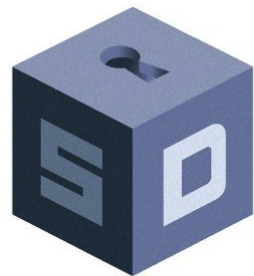


Dissecting Browser Privacy

yan
AppSec California 2017



SECUREDROP



- Open source browser based on Chromium
- Privacy
- Speed
- Ad-free funding model for websites

<https://brave.com>

<https://github.com/brave>

What are specific, achievable privacy goals for a browser?

1. Prevent third parties from accessing and tampering with browser communication to servers

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

HTTP Activity Client-to-Server

KEYSCORE

```
GET /search?tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next HTTP/1.1
Accept: */*
Referer: http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu
Accept-Language: en-GB
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: search.bbc.co.uk
Cookie: BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2F4%2e0%20%28cc
Cache-Control: max-stale=0
Connection: Keep-Alive
X-BlueCoast-Via: 66808702E9A98546
```

Search term: Musharraf

Host	URL Path	URL Args
search.bbc.co.uk	/search	tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next

Search on BBC

Search Terms	Language	Browser	Via
musharraf	en	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	66808702E9A98546

Referer: http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu

Cookie: BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2F4%2e0%20%28cc

www.wired.com

Xfinity CLOSE X

XFINITY Internet Service: Action Needed

Dear Comcast Customer,

Our records indicate that the cable modem, which you currently use for your XFINITY Internet service, may not be able to receive the full range of our speeds. To ensure you're receiving the full benefits of your XFINITY Internet service, please replace your cable modem.

Please visit <http://mydeviceinfo.comcast.net/> for a list of modems certified to work on our network.

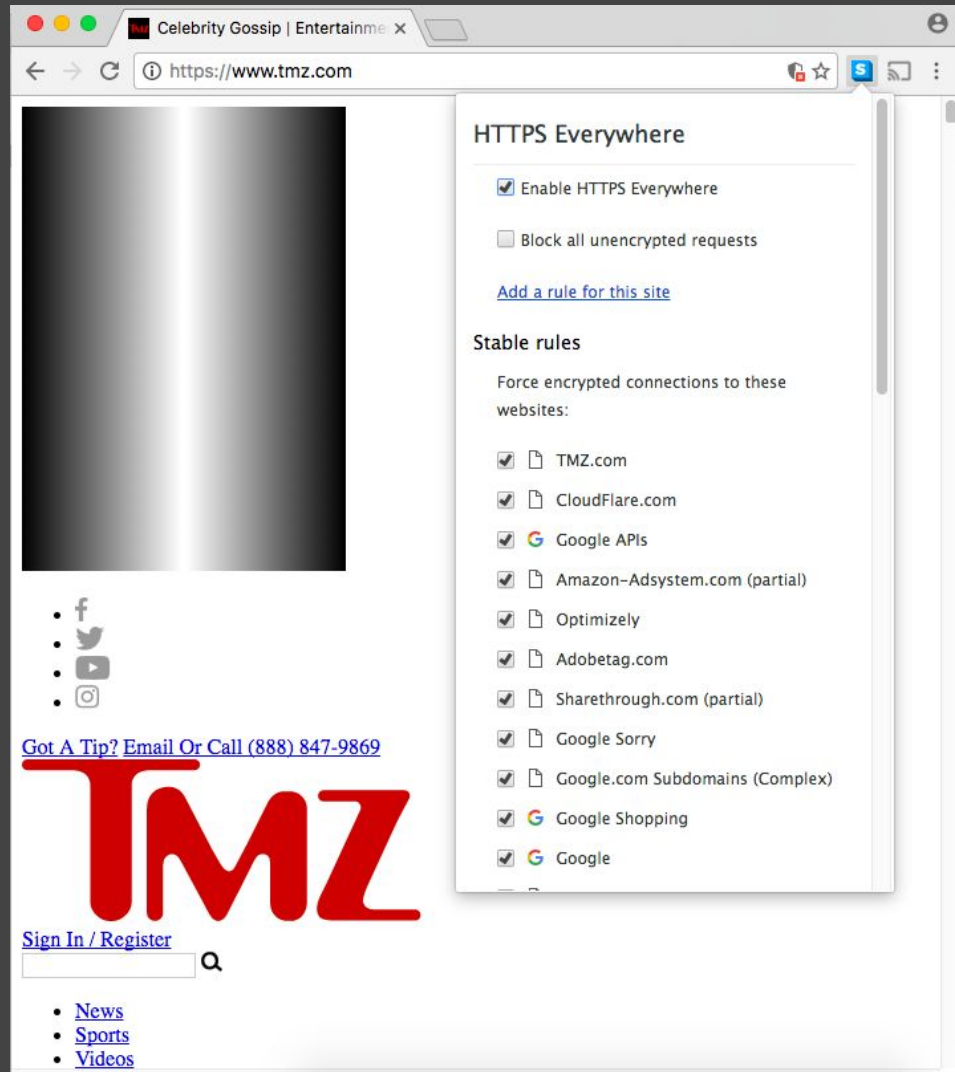
Thank you.

[PRIVACY STATEMENT](#)

COMCAST

HTTPS Everywhere

- A very large (~7.5 MB) regular expression that rewrites URLs to HTTPS when available
- Browser extension for Chrome, Firefox, Opera
- Built in to Tor Browser and Brave
- Sometimes breaks things (mixed content, redirect loops, captive portals)



The screenshot shows a web browser window with the URL <https://www.t TMZ.com>. The page content includes a large black image placeholder, social media icons for Facebook, Twitter, YouTube, and Instagram, a link to "Got A Tip? Email Or Call (888) 847-9869", the large red "TMZ" logo, and a "Sign In / Register" link with a search input field. At the bottom, there are links for "News", "Sports", and "Videos".

The "HTTPS Everywhere" extension settings panel is open on the right side of the browser. It features the following options:

- Enable HTTPS Everywhere
- Block all unencrypted requests
- [Add a rule for this site](#)
- Stable rules**
 - Force encrypted connections to these websites:
 - TMZ.com
 - CloudFlare.com
 - Google APIs
 - Amazon-Adsystem.com (partial)
 - Optimizely
 - Adobetag.com
 - Sharethrough.com (partial)
 - Google Sorry
 - Google.com Subdomains (Complex)
 - Google Shopping
 - Google

2. Prevent sites from seeing the user's activity on other origins.

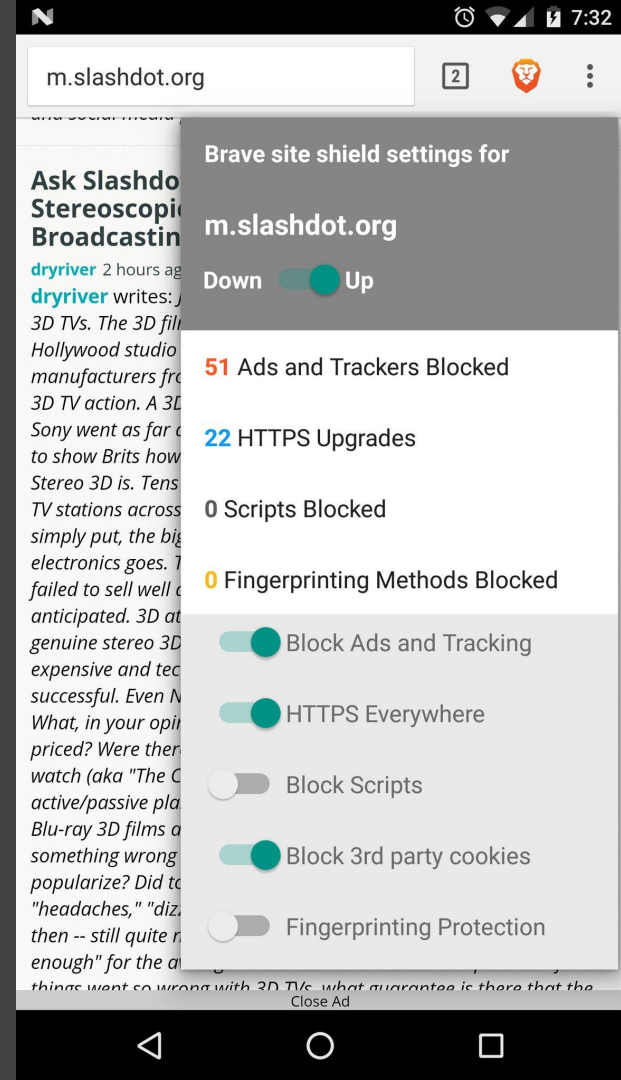


Block 3rd party cookies + blacklist tracking domains

Brave uses tracker and ad block lists from Disconnect.me and Adblock Plus

3p cookies/localStorage blocked by default in Brave, Tor Browser, and Safari

Disconnect's Tracking Protection list is also used in Firefox Private Browsing mode



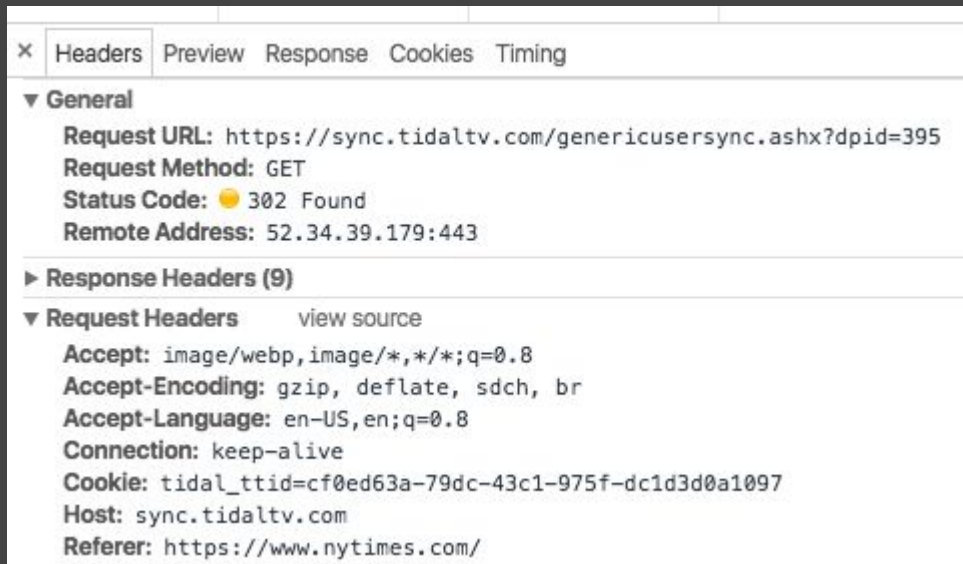
Blocking 3rd party refer(r)er

Default policy:

- HTTPS -> HTTP: no referrer
- Otherwise: referrer sent
- Applies to navigations & subresource requests

Uses:

- ad tracking
- website analytics
- access control (do not do this!!)



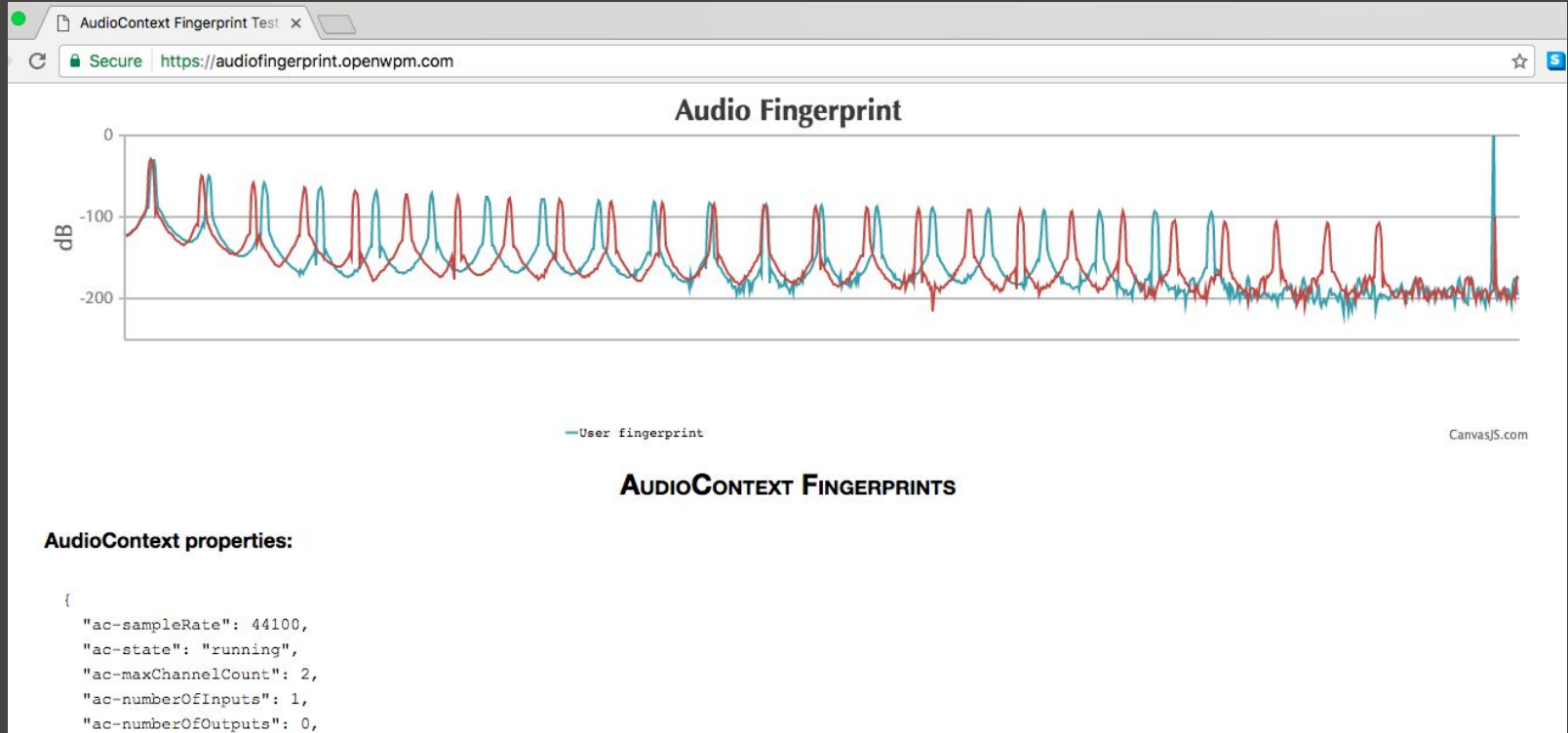
Blocking 3rd party refer(r)er

Brave's policy:

- Same as default behavior for navigations & 1st-party subresources
- For 3rd-party subresources, send the origin of the 3rd-party

No complaints so far except for font-loading domains (???)

3. Prevent unwanted leakage of details about a user's browser, OS, and device



Fingerprinting

- Too many methods
- Many are used legitimately (ex: exposing internal IP address in WebRTC signaling)
- Prioritize blocking fingerprinting methods that have easily-available PoC (ex: fingerprintjs) or have been found in the wild. See <https://webtap.princeton.edu/>

https://jonathanmayer.org/papers_data/trackingsurvey12.pdf

Table III
NON-COOKIE WEB TRACKING TECHNOLOGIES

(a) "Supercookies"
HTTP authentication [†] [84]
HTTP caching ("cache cookies")
cache control
ETags* ("ETag cookies") [85]
Last-Modified [85] (e.g. [86])
cache content
resource (e.g. JavaScript, HTML, CSS, or media)*
status code
redirect location (e.g. [87])
hits and misses (e.g. [88])
TLS/SSL session ID [89]
browsing history ^{††}
userData storage (Internet Explorer only)*
HTML5 storage (session, local, and global)*
HTML5 protocol handlers [†]
HTML5 content handlers [†]
W3C geolocation API permission [†]
window.name property* (session only)
HTTP strict transport security [90]
plug-in storage* (e.g. Flash local shared objects, or "Flash cookies")
DNS cache

* Observed in use by a third-party website.
† User intervention required.
†† Largely inaccessible in newer browsers, but see [88], [91].

(b) Active "Fingerprinting"

operating system
CPU type
user agent
time zone
clock skew
display settings
installed fonts
installed plugins
enabled plugins
supported MIME types
cookies enabled
third-party cookies enabled

(c) Passive "Fingerprinting"

IP address
operating system
user agent
language
HTTP accept headers

Fingerprinting protection in Brave

Default enabled:

- Battery Status API (off by default)
- User-agent (mimic Chrome)
- Set `navigator.plugins` and `navigator.mimeTypes` to `[]`

Default disabled:

- Canvas
- WebGL
- AudioContext
- WebRTC IP leakage



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.38	1.3	DOM localStorage: Yes, DOM session
Hash of canvas fingerprint	7.81	224.25	891f3debe00dbd3d1f0
Screen Size and Color Depth	4.26	19.23	1440x900
Browser Plugin Details	1.68	3.21	undefined
Time Zone	2.95	7.75	0
DNT Header Enabled?	1.22	2.33	False
HTTP_ACCEPT Headers	7.3	157.12	text/html, */*; q=0.01 gzip,
Hash of WebGL fingerprint	5.12	34.71	undetermin
Language	1.02	2.03	en-US
System Fonts	5.64	49.78	Andale Mono, Arial, Arial Black, Arial Hebrew, Arial Unicode MS, Comic Sans MS, Courier, C ca, Helvetica Neue, Impact, LUCIDA GRANDI ino, Tahoma, Times, Times New Roman, Treb dings 2, Wingdings 3
Platform	3.12	8.71	MacInte
			Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11

Site shield settings for
panopticlick.eff.org

Shields

Down



Up

0

Ads and
trackers
Blocked

0

HTTPS
Upgrades

0

Scripts
Blocked

2

Fingerprinting
Methods
BlockedCanvas: <https://panopticlick.eff.org/results?>WebGL: <https://panopticlick.eff.org/results?>

Advanced Controls

Ad Control

Block Ads

Cookie Control

Block 3rd Party Cookies



HTTPS Everywhere



Fingerprinting Protection ?



Block Scripts

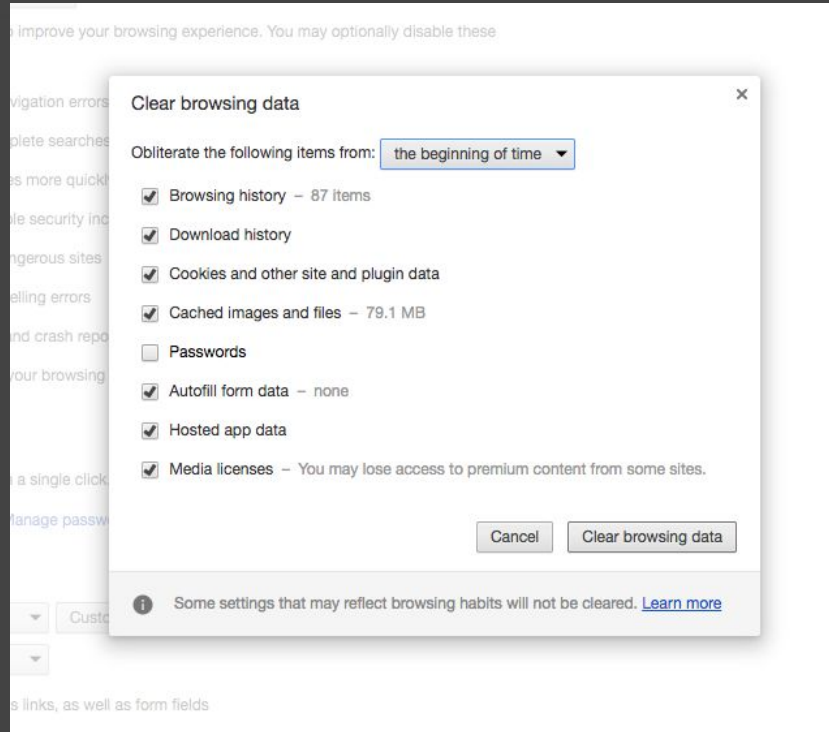


Block Phishing / Malware

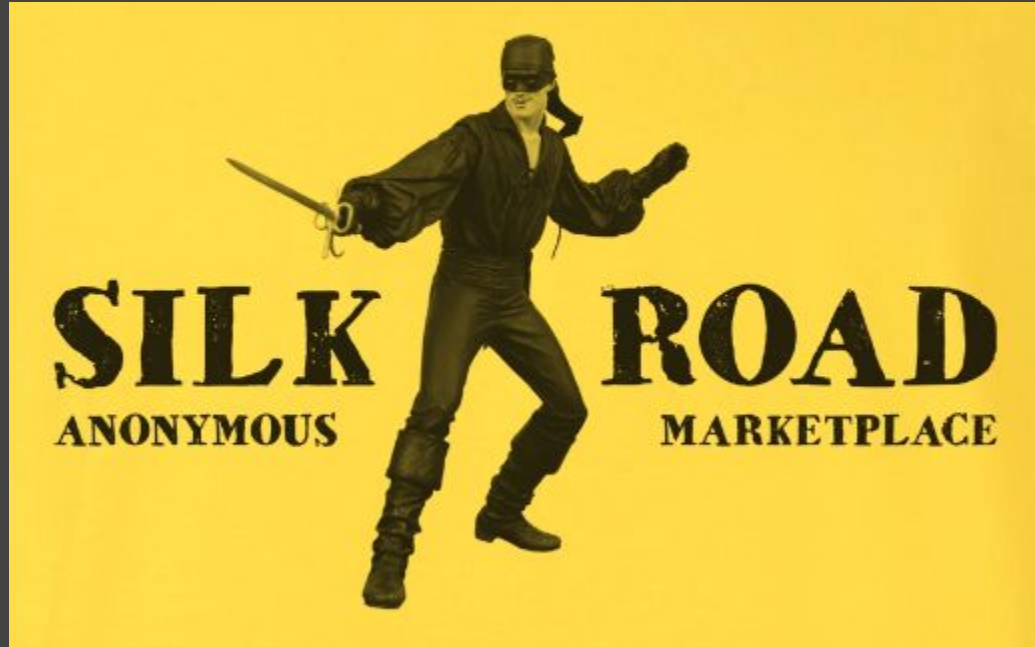
Edit default shield settings...

Reload

4. Prevent linkability across separate browser sessions



5. Forensic deniability



Tradeoffs

Privacy vs. Availability

WhatsApp backdoor allows snooping on encrypted messages

Exclusive: Privacy campaigners criticise WhatsApp vulnerability as a 'huge threat to freedom of speech' and warn it could be exploited by government agencies



Research shows that WhatsApp can read messages due to the way the company has implemented its end-to-end encryption protocol. Photograph: Ritchie B Tongo/EPA

“...when a contact's key changes, should WhatsApp require the user to manually verify the new key before continuing, or should WhatsApp display an advisory notification and continue without blocking the user. **Given the size and scope of WhatsApp's user base, we feel that their choice to display a non-blocking notification is appropriate.**”

<https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/>



Alice

Bob



Bob sees M0

$E(M0, k_bob)$

Bob drops his phone in the ocean



$E(M1, k_bob)$

Bob turns gets a new phone



Hey Alice, this is Bob's new key: k'_bob

Alice's WhatsApp client automatically re-encrypts M1 using k'_bob & sends it



Bob sees M1

$E(M1, k'_bob)$

Alice is notified that Bob's key has changed

Availability++

- Alice doesn't have to take any actions to deliver M1 after hitting 'send'
- Bob seamlessly receives M1 when he turns on his new phone

Privacy--

- Any message sent may be re-encrypted for NSA. Alice has no way to know in advance, Can detect the attack after-the-fact.



This site cannot be loaded due to a certificate error: **https://self-signed.badssl.com/**

net::ERR_CERT_AUTHORITY_INVALID

[Back to safety](#)

[Advanced settings](#)



iCloud has stopped responding.

An error has prevented this application from working properly. Help Apple improve its products by sending us diagnostic and usage information about iCloud.

► Details

By clicking "Send to Apple" you agree that Apple will collect and use this information as part of its support services and to improve its products and services. This report will include personal information such as your member name and user data. To learn more about Apple Privacy Policy, see <https://www.apple.com/privacy/>.

Reload

Send to Apple

Site shield settings for www.icloud.com

Shields
Down Up

0

Ads and trackers Blocked

0

HTTPS Upgrades

0

Scripts Blocked

1

Fingerprinting Method Blocked

Canvas: <https://www.icloud.com/>

▼ Advanced Controls

Ad Control

Block Ads

Cookie Control

Block 3rd Party Cookies

HTTPS Everywhere

Fingerprinting Protection ⓘ

Block Scripts

Block Phishing / Malware

Edit default shield settings...

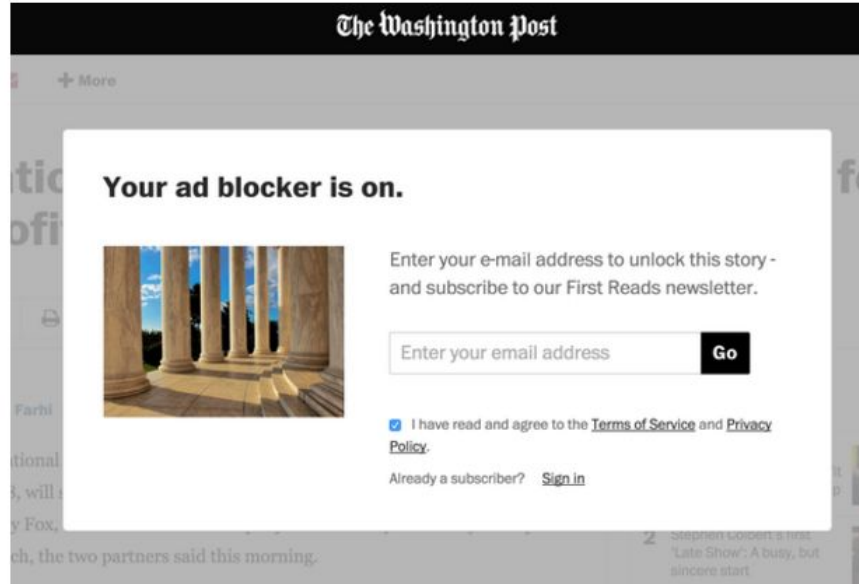
Reload



Matthew Keys
@MatthewKeysLive

Follow

Washington Post disables reading of articles for people with ad blocker software.



RETWEETS
148

FAVORITES
54



Ad-blocker blockers



Hide My AdBlocker

offered by borodin.evgeniy85

★★★★☆ (483)

Productivity

115,468 users

ADD TO CHROME



OVERVIEW

REVIEWS

RELATED

G+ 263

PutLocker.com Upload My Files Go Pro Login Sign Up

man.up.101.hdtv-lol.avi (77.83 MB)

Download faster with our downloader Tired of ads and waiting? Go Pro!

[Download Now](#)

We've detected that you're using AdBlock or some other adblocking software. Your wait time has been increased. Please disable AdBlock for this website to avoid delays.

Please wait for 24 seconds [Get Pro Account](#)

Choose Method of Access

	Continue as Free User	Get Pro Account
Account Type:	Free	Premium
Access Priority:	Low	High
Downloading Originals:	No	Yes
Mobile Access:	No	Yes
Max Filesize:	1GB	5GB
Upload at Once:	10	100

Compatible with your device

This extension hides your AdBlocker from Anti-AdBlock scripts on websites such as putlocker.com, watchfreeinhd.com and more.

This is an anti-anti-adblock extension, which removes time penalties and popups/warnings about your activated AdBlocker.

- Works on
- gmx.net,
 - web.de,
 - sockshare.com,
 - putlocker.com,

[Report Abuse](#)

Version: 1.2

Updated: October 8, 2015

Size: 52.07KB

Language: English

Ad-blocker blocker blockers

Privacy vs. Security

Example:

HSTS cross-origin history sniffing

summary

- Dynamic HSTS: Site sends an HTTP header that says “Only access me over HTTPS for the next N seconds.”
- Dynamic HSTS is by definition dependent on browsing history.
- This can indirectly leak data about a user’s browsing history.

1. sneaky.com wants to fingerprint users.
2. example.com is known to support HSTS.
3. sneaky.com/index.html embeds ``.

What happens then?

Case 1: Browser has never visited example.com

-> makes a network round-trip, gets 301/302 to <https://example.com>

Case 2: Browser visited example.com before.

-> HSTS causes an “internal” redirect (307) to <https://example.com/> ~immediately

If we can measure the HTTP to HTTPS redirect latency, we can distinguish Case 1 from Case 2!

Q: How do we measure that?

A: Abuse one more browser security feature.

Content-Security-Policy:


img-src: https://*;

script-src: 'self'
*.scripts.com
cdn.example.com

Allow images to load
from HTTPS origins
only



Allow scripts to load
from the page's origin,
*.scripts.com, and
cdn.example.com only.



The Missing Ingredient:

Set CSP to **'img-src http://*'**

HTTPS image requests are blocked and fire an error event to JS listeners.

This is a “non-destructive” cache attack.

Why is this useful?

1. JS only lets us listen for `img onerror` and `onload` events. Turns out CSP violation triggers `onerror` consistently and early in the fetch pipeline.
2. If browser ever completes a request for <https://example.com>, it will get the HSTS pin and future results are polluted. CSP prevents this from happening!

After setting CSP:

Case 1: Browser has never visited example.com

-> makes network request, gets 301/302 to <https://example.com>, img onerror fires.

Case 2: Browser visited example.com before.

-> HSTS rewrites src to <https://example.com/>
~immediately, img onerror fires.

How long does the HTTP to HTTPS redirect take?

Case 1: Browser has never visited example.com

-> Order of 100ms depending on network latency and site response time.

Case 2: Browser visited example.com before.

-> Order of 1ms, independent of the site and network conditions.

CSS visited-selector bug

Slide from Michael Coates, 2011 ->

CSS History Sniffing

- Determine user's browsing habits with CSS
- Visited link different than non-visited link
- CSS and element inspection determines visited pages
- Issued fixed March 2010



Visited Link

Unvisited Link

```
if (getComputedStyle(link, "").color ==
    "rgb(0, 0, 128)")
{
    // link.href has not been visited
} else {
    // link.href has been visited
}
}
```

<http://dbaron.org/mozilla/visited-privacy>

New plan:

1. Scrape Alexa Top 1M for hosts that send HSTS and aren't preloaded.
2. Load all the HSTS hosts asynchronously on one page.
3. Measure the onerror timing & separate hosts into visited and unvisited.

Mitigations

- Decrease JS timer resolution: can be worked around
- First-party storage isolation (“double-keying”): reduces security
- HTTPS Everywhere / expanding HSTS preload: get rid of dynamic HSTS

CVE-2016-1617 addressed in CSP Level 3

3. The URL matching algorithm now treats insecure schemes and ports as matching their secure variants. That is, the source expression `http://example.com:80` will match both `http://example.com:80` and `https://example.com:443`.

Likewise, `'self'` now matches `https:` and `wss:` variants of the page's origin, even on pages whose scheme is `http`.



WebKit

Open Source Web Browser Engine

[Blog](#)

[Downloads](#)

[Feature Status](#)

[Reporting Bugs](#)

[Contribute](#) ▾

Release Notes for Safari Technology Preview 21

Jan 11, 2017

by Jon Davis

[@jonathandavis](#)

[Safari Technology Preview](#) Release 21 is now [available for download](#) for macOS Sierra. If you already have Safari Technology Preview installed, you can update from the Mac App Store's Updates tab. This release covers WebKit revisions [209803-210274](#).

Security

- Allowed HTTPS URLs to match HTTP script-src expressions for Content Security Policy ([r209821](#))

Other security vs privacy examples

- Sniff history using site-specific settings (ex: NoScript)
- Fingerprint use of hardened browser settings (Tor, adblocking, etc.)



Other ways to win

How is CVE formed?

[N/A][[664411](#)] **High** CVE-2016-9651: Private property access in V8. *Credit to Guang Gong of Alpha Team Of Qihoo 360 reported through Pwnfest*

[\$7500][[658535](#)] **High** CVE-2016-5208: Universal XSS in Blink. *Credit to Mariusz Mlynski*

[\$7500][[655904](#)] **High** CVE-2016-5207: Universal XSS in Blink. *Credit to Mariusz Mlynski*

[\$7500][[653749](#)] **High** CVE-2016-5206: Same-origin bypass in PDFium. *Credit to Rob Wu (robwu.nl)*

[\$7500][[646610](#)] **High** CVE-2016-5205: Universal XSS in Blink. *Credit to Anonymous*

[\$7500][[630870](#)] **High** CVE-2016-5204: Universal XSS in Blink. *Credit to Mariusz Mlynski*

[\$5000][[664139](#)] **High** CVE-2016-5209: Out of bounds write in Blink. *Credit to Giwan Go of STEALIEN*

[\$3000][[644219](#)] **High** CVE-2016-5203: Use after free in PDFium. *Credit to Anonymous*

[\$3500][[654183](#)] **High** CVE-2016-5210: Out of bounds write in PDFium. *Credit to Ke Liu of Tencent's Xuanwu LAB*

[\$3000][[653134](#)] **High** CVE-2016-5212: Local file disclosure in DevTools. *Credit to Khalil Zhani*

[\$3000][[649229](#)] **High** CVE-2016-5211: Use after free in PDFium. *Credit to Anonymous*

[\$500][[652548](#)] **High** CVE-2016-5213: Use after free in V8. *Credit to Khalil Zhani*

[N/A][[601538](#)] **Medium** CVE-2016-5214: File download protection bypass. *Credit to Jonathan Birch and MSVR*

[\$3000][[653090](#)] **Medium** CVE-2016-5216: Use after free in PDFium. *Credit to Anonymous*

[\$3000][[619463](#)] **Medium** CVE-2016-5215: Use after free in Webaudio. *Credit to Looben Yang*

[\$2500][[654280](#)] **Medium** CVE-2016-5217: Use of unvalidated data in PDFium. *Credit to Rob Wu (robwu.nl)*

[\$2000][[660498](#)] **Medium** CVE-2016-5218: Address spoofing in Omnibox. *Credit to Abdulrahman Alqabandi (@qab)*

[\$1500][[657568](#)] **Medium** CVE-2016-5219: Use after free in V8. *Credit to Rob Wu (robwu.nl)*

[\$1000][[660854](#)] **Medium** CVE-2016-5221: Integer overflow in ANGLE. *Credit to Tim Becker of ForAllSecure*

[\$1000][[654279](#)] **Medium** CVE-2016-5220: Local file access in PDFium. *Credit to Rob Wu (robwu.nl)*

[\$500][[657720](#)] **Medium** CVE-2016-5222: Address spoofing in Omnibox. *Credit to xisigr of Tencent's Xuanwu Lab*

Chrome 55

<https://chromereleases.googleblog.com/2016/12/stable-channel-update-for-desktop.html>

8 out of 26 externally-reported CVEs are in
PDFium

PDF.js to the rescue

- Pure HTML5/CSS/JS PDF reader
- Maintained by Mozilla
- Default PDF reader in Firefox

<https://github.com/mozilla/pdf.js/>

Flash must die



Adobe Security Bulletin

Security updates available for Adobe Flash Player

Release date: December 8, 2015

Last updated: June 3, 2016

Vulnerability identifier: APSB15-32

Priority: [See table below](#)

CVE number: CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8418, CVE-2015-8454, CVE-2015-8455, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8456, CVE-2015-8457, CVE-2015-8652, CVE-2015-8653, CVE-2015-8654, CVE-2015-8655, CVE-2015-8656, CVE-2015-8657, CVE-2015-8658, CVE-2015-8820, CVE-2015-8821, CVE-2015-8822, CVE-2015-8823

Platform: All Platforms



Insert image

Upload

Take a snapshot

By URL

Your albums

Google Drive

Search

Unable to find Flash Player 10.1. Please install Flash Player or upgrade your Flash Player to Flash 10.1 or greater [here](#).



Control-click to play Shockwave Flash.

**How to deprecate Flash
without breaking the web?**

1. Don't bundle Flash with the browser or enable it by default.

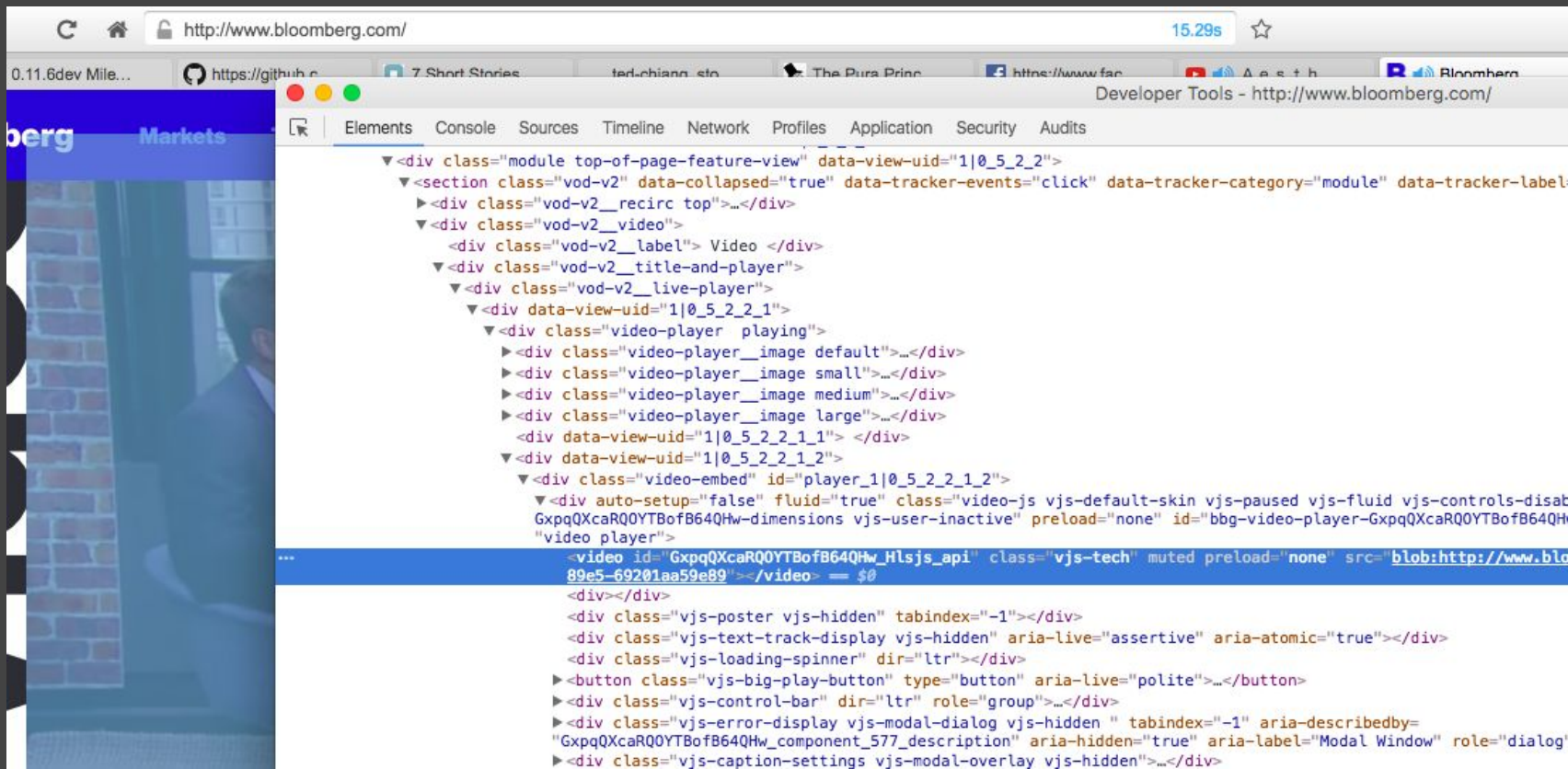
Plugin Settings

Enable Adobe Flash support

i Brave uses a special version of Pepper Flash which must be installed from [Adobe](#).

i Flash not working? Try the troubleshooting tips on our [wiki](#).

2. Pretend Flash isn't installed in navigator.plugins to trigger HTML5 fallback

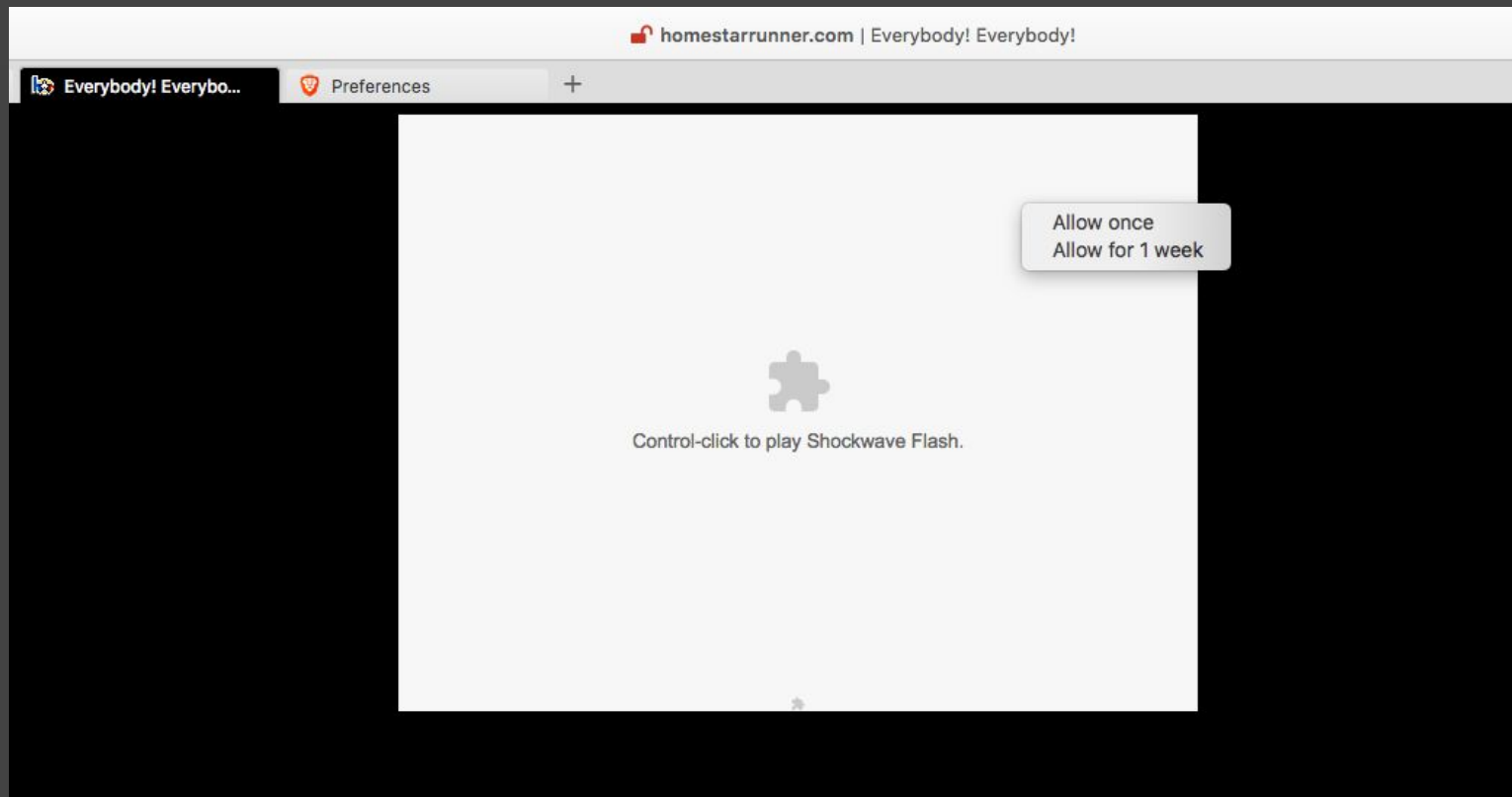


The screenshot shows a web browser window with the address bar displaying `http://www.bloomberg.com/`. The page content is partially visible on the left, showing a blue header with the word "Markets" and a video player interface. The developer tools are open, showing the "Elements" panel with a tree view of the DOM. The selected element is a video player, and the console shows the HTML code for the video player, including the `<video>` tag and various control elements.

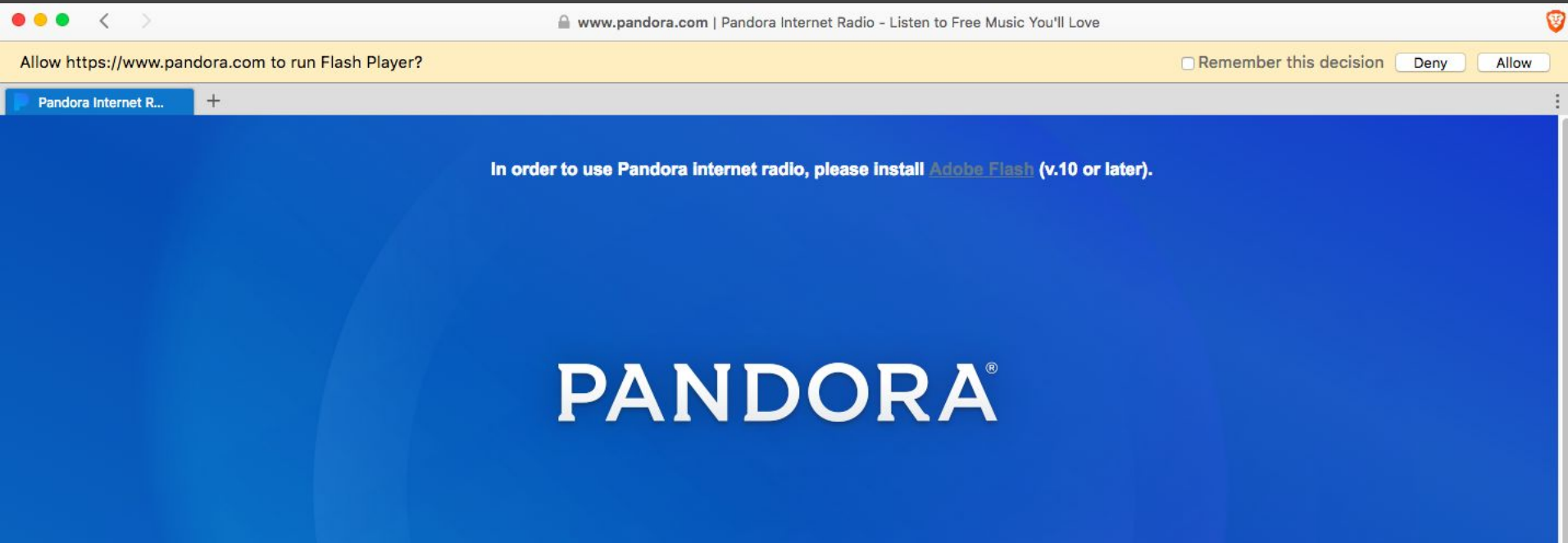
```
<div class="module top-of-page-feature-view" data-view-uid="1|0_5_2_2">
  <section class="vod-v2" data-collapsed="true" data-tracker-events="click" data-tracker-category="module" data-tracker-label...
    <div class="vod-v2_recirc top">...</div>
    <div class="vod-v2__video">
      <div class="vod-v2_label"> Video </div>
      <div class="vod-v2__title-and-player">
        <div class="vod-v2__live-player">
          <div data-view-uid="1|0_5_2_2_1">
            <div class="video-player playing">
              <div class="video-player__image default">...</div>
              <div class="video-player__image small">...</div>
              <div class="video-player__image medium">...</div>
              <div class="video-player__image large">...</div>
              <div data-view-uid="1|0_5_2_2_1_1"> </div>
            <div data-view-uid="1|0_5_2_2_1_2">
              <div class="video-embed" id="player_1|0_5_2_2_1_2">
                <div auto-setup="false" fluid="true" class="video-js vjs-default-skin vjs-paused vjs-fluid vjs-controls-disab...
                  GxpqQXcaRQ0YTBofB64QHW-dimensions vjs-user-inactive" preload="none" id="bbg-video-player-GxpqQXcaRQ0YTBofB64QH...
                  "video player">
                    <video id="GxpqQXcaRQ0YTBofB64QHW_Hlsjs_api" class="vjs-tech" muted preload="none" src="blob:http://www.blo...
                      89e5-69201aa59e89"></video> = $0
                  <div></div>
                  <div class="vjs-poster vjs-hidden" tabindex="-1"></div>
                  <div class="vjs-text-track-display vjs-hidden" aria-live="assertive" aria-atomic="true"></div>
                  <div class="vjs-loading-spinner" dir="ltr"></div>
                  <button class="vjs-big-play-button" type="button" aria-live="polite">...</button>
                  <div class="vjs-control-bar" dir="ltr" role="group">...</div>
                  <div class="vjs-error-display vjs-modal-dialog vjs-hidden" tabindex="-1" aria-describedby=...
                    "GxpqQXcaRQ0YTBofB64QHW_component_577_description" aria-hidden="true" aria-label="Modal Window" role="dialog...
                  <div class="vjs-caption-settings vjs-modal-overlay vjs-hidden">...</div>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </section>
</div>
```


3. After being enabled, user must express intent to run Flash on an origin before it can be detected.

Click-to-play for visible elements



Handle Flash installer redirects for pages that don't load Flash objects until Flash is detected
























4. Expire Flash approvals

Saved Site Permissions

Run Adobe Flash Player([Clear all](#))

- ✘ <http://homestarrunner.com>: *Allow until 1/30/2017, 9:16:05 AM*
- ✘ <https://www.pandora.com>: *Allow once*

5. Deal with 2948238294829 support complaints

<input type="checkbox"/>	 Flash not working on http://www.mlrtahoe.com/the-resort/webcam/ plugin/flash webcompat #6612 opened 11 days ago by alexwykoff  0.13.1	
<input type="checkbox"/>	 Flash not working on Webkinz.com/ plugin/flash webcompat #6538 opened 18 days ago by srirambv	
<input type="checkbox"/>	 Flash control is not displaying for VMware vSphere web client bug plugin/flash #6526 opened 19 days ago by alexwykoff	
<input type="checkbox"/>	 "enable flash" notification should display when navigating to the adobe flash installer page if flash is installed and not enabled plugin/flash #6381 opened on Dec 22, 2016 by bridiver	
<input type="checkbox"/>	 Flash not loading on http://www.clubpenguin.com/ & http://www.binweevils.com/ plugin/flash webcompat #6162 opened on Dec 12, 2016 by srirambv	 2
<input type="checkbox"/>	 Flash Play Supports info-needed plugin/flash #6043 opened on Dec 6, 2016 by bnmnb	 2
<input type="checkbox"/>	 Could not load plugin error on FB videos plugin/flash #6025 opened on Dec 5, 2016 by srirambv	
<input type="checkbox"/>	 Google Finance interactive charts doesn't work with Brave plugin/flash webcompat #5487 opened on Nov 8, 2016 by srirambv	 1
<input type="checkbox"/>	 Flash UX improvement tracking issue plugin/flash #4789 opened on Oct 14, 2016 by alexwykoff  1.1.0	 2
<input type="checkbox"/>	 flash on xfinity tv plugin/flash #4639 opened on Oct 8, 2016 by darkdh	
<input type="checkbox"/>	 Audio Stream window does not open plugin/flash webcompat #4588 opened on Oct 6, 2016 by Evangelistken	 1
<input type="checkbox"/>	 Flash cover slide not shown on youku.com plugin/flash #4532 opened on Oct 5, 2016 by alexwykoff	
<input type="checkbox"/>	 Certain Flash games on Facebook doesn't load plugin/flash webcompat #4397 opened on Sep 30, 2016 by srirambv	

tl;dr

Browsers are a good place to improve privacy on the web.

Most browser features that can be abused for tracking also have legitimate uses. :(

Take away features until people complain too much.

Thanks

yan@brave.com
@bcrypt