

Chrome Security UI Surface List

contact: lgarron@
visibility: **PUBLIC**
last updated: 2017-05-30
canonical link (for Googlers): go/security-ui

The [Enamel](#) team focuses on security UX, which also involves a lot of [UI](#).
Here's a list of security-related surfaces visible to the user.

This list aims to be comprehensive. Please add a section or a comment if you see something incomplete/inaccurate.

NOTE: This document is not maintained. Consider it a snapshot of security UI during 2015-2017.

[Omnibox](#)

[Origin in the omnibox](#)

[Page security state icon](#)

[Origin Info Bubble \(OIB\)](#)

[Security Summary](#)

[Site data and permissions](#)

[Connection Info](#)

[Page Actions \(right side of omnibox\)](#)

[Active web API permissions](#)

[Blocked web API permissions](#)

[Blocked content settings](#)

[Mixed script shield \(for blocked "active mixed content"\)](#)

[Downloads](#)

[Blocked download in download shelf](#)

[Blocked download in chrome://downloads](#)

[Interstitials](#)

[SSL interstitial](#)

[Malware \(Safe Browsing\) interstitial](#)

[Phishing \(Safe Browsing\) interstitial](#)

[Spoofing Interstitial](#)

[Permissions and Web APIs](#)

[Permission requests \(infobars or bubbles\)](#)

[Recording icon on tab \(or as notification on Android\) while WebRTC is capturing the camera/mic](#)

[Add to Homescreen on Android \(grants perma-fullscreen\)](#)

[Extensions](#)

[Extension or app installation: permission prompt](#)

[Extension or app update: permission prompt](#)
[Extension blocked due to Safe Browsing list \(infobar\)](#)
[Extension removed due to Safe Browsing list \(bubble\)](#)

[Prompts and Dialogues](#)

[Infobar about unsafe flags on startup](#)
[<input type="file"> chooser](#)
[Password autofill \(and perhaps password manager\)](#)
[Credit Cards?](#)
[External protocol \(irc://, tel:, etc\) prompt](#)
[HTTP basic authentication dialog](#)
[Client-side certificate selector \(provided by the OS?\)](#)
[Smart card PIN prompt](#)
[Certificate Viewer](#)

[Settings](#)

[chrome://settings](#)
[Settings reset/tampered with error bubble](#)
[Sync sign-in](#)
[Extension browser actions/page actions/context menu items/keyboard shortcuts/omnibox keywords can modify the active tab when activated \(without any permissions\)](#)

[Other](#)

[Url bar hiding logic on Android](#)
[External Documentation](#)
[Chrome Plate](#)

[Developer Features](#)

[chrome://net-internals/](#)
[Console Warnings](#)
[XSS Auditor](#)

[UI that displays origin](#)

[Hosted App](#)
[Web Notification](#)

[NOT Security UI](#)

[Status bubble \(appears while hovering over a link\)](#)

[Other Security-Related Places \(i.e. On the Web\)](#)

[Related Documents](#)


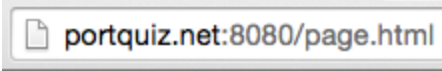
[Notes](#)

[TODO](#)

Omnibox

Origin in the omnibox

Screenshots:

Host in darker text	
Non-default port	

a.k.a: URL (bar)

Security Properties: Displays the [origin](#) (scheme, host, port), which defines a unique website from a security perspective. See [same-origin policy \(SOP\)](#). We emphasize the scheme when it's HTTPS, and display the host in black (while the rest of the URL is gray).

Implementation Code: [OmniboxViewViews::EmphasizeURLComponents\(\)](#)

Manual steps: Browse the web

Automated Tests: ?

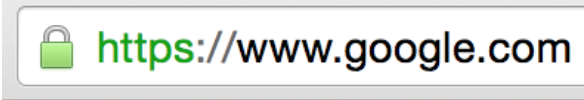
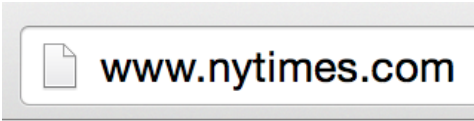
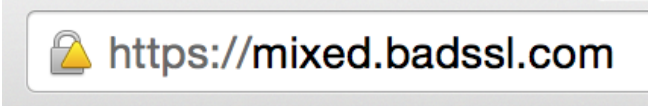
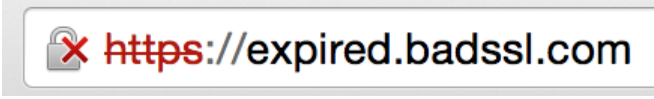
Platforms: All

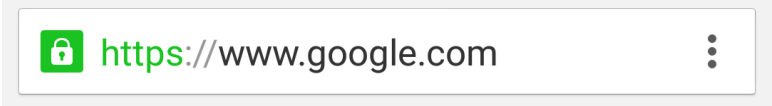
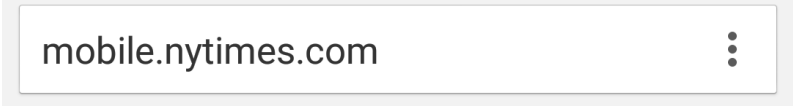
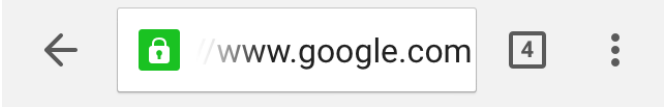
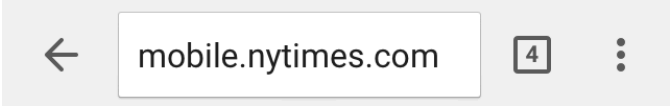
Help Center: N/A

Related Bugs:

Page security state icon

Screenshots:

Desktop, HTTPS	
Desktop, HTTP	
Desktop, Mixed (until M45)	
Desktop, broken HTTPS	

Android, HTTPS	
Android phone, HTTP	
iOS, HTTPS	
iOS, HTTP	

a.k.a: lock icon, security indicator, security badge

Security Properties: Displays the security state of the current page

Implementation Code:

- [GetSecurityLevelForWebContents\(\)](#)
- [OmniboxViewViews::EmphasizeURLComponents\(\)](#)

Manual steps: Visit badssl.com to test pages that trigger various lock icons. Note that it also has another purpose: it can be dragged like a URL to the web content ([re-]load the URL), the tab bar (open in new tab), the desktop (make web shortcut on the filesystem), the Bookmarks bar (make bookmark), etc.

Automated Tests: [BrowserTest.SecurityStyleChangedObserver](#)

Platforms: All.

- Note that mobile phones (but not tablets) omit the icon for HTTP pages, to save space.
- The original desired rendering of the strikethrough is diagonal, but [not all platforms support that](#) (so they use a horizontal strikethrough instead).

Help Center: [Check Chrome's connection to a site](#)

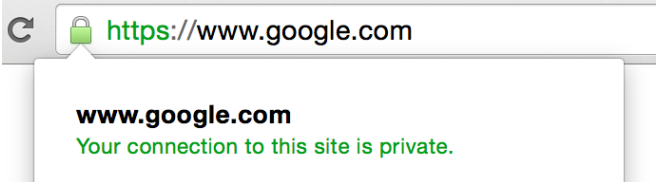
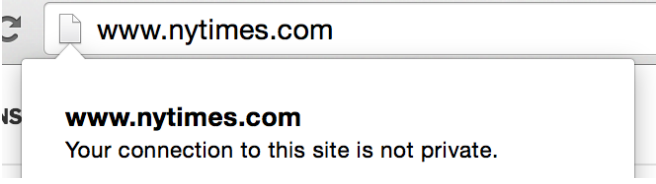
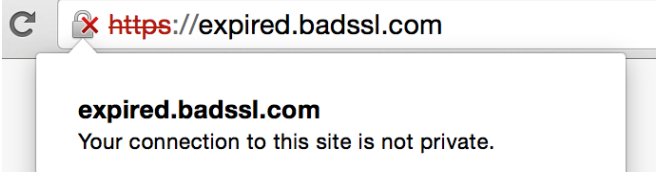
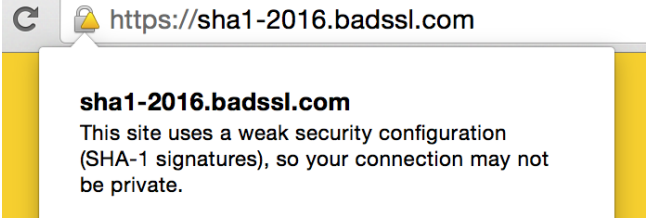
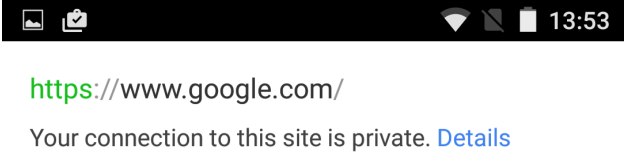
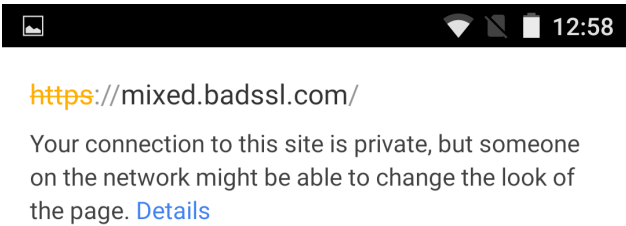
Related Bugs: <https://crbug.com/588377>

Origin Info Bubble (OIB)

a.k.a: Page Info/PageInfo, Website Settings

Security Summary

Screenshots:

Desktop, HTTPS	
Desktop, HTTP	
Desktop, broken	
Desktop, SHA-1	
Android, HTTPS	
Android, Mixed	

a.k.a: Identity Status Text, OIB (origin info bubble), Page Info

Security Properties: Describes the overall page security state.

- Note: this currently only identity (i.e. cert) status into account on Desktop (crbug.com/517589).

Implementation Code:

- Desktop: [WebsiteSettingsUI::IdentityInfo::GetIdentityStatusText\(\)](#)
- Android: [WebsiteSettingsPopup.getConnectionMessageId\(\)](#)

Manual steps: Click on a lock icon.

Automated Tests: None?

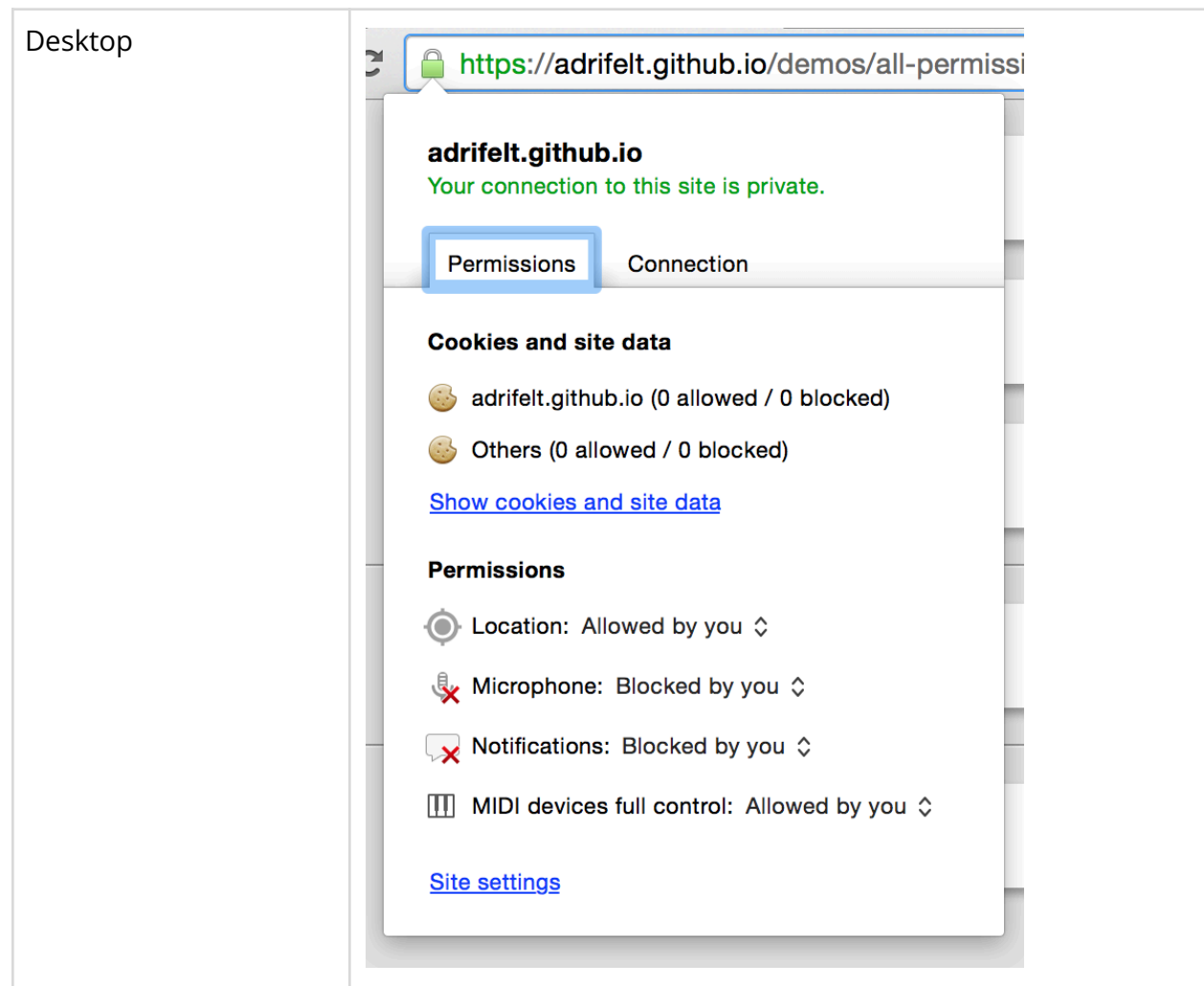
Platforms: Missing from iOS (crbug.com/457767)

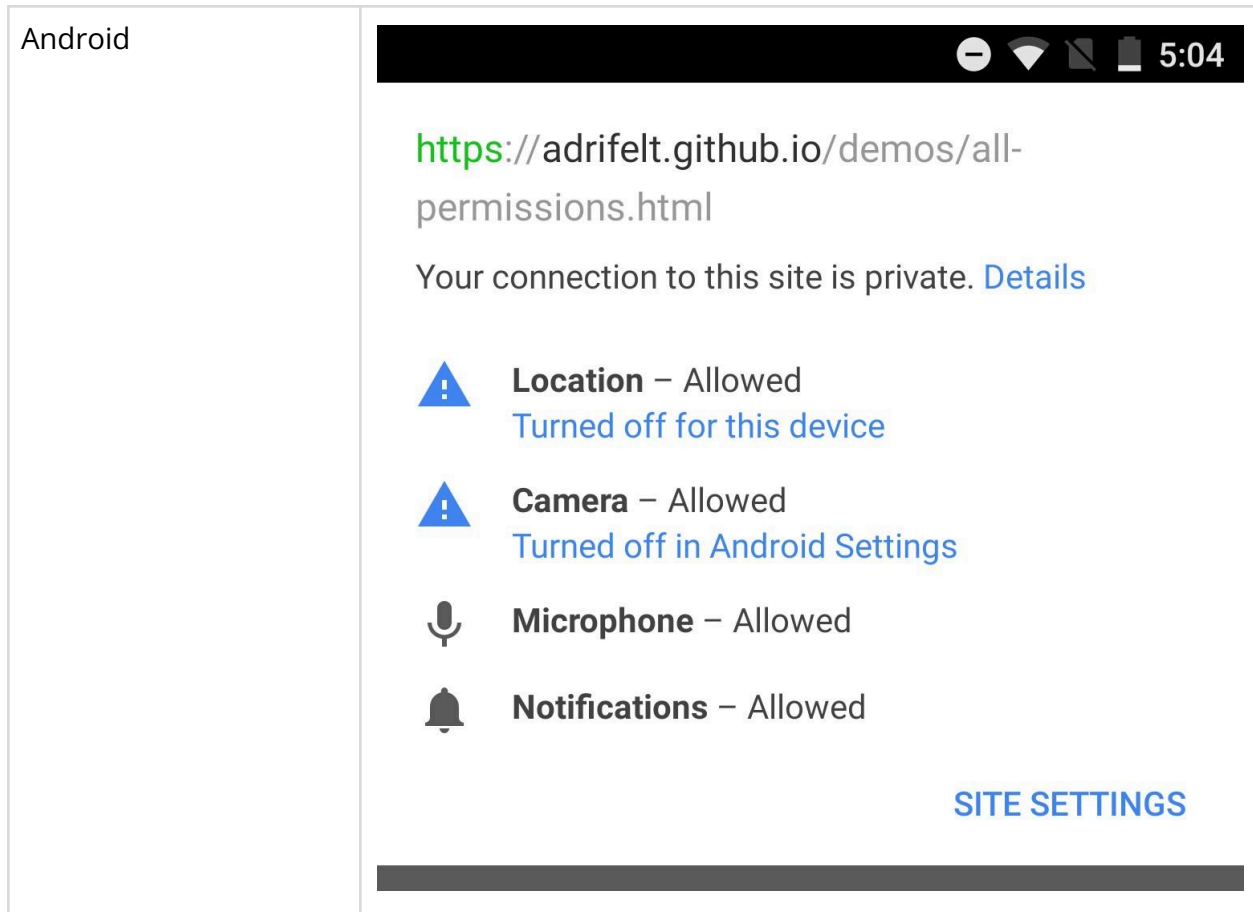
Help Center: N/A

Related Bugs:

Site data and permissions

Screenshots:





a.k.a: Website Settings

Security Properties:

- Displays site data stored by the origin of the current page (note: cookies are messy).
- Displays web API permissions with non-default values.

Implementation Code: website-settings.cc

Manual steps: Try the [all-permissions.html](https://adrifelt.github.io/demos/all-permissions.html) demo to test permissions.

- To trigger "Location: Turned off for this device" on Android (≥ 4.4):
 - Grant location permission to a site
 - Android Settings → Location → Off
 - Re-open chrome and open Website Settings
 - Clicking the message should reopen Location settings
- To trigger "Turned off in Android settings" on Android M:
 - Grant location, camera or microphone to a site
 - Android Settings → Apps → Chromium → Permissions
 - Turn off required permission
 - Re-open chrome and open Website Settings
 - Clicking the message should perform a Android permission request
 - If "Never ask again" is checked in the Android permission request, subsequent clicks on the message will reopen Android App Settings

Automated Tests: website-settings.unittest.cc

Platforms: Tap/click on the lock icon. Not available on iOS.

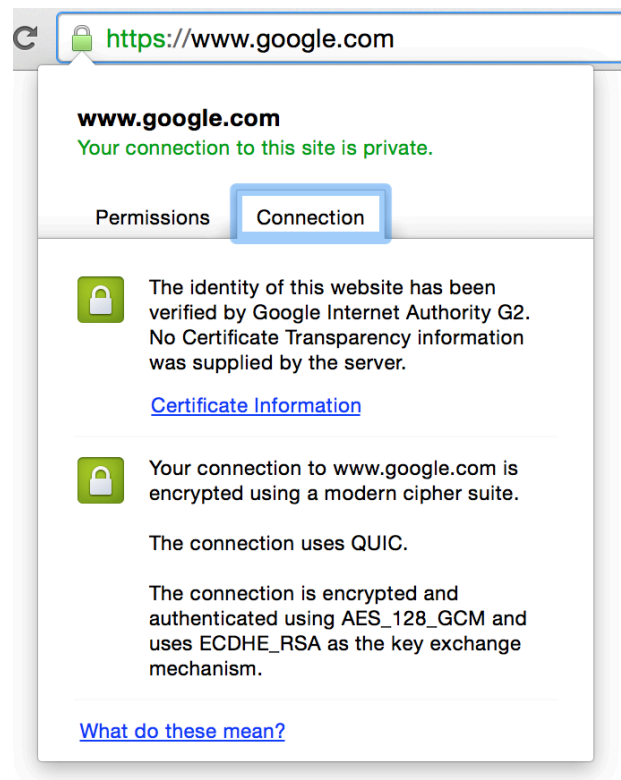
Help Center: [Manage website permissions](#)

Related Bugs:

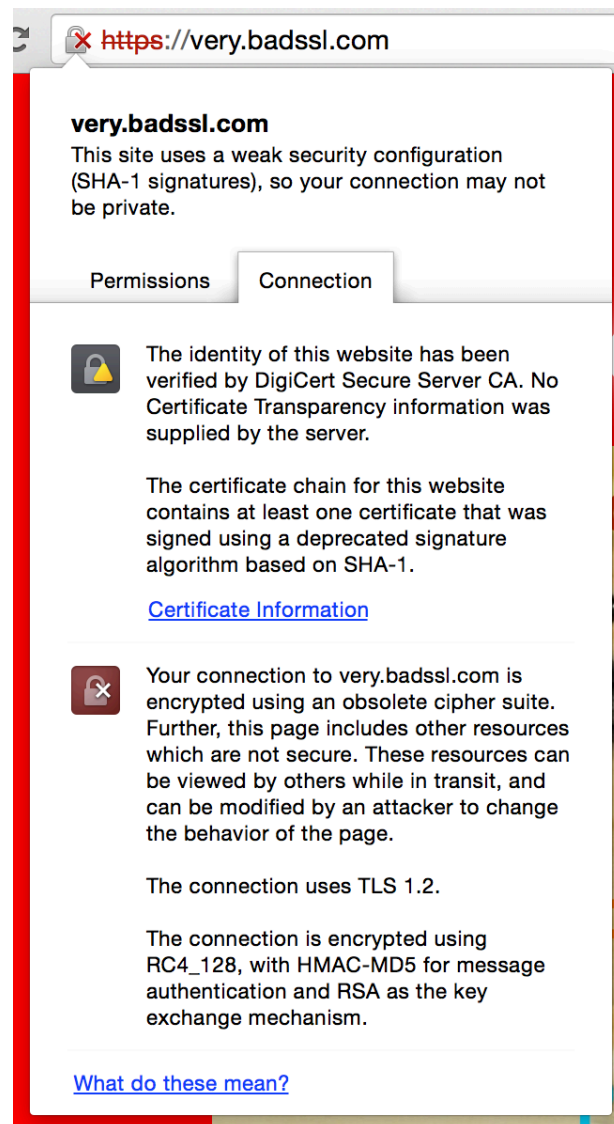
Connection Info

Screenshots:

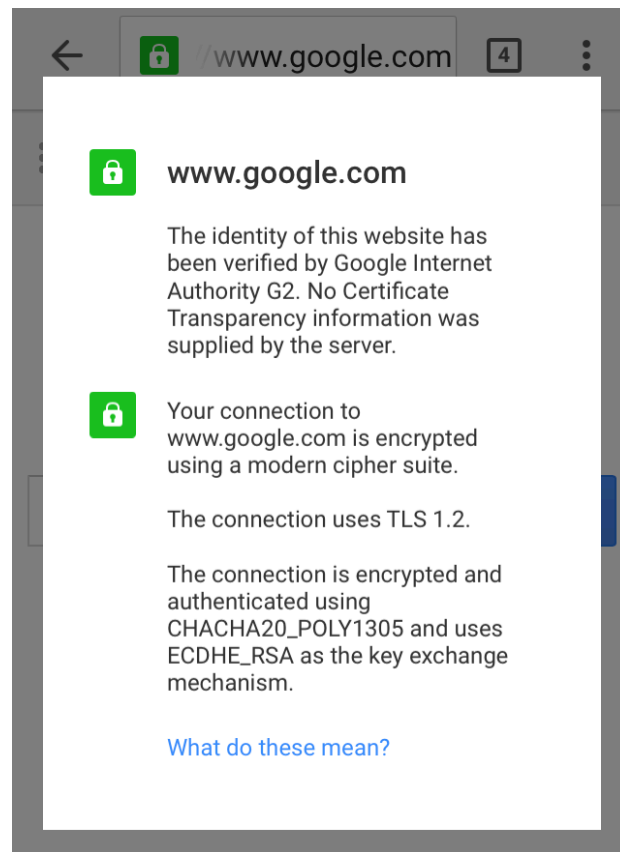
Desktop, HTTPS



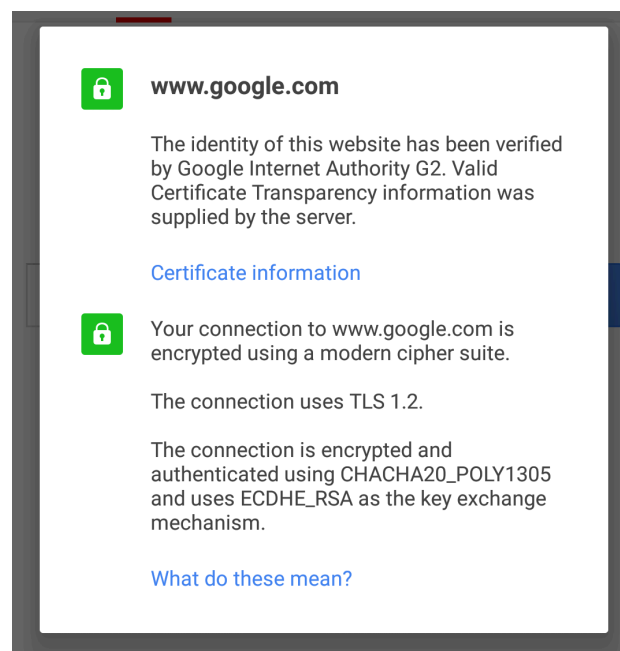
Desktop, with various error conditions



iOS



Android



a.k.a: -
Security Properties:

- Displays identity (i.e. cert) and connection info of the current page.
- Used to include a “last visited” date ([removed in M46](#)).

Implementation Code: [WebsiteSettings::Init\(\)](#)

Manual steps: Visit [badssl.com](#) to test pages that trigger various connection info combinations.

- Desktop: Click on the lock icon to open the OIB, then click on the “Connection” tab.
 - If the lock icon for an HTTPS page is not green, the OIB should immediately display the Connection tab when you click on the lock icon.
- iOS: Tap on the lock icon.
- Android: Tap on the lock icon, then tap “Details”.

Automated Tests: [website_settings_unittest.cc](#)

Platforms: All

Help Center: [Check Chrome's connection to a site](#)


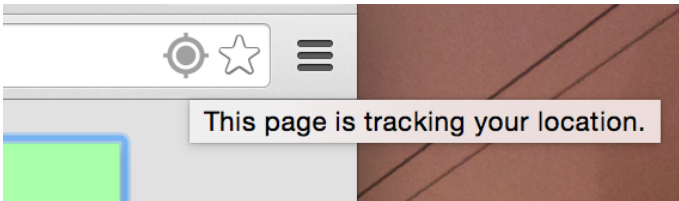
Related Bugs:

Page Actions (right side of omnibox)

Note that [extensions can also implement new page actions](#).

Active web API permissions

Screenshots:

Desktop	
Desktop hover title	

a.k.a:

Security Properties:

Implementation Code:

Manual steps: Visit <https://adrifelt.github.io/demos/all-permissions.html>

- Hovering over icon should give description

Automated Tests:

Platforms:


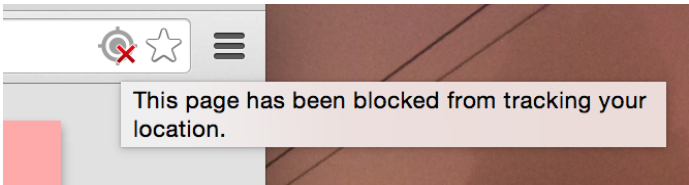
- Page actions on desktop
- Settings on Android, but no UI
- Nothing on iOS

Help Center:

Related Bugs:

Blocked web API permissions

Screenshots:

Desktop	
Desktop hover title	

a.k.a: Blocked content (settings)

Security Properties:

Implementation Code:

Manual steps: Visit <https://adrifelt.github.io/demos/all-permissions.html>

- Hovering over icon should give description

Automated Tests:

Platforms:

- Page actions on desktop
- Settings on Android, but no UI
- Nothing on iOS

Help Center:

Related Bugs:

Blocked content settings

Screenshots:

Blocked images (desktop)	
-----------------------------	---

Blocked Javascript (desktop)	
Blocked plugin (desktop)	

a.k.a:

Security Properties:

Implementation Code:

Manual steps: chrome://settings/content

Automated Tests:

Platforms:

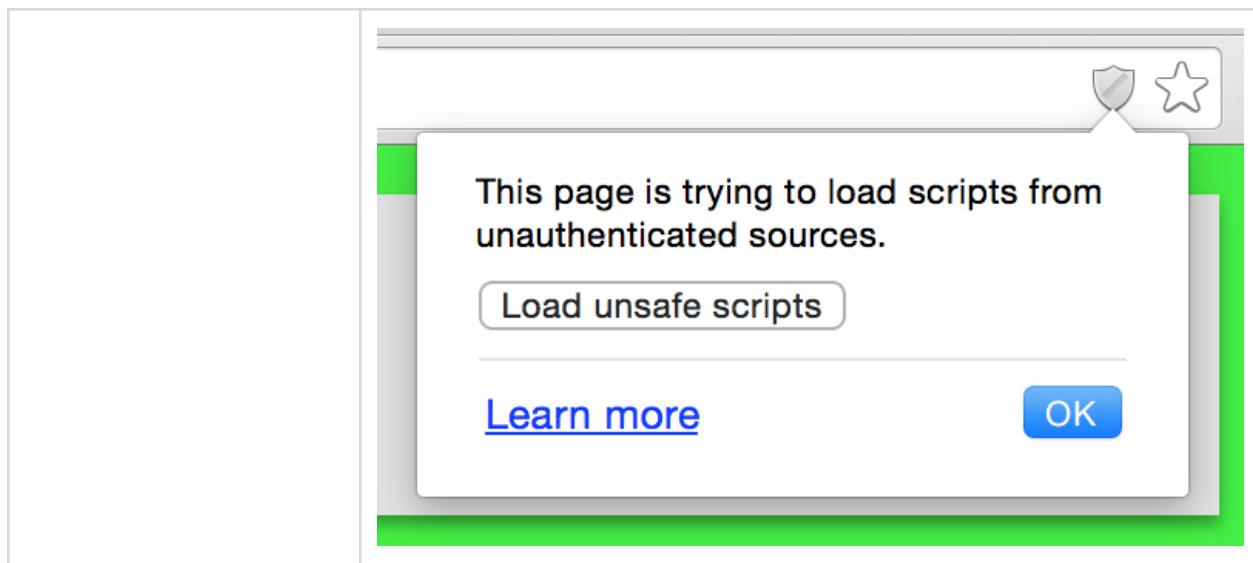
- Page actions on desktop
- Settings on Android, but no UI
- Nothing on iOS

Help Center:

Related Bugs:

[Mixed script shield \(for blocked “active mixed content”\)](#)

Screenshots:



a.k.a: Mixed Script Shield, (Active) Mixed Content Shield

Security Properties:

Implementation Code:

Manual steps:

- Visit <https://mixed-script.badssl.com/>
- Click on the mixed content shield

Automated Tests:

Platforms:

- Shield on desktop
- Active mixed content [can't be blocked on iOS 8 or earlier](#) (ther is no shield; the active mixed content just runs)
- Always blocked on Android

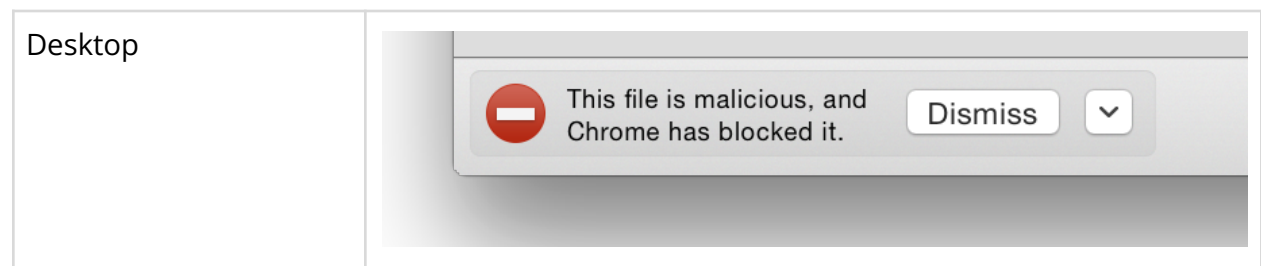
Help Center:

Related Bugs:

Downloads

[Blocked download in download shelf](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

- <https://testsafebrowsing.appspot.com/>
- <http://download.safebrowsingtest.com/download>

Automated Tests:

Platforms: Desktop only?


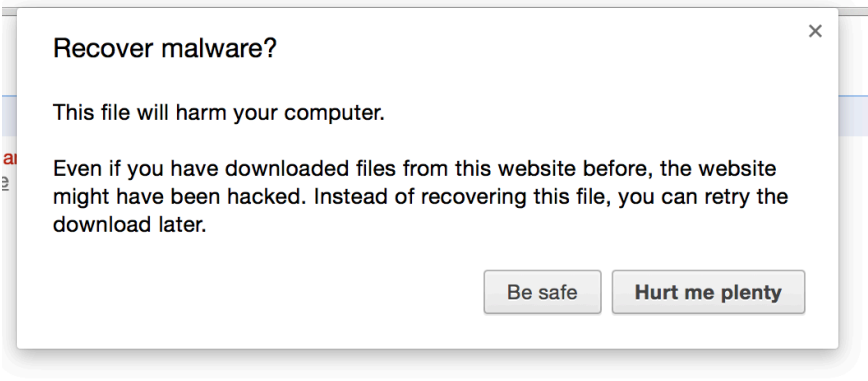
Help Center:

https://support.google.com/chrome/answer/6261569?p=ib_download_blocked&hl=en&rd=1

Related Bugs:

[Blocked download in chrome://downloads](#)

Screenshots:

Desktop, at chrome://downloads/	 This file is malicious, and Chrome has blocked it. Recover malicious file Remove from list
Desktop, after clicking "Recover malicious file" (as of late 2014)	

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

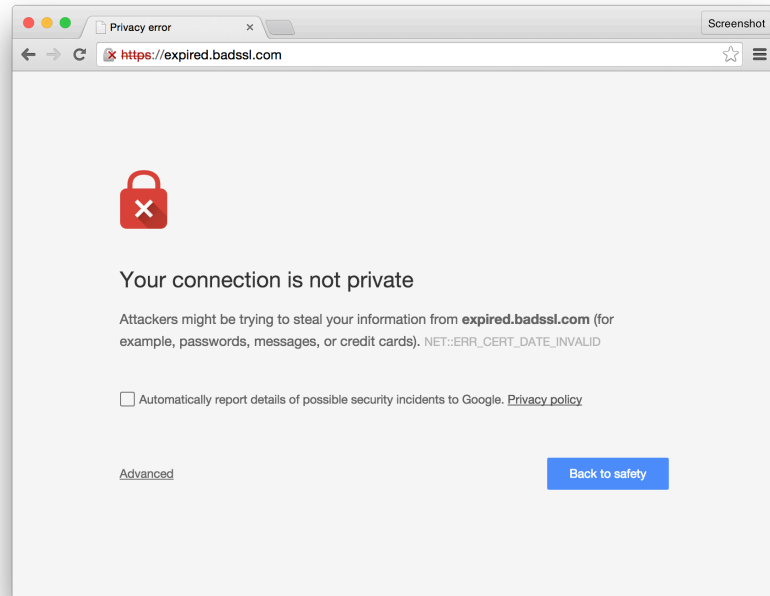
Interstitials

Manual steps: chrome://interstitials/

[SSL interstitial](#)

Screenshots:

Desktop



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <https://badssl.com/>

Automated Tests:

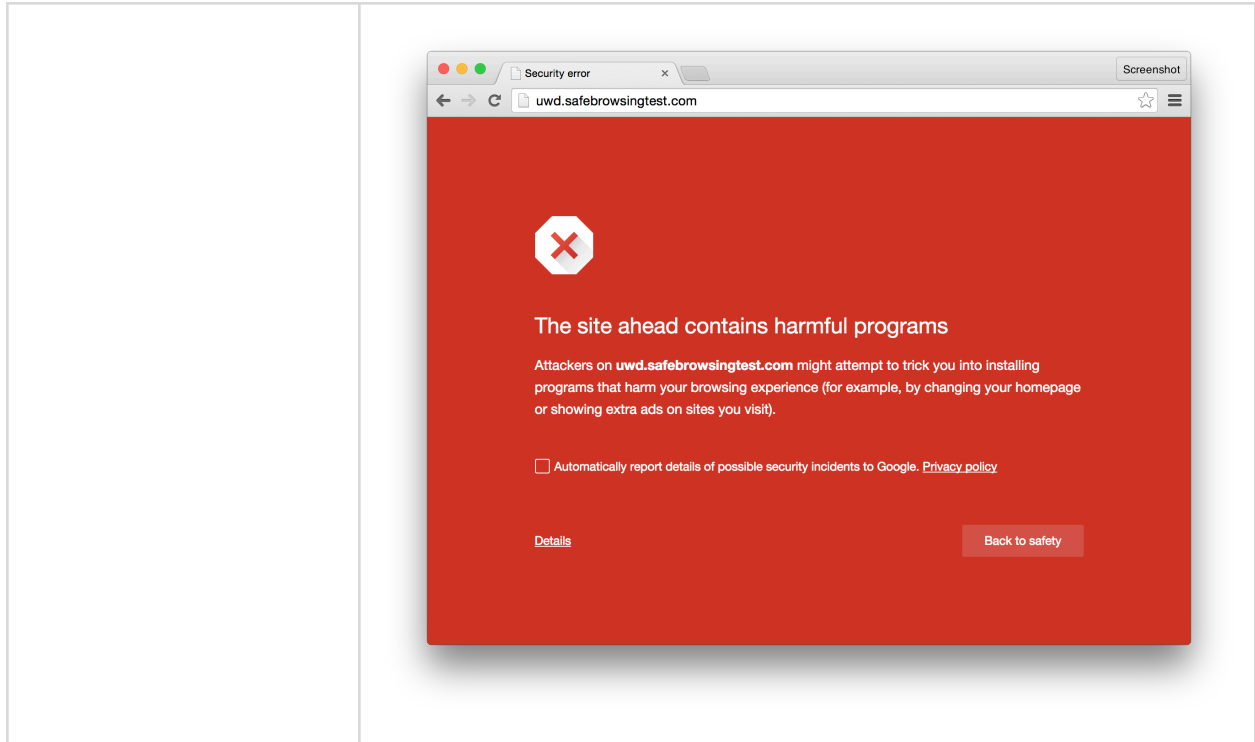
Platforms: All

Help Center:

Related Bugs: [483199](#) (iOS refreshing)

Malware (Safe Browsing) interstitial

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <http://uwd.safebrowsing.com/>

Automated Tests:

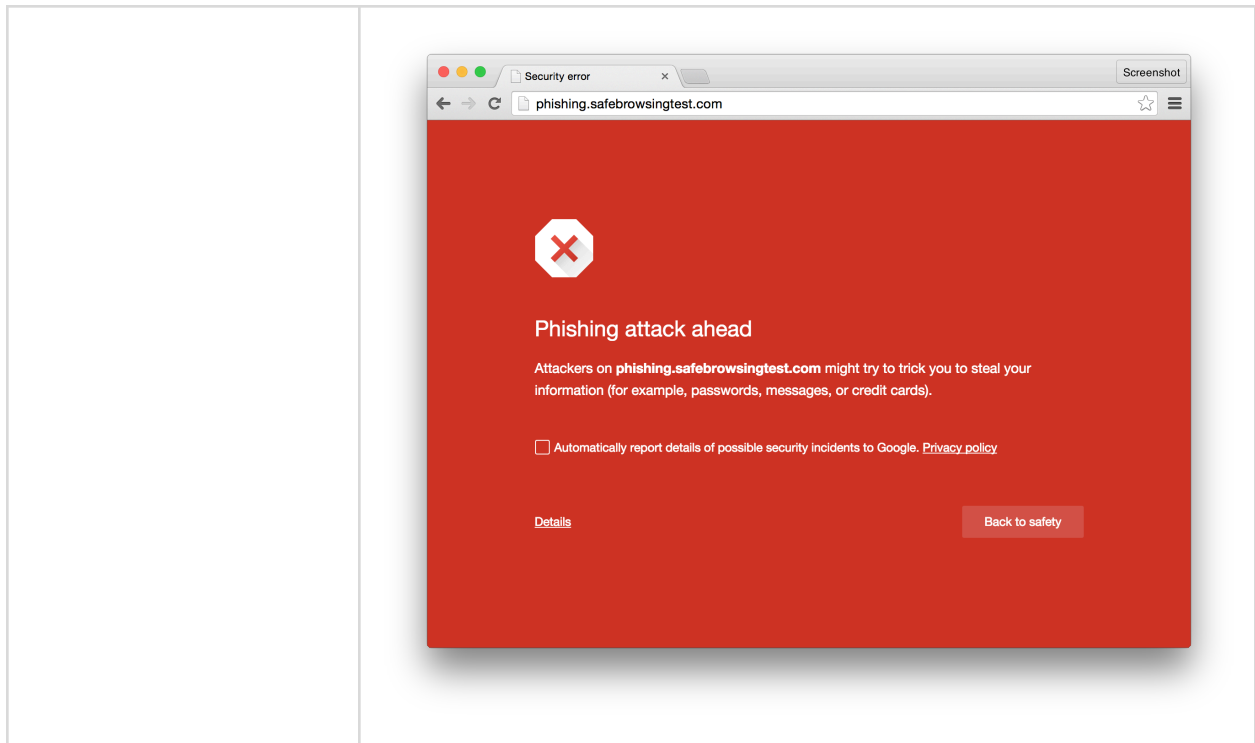
Platforms:

Help Center:

Related Bugs:

[Phishing \(Safe Browsing\) interstitial](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <http://phishing.safebrowsing.com/>

Automated Tests:

Platforms:

Help Center:

Related Bugs:

Spoofing Interstitial

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <http://phishing.safebrowsing.com/>

Automated Tests:

Platforms:

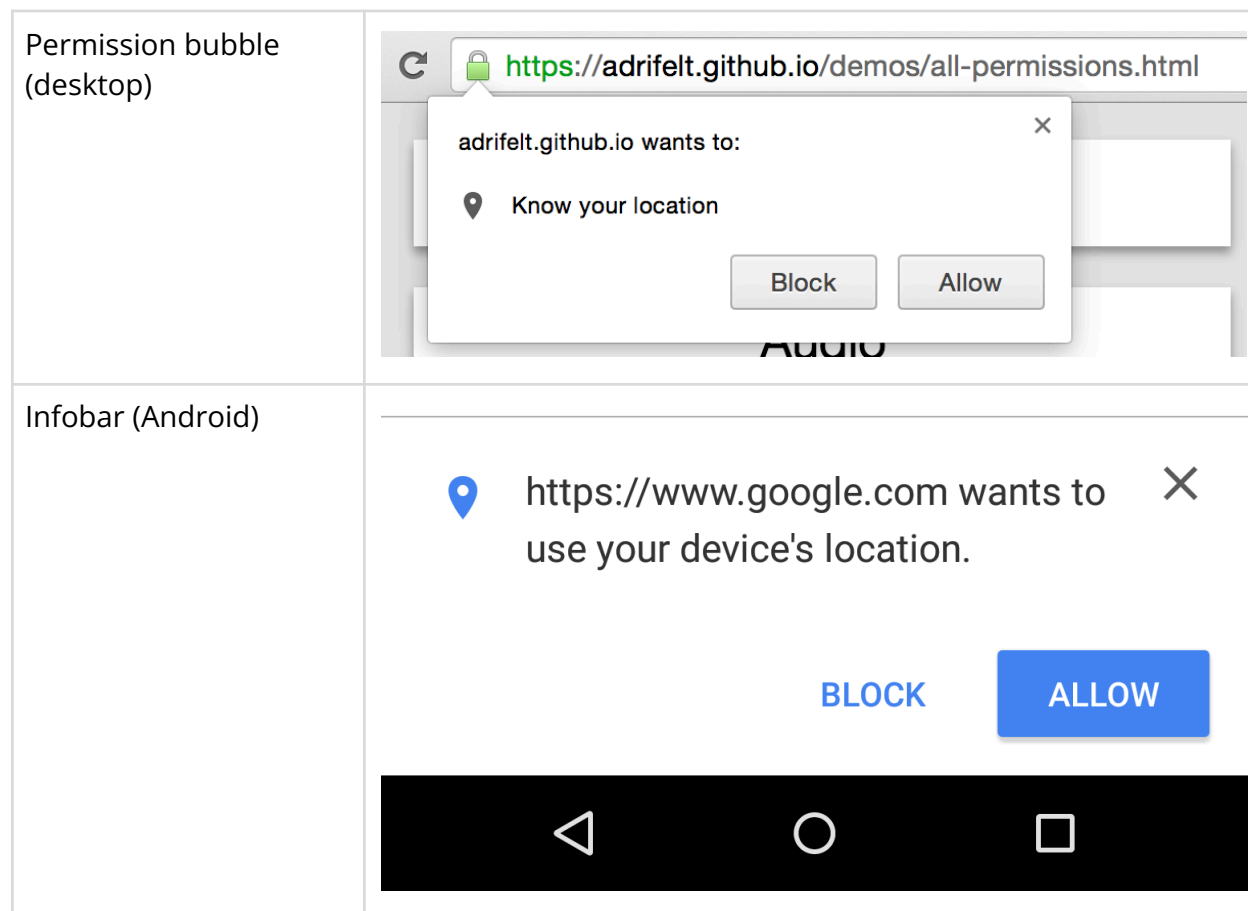
Help Center:

Related Bugs: <https://crbug.com/474296>

Permissions and Web APIs

Permission requests (infobars or bubbles)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <https://adrifelt.github.io/demos/all-permissions.html>

Automated Tests:

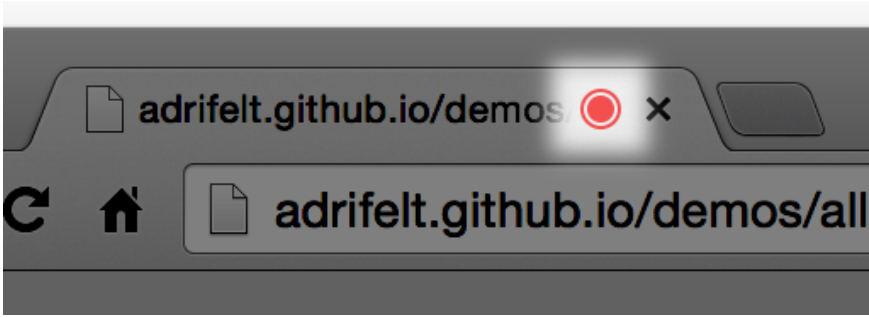
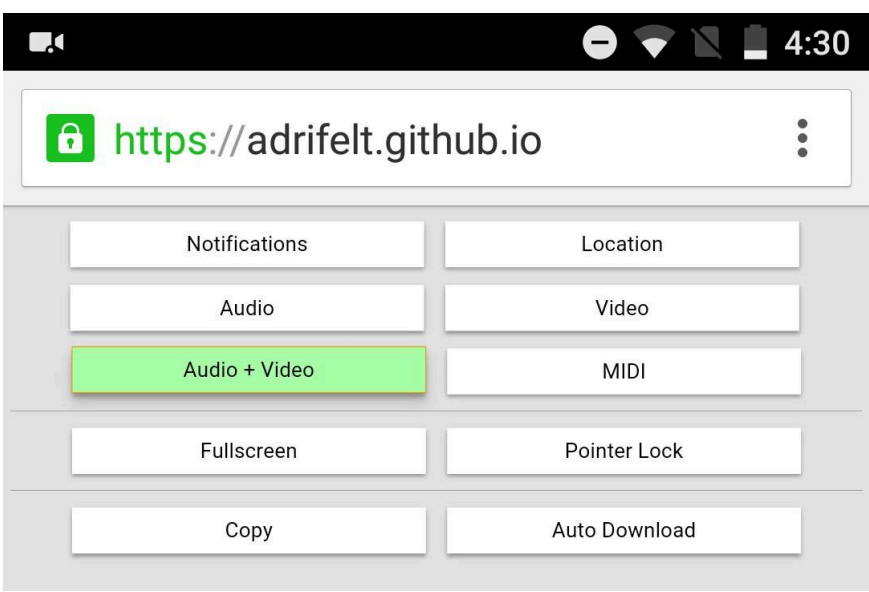
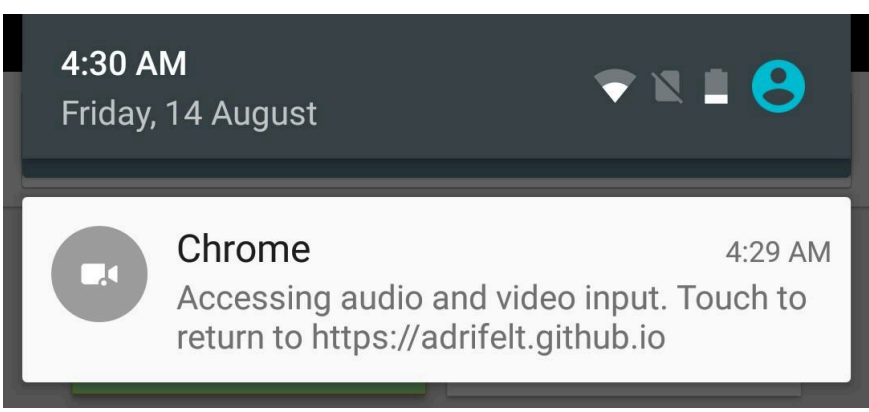
Platforms: Not available on iOS (falls back to per-site global WebView settings).

Help Center:

Related Bugs:

Recording icon on tab (or as notification on Android) while WebRTC is capturing the camera/mic

Screenshots:

Desktop	
Android status bar	
Android notifications shade	

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests: Visit <https://adrifelt.github.io/demos/all-permissions.html> and click on "Audio" or "Video"

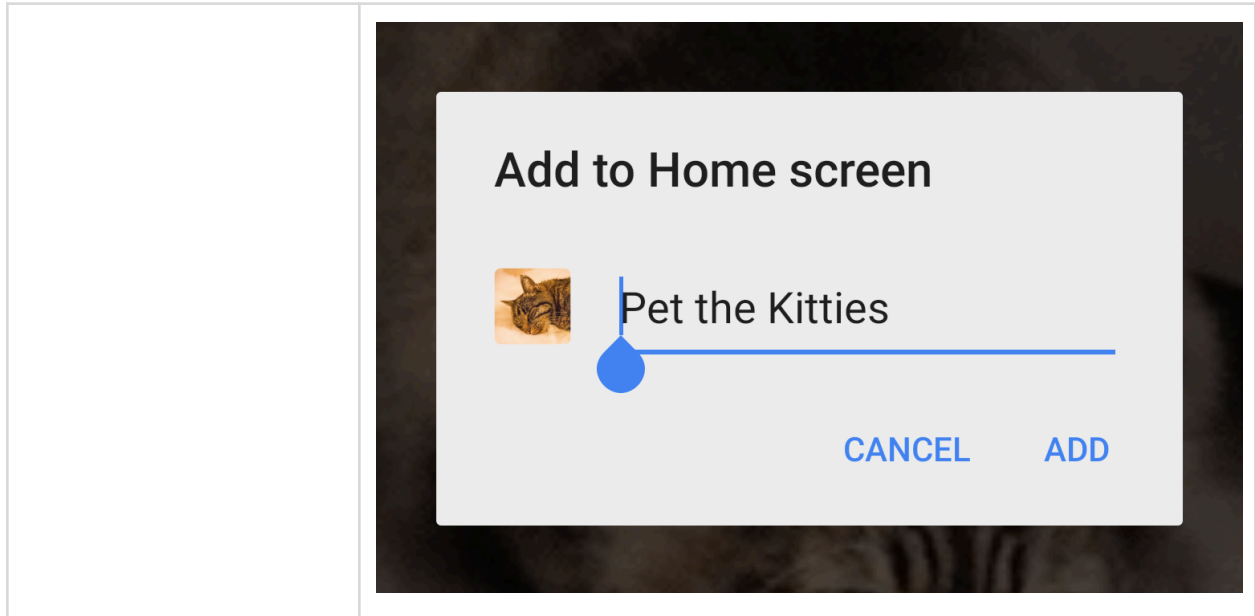
Platforms: Desktop and Android

Help Center:

Related Bugs:

[Add to Homescreen on Android \(grants perma-fullscreen\)](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

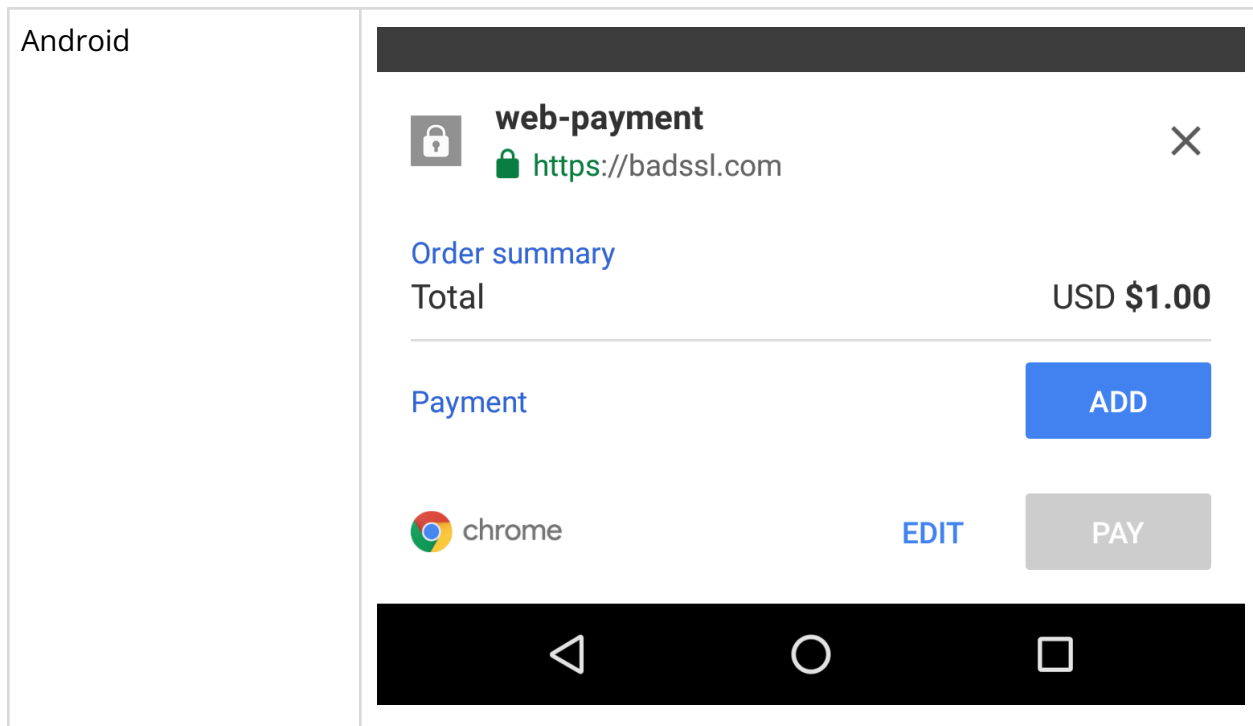
Platforms: Android only

Help Center:

Related Bugs:

[Web Payments API](#)

Screenshots:



a.k.a:

Security Properties: Shows the page origin (also shows untrusted page title and favicon)

Implementation Code:

Manual steps:

Automated Tests:

Platforms: Android only

Help Center:

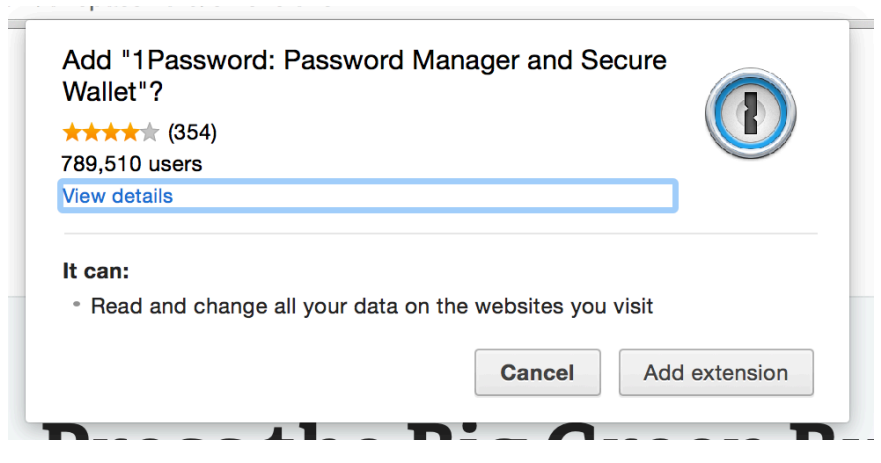
Related Bugs:

Extensions

Extension or app installation: permission prompt

Screenshots:

Desktop



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <https://agilebits.com/onepassword/extensions>

<https://chrome.google.com/webstore/category/extensions>

Automated Tests:

Platforms: No extensions on mobile.

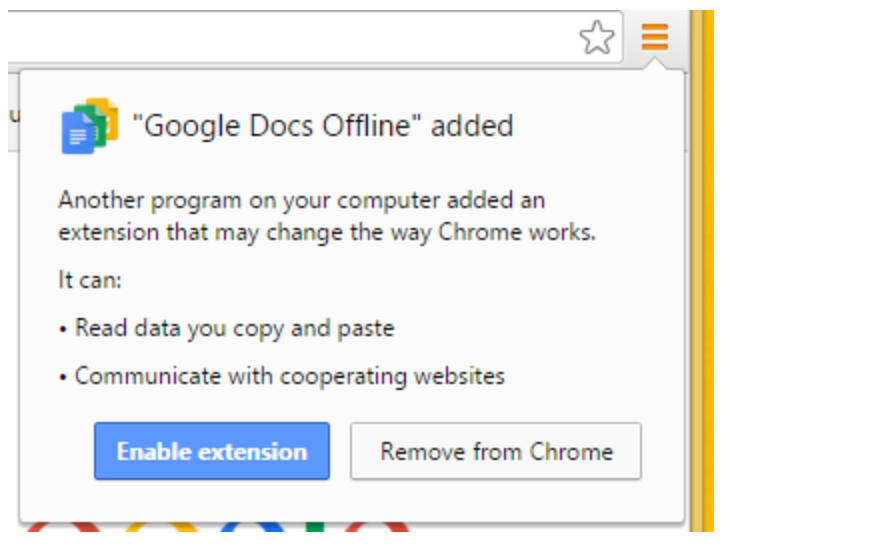
Help Center:

Related Bugs:

Extension or app update: permission prompt

Screenshots:

Desktop



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

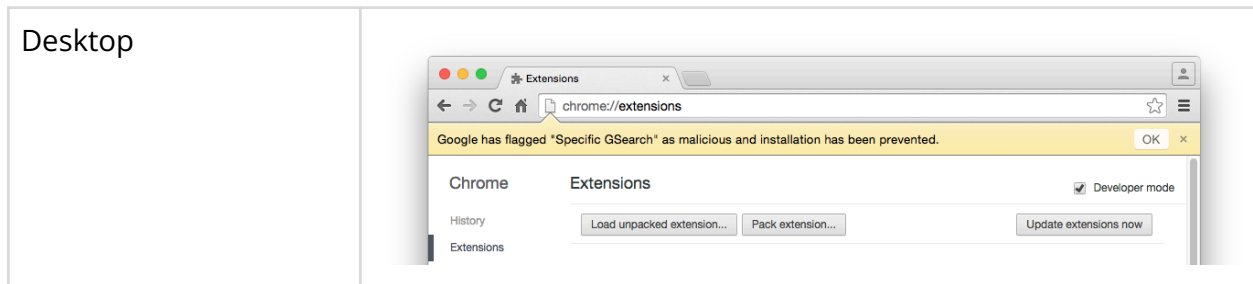
Platforms:

Help Center:

Related Bugs:

Extension blocked due to Safe Browsing list (info bar)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: Download "[Specific GSearch](#)" and drag onto chrome://extensions

Automated Tests:

Platforms: Extensions are only available on desktop.

Help Center:

Related Bugs:

Extension removed due to Safe Browsing list (bubble)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

- Start Chrome with a fresh user data dir (so that the extension blacklist is not loaded yet).
- Download "[Specific GSearch](#)" and drag onto chrome://extensions
- Wait.

Automated Tests:

Platforms: Extensions are only available on desktop.

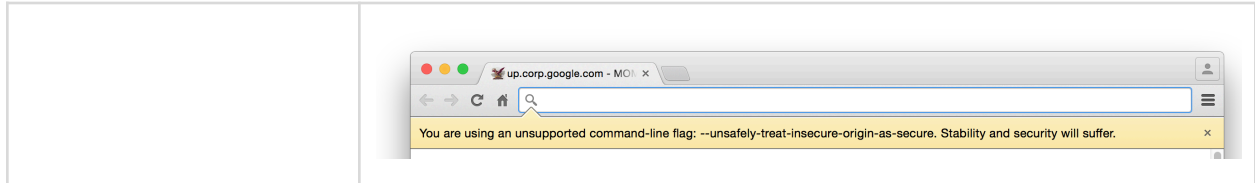
Help Center:

Related Bugs:

Prompts and Dialogues

Infobar about unsafe flags on startup

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: Run Chrome using the flag `--disable-web-security` or `--unsafely-treat-insecure-origin-as-secure=http://example.com`

Automated Tests:

Platforms:

Help Center:

Related Bugs:

`<input type="file">` chooser

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

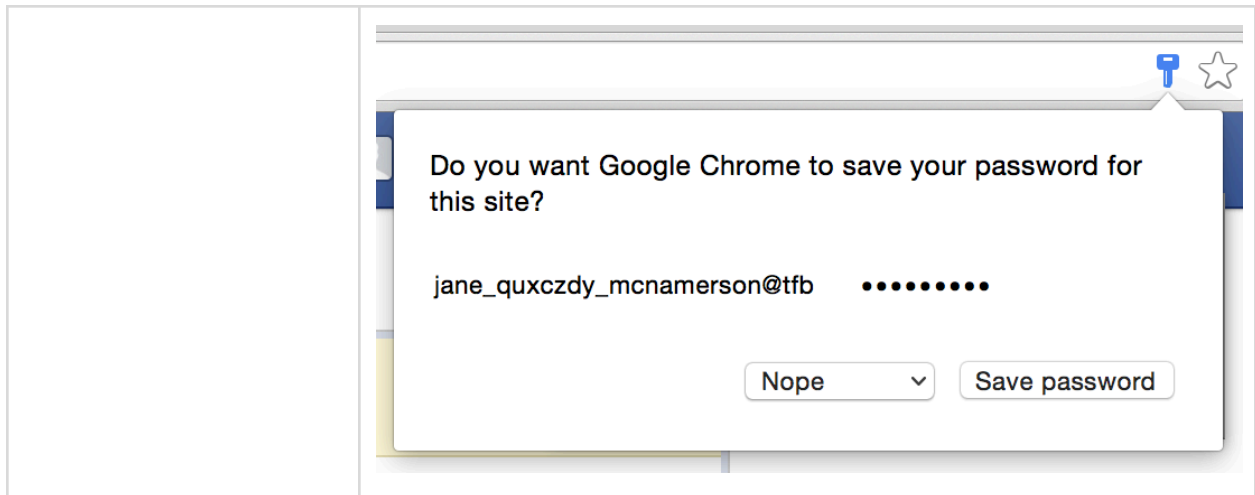
Platforms:

Help Center:

Related Bugs:

Password autofill (and perhaps password manager)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

[Credit Cards?](#)

[External protocol \(irc://, tel:, etc\) prompt](#)

Screenshots:

--	--

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

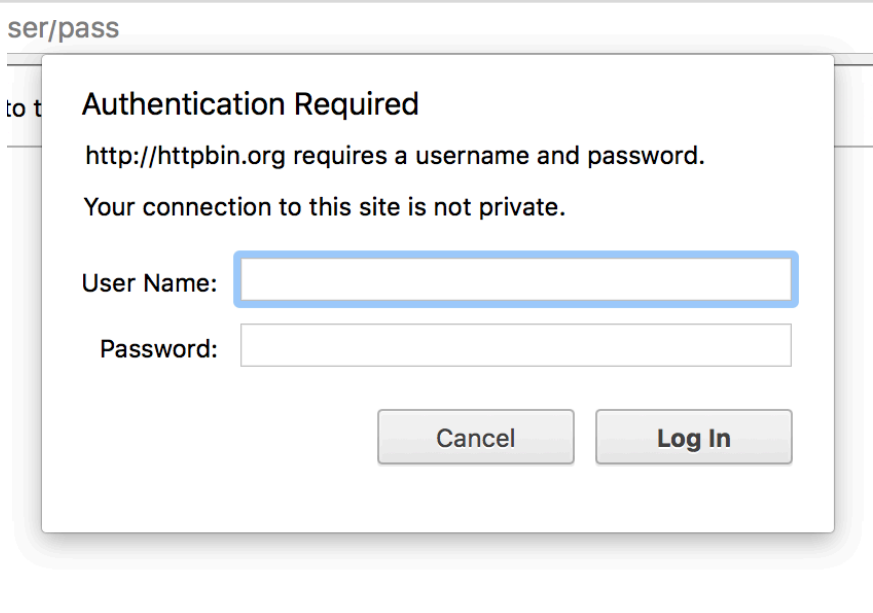
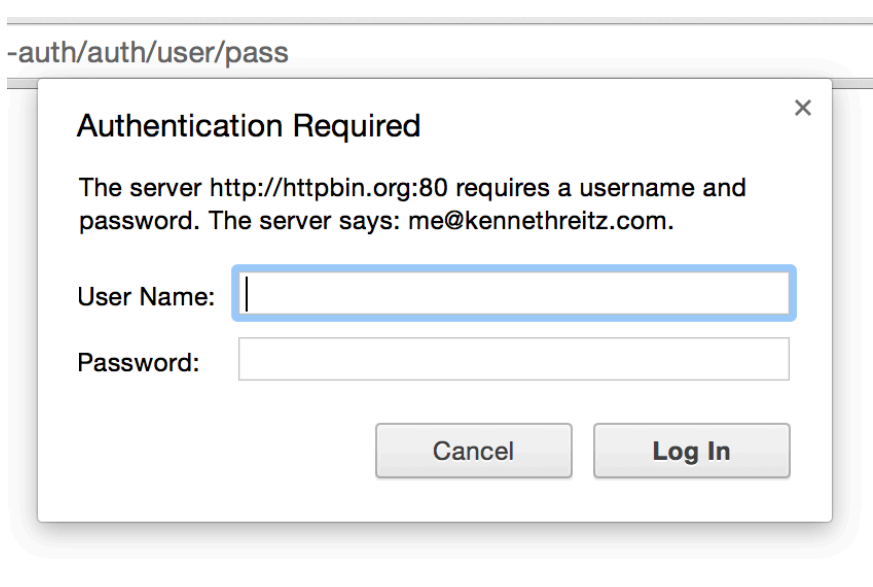
Help Center:

Related Bugs:

[HTTP basic authentication dialog](#)

Screenshots:

Desktop	
---------	--

	
Desktop (older version with realm)	

a.k.a:

Security Properties:

Implementation Code:

Manual steps: <http://httpbin.org/digest-auth/auth/user/pass>

Automated Tests:

Platforms:

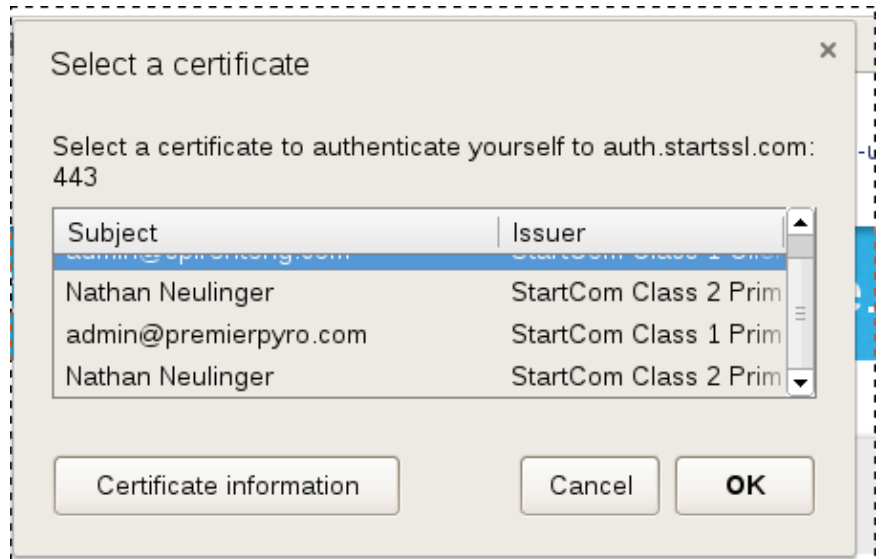
Help Center:

Related Bugs: <https://crbug.com/516763>

[Client-side certificate selector \(provided by the OS?\)](#)

Screenshots:

Desktop (Linux)



(from <https://crbug.com/580805>)

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

- Android has one (TODO: find a public screenshot)

Help Center:

Related Bugs:

[Smart card PIN prompt](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

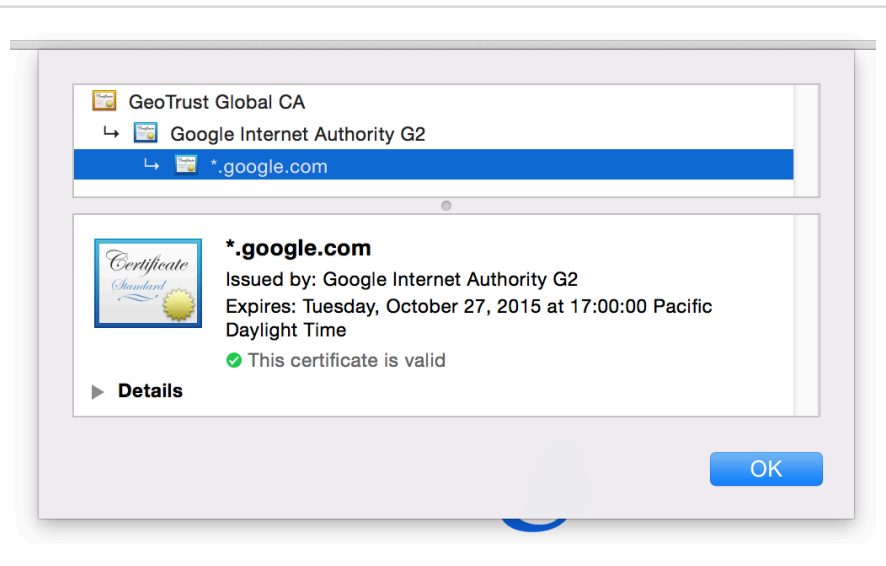
Help Center:

Related Bugs:

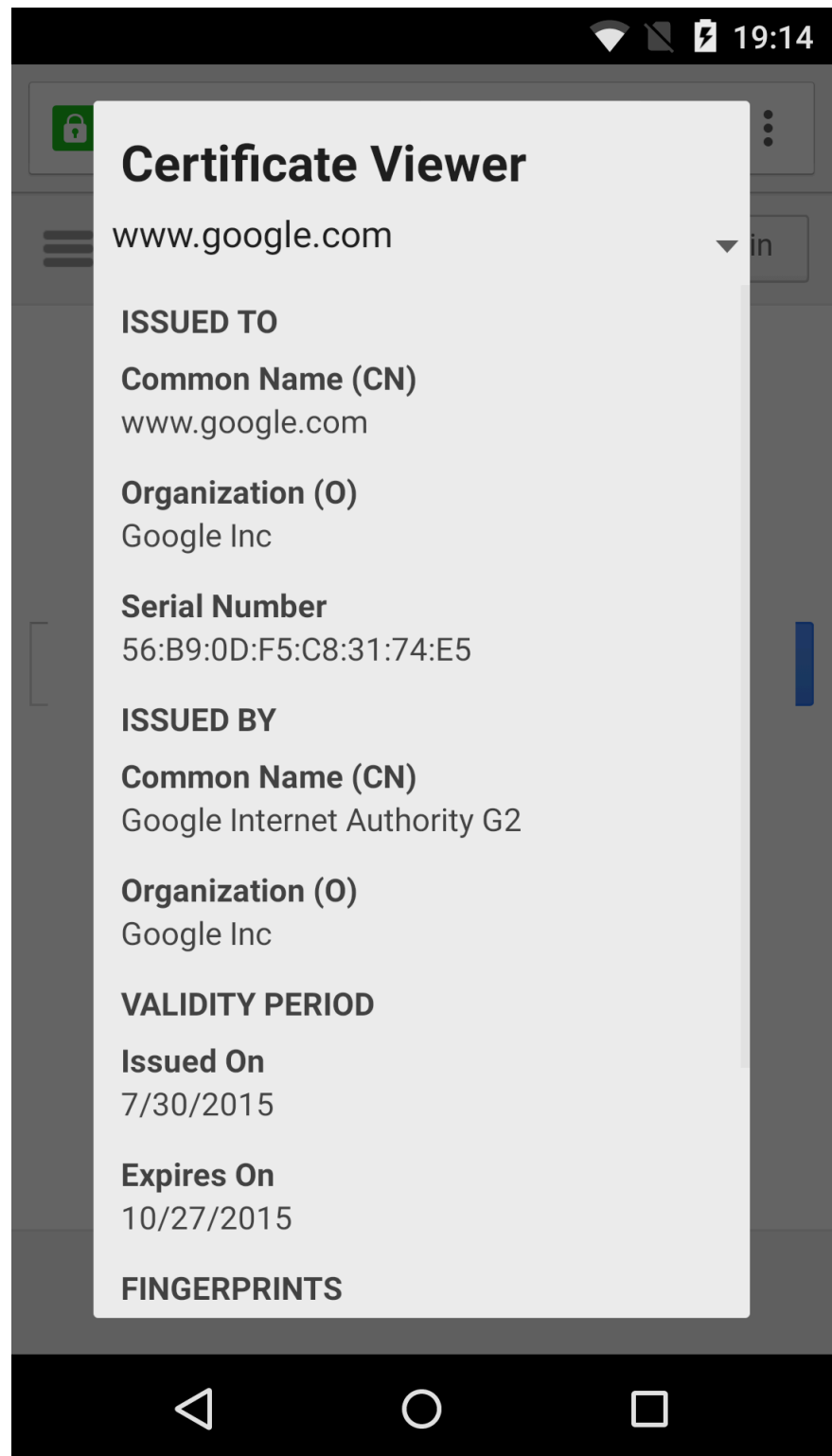
Certificate Viewer

Screenshots:

Desktop



Android



a.k.a:
Security Properties:

Implementation Code:**Manual steps:****Desktop:**

- Click on the lock icon to open the OIB.
- Click on the connection tab.
- Click on "Certificate Information".

Desktop:

- Click on the lock icon to open the OIB.
- Click on the connection tab.
- Click on "Certificate Information".
- Tap on the lock icon
- Tap "Details".
- Tap "Connection Information"

Automated Tests:**Platforms:**

- Uses native viewer on Mac, Linux, Windows.
- Implemented separately on Chrome OS (to match Firefox).
- Not available on iOS.

Help Center:**Related Bugs:**

Settings

<chrome://settings>

[Settings reset/tampered with error bubble](#)

Screenshots:**a.k.a:****Security Properties:****Implementation Code:****Manual steps:****Automated Tests:****Platforms:****Help Center:****Related Bugs:**

[Sync sign-in](#)

Screenshots:

--	--

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

Extension browser actions/page actions/context menu items/keyboard shortcuts/omnibox keywords can modify the active tab when activated (without any permissions)

Screenshots:

--	--

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

Other

Url bar hiding logic on Android

Screenshots:

--	--

a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

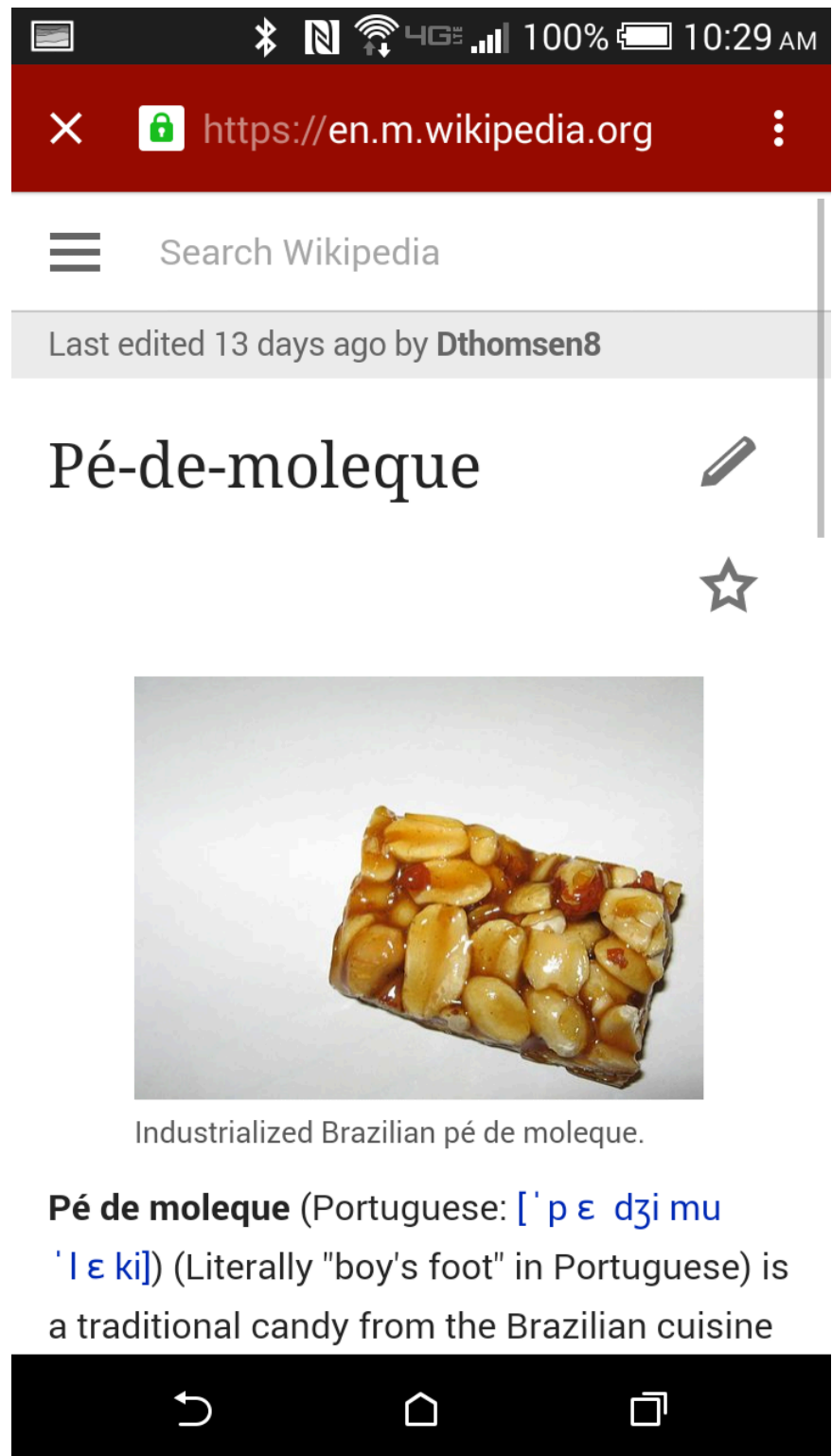
External Documentation

- a. User Documentation (e.g. Google Help Center, [security tools](#), [security overview](#), various specific pages)
- b. Chromium Dev Documentation ([Security](#), [Enamel](#), [Privacy](#), etc.)

Chrome Plate

Screenshots:

Android



a.k.a:
Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms: Android only

Help Center:

Related Bugs:

Developer Features

<chrome://net-internals/>

- HSTS: <chrome://net-internals/#hsts>
- Arguably also [#spdy](#) and [#quic](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

Platforms:

Help Center:

Related Bugs:

Console Warnings

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

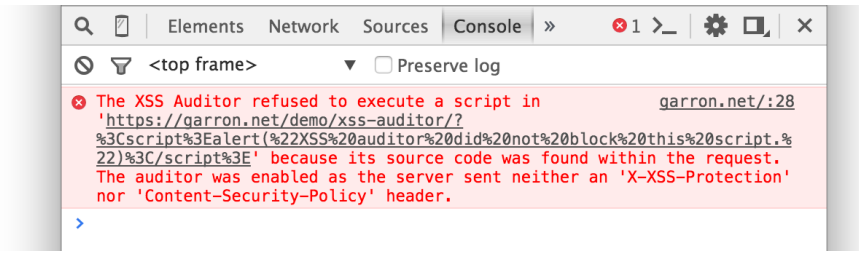
Platforms:

Help Center:

Related Bugs:

XSS Auditor

Screenshots:

Console	
Highlighting in view-source: (The red highlight is the script that was blocked because it appeared in the URL.)	<pre>

 <hr>
 If the script was blocked, your console should show an error message like this:

 <script>alert("XSS auditor did not block this script.")</script> </body> </html> </pre>

a.k.a:

Security Properties: Blocks various straightforward XSS attacks using the heuristic that a script is injected if its source appears in the URL. Note: There is no end-user-facing UI, which is intentional.

Implementation Code:

Manual steps: <https://garron.net/demo/xss-auditor/>

Automated Tests:

Platforms:

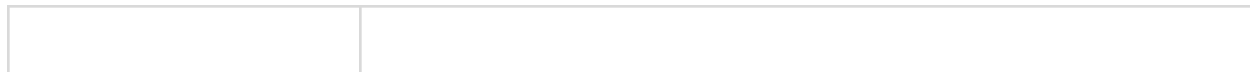
Help Center:

Related Bugs:

UI that displays origin

[Hosted App](#)

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps:

Automated Tests:

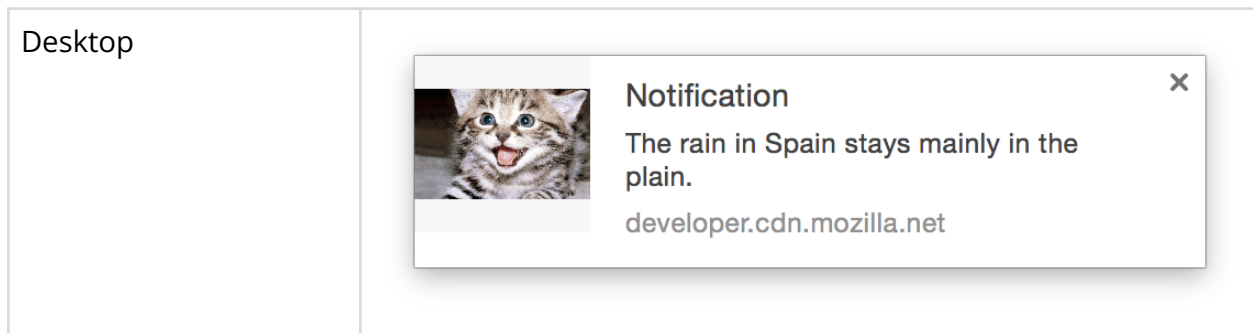
Platforms:

Help Center:

Related Bugs:

Web Notification

Screenshots:



a.k.a:

Security Properties:

Implementation Code:

Manual steps: <https://developer.mozilla.org/en-US/demos/detail/html5-notifications>

Automated Tests:

Platforms:

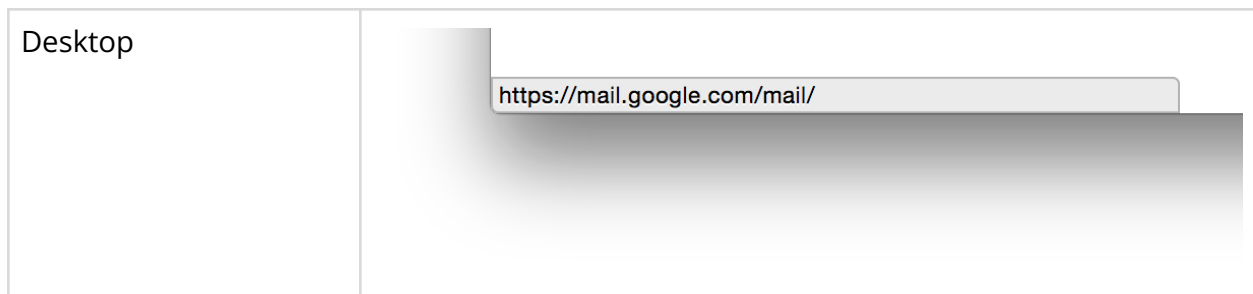
Help Center:

Related Bugs:

NOT Security UI

Status bubble (appears while hovering over a link)

Screenshots:



a.k.a:

Security Properties:

- Doesn't actually give any guarantee that clicking on the link will visit the displayed URL.
 - From the [Severity Guidelines](#): "Note that the [status bubble](#) is not a security indicator."
- Trivial to spoof: <https://garron.net/web/spoof-link/>

Implementation Code:

Manual steps: Hover over an <a> link on any page.

Automated Tests:

Platforms:

Help Center:

Related Bugs: [Cr-UI-Browser-StatusBubble](#) (label)

Other Security-Related Places (i.e. On the Web)

These need to be accurate and safe, because users/devs will read them to figure out why something is happening in Chrome / how to get around it.

- Google Help Center, Chromium Documentation (see above)
 - Developer Relations?
 - Webmaster Tools
-

Related Documents

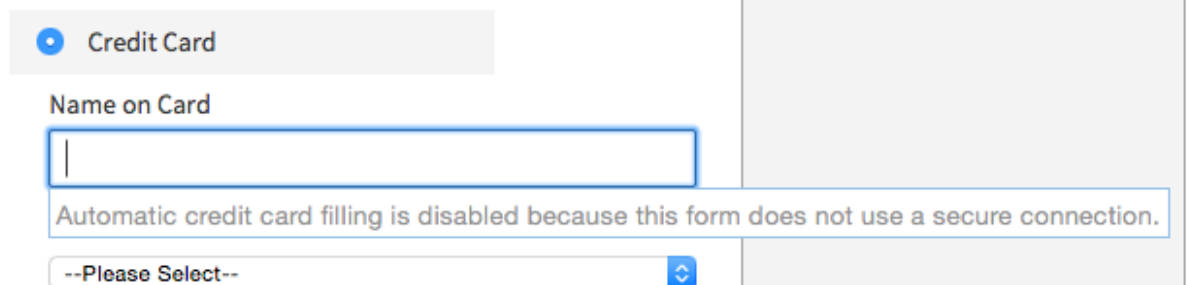
- [Plans for chrome security ui](#) (Google-internal)
- [Page Security UI in Chrome: Cross-Platform Consistency Bugs](#)
- [HTTPS Lock Iconography and Colors](#) (draft)

Notes

TODO

- “trusted” vs. unspoofable vs. affects Chrome behaviour vs. users probably trust it
- Page reload bar
 - Permissions
- UWS Software Removal prompt?
- <https://docs.google.com/document/d/1u5LlnTK2PULgm9KFOIA8LR6RBq0eSTyGGzNs3iKPuaA/edit#heading=h.qeip25hxwmie>
 - Valid HTTPS: <https://www.google.com>
 - Valid EV HTTPS: <https://www.mozilla.org/en-US/>
 - Mixed content: <https://www.bennish.net/mixed-content.html>
 - HTTP: <http://www.example.com>
 - Broken HTTPS with HSTS failure: <https://test.hstsfail.appspot.com>
 - Broken HTTPS: <https://www.irs.gov>
 - Malware: <http://malware.testing.google.test/testing/malware/>
 - Phishing: <http://phishing.safebrowsingtest.com/>
 - Unwanted software: phishing.safebrowsingtest.com

- Trigger a web permission request:
<https://adrifelt.github.io/demos/all-permissions.html>
- Android M permission flows
- https://docs.google.com/document/d/1Itf8Zv_MQ0aj9QKLDAD4VbZojBmLR07oMPYX8RQ1Yw/edit
- Manage Certificates (in Settings)
- Add OWNER/contact, at least in each section? (Or depend on the code for this?)
- Link from
<https://www.chromium.org/Home/chromium-security/security-faq#TOC-Where-are-the-security-indicators-located-in-the-browser-window->
- Fullscreen notification / Pointer Lock Bubble
- <https://crbug.com/504025>



- Figure out where <https://support.google.com/chrome/answer/6098869> goes
- Android (i) button in menu to pull up PageInfo
- ChromePlate (Chrome Custom Tabs)
- iOS test domains on badssl.com :
 - badssl.com
 - expired.badssl.com
 - mixed.badssl.com/mixed/image
 - mixed.badssl.com/mixed/iframe
- [Issue 466154](#) (chrome.identity.launchWebAuthFlow is phishable and insecure)
- <https://crbug.com/437993>
- "Your connection is being controlled" for extensions
 - <https://bugs.chromium.org/p/chromium/issues/detail?id=610833>
- Geolocation consistency disclosure infobar (Android)
- High Contrast Black
- Android split-screen thin omnibox mode
 - [Google-internal screenshots](#)
- Web Payment UI
- Verbose Extensions

