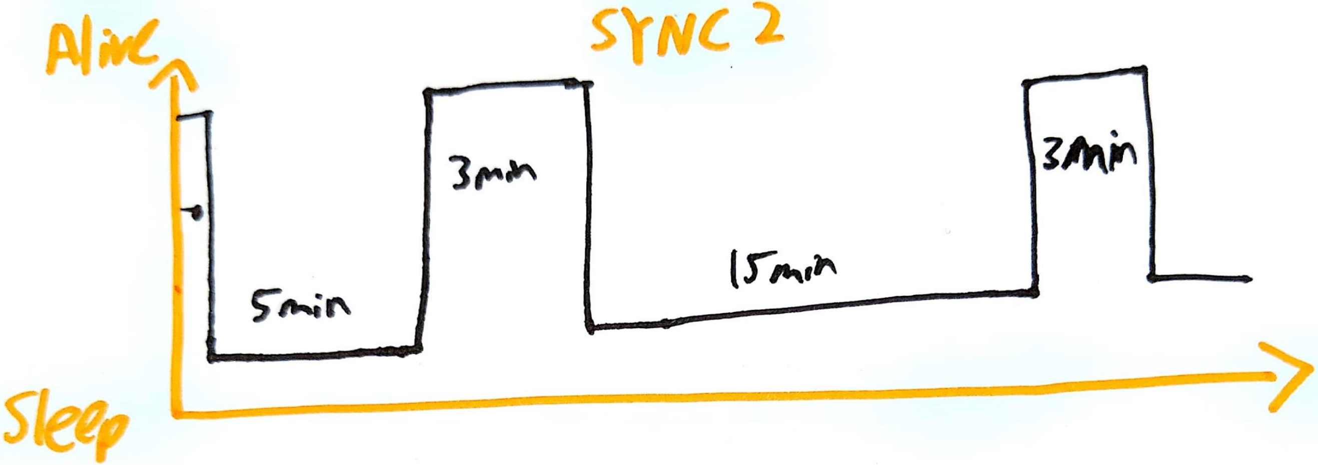
Extending Run Duration





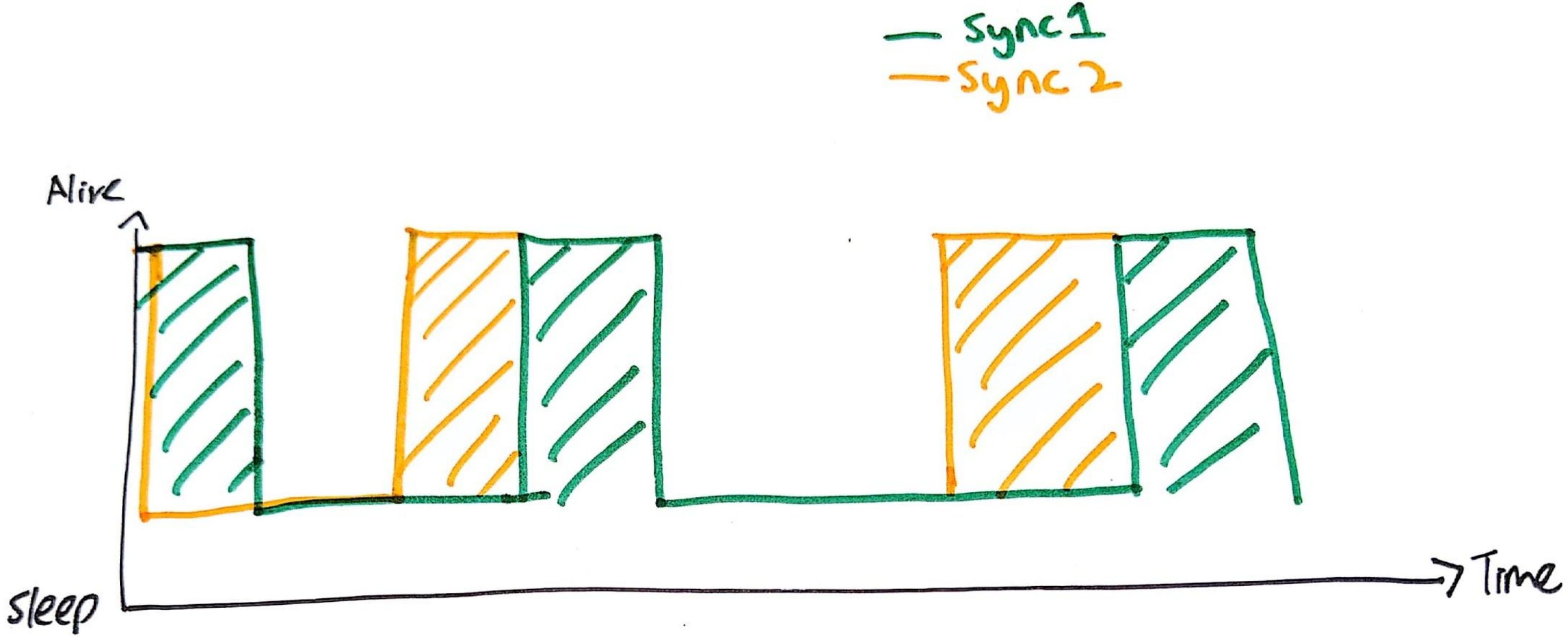
SYNC 1

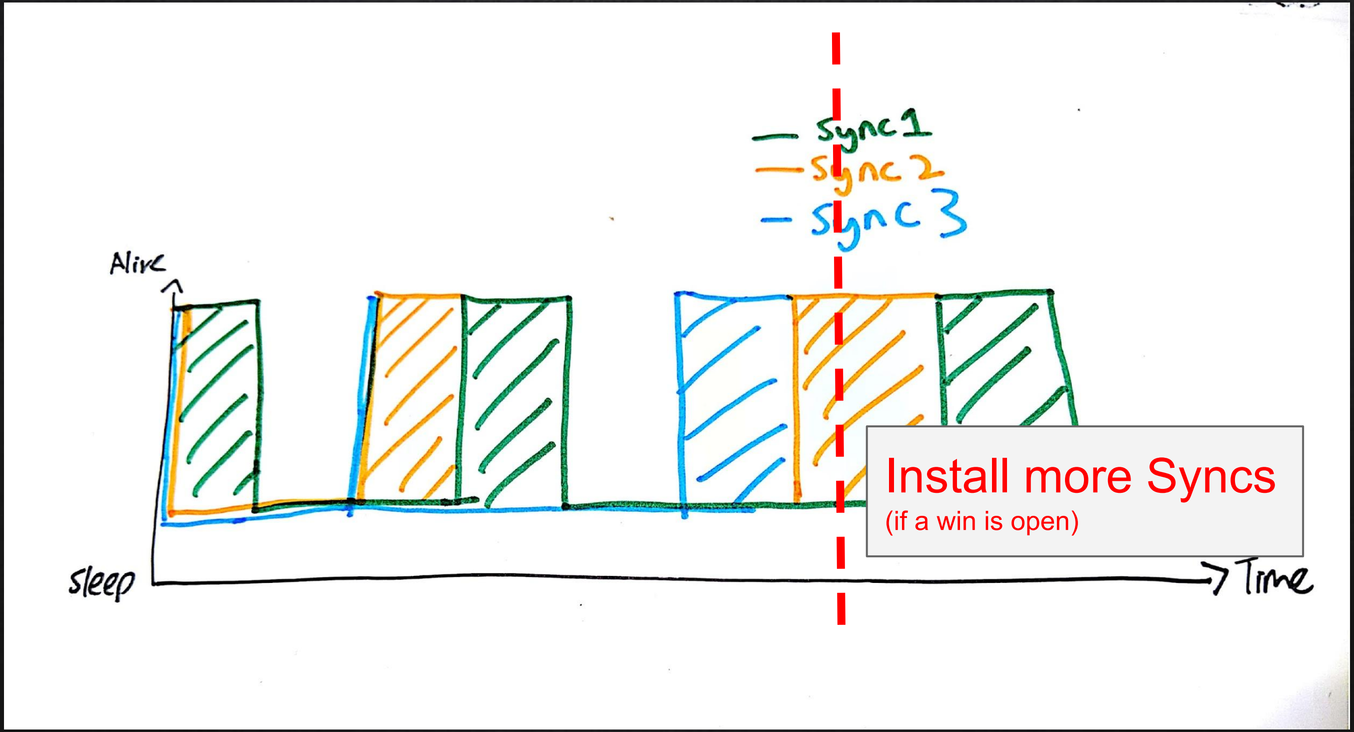
Alive
Sleep
3min
5min
3min
15min
3min



SYNC 2

Alive
Sleep
5min
3min
15min
3Min


— Sync 1
— Sync 2
Alive
Sleep
Time

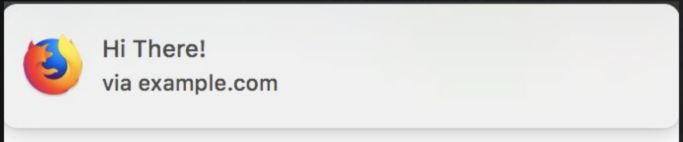


Install more Syncs

(if a win is open)

Push

- ✖ Can we do more?
- ✖ Web Push
  - ○ Notification API



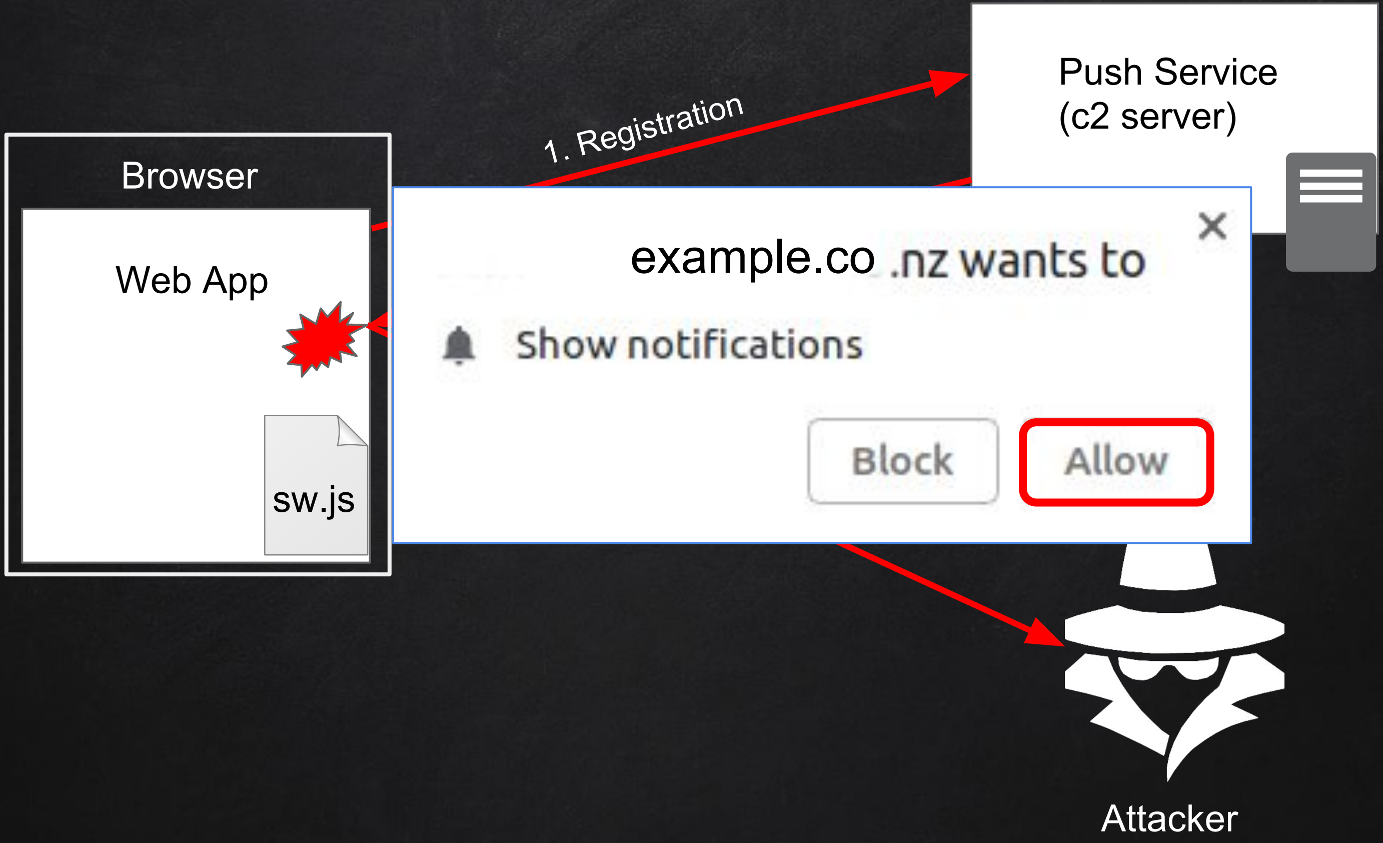
Hi There!
via example.com

```
self.addEventListener('push', function(e){

<Malicious Callback Code >

}); // Alive for ~2 Minutes
```

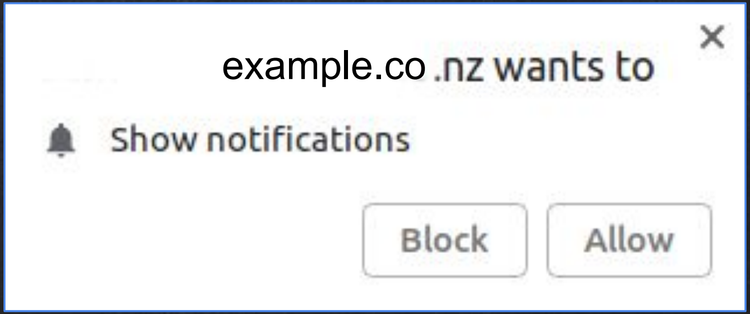
Push



example.co .nz wants to

Show notifications

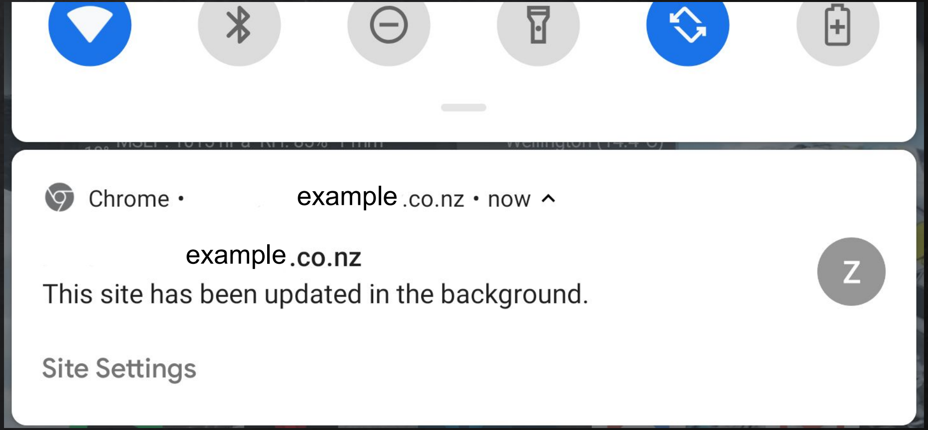
Push



example.co .nz wants to

Show notifications

- PUSH – First 3 Blind
- Desktop: Browser Running
- Mobile: Doesn't Matter

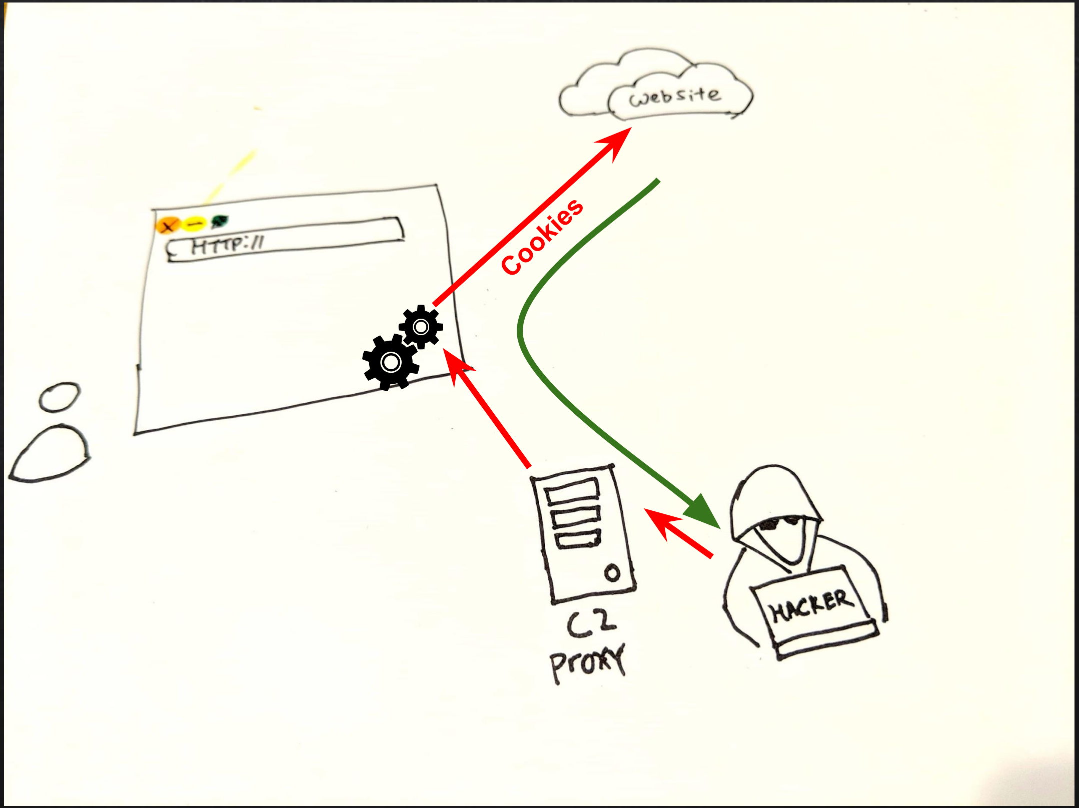


Chrome • example .co.nz • now

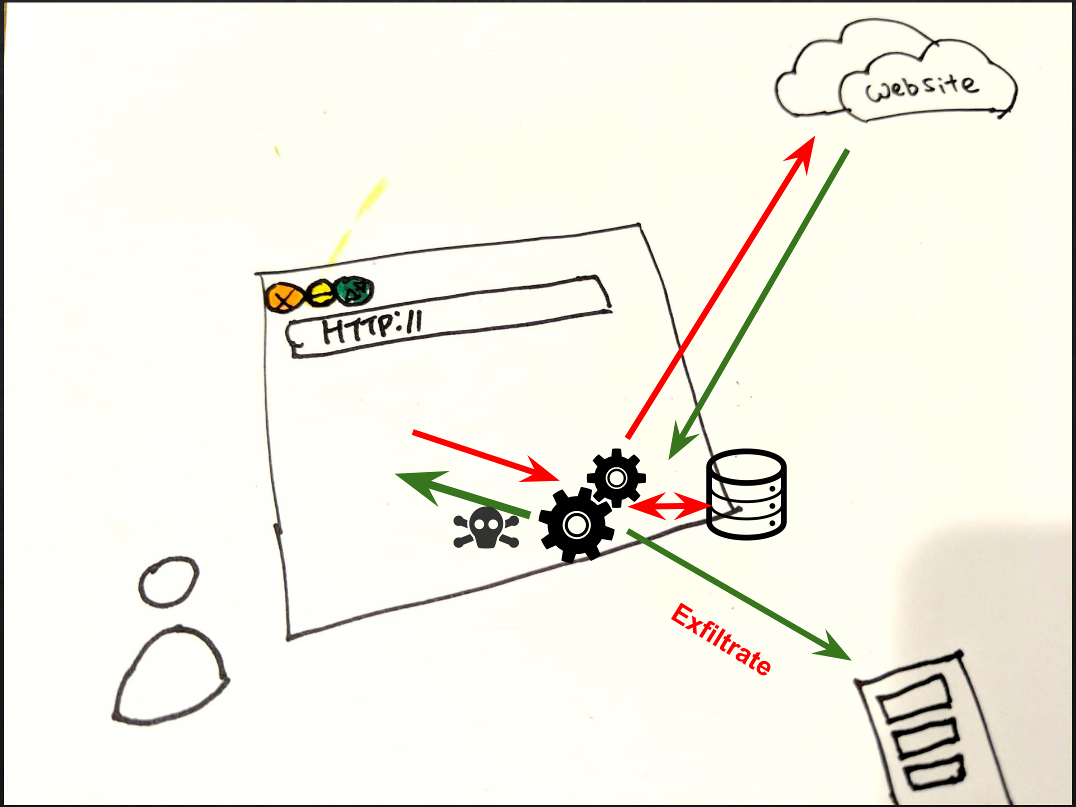
example .co.nz

This site has been updated in the background.

DEMO



Fetch Event



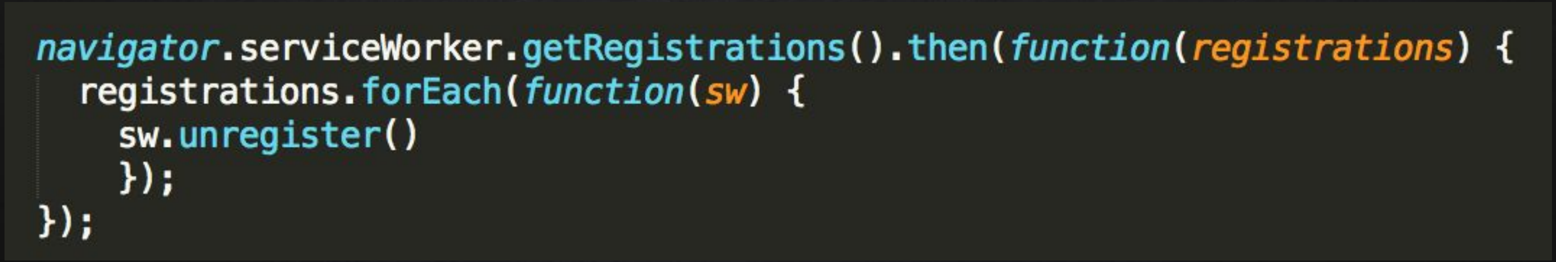
Mitigations

Mitigations (as developer)

- No XSS
  - Content Security Policy
- Disallow JS Upload
- Content-Type: text/plain
  - Everything but *application/javascript*
- Separate Domain to Serve Uploads
- JSONP: Word Characters Only in Callback

✘ SW outlives XSS

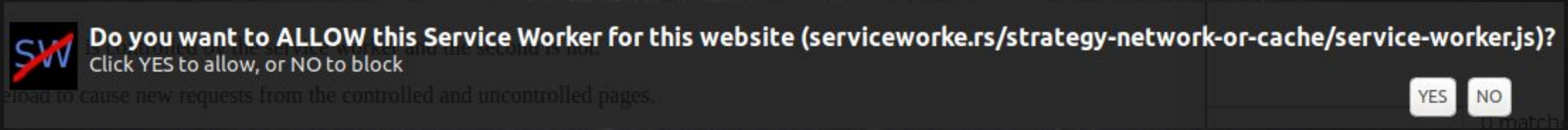
- Fixing the XSS is not sufficient
- Removing the malicious SW.js from server is not sufficient



```
navigator.serviceWorker.getRegistrations().then(function(registrations) {
  registrations.forEach(function(sw) {
    sw.unregister()
    });
});
```

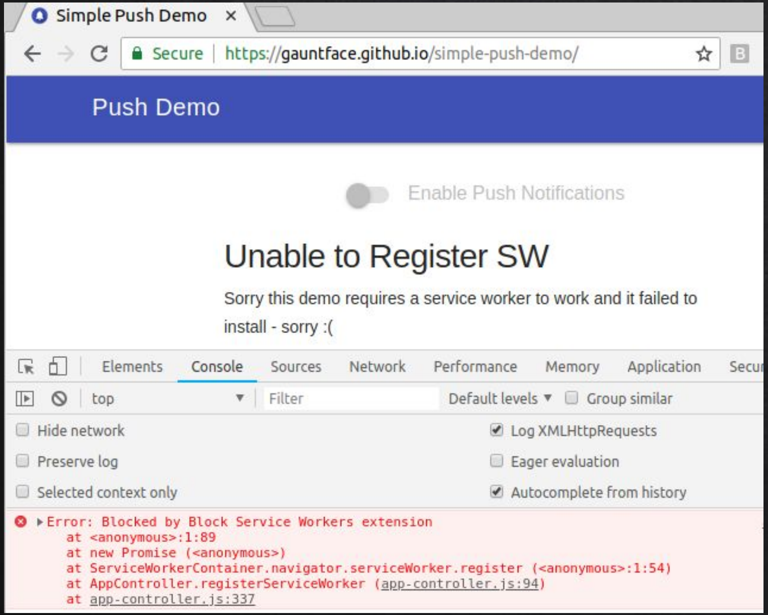
As a user....

Protections – Block Service Workers



Do you want to ALLOW this Service Worker for this website (serviceworke.rs/strategy-network-or-cache/service-worker.js)?

Click YES to allow, or NO to block



Unable to Register SW

Sorry this demo requires a service worker to work and it failed to install - sorry :(

□ Group similar

□ Hide network

□ Preserve log

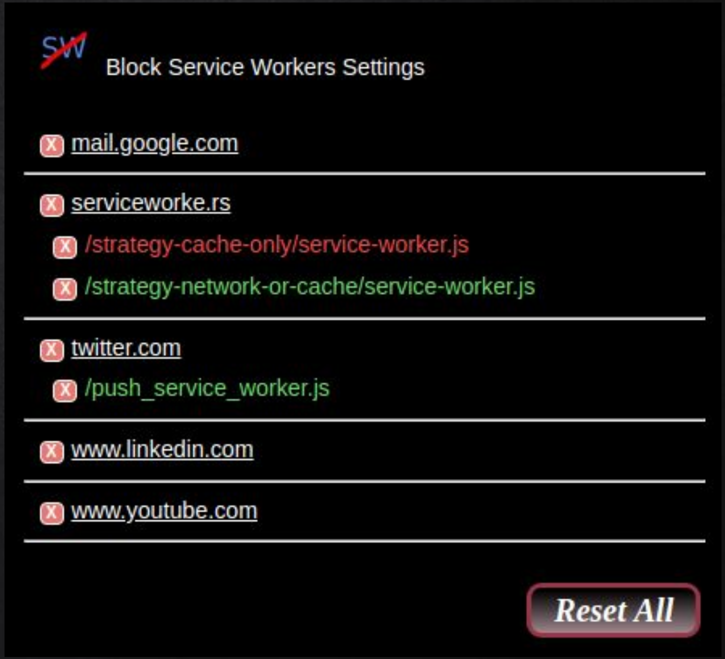
□ Selected context only

☑ Log XMLHttpRequests

□ Eager evaluation

☑ Autocomplete from history

```
Error: Blocked by Block Service Workers extension
    at <anonymous>:1:89
    at new Promise (<anonymous>)
    at ServiceWorkerContainer.navigator.serviceWorker.register (<anonymous>:1:54)
    at AppController.registerServiceWorker (app-controller.js:94)
    at app-controller.js:337
```



Block Service Workers Settings

- mail.google.com
- serviceworke.rs
  - /strategy-cache-only/service-worker.js
  - /strategy-network-or-cache/service-worker.js
- twitter.com
  - /push_service_worker.js
- www.linkedin.com
- www.youtube.com

* https://github.com/clod81/block_service_workers

* https://chrome.google.com/webstore/detail/block-service-workers/ceokjgeibfjfcboemhdpkdalankbmnej

* https://addons.mozilla.org/en-US/firefox/addon/block-service-worker

Summary

- Provides Persistent Access
- Situational
- Service Worker active development
    - Periodic Sync

THANKS

Claudio Contin - @claudiocontin

Emmanuel Law - @libnex