Security and Privacy Settings for Firefox Power Users

François Marier <francois@mozilla.com>

enable

disable

restrict

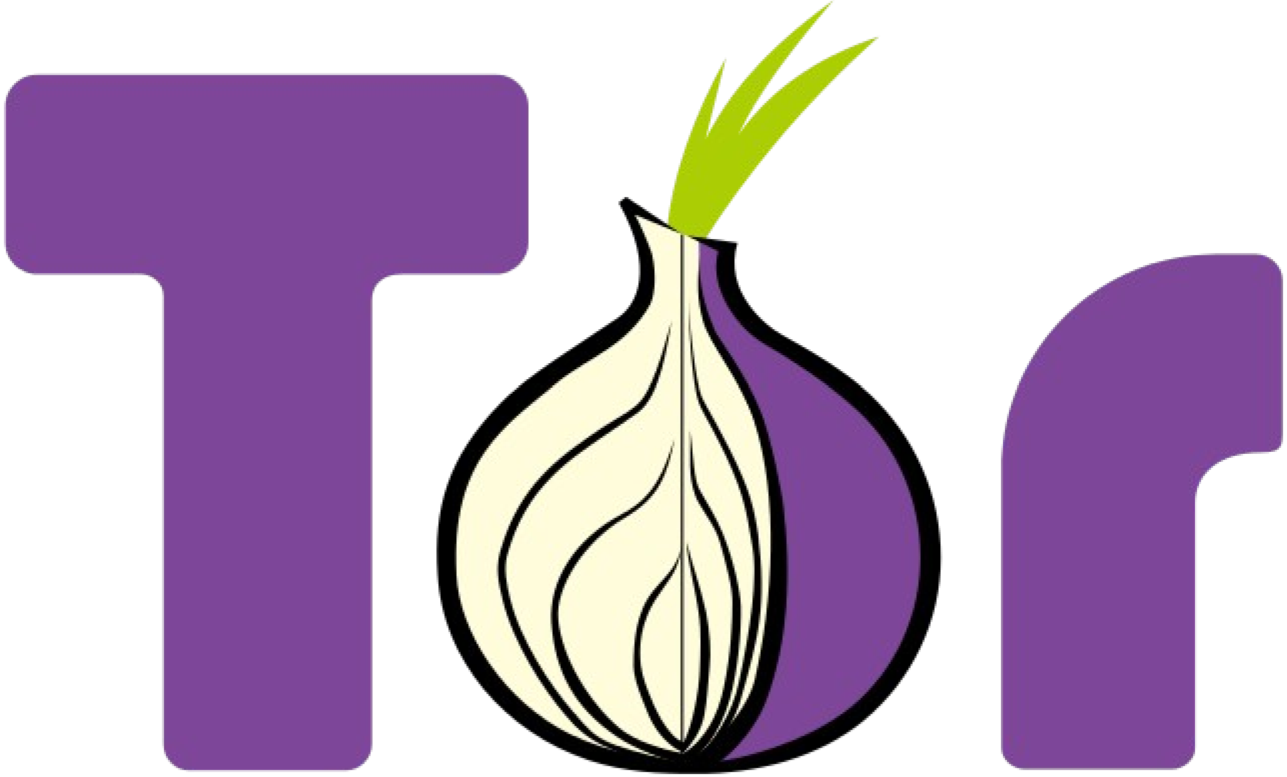
enable

disable

restrict

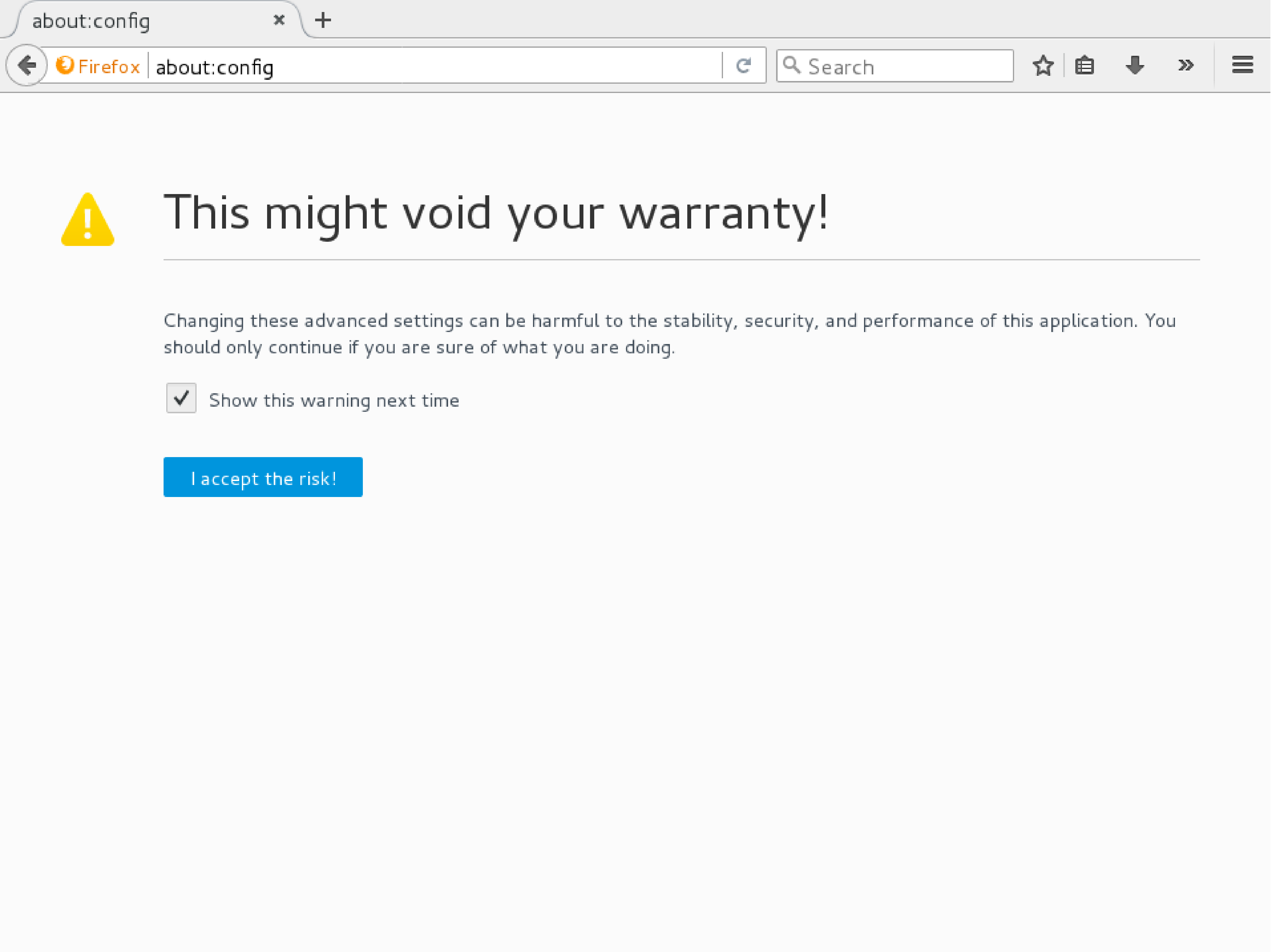
~~eliminating all fingerprinting~~

~~eliminating all fingerprinting~~



features to enable

✓

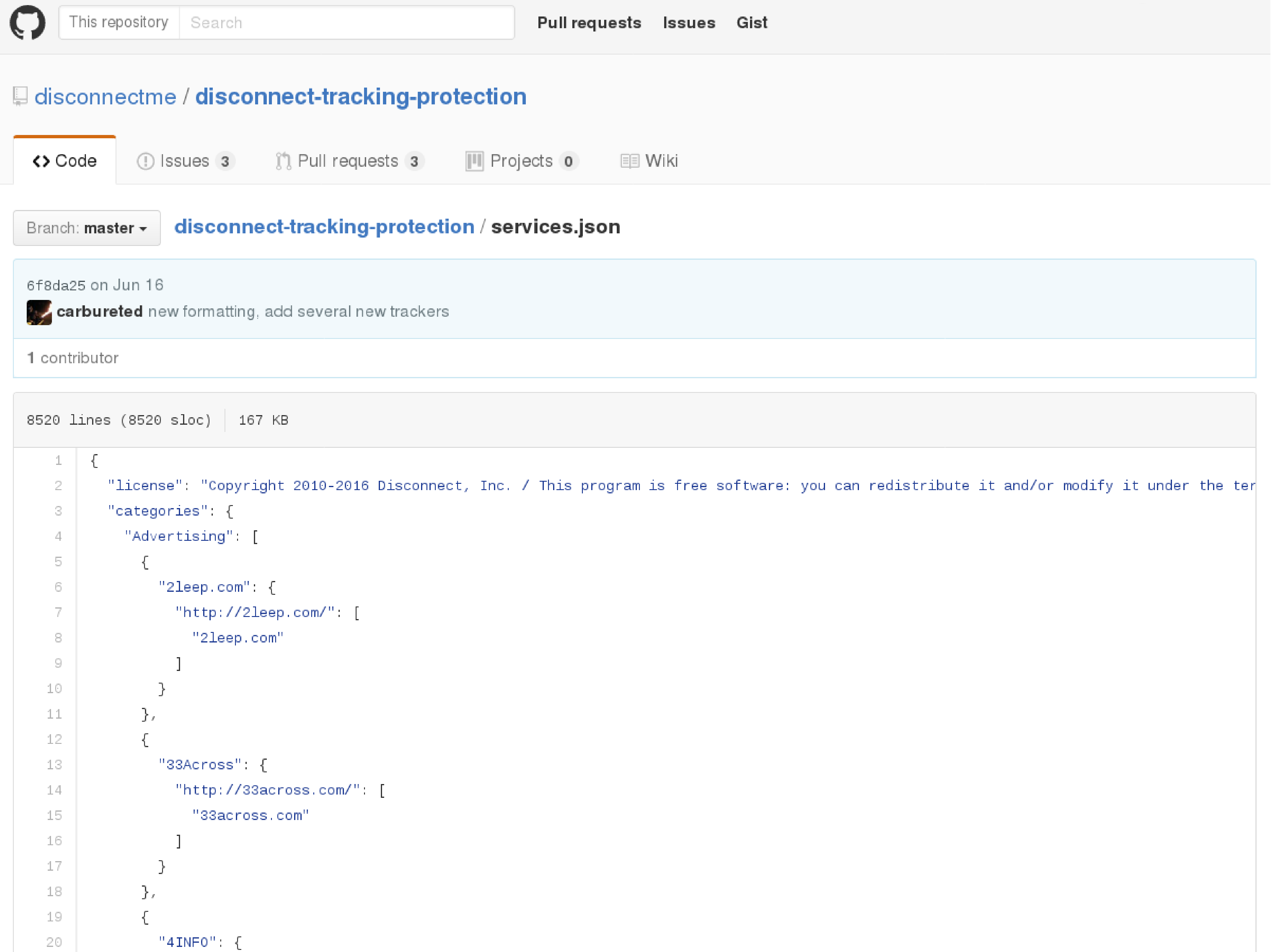


This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

`privacy.trackingprotection.enabled`



disconnectme / disconnect-tracking-protection

disconnect-tracking-protection / services.json

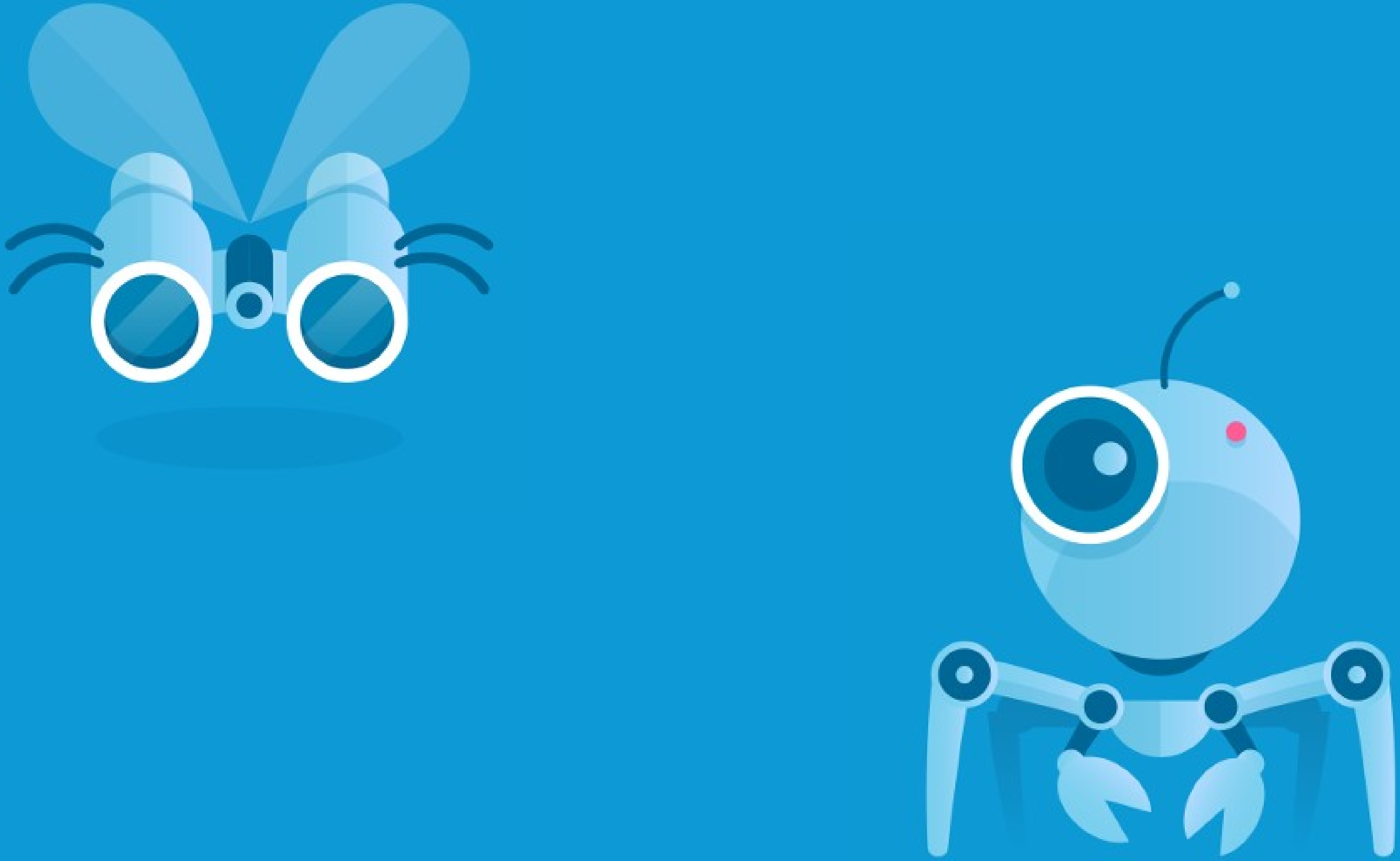
6f8da25 on Jun 16

carbureted new formatting, add several new trackers

1 contributor

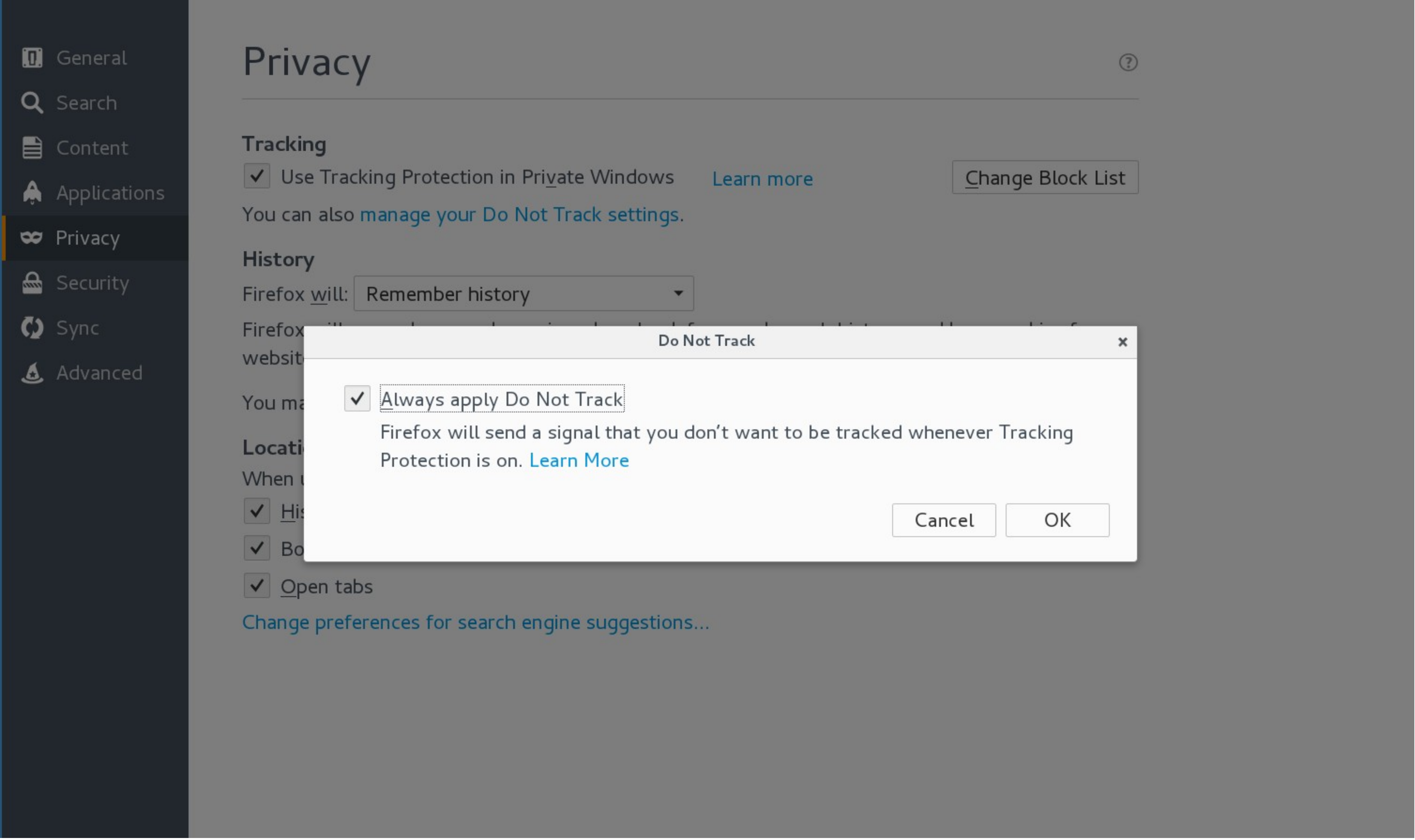
8520 lines (8520 sloc) | 167 KB

```
{
  "license": "Copyright 2010-2016 Disconnect, Inc. / This program is free software: you can redistribute it and/or modify it under the ter
  "categories": {
    "Advertising": [
      {
        "2leep.com": {
          "http://2leep.com/": [
            "2leep.com"
          ]
        }
      },
      {
        "33Across": {
          "http://33across.com/": [
            "33across.com"
          ]
        }
      },
      {
        "4INFO": {
```



feeding.cloud.geek.nz/posts/how-tracking-protection-works-in-firefox

Do Not Track



Privacy

Tracking

☑ Use Tracking Protection in Private Windows Learn more

You can also manage your Do Not Track settings.

History

Firefox will: Remember history

Firefox

websit

You ma

Locati

When u

☑ His

☑ Bo

☑ Open tabs

Change preferences for search engine suggestions…

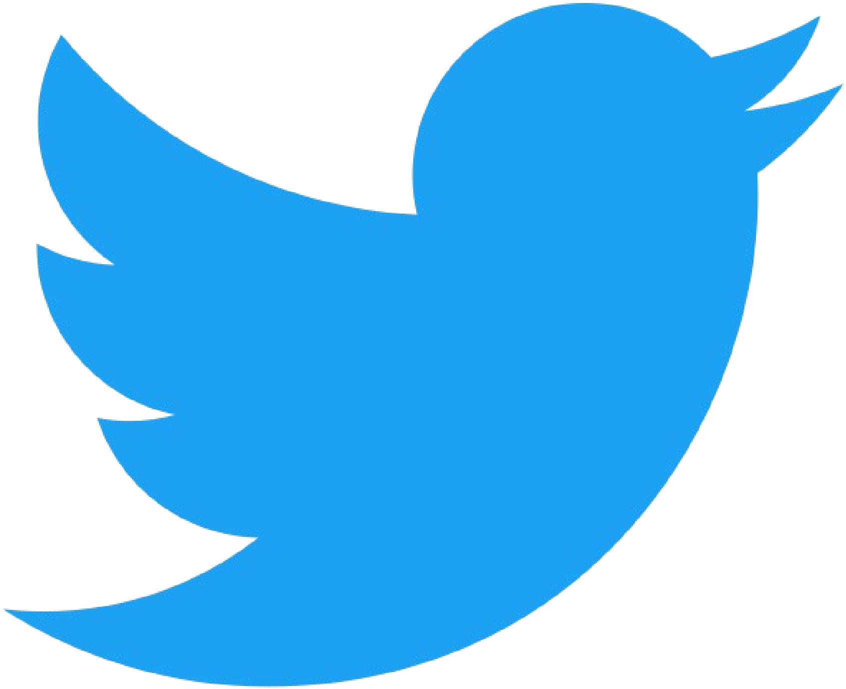
Do Not Track

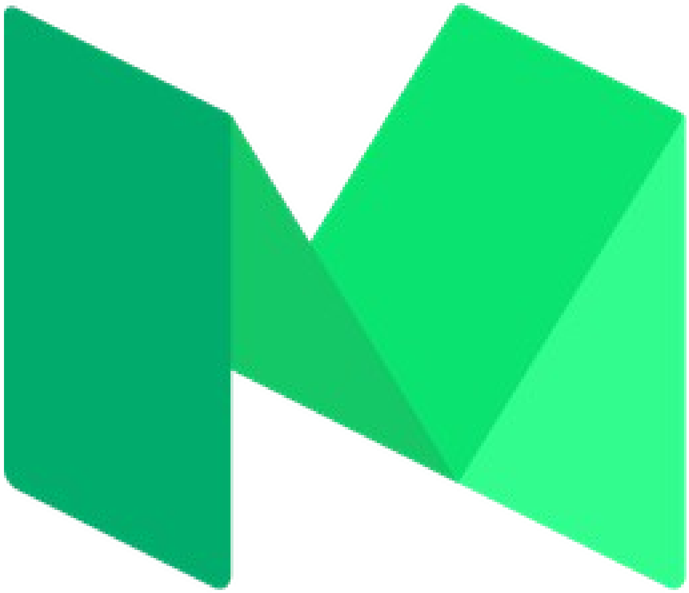
☑ Always apply Do Not Track

Firefox will send a signal that you don’t want to be tracked whenever Tracking Protection is on. Learn More

`privacy.donottrackheader.enabled`

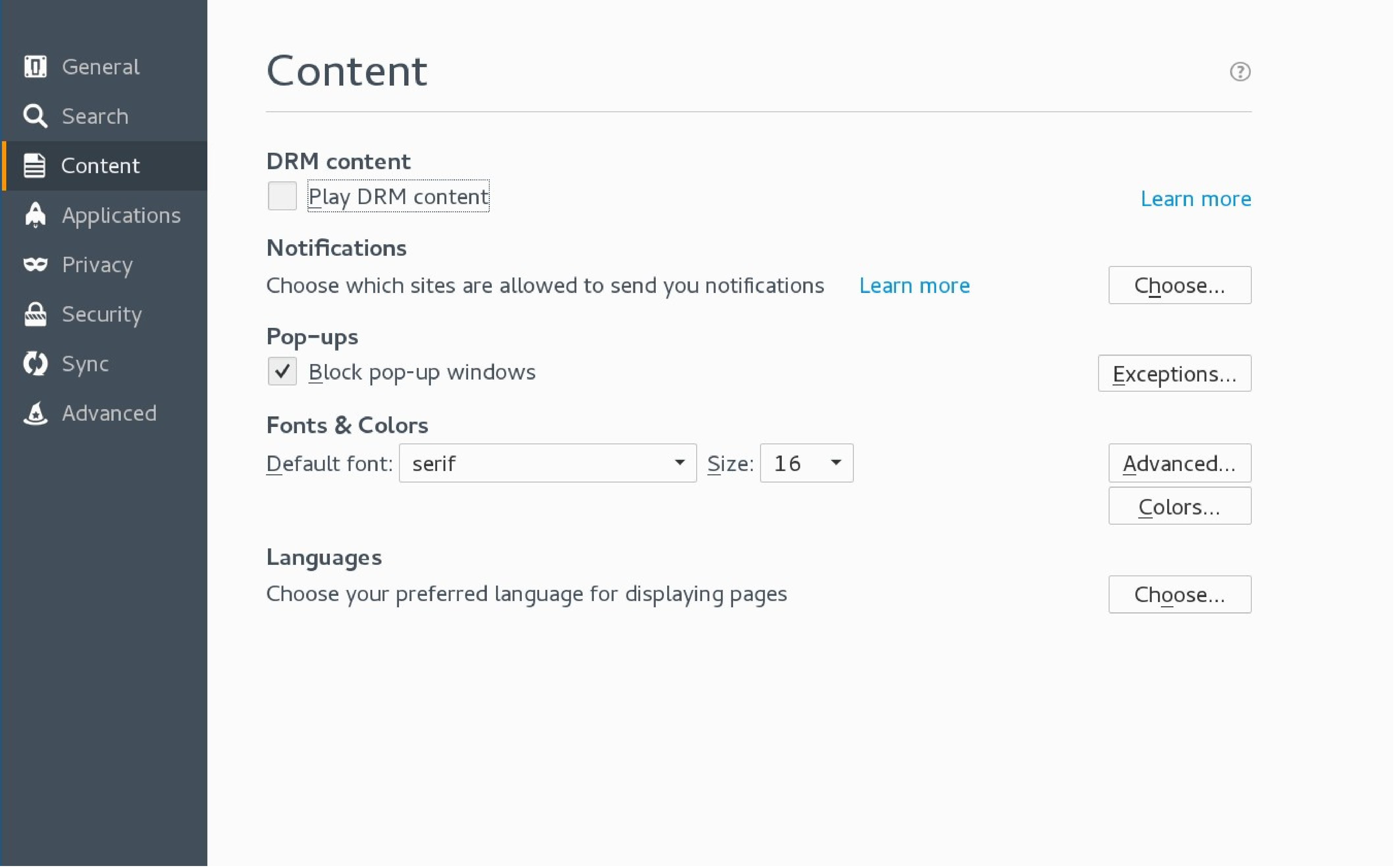
```
privacy.donottrackheader.enabled
```





features to disable

DRM | NO ONE ADMITTED



Content

DRM content

□ Play DRM content

Notifications

Choose which sites are allowed to send you notifications Learn more

Pop-ups

☑ Block pop-up windows

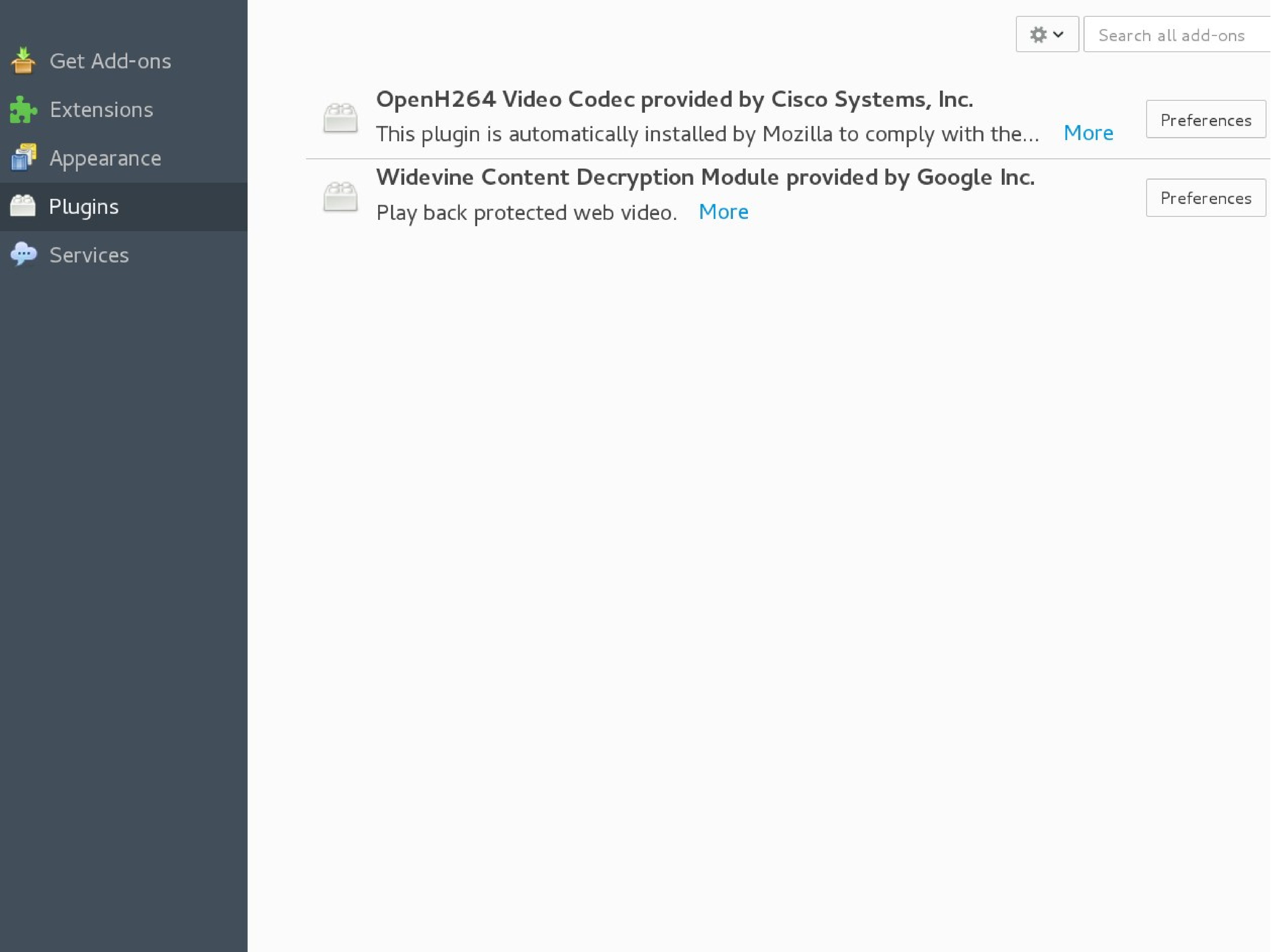
Fonts & Colors

Default font: serif Size: 16

Languages

Choose your preferred language for displaying pages

```
media.eme.enabled
```



OpenH264 Video Codec provided by Cisco Systems, Inc.

This plugin is automatically installed by Mozilla to comply with the...

Widevine Content Decryption Module provided by Google Inc.

Play back protected web video.

Gyrophone: Recognizing Speech From Gyroscope Signals

Yan Michalevsky Dan Boneh
Computer Science Department
Stanford University

Gabi Nakibly
National Research & Simulation Center
Rafael Ltd.

Abstract

We show that the MEMS gyroscopes found on modern smart phones are sufficiently sensitive to measure acoustic signals in the vicinity of the phone. The resulting signals contain only very low-frequency information (<200Hz). Nevertheless we show, using signal processing and machine learning, that this information is sufficient to identify speaker information and even parse speech. Since iOS and Android require no special permissions to access the gyro, our results show that apps and active web content that cannot access the microphone can nevertheless eavesdrop on speech in the vicinity of the phone.

1 Introduction

Modern smartphones and mobile devices have many sensors that enable rich user experience. Being generally put to good use, they can sometimes unintentionally expose information the user does not want to share. While gyroscopes are sufficiently sensitive to measure acoustic vibrations. This leads to the possibility of recovering speech from gyroscope readings, namely using the gyroscope as a crude microphone. We show that the sampling rate of the gyroscope is up to 200 Hz which covers some of the audible range. This raises the possibility of eavesdropping on speech in the vicinity of a phone without access to the real microphone.

As the sampling rate of the gyroscope is limited, one cannot fully reconstruct a comprehensible speech from measurements of a single gyroscope. Therefore, we resort to automatic speech recognition. We extract features from the gyroscope measurements using various signal processing methods and train machine learning algorithms for recognition. We achieve about 50% success rate for speaker identification from a set of 10 speakers. We also show that while limiting ourselves to a small vocabulary consisting solely of digit pronunciations (”one”, ”two”, ”three”, ...) and achieve speech recognition success rate of 65% for the speaker dependent case and up

19 Apr 2017 on w3c | privacy | web browser | firefox | privacy engineering | chrome | sensors | light sensor

Stealing sensitive browser data with the W3C Ambient Light Sensor API

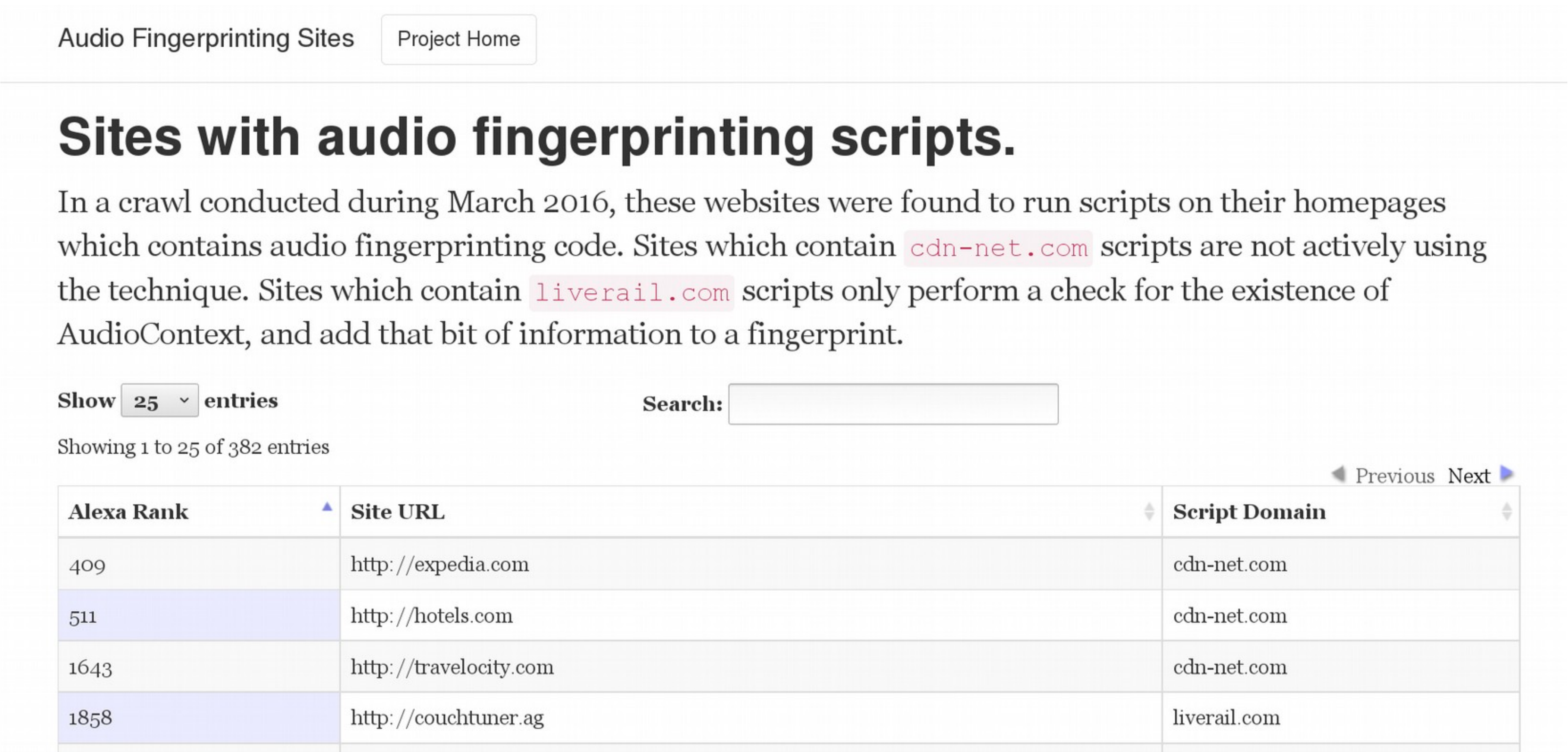
In this post we describe and demonstrate a neat trick to **exfiltrate sensitive information from your browser** using a surprising tool: **your smartphone or laptop's ambient light sensor**.

In short:

1. We provide background about the light sensor API and current discussions to expose it more broadly to websites.
2. We show how the color of the screen of the user's device can affect light sensor readings, and explain why this has dangerous security and privacy consequences. We focus on **extracting browsing history** and **stealing data from cross-origin frames**, which makes it possible for

```
device.sensors.enabled
```

dom.webaudio.enabled

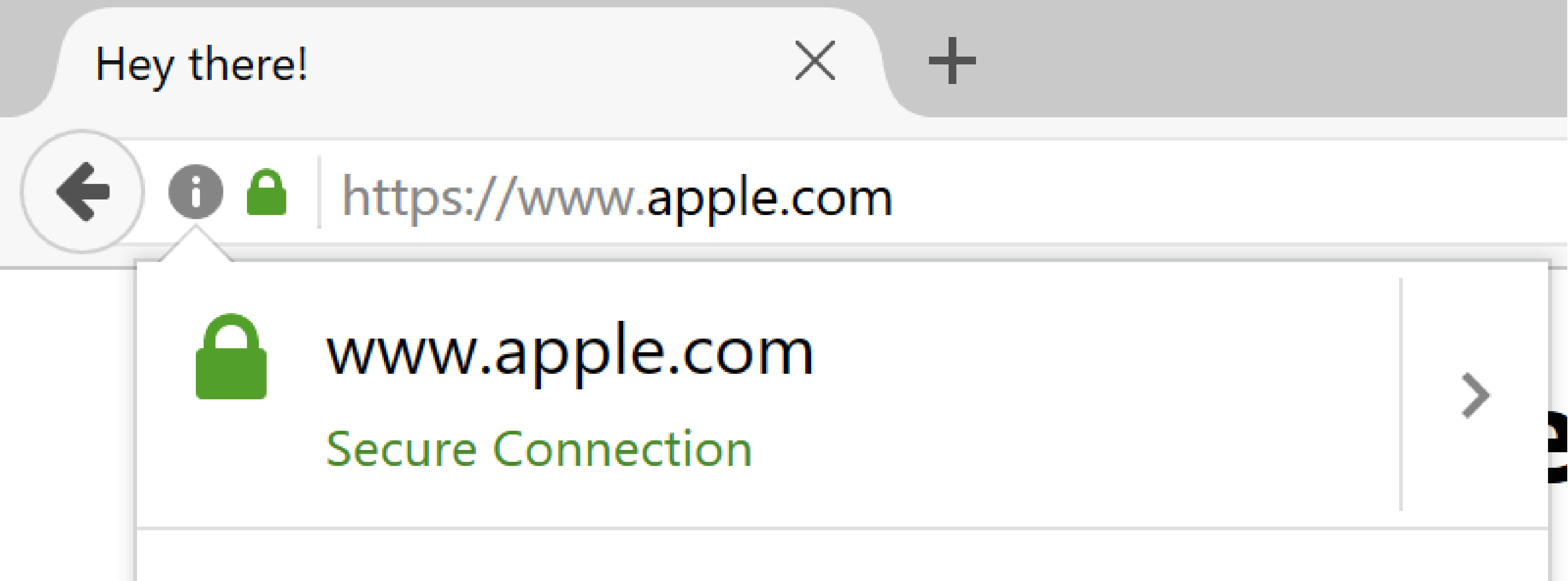


Sites with audio fingerprinting scripts.

In a crawl conducted during March 2016, these websites were found to run scripts on their homepages which contains audio fingerprinting code. Sites which contain `cdn-net.com` scripts are not actively using the technique. Sites which contain `liverail.com` scripts only perform a check for the existence of AudioContext, and add that bit of information to a fingerprint.

Showing 1 to 25 of 382 entries

Alexa Rank	Site URL	Script Domain
409	http://expedia.com	cdn-net.com
511	http://hotels.com	cdn-net.com
1643	http://travelocity.com	cdn-net.com
1858	http://couchtuner.ag	liverail.com



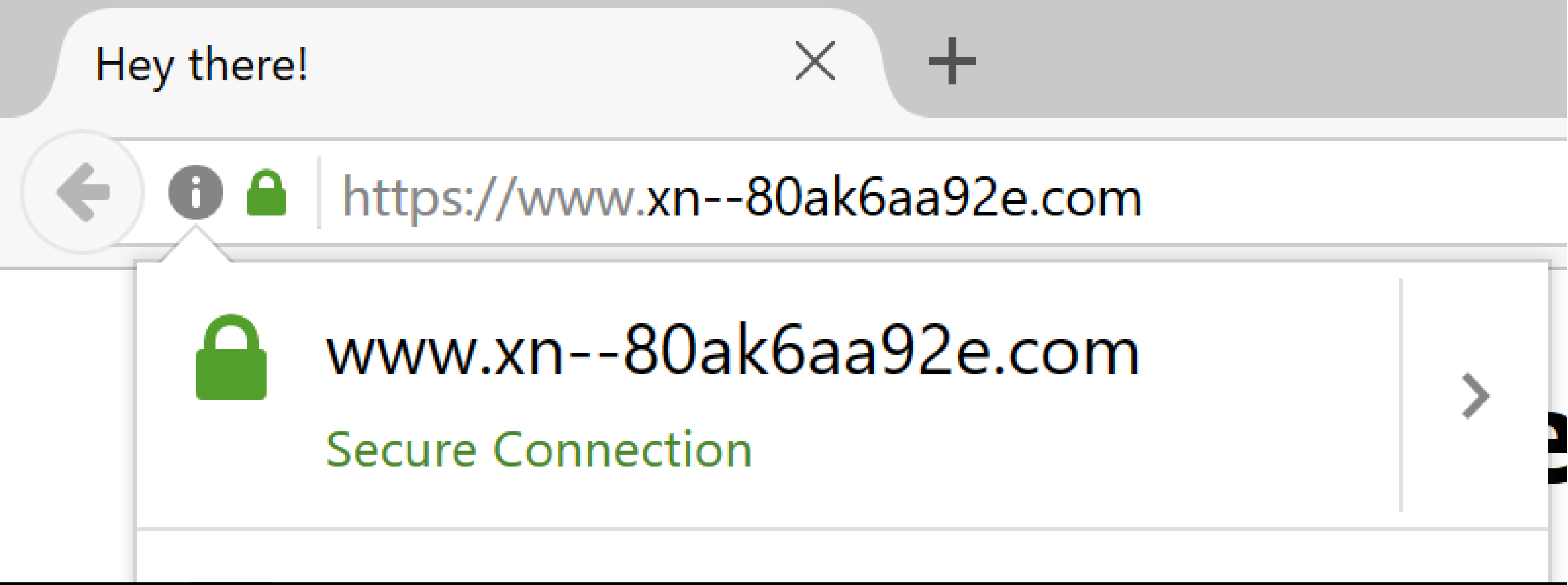
Hey there!

https://www.apple.com

www.apple.com

Secure Connection

IDN spoofing



Hey there!

https://www.xn--80ak6aa92e.com

www.xn--80ak6aa92e.com

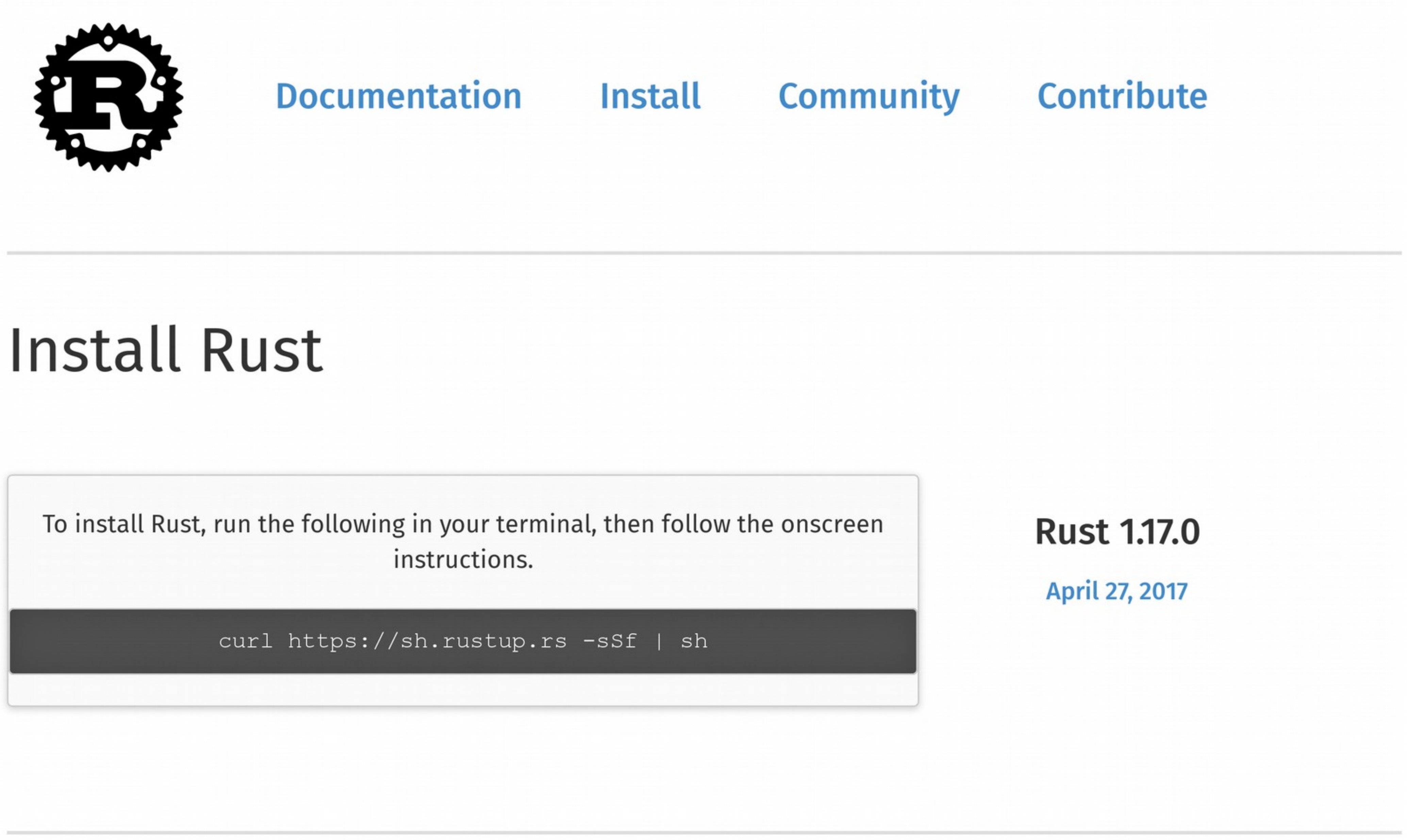
Secure Connection

```
network.IDN_show_punycode
```

www.fsf.org

www.eff.org

```
layout.css.visited_links_enabled
```



Install Rust

To install Rust, run the following in your terminal, then follow the onscreen instructions.

```
curl https://sh.rustup.rs -sSf | sh
```

Rust 1.17.0

April 27, 2017

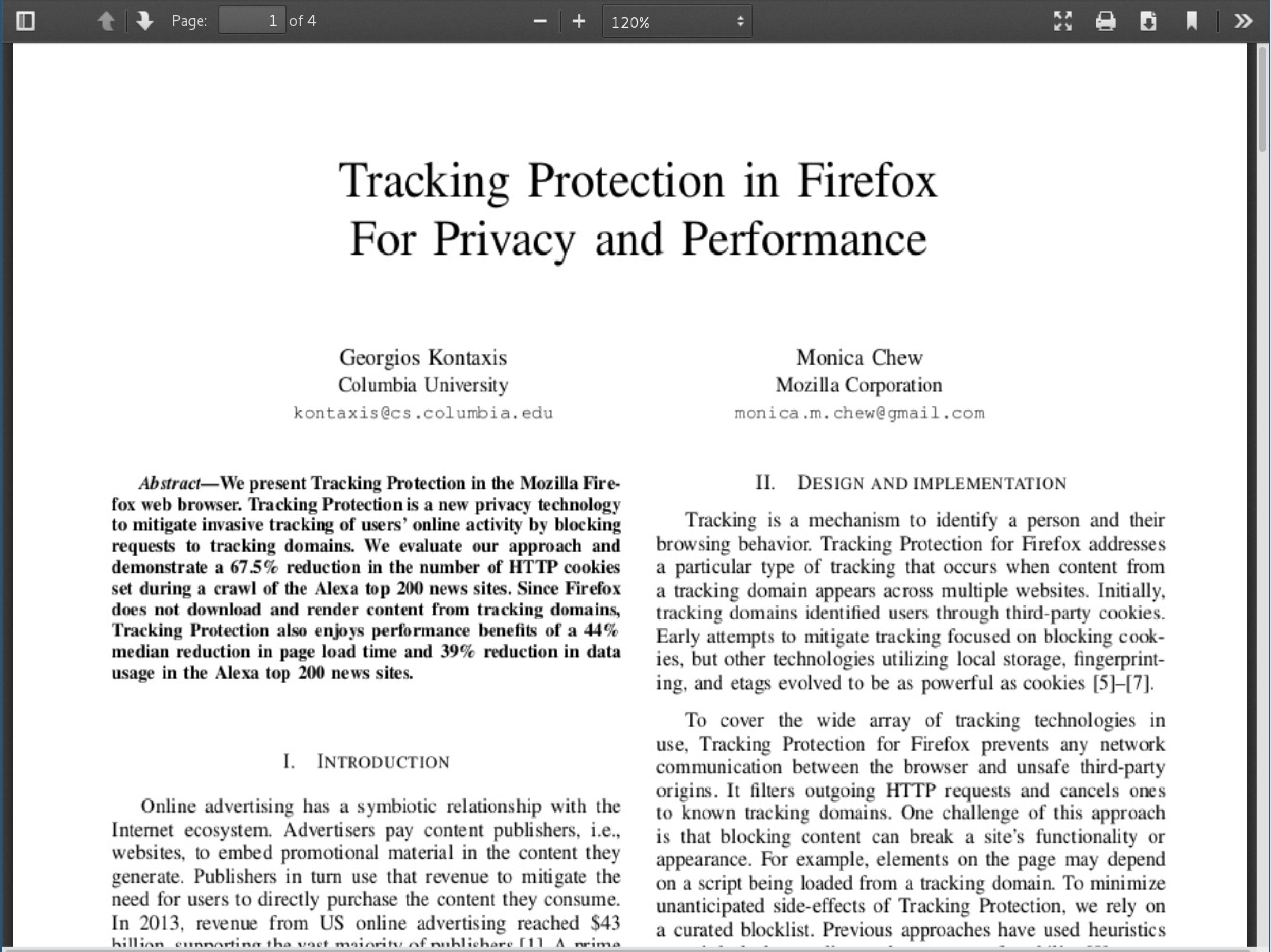
dom.allow_cut_copy

chrome

Simple Service Discovery Protocol

```
browser.casting.enabled
```

```
dom.vr.enabled
dom.gamepad.enabled
```



Tracking Protection in Firefox For Privacy and Performance

Georgios Kontaxis
Columbia University
kontaxis@cs.columbia.edu

Monica Chew
Mozilla Corporation
monica.m.chew@gmail.com

***Abstract*—We present Tracking Protection in the Mozilla Firefox web browser. Tracking Protection is a new privacy technology to mitigate invasive tracking of users' online activity by blocking requests to tracking domains. We evaluate our approach and demonstrate a 67.5% reduction in the number of HTTP cookies set during a crawl of the Alexa top 200 news sites. Since Firefox does not download and render content from tracking domains, Tracking Protection also enjoys performance benefits of a 44% median reduction in page load time and 39% reduction in data usage in the Alexa top 200 news sites.**

I. Introduction

Online advertising has a symbiotic relationship with the Internet ecosystem. Advertisers pay content publishers, i.e., websites, to embed promotional material in the content they generate. Publishers in turn use that revenue to mitigate the need for users to directly purchase the content they consume. In 2013, revenue from US online advertising reached $43 billion, supporting the vast majority of publishers [1]. A prime

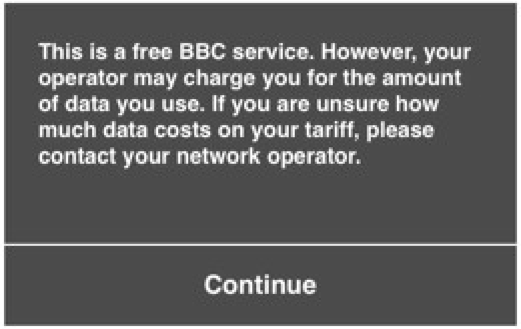
II. Design and Implementation

Tracking is a mechanism to identify a person and their browsing behavior. Tracking Protection for Firefox addresses a particular type of tracking that occurs when content from a tracking domain appears across multiple websites. Initially, tracking domains identified users through third-party cookies. Early attempts to mitigate tracking focused on blocking cookies, but other technologies utilizing local storage, fingerprinting, and etags evolved to be as powerful as cookies [5]–[7].

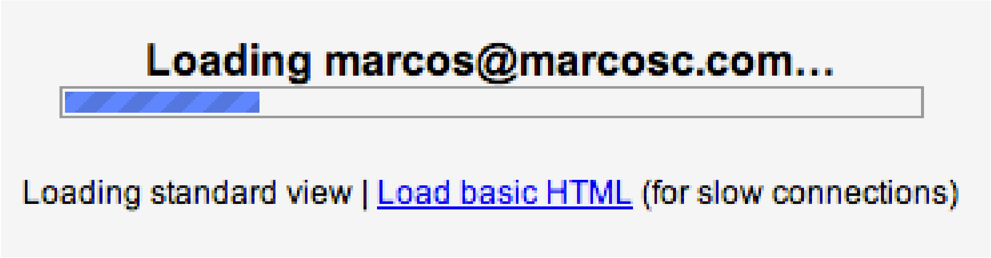
To cover the wide array of tracking technologies in use, Tracking Protection for Firefox prevents any network communication between the browser and unsafe third-party origins. It filters outgoing HTTP requests and cancels ones to known tracking domains. One challenge of this approach is that blocking content can break a site's functionality or appearance. For example, elements on the page may depend on a script being loaded from a tracking domain. To minimize unanticipated side-effects of Tracking Protection, we rely on a curated blocklist. Previous approaches have used heuristics

```
pdfjs.disabled
```

network information



This is a free BBC service. However, your operator may charge you for the amount of data you use. If you are unsure how much data costs on your tariff, please contact your network operator.



Loading marcos@marcosc.com...

Loading standard view | Load basic HTML (for slow connections)

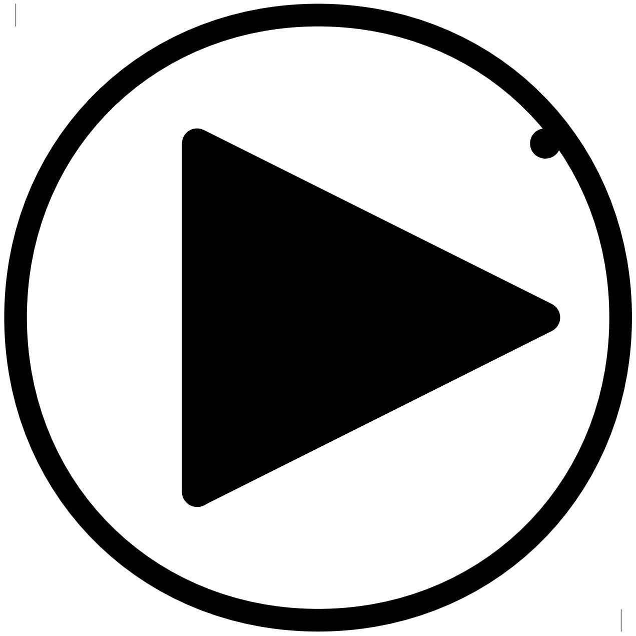
```
navigator.connection.type;
navigator.connection.type;
```

```
bluetooth, cellular, ethernet, none,
wifi, wimax, other, mixed, unknown
```

```
navigator.connection.type;

bluetooth, cellular, ethernet, none,
wifi, wimax, other, mixed, unknown

navigator.connection.downlinkMax;
```

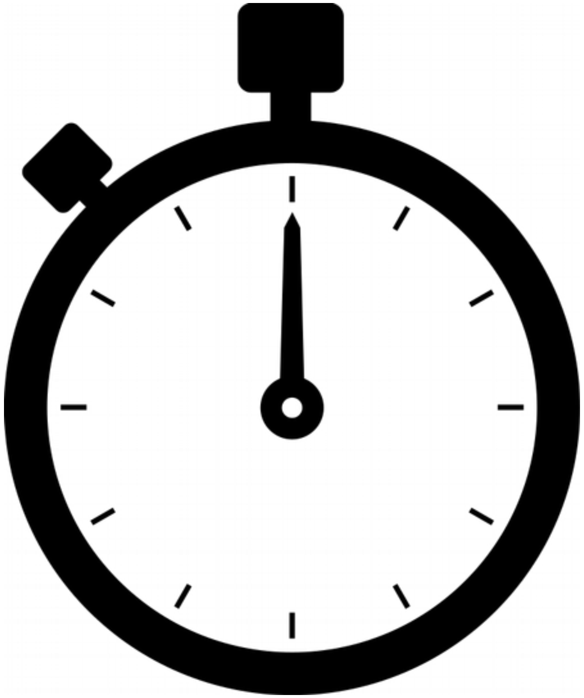
```
dom.netinfo.enabled
```

`media.video_stats.enabled`

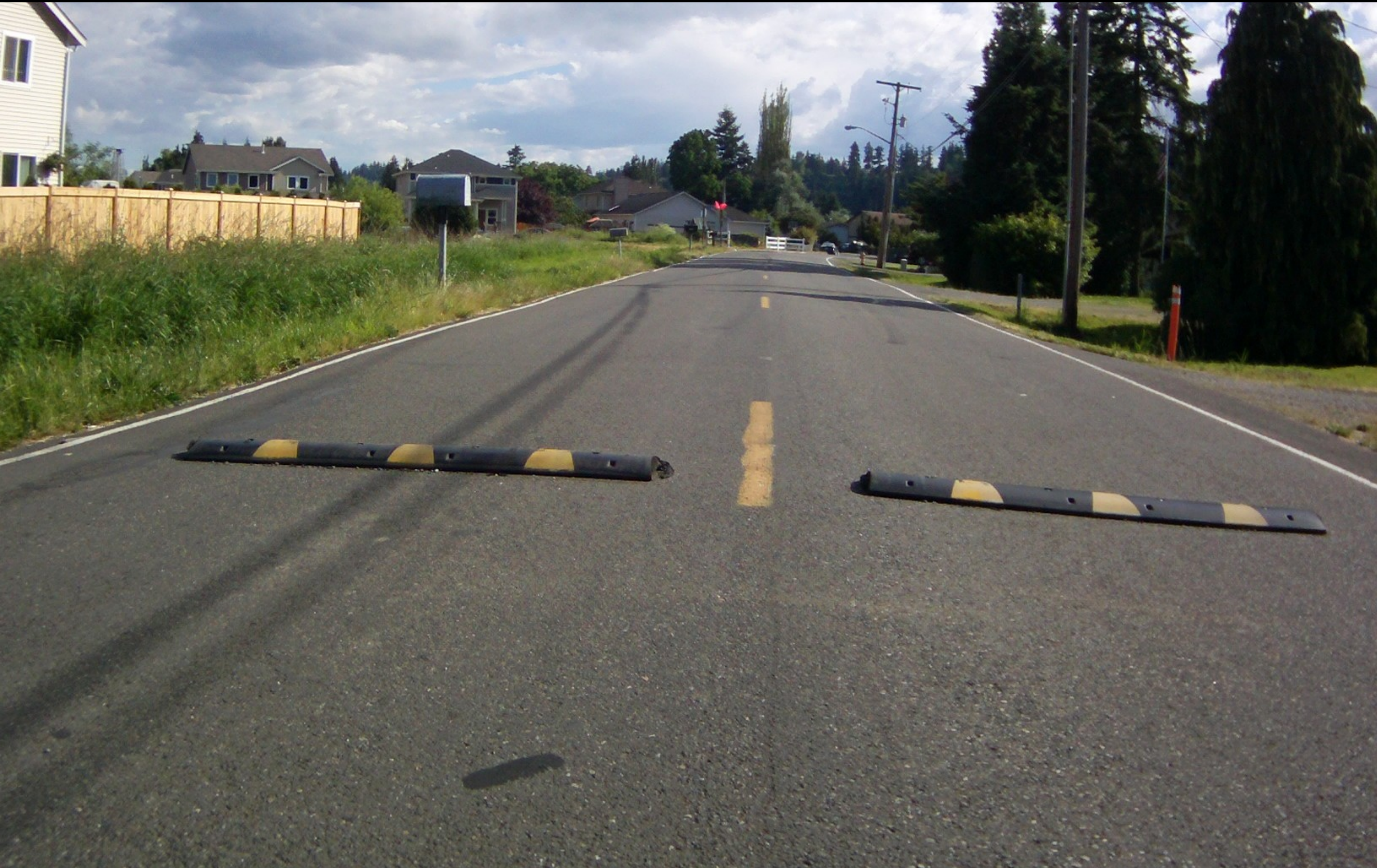


webgl.enable-debug-renderer-info

dom.enable_performance

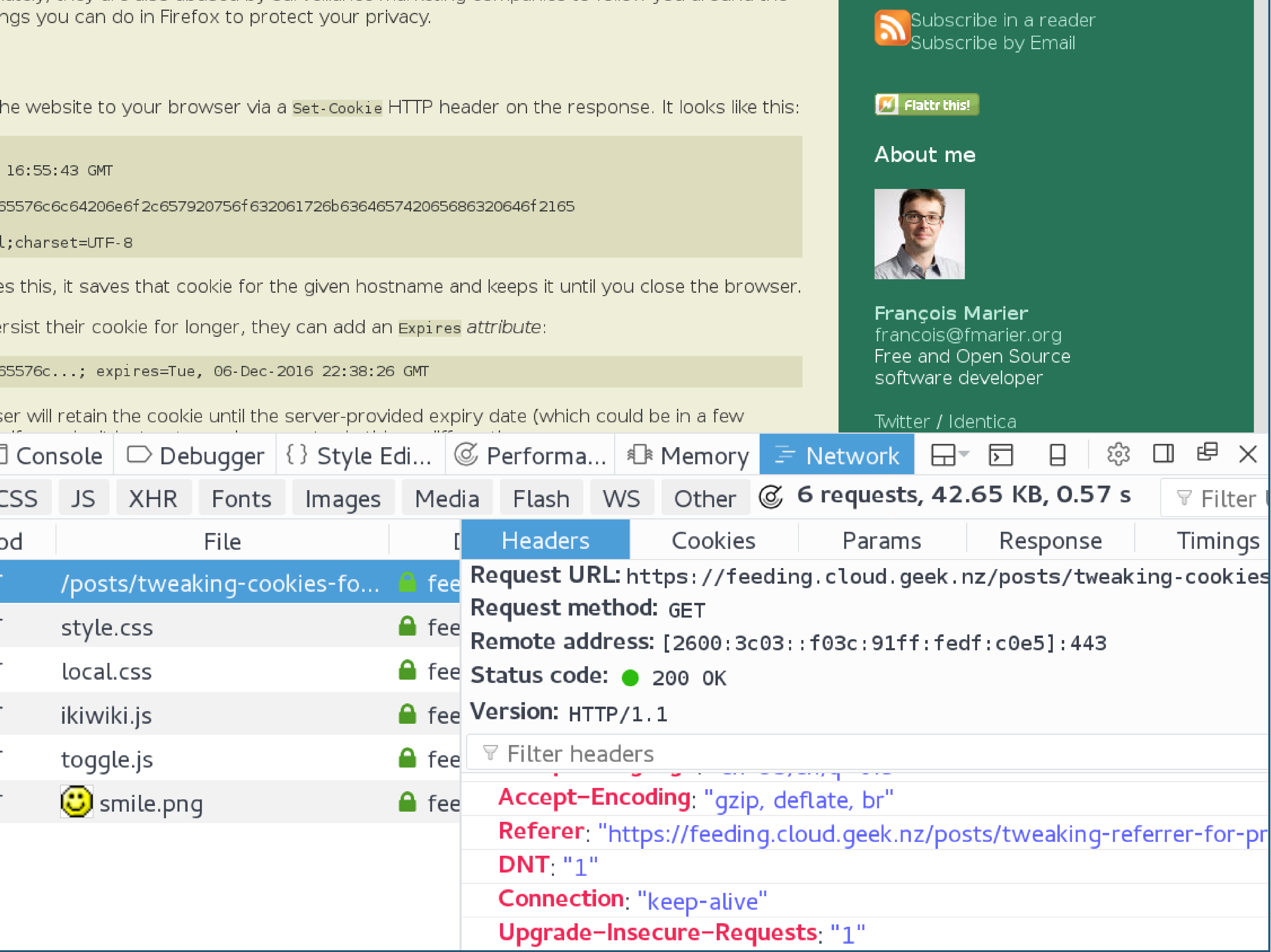


features to restrict



```
network.cookie.cookieBehavior = 0

network.cookie.thirdparty.sessionOnly = true

privacy.clearOnShutdown.cookies = false

network.cookie.lifetimePolicy = 3

network.cookie.lifetime.days = 5
```

feeding.cloud.geek.nz/posts/tweaking-cookies-for-privacy-in-firefox



ngs you can do in Firefox to protect your privacy.

he website to your browser via a `Set-Cookie` HTTP header on the response. It looks like this:

```
 16:55:43 GMT
55576c6c64206e6f2c657920756f632061726b6364657420656863320646f2165
l;charset=UTF-8
```

es this, it saves that cookie for the given hostname and keeps it until you close the browser.

rsist their cookie for longer, they can add an `Expires` *attribute*:

```
55576c...; expires=Tue, 06-Dec-2016 22:38:26 GMT
```

ser will retain the cookie until the server-provided expiry date (which could be in a few

About me

François Marier
francois@fmarier.org
Free and Open Source
software developer

Twitter / Identica

6 requests, 42.65 KB, 0.57 s

File	
/posts/tweaking-cookies-fo...	fee
style.css	fee
local.css	fee
ikiwiki.js	fee
toggle.js	fee
smile.png	fee

Request URL: https://feeding.cloud.geek.nz/posts/tweaking-cookies

Request method: GET

Remote address: [2600:3c03::f03c:91ff:fedf:c0e5]:443

Status code: ● 200 OK

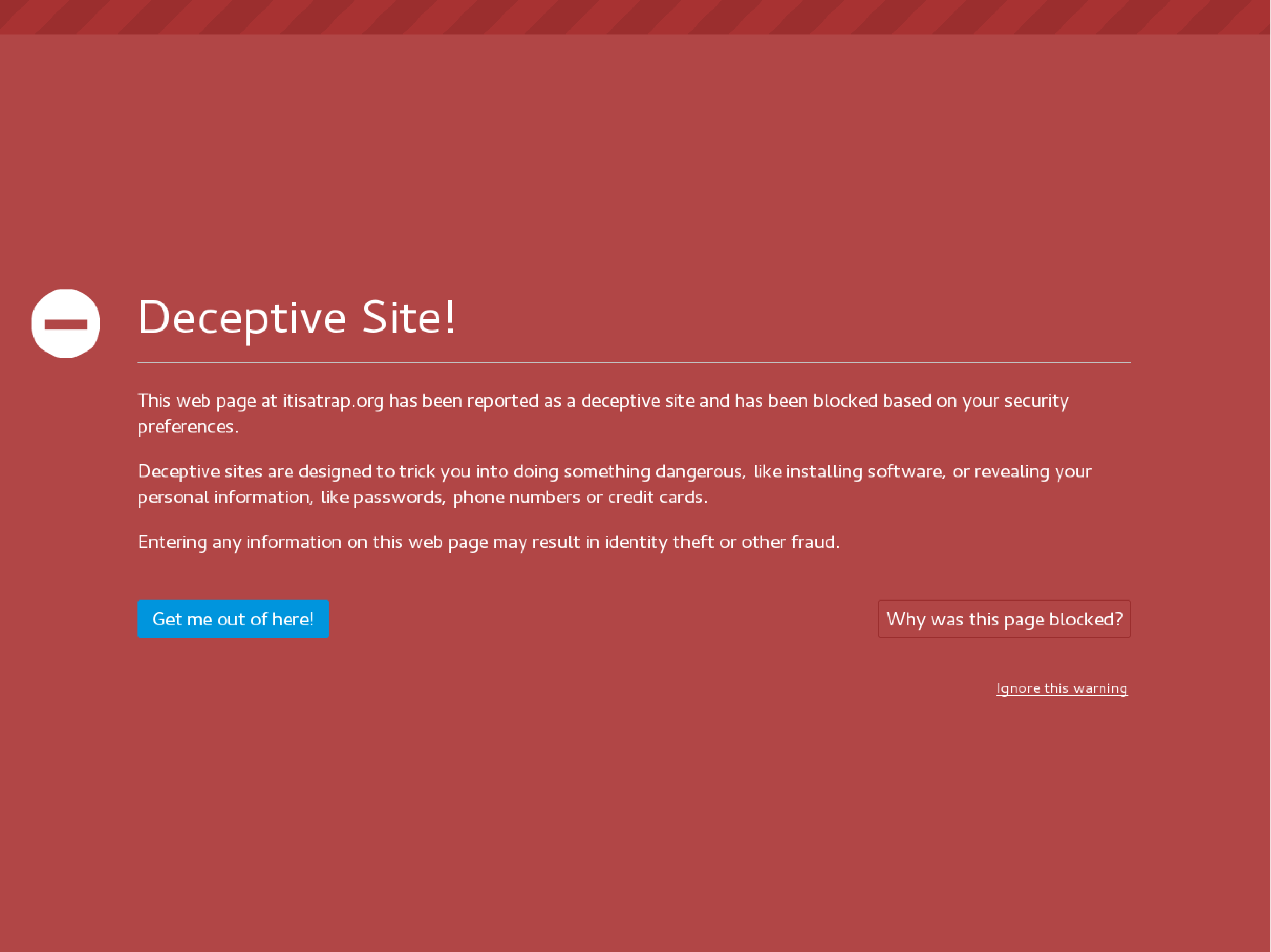
Version: HTTP/1.1

Filter headers

```
Accept-Encoding: "gzip, deflate, br"
Referer: "https://feeding.cloud.geek.nz/posts/tweaking-referrer-for-pr
DNT: "1"
Connection: "keep-alive"
Upgrade-Insecure-Requests: "1"
```

```
network.http.referer.XoriginPolicy = 1
network.http.referer.XoriginPolicy = 1

network.http.referer.XOriginTrimmingPolicy = 2
```

feeding.cloud.geek.nz/posts/tweaking-referrer-for-privacy-in-firefox

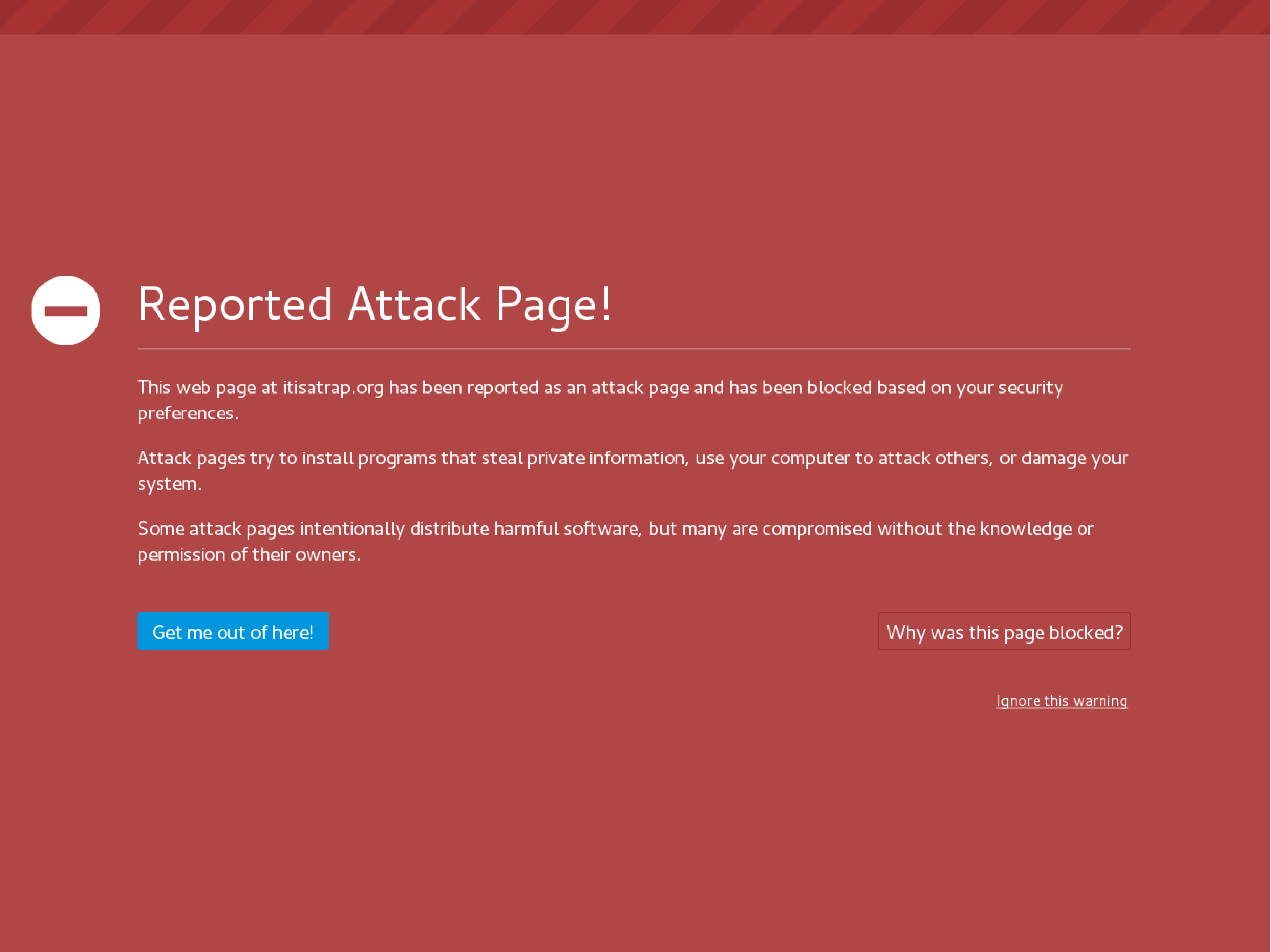


Deceptive Site!

This web page at itisatrap.org has been reported as a deceptive site and has been blocked based on your security preferences.

Deceptive sites are designed to trick you into doing something dangerous, like installing software, or revealing your personal information, like passwords, phone numbers or credit cards.

Entering any information on this web page may result in identity theft or other fraud.

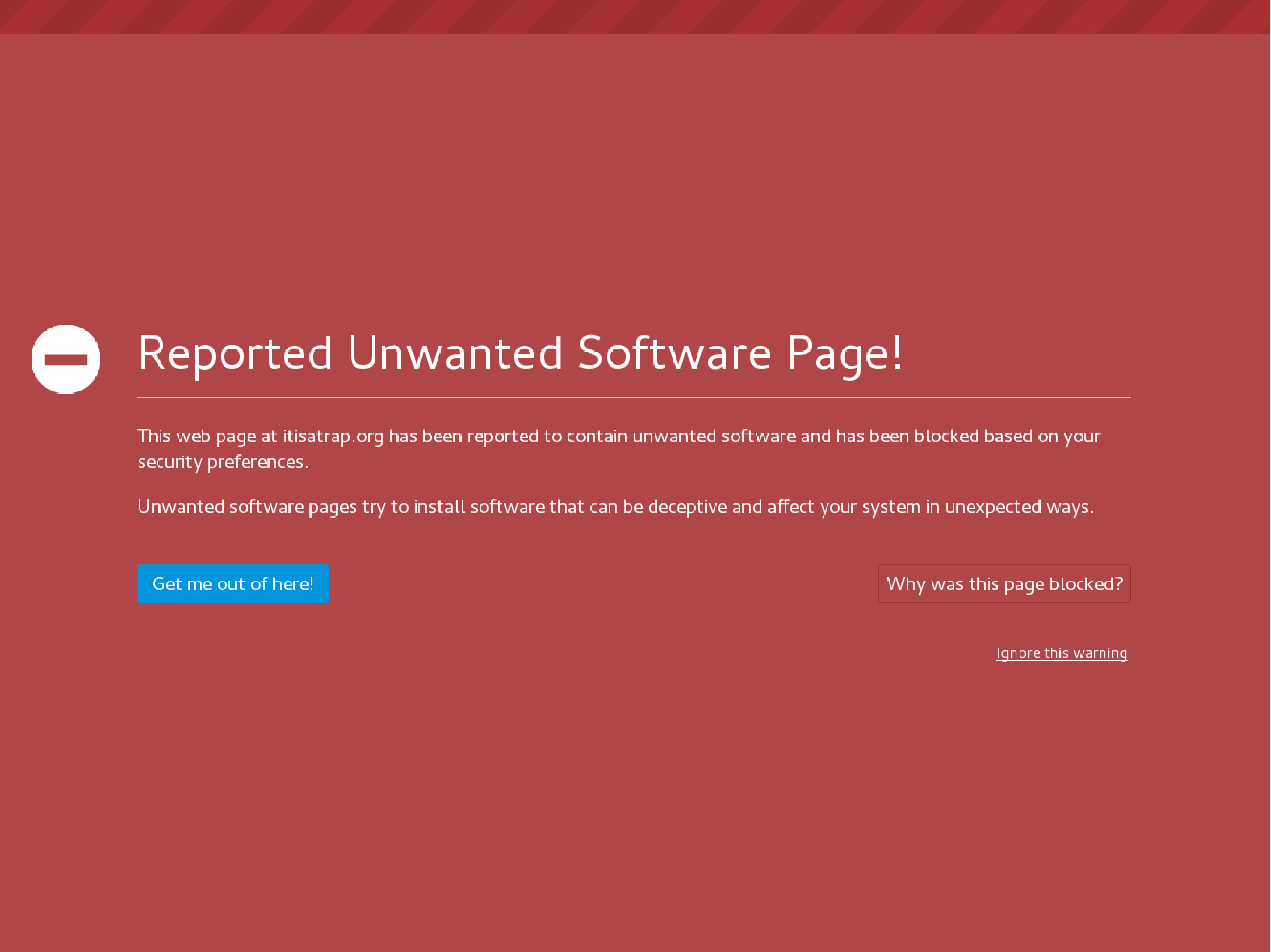


Reported Attack Page!

This web page at itisatrap.org has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.



Reported Unwanted Software Page!

This web page at itisatrap.org has been reported to contain unwanted software and has been blocked based on your security preferences.

Unwanted software pages try to install software that can be deceptive and affect your system in unexpected ways.

pre-downloaded lists

of URL **hash prefixes**

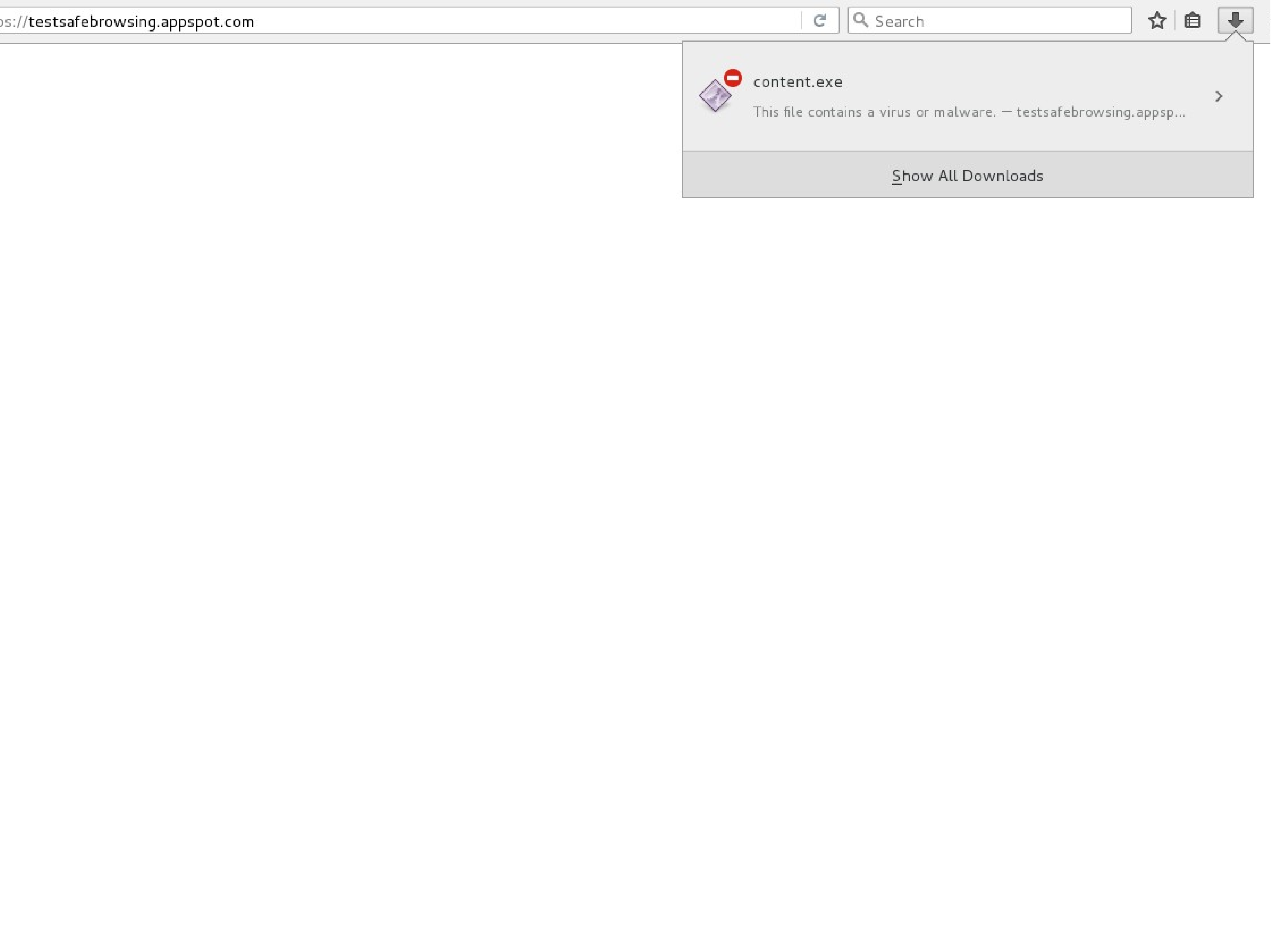
feeding.cloud.geek.nz/

5b31c2702efc7c81e4d197cd80113396
54da10d3315636cccbb536e868ff82a6

5b31c2702efc7c81e4d197cd80113396
54da10d3315636cccbb536e868ff82a6

5b31c2702efc7c81e4d197cd80113396
54da10d3315636cccbb536e868ff82a6

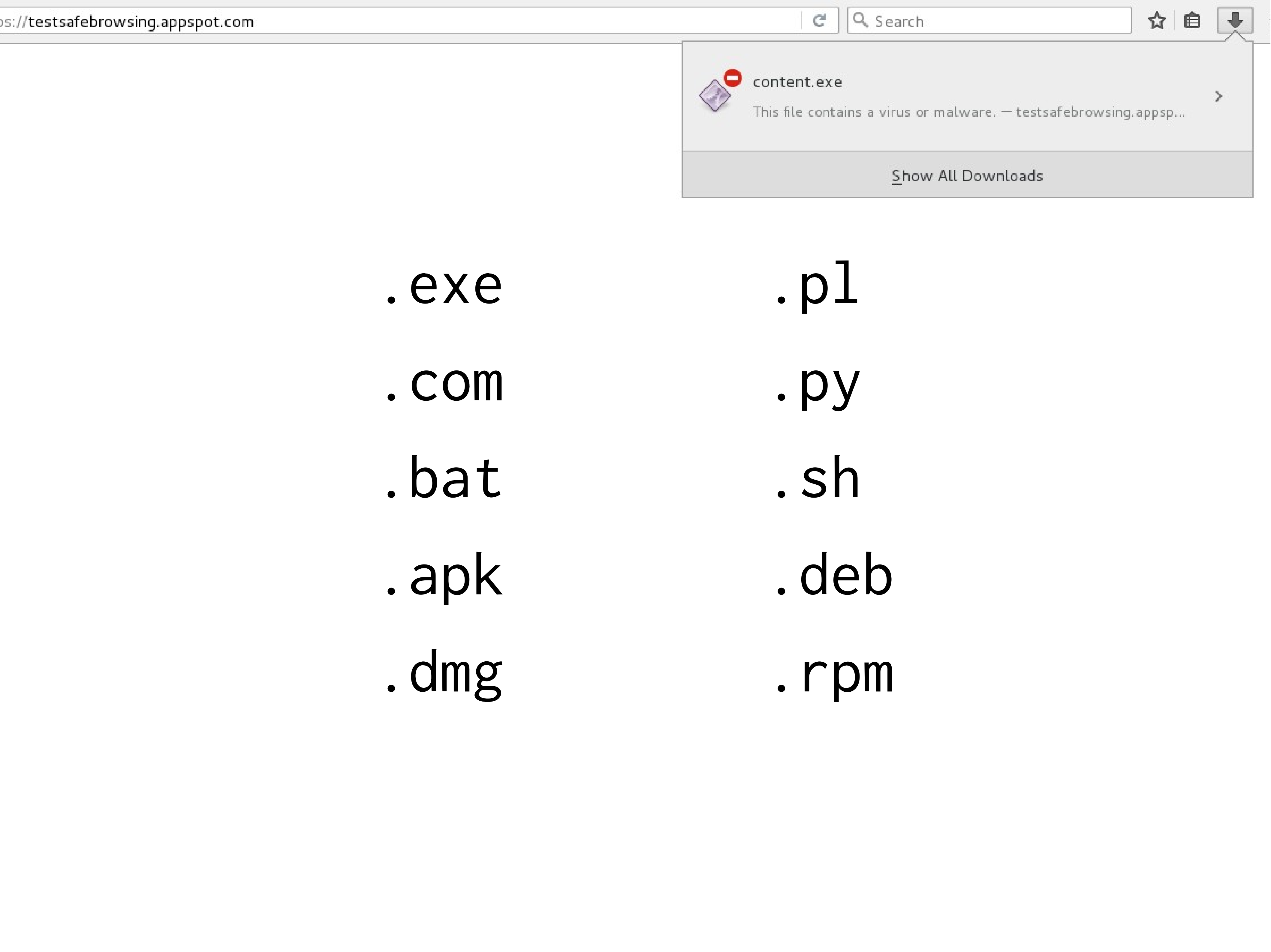
feeding.cloud.geek.nz/posts/how-safe-browsing-works-in-firefox



ps://testsafebrowsing.appspot.com

content.exe

This file contains a virus or malware. — testsafebrowsing.appsp...



content.exe

This file contains a virus or malware. — testsafebrowsing.appsp...

.exe

.com

.bat

.apk

.dmg

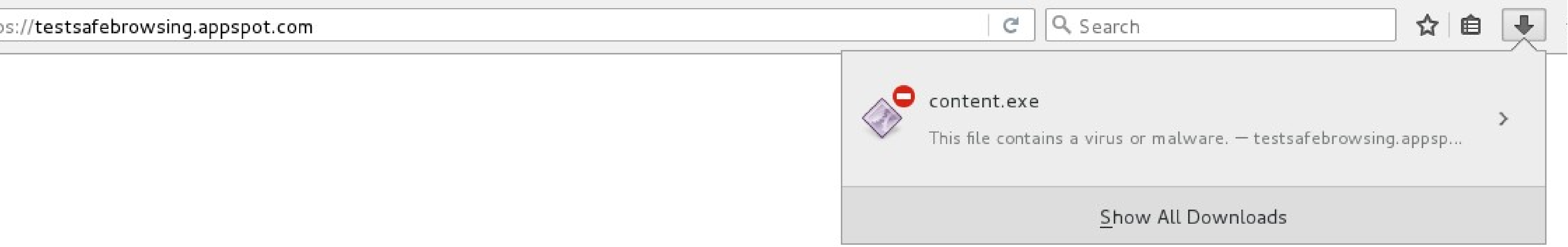
.pl

.py

.sh

.deb

.rpm



content.exe

This file contains a virus or malware. — testsafebrowsing.appsp...

.exe

.com

.bat

.apk

.dmg

.pl

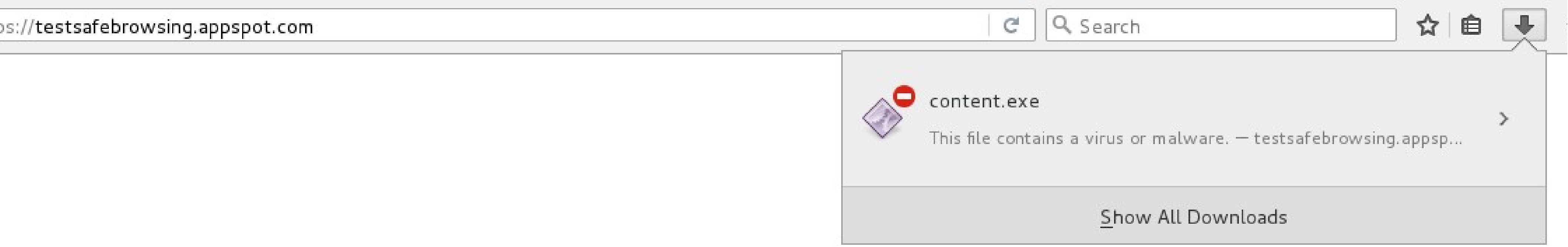
.py

.sh

.deb

.rpm

`toolkit/components/downloads/ApplicationReputation.cpp`



s://testsafebrowsing.appspot.com

Search

content.exe

This file contains a virus or malware. — testsafebrowsing.appsp...

Show All Downloads

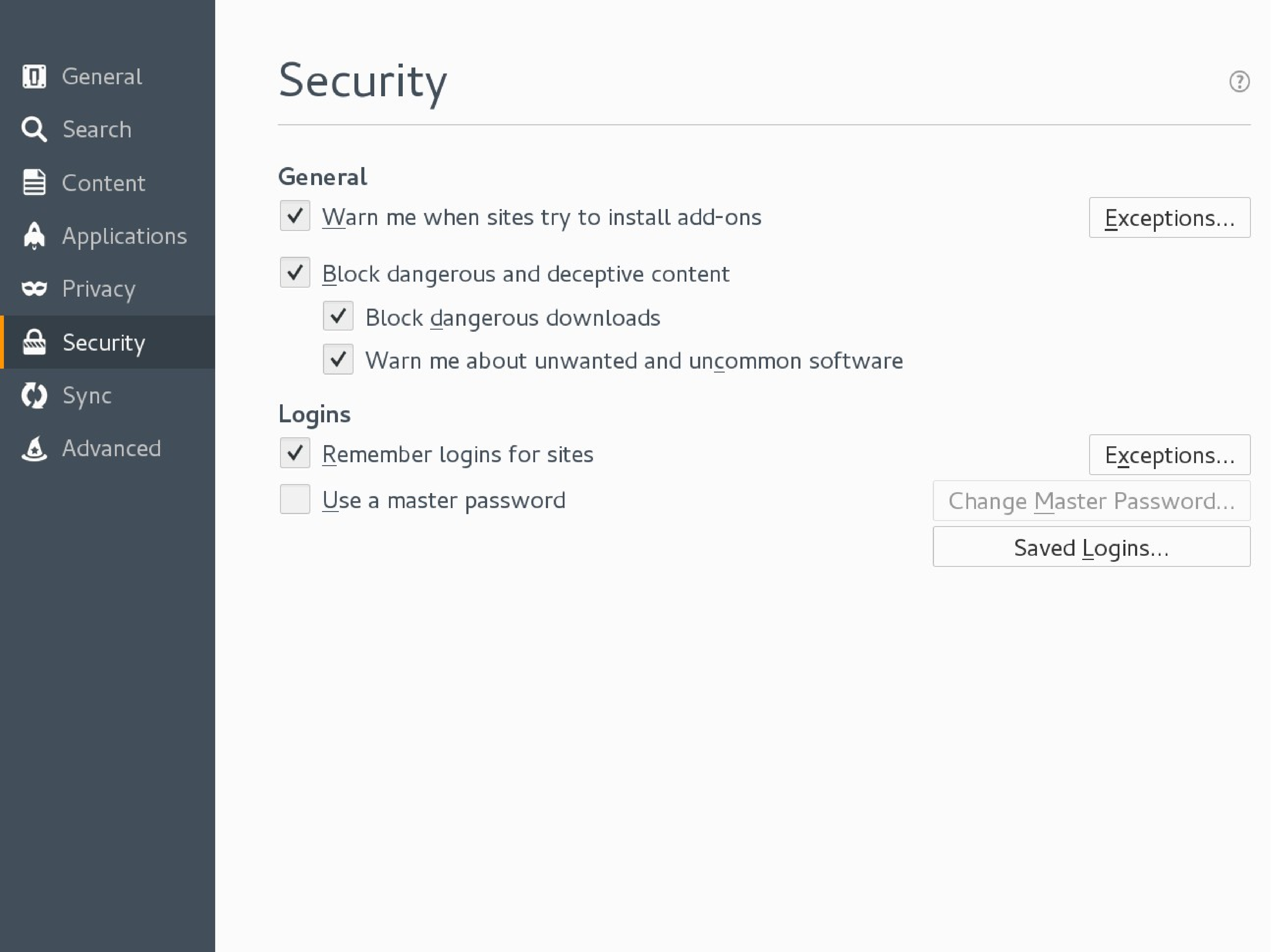
filename and size

URLs

hash of contents

locale

`toolkit/components/downloads/ApplicationReputation.cpp`



Security

General

☑ Warn me when sites try to install add-ons

☑ Block dangerous and deceptive content

- ☑ Block dangerous downloads
- ☑ Warn me about unwanted and uncommon software

Logins

☑ Remember logins for sites

□ Use a master password

browser.safebrowsing.downloads.remote.enabled

feeding.cloud.geek.nz/posts/how-safe-browsing-works-in-firefox

WebRTC

skype™

Internet Engineering Task Force (IETF)
Request for Comments: 6336
Updates: 5245
Category: Standards Track
ISSN: 2070-1721
July 2011

M. Westerlund
Ericsson
C. Perkins
University of Glasgow

IANA Registry for Interactive Connectivity Establishment (ICE) Options

Abstract

It has been identified that "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols" (RFC 5245) is missing a registry for ICE options. This document defines this missing IANA registry and updates RFC 5245.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the revealing non-VPN IP address

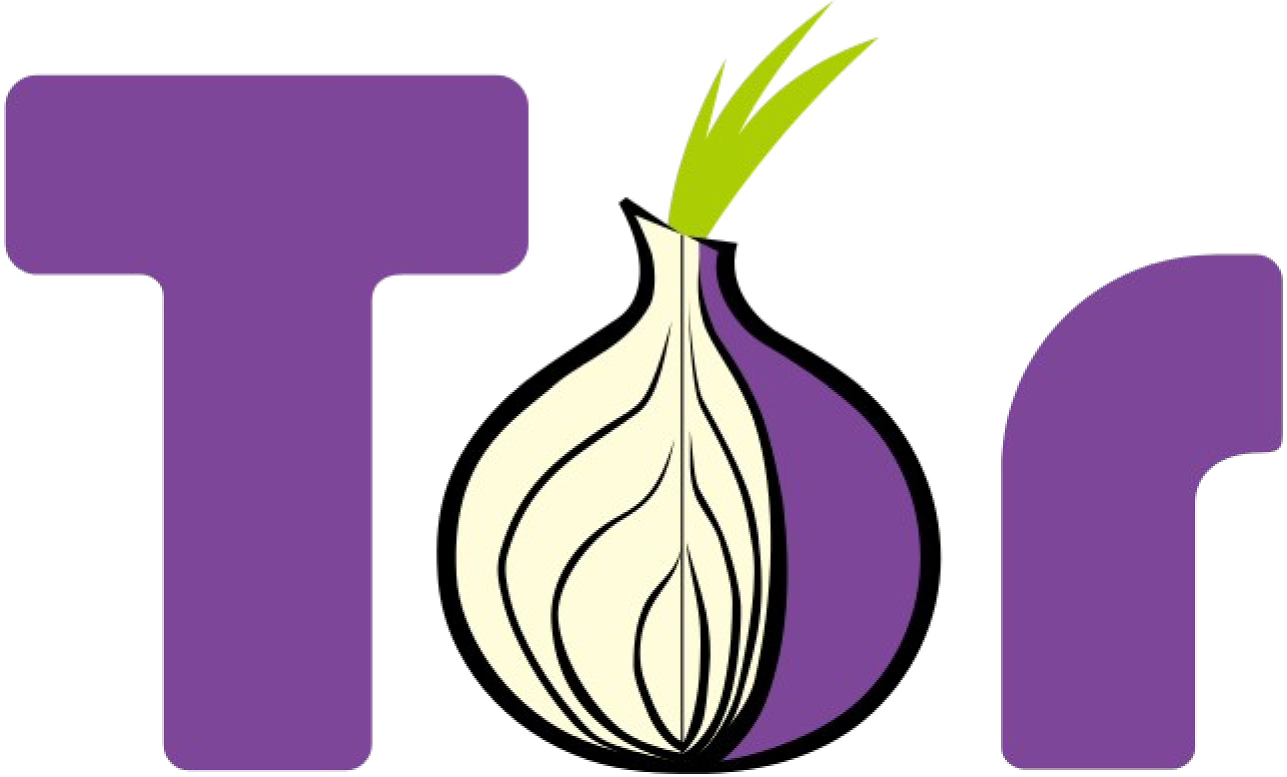
leaking internal IP address

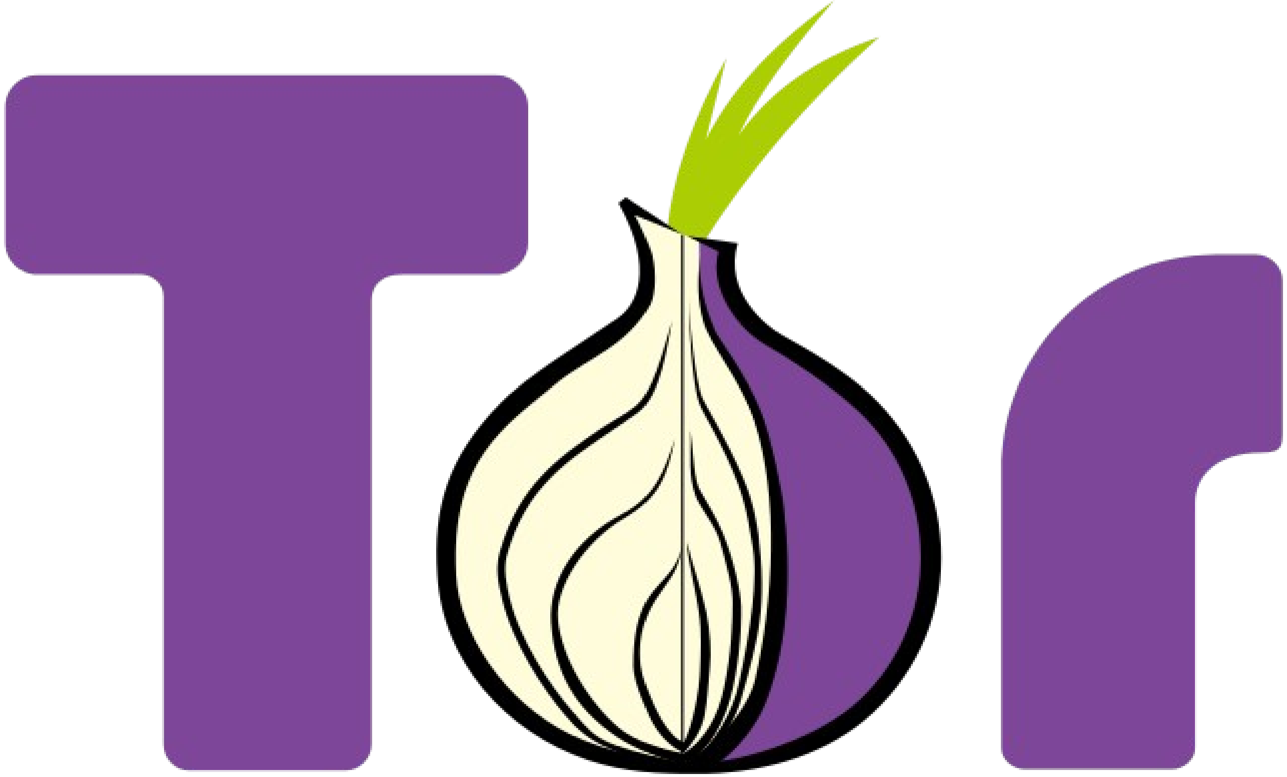
fixed
in 51

~~revealing non-VPN IP address~~

leaking internal IP address

```
media.peerconnection.ice.no_host = true
```


Tor

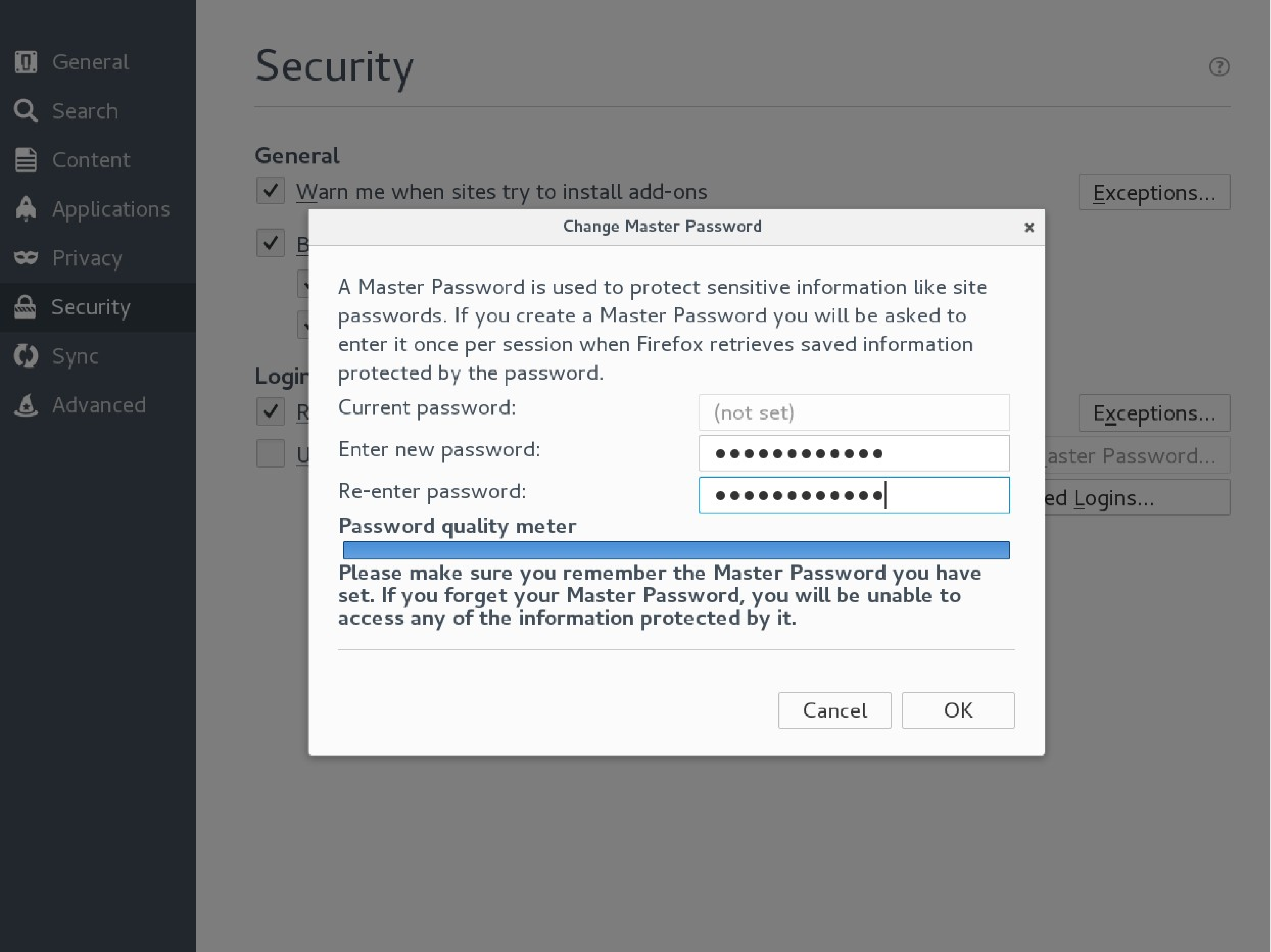


wiki.mozilla.org/Security/Tor_Uplift

privacy.resistFingerprinting

other things to keep in mind

p@ssW0rd5



☑ Warn me when sites try to install add-ons

A Master Password is used to protect sensitive information like site passwords. If you create a Master Password you will be asked to enter it once per session when Firefox retrieves saved information protected by the password.

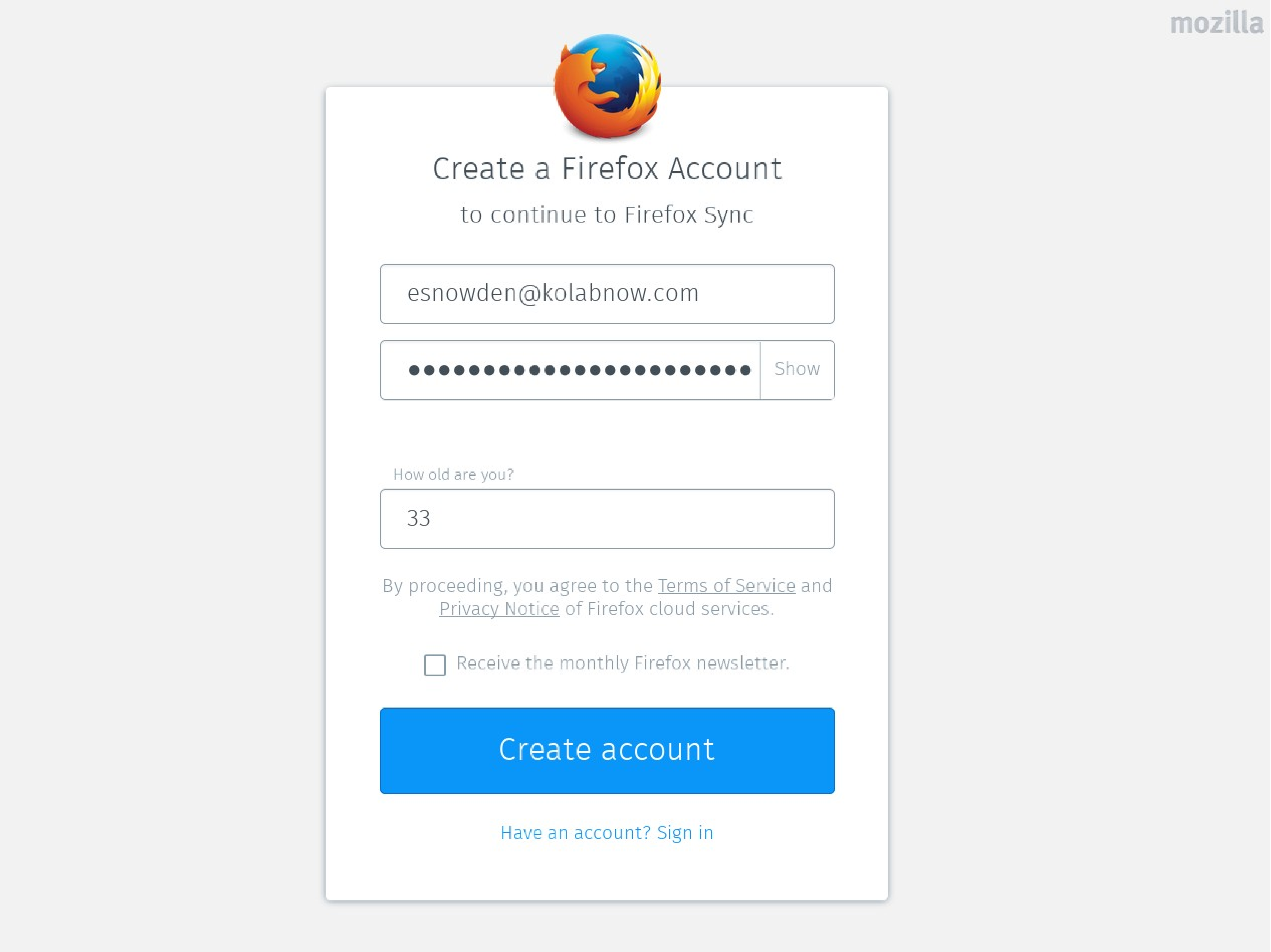
Current password: (not set)

Enter new password: ●●●●●●●●●●●●

Re-enter password: ●●●●●●●●●●●●

Password quality meter

Please make sure you remember the Master Password you have set. If you forget your Master Password, you will be unable to access any of the information protected by it.



Create a Firefox Account

to continue to Firefox Sync

esnowden@kolabnow.com

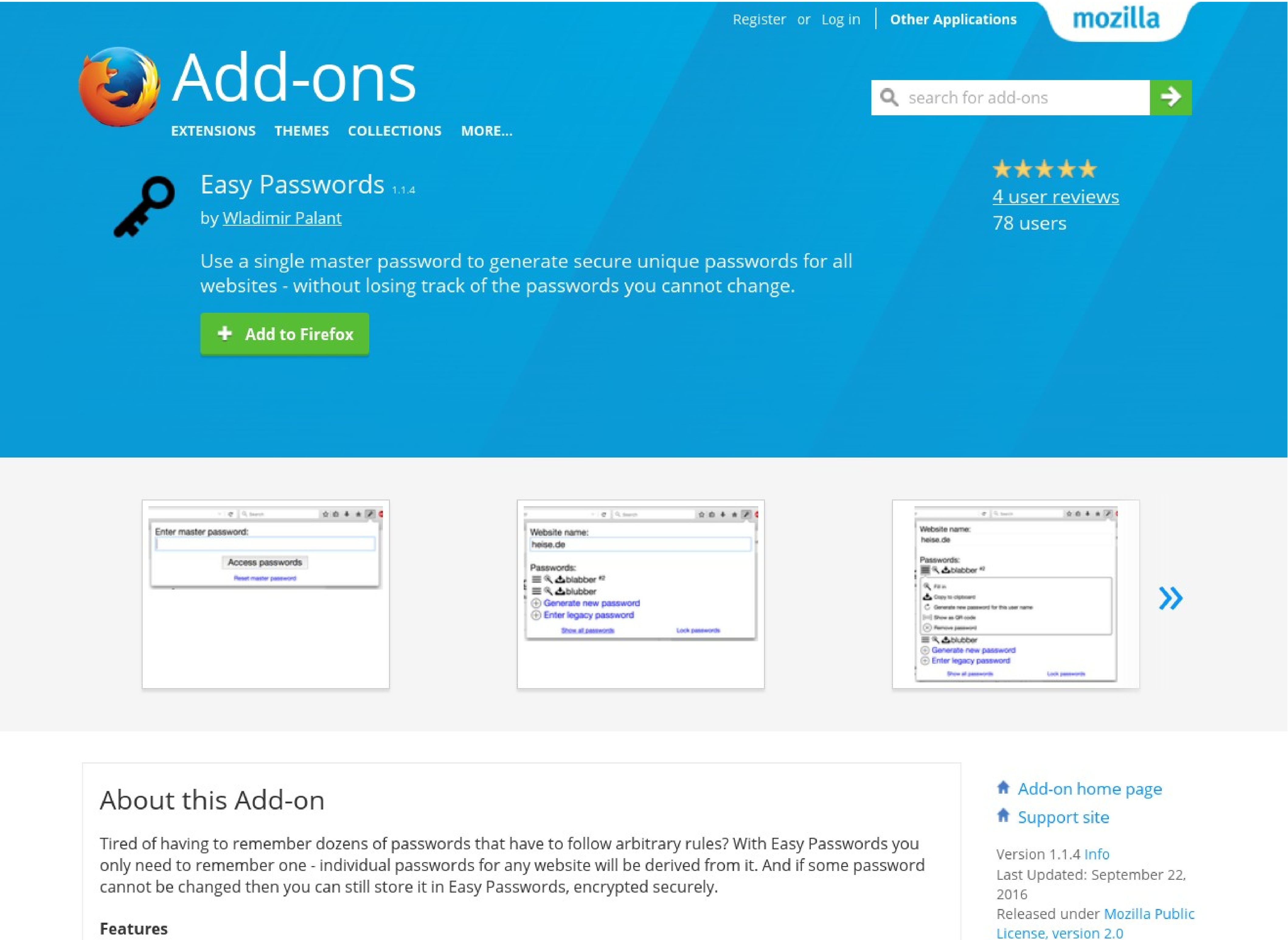
●●●●●●●●●●●●●●●●●●●●●●● Show

How old are you?

33

By proceeding, you agree to the Terms of Service and Privacy Notice of Firefox cloud services.

□ Receive the monthly Firefox newsletter.



Add-ons

Easy Passwords 1.1.4

by Wladimir Palant

★★★★★
4 user reviews
78 users

Use a single master password to generate secure unique passwords for all websites - without losing track of the passwords you cannot change.

+ Add to Firefox

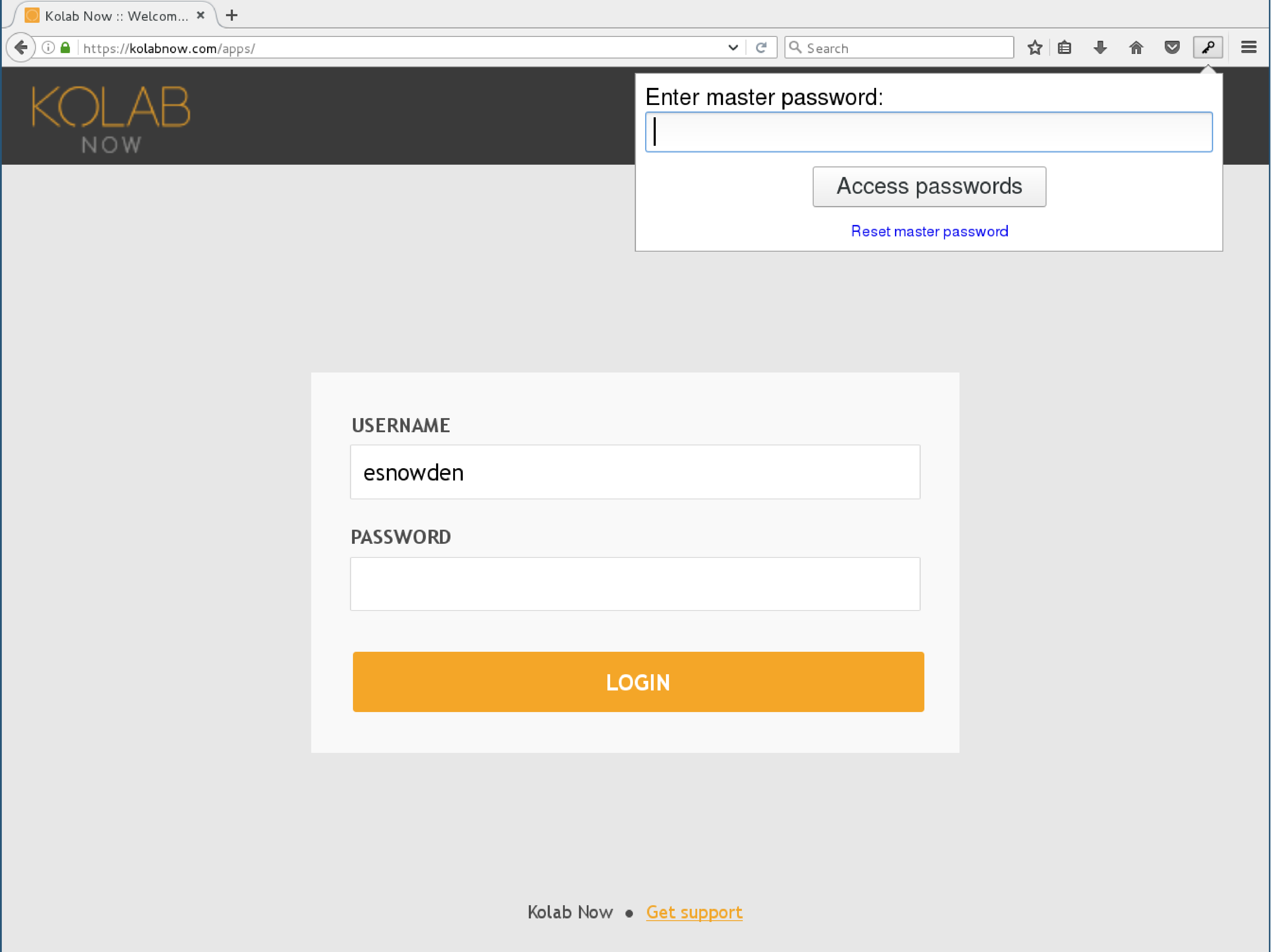
About this Add-on

Tired of having to remember dozens of passwords that have to follow arbitrary rules? With Easy Passwords you only need to remember one - individual passwords for any website will be derived from it. And if some password cannot be changed then you can still store it in Easy Passwords, encrypted securely.

Features

Add-on home page
Support site

Version 1.1.4 Info
Last Updated: September 22, 2016
Released under Mozilla Public License, version 2.0



Enter master password:

Access passwords

Reset master password

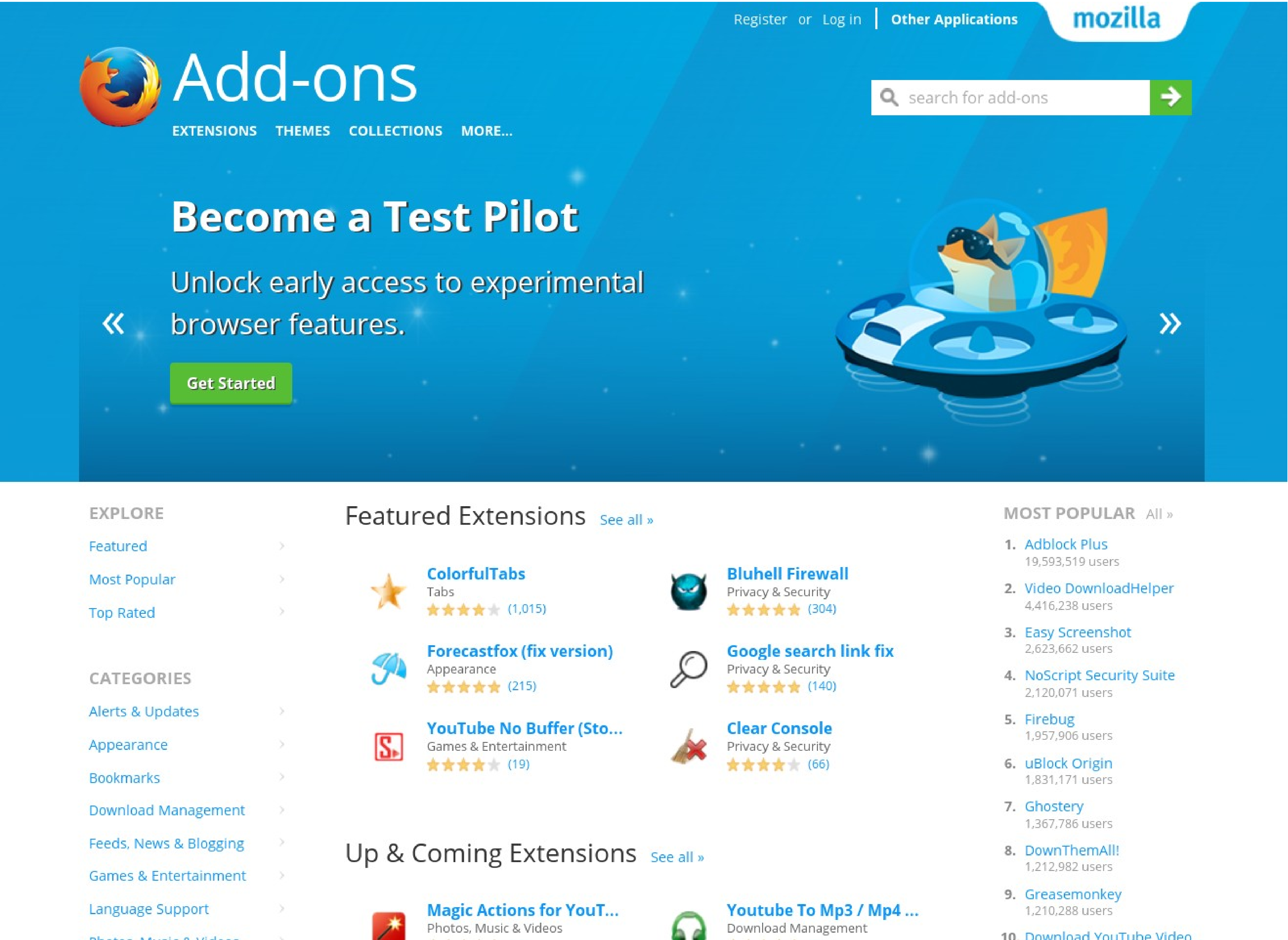
USERNAME

esnowden

PASSWORD

LOGIN

Kolab Now ● Get support



Register or Log in | **Other Applications** mozilla

Add-ons

EXTENSIONS THEMES COLLECTIONS MORE...

search for add-ons

Become a Test Pilot

Unlock early access to experimental browser features.

« **Get Started** »

EXPLORE

- Featured ›
- Most Popular ›
- Top Rated ›

CATEGORIES

- Alerts & Updates ›
- Appearance ›
- Bookmarks ›
- Download Management ›
- Feeds, News & Blogging ›
- Games & Entertainment ›
- Language Support ›
- Photos, Music & Videos ›

Featured Extensions See all »

ColorfulTabs
Tabs
★★★★☆ (1,015)

Bluhell Firewall
Privacy & Security
★★★★★ (304)

Forecastfox (fix version)
Appearance
★★★★★ (215)

Google search link fix
Privacy & Security
★★★★★ (140)

YouTube No Buffer (Sto...
Games & Entertainment
★★★★☆ (19)

Clear Console
Privacy & Security
★★★★☆ (66)

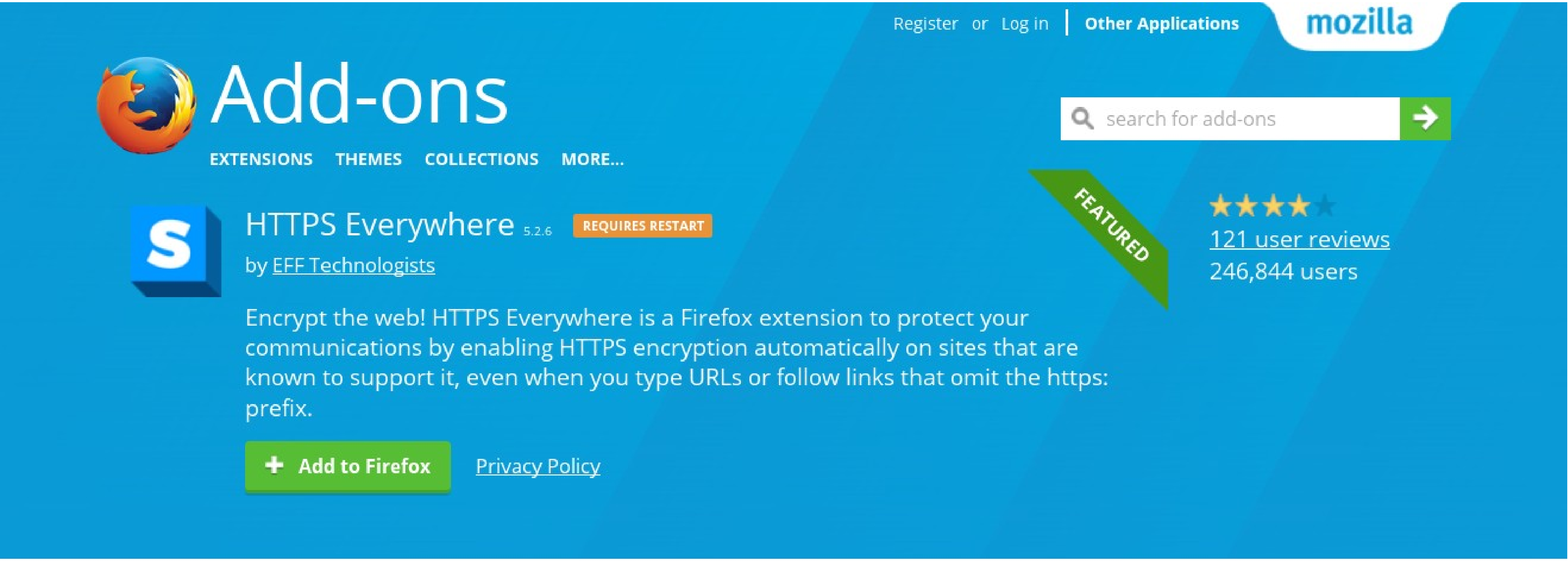
Up & Coming Extensions See all »

Magic Actions for YouT...
Photos, Music & Videos

Youtube To Mp3 / Mp4 ...
Download Management

MOST POPULAR All »

1. Adblock Plus
19,593,519 users
2. Video DownloadHelper
4,416,238 users
3. Easy Screenshot
2,623,662 users
4. NoScript Security Suite
2,120,071 users
5. Firebug
1,957,906 users
6. uBlock Origin
1,831,171 users
7. Ghostery
1,367,786 users
8. DownThemAll!
1,212,982 users
9. Greasemonkey
1,210,288 users
10. Download YouTube Video



Register or Log in | Other Applications

mozilla

Add-ons

EXTENSIONS THEMES COLLECTIONS MORE...

search for add-ons

HTTPS Everywhere 5.2.6 REQUIRES RESTART

by EFF Technologists

FEATURED

★★★★☆

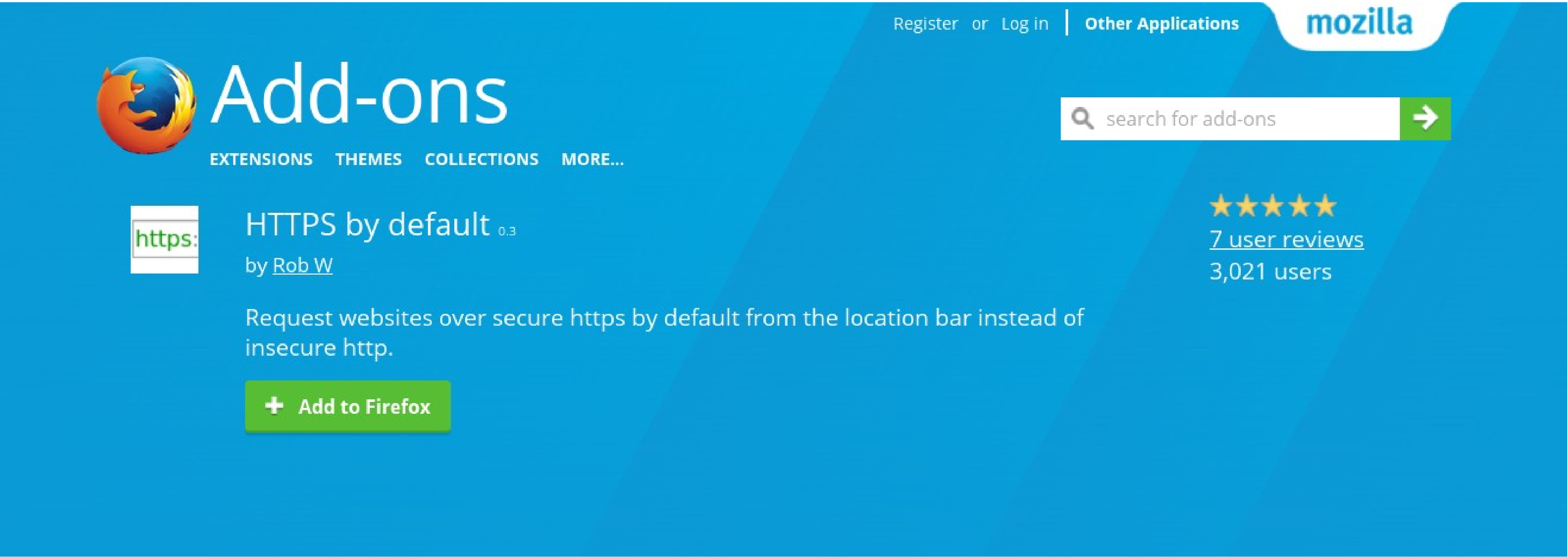
121 user reviews

246,844 users

Encrypt the web! HTTPS Everywhere is a Firefox extension to protect your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type URLs or follow links that omit the https: prefix.

+ Add to Firefox

Privacy Policy



Register or Log in | Other Applications

mozilla

Add-ons

EXTENSIONS THEMES COLLECTIONS MORE...

search for add-ons

https:

HTTPS by default 0.3

by Rob W

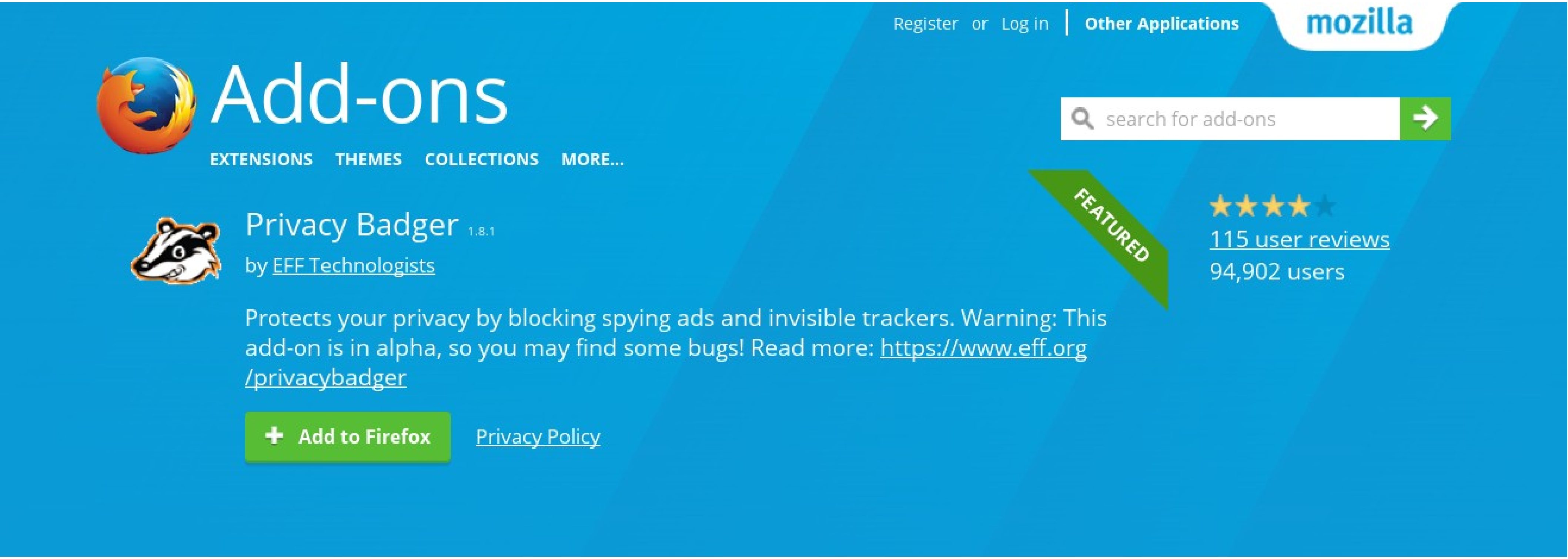
★★★★★

7 user reviews

3,021 users

Request websites over secure https by default from the location bar instead of insecure http.

+ Add to Firefox



Register or Log in | Other Applications
mozilla
Add-ons
search for add-ons
EXTENSIONS THEMES COLLECTIONS MORE...
FEATURED

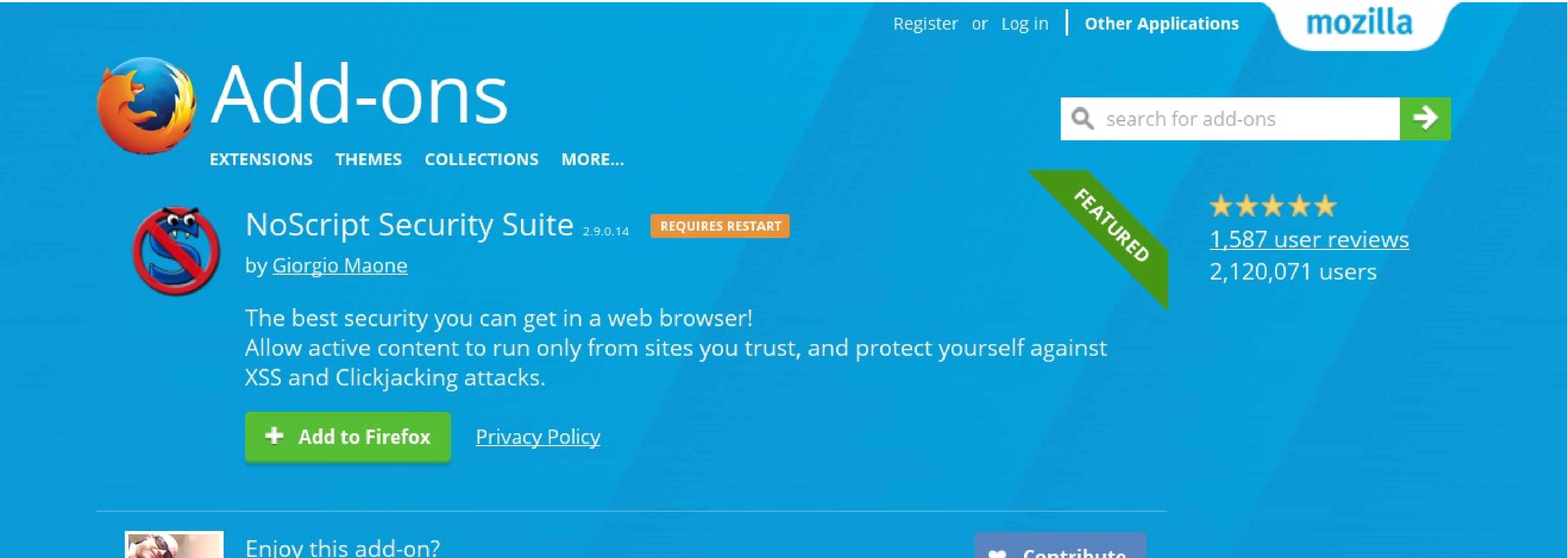
Privacy Badger 1.8.1

by EFF Technologists

Protects your privacy by blocking spying ads and invisible trackers. Warning: This add-on is in alpha, so you may find some bugs! Read more: https://www.eff.org/privacybadger

★★★★☆
115 user reviews
94,902 users

+ Add to Firefox
Privacy Policy



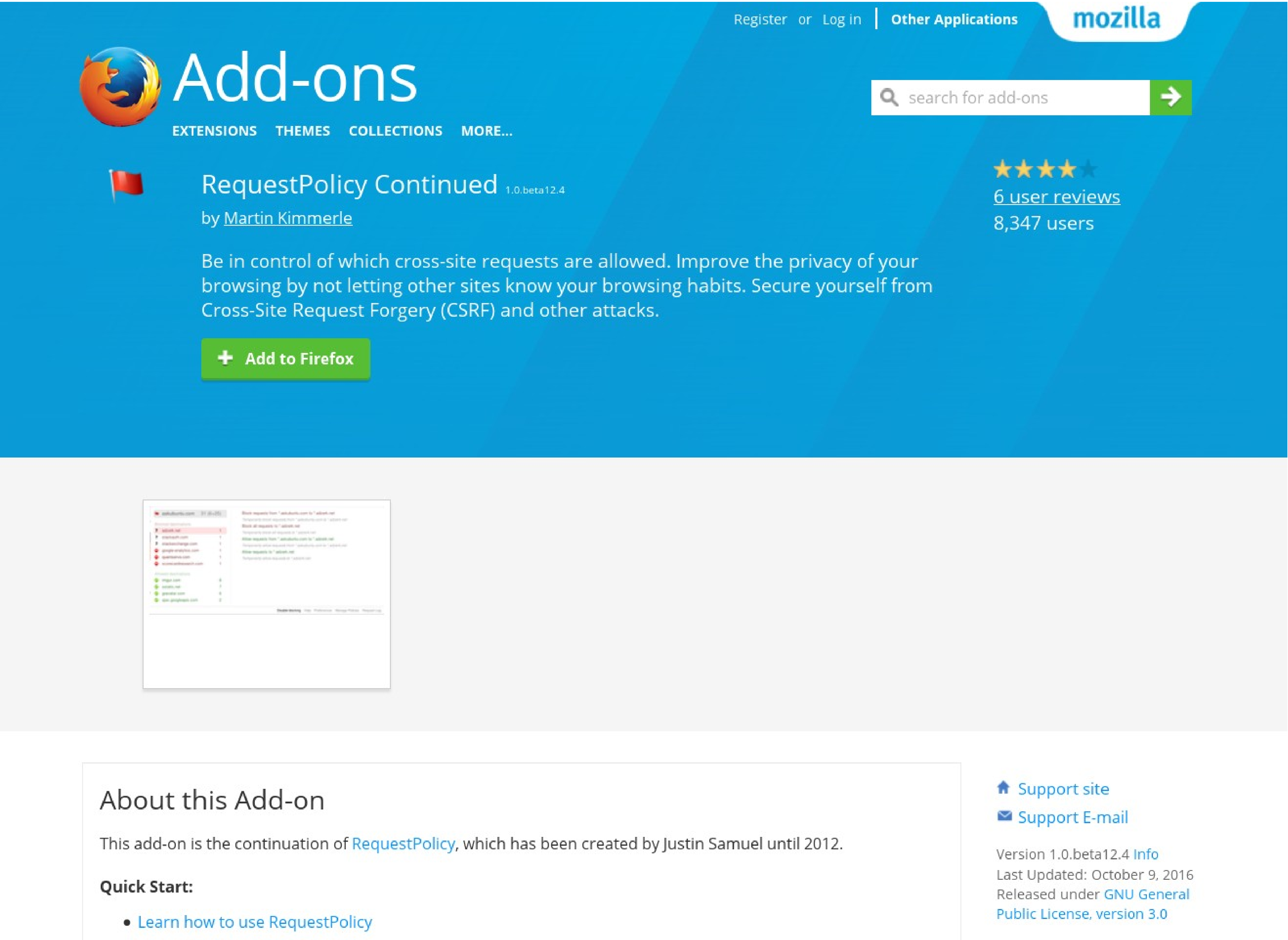
Register or Log in | Other Applications
mozilla
Add-ons
search for add-ons
EXTENSIONS THEMES COLLECTIONS MORE...
FEATURED

NoScript Security Suite 2.9.0.14 REQUIRES RESTART

by Giorgio Maone

The best security you can get in a web browser!
Allow active content to run only from sites you trust, and protect yourself against XSS and Clickjacking attacks.

★★★★★
1,587 user reviews
2,120,071 users



RequestPolicy Continued 1.0.beta12.4

by Martin Kimmerle

Be in control of which cross-site requests are allowed. Improve the privacy of your browsing by not letting other sites know your browsing habits. Secure yourself from Cross-Site Request Forgery (CSRF) and other attacks.

★★★★☆

6 user reviews

8,347 users

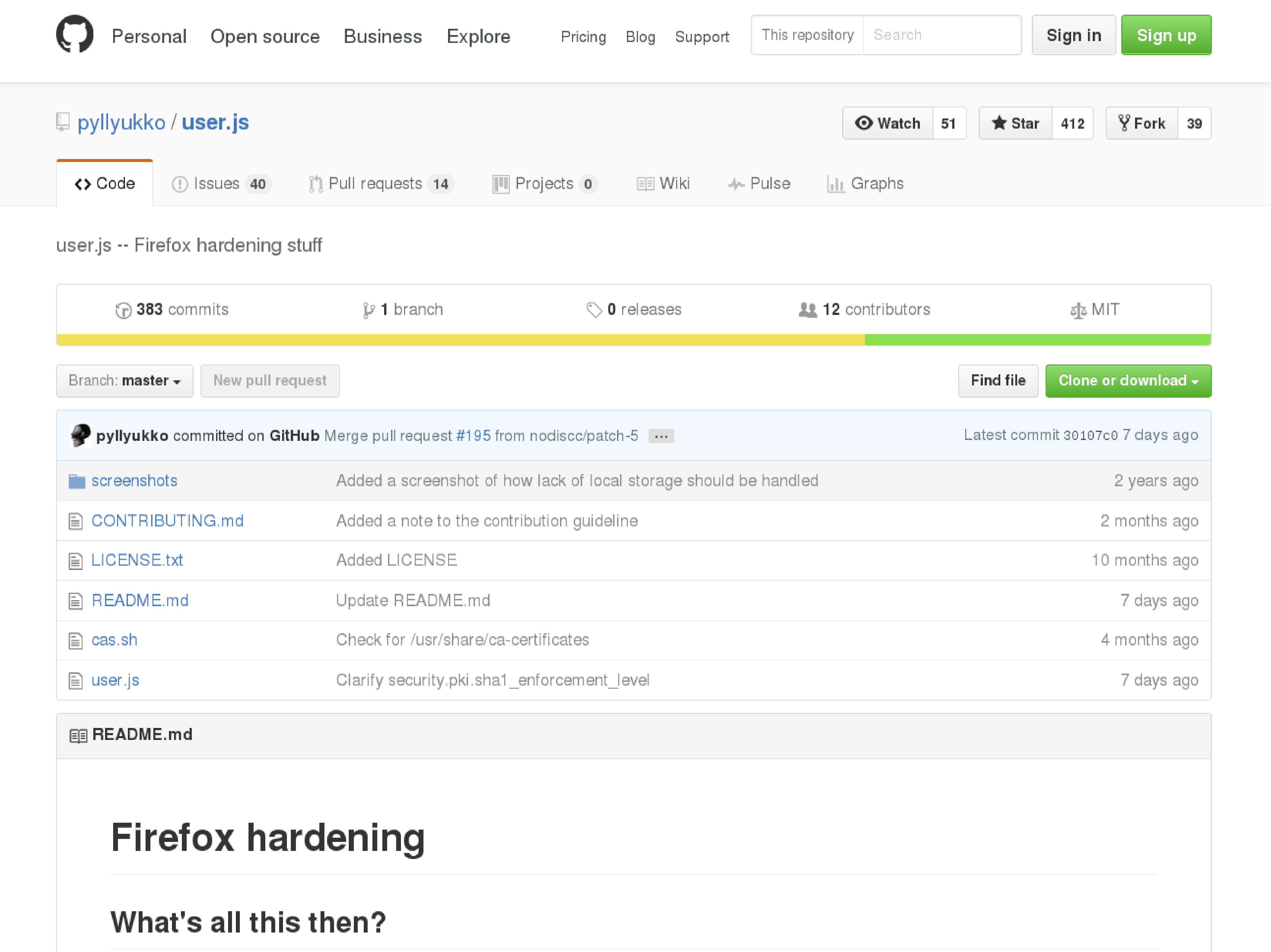
About this Add-on

This add-on is the continuation of RequestPolicy, which has been created by Justin Samuel until 2012.

Quick Start:

- Learn how to use RequestPolicy

Version 1.0.beta12.4 Info
Last Updated: October 9, 2016
Released under GNU General Public License, version 3.0



pyllyukko / user.js

user.js -- Firefox hardening stuff

383 commits · 1 branch · 0 releases · 12 contributors · MIT

pyllyukko committed on GitHub Merge pull request #195 from nodiscc/patch-5 … Latest commit 30107c0 7 days ago

screenshots	Added a screenshot of how lack of local storage should be handled	2 years ago
CONTRIBUTING.md	Added a note to the contribution guideline	2 months ago
LICENSE.txt	Added LICENSE	10 months ago
README.md	Update README.md	7 days ago
cas.sh	Check for /usr/share/ca-certificates	4 months ago
user.js	Clarify security.pki.sha1_enforcement_level	7 days ago

README.md

Firefox hardening

What's all this then?

```
user_pref("privacy.trackingprotection.enabled",true);
user_pref("privacy.donottrackheader.enabled", true);

user_pref("device.sensors.enabled", false);
user_pref("media.eme.enabled", false);
user_pref("browser.casting.enabled", false);
user_pref("pdfjs.disabled", true);
user_pref("dom.vr.enabled", false);
user_pref("dom.gamepad.enabled", false);
user_pref("dom.webaudio.enabled", false);
user_pref("dom.allow_cut_copy", false);

user_pref("dom.netinfo.enabled", false);
user_pref("media.video_stats.enabled", false);
user_pref("dom.enable_performance", false);
user_pref("webgl.enable-debug-renderer-info", false);

user_pref("media.peerconnection.ice.no_host", true);
user_pref("privacy.resistFingerprinting", true);
user_pref("network.http.referer.XOriginPolicy", 1);

user_pref("privacy.clearOnShutdown.cookies", false);
user_pref("network.cookie.cookieBehavior", 0);
user_pref("network.cookie.lifetimePolicy", 3);
user_pref("network.cookie.lifetime.days", 5);
user_pref("network.cookie.thirdparty.sessionOnly", true);

user_pref("layout.css.visited_links_enabled", false);
user_pref("network.IDN_show_punycode", true);
user_pref("browser.urlbar.trimURLs", false);
user_pref("browser.xul.error_pages.expert_bad_cert", true);
```

?

@fmarier

Photo Credits:

shooting star: https://www.flickr.com/photos/funcrush/9496927983/

yellow triangle: https://www.flickr.com/photos/tillwe/2974932670/

jail cell: https://www.flickr.com/photos/mikecogh/5997920696

speedbump: https://www.flickr.com/photos/jputnam/9078451876/

cookie: https://www.flickr.com/photos/amagill/34754258/

chromecast: https://www.flickr.com/photos/medithit/10165535814/

lamp: https://www.flickr.com/photos/60588258@N00/3806005225