

Security and Privacy on the Web in 2016

Security and Privacy

for **users**, **sysadmins** and **developers**

security

security

for users

Safe Browsing



Reported Attack Page!

This web page at nsa.gov 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.

Get me out of here!

Why was this page blocked?

[Ignore this warning](#)

pre-downloaded URL hash prefixes

pre-downloaded URL hash prefixes

list updated every 30 minutes

pre-downloaded URL hash prefixes

list updated every 30 minutes

server completions on prefix hit (with noise entries)

pre-downloaded URL hash prefixes

list updated every 30 minutes

server completions on prefix hit (with noise entries)

separate cookie jar

pre-downloaded URL hash prefixes

list updated every 30 minutes

server completions on prefix hit (with noise entries)

separate cookie jar

list entries expire after 45 minutes

about:config

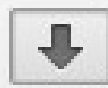
browser.safebrowsing.enabled (phishing)

browser.safebrowsing.malware.enabled (malware)

Download Protection



Search →



test



Blocked: May contain a virus or spyware — googlegroups.com — ...

[Show All Downloads](#)

is it on the pre-downloaded list of dangerous hosts?

is it on the pre-downloaded list of dangerous hosts?

is it signed by a known good software provider?

is it on the pre-downloaded list of dangerous hosts?

is it signed by a known good software provider?

is it an executable file (.exe, .com, .pif, .dmg, etc.)?

is it on the pre-downloaded list of dangerous hosts?

is it signed by a known good software provider?

is it an executable file (.exe, .com, .pif, .dmg, etc.)?

what does the apprep server think about it?

about:config

browser.safebrowsing.downloads.remote.enabled

browser.safebrowsing.downloads.remote.block_potentially_unwanted

browser.safebrowsing.downloads.remote.block_uncommon

<https://feeding.cloud.geek.nz/posts/how-safe-browsing-works-in-firefox/>

security

for developers

Content Security Policy aka *CSP*

mechanism for preventing XSS

telling the browser what external
content is **allowed to load**

What's on your mind?

```
Hi y'all<script>  
alert('p0wned');  
</script>!
```

Tweet!

without CSP

John Doe - just moments ago

Hi y'a

p0wned

ok

with CSP

John Doe - just moments ago

Hi y'all!

The image shows the bottom portion of a web browser window, specifically the developer console. The console is open to the 'Security' tab, which is highlighted with a red dot. The error message reads: 'Content Security Policy: The page's settings blocked the loading of a resource: csp-blocked.h... :6 An attempt to execute inline scripts has been blocked'. The console interface includes a toolbar with icons for various tools (Cons..., Inspec..., Debug..., Style Edi..., Prof..., Netw...) and a search bar labeled 'Filter output'. The error message is preceded by a red warning icon.

```
Content-Security-Policy:  
  script-src 'self'  
    https://cdn.example.com
```

script-src
object-src
style-src
img-src
media-src
frame-src
font-src
connect-src

Strict Transport Security aka *HSTS*

mechanism for preventing
HTTPS to HTTP downgrades

telling the browser that your site
should **never be reached** over HTTP



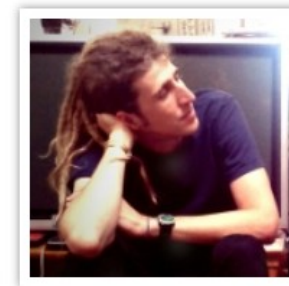
Software >> sslstrip

[Download](#) `sslstrip 0.9`[GitHub](#) [Project page](#)

This tool provides a demonstration of the HTTPS stripping attacks that I presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial. For more information on the attack, see the video from the presentation below.



Moxie Marlinspike

moxie.website@moxie.org[@moxie](#)[GPG Key](#)

no HSTS, no sslstrip

GET bank.com → 301

GET https://bank.com → 200

no HSTS, **with** sslstrip

GET bank.com → 200

what does HSTS look like?

```
$ curl -i https://bank.com
```

```
HTTP/1.1 200 OK
```

```
Cache-Control: private
```

```
Content-Type: text/html; charset=utf-8
```

```
Strict-Transport-Security: max-age=31536000
```

```
...
```

with HSTS, **with** sslstrip

GET <https://bank.com> → 200

no HTTP traffic for
sslstrip to tamper with



Subresource Integrity

W3C Editor's Draft 27 May 2015

This version:

<http://w3c.github.io/webappsec/specs/subresourceintegrity/>

Latest published version:

<http://www.w3.org/TR/SRI/>

Latest editor's draft:

<http://w3c.github.io/webappsec/specs/subresourceintegrity/>

Editors:

[Devdatta Akhawe, Dropbox, Inc.](#)

[Francois Marier, Mozilla](#)

[Frederik Braun, Mozilla](#)

[Joel Weinberger, Google, Inc.](#)

Participate:

[We are on Github.](#)

[File a bug.](#)

[Commit history.](#)

[Mailing list.](#)

Implementation status:

[Blink/Chromium](#)

[Gecko](#)

[Copyright](#) © 2014-2015 [W3C](#)® ([MIT](#), [ERCIM](#), [Keio](#), [Beihang](#)). [W3C liability](#), [trademark](#) and [document use](#) rules apply.

Abstract

This specification defines a mechanism by which user agents may verify that a fetched resource has been delivered without manipulation.

Status of This Document

cricket world cup

DRAMATIC RESCUE



Frantic effort to rescue woman

5:05 PM Police plunge into water and use rocks to save a woman trapped in a sinking car.

Three dead in crash

5:24 PM Three people die and one is critically injured after a logging truck crash in Tokoroa.

NZ stumble to three-wicket win

4:44 PM Black Caps go two-from-two in World Cup, but not before losing seven wickets.

Fugitive in court

Man who was on the run from sex and fraud allegations enters no plea in Sydney court.

Ferry crash 'kind of shocking'

15 min ago Seventeen people hurt as an Auckland harbour ferry crashes into a wharf.

Proposal to outsource NZ Post jobs

5:03 PM Staff at New Zealand Post are told of proposal to outsource 24 financial support jobs to the Philippines.



Labour leader broke law - Greens



Paul Henry's co-hosts named

Ad Feedback

Keep up with NZ's
No. 1 news site.
LIKE US ON FACEBOOK








latest news headlines

- 5:44 PM Ford NZ recalls 1485 vehicles
- 5:33 PM Labour and Greens: Unhappily ever after?
- 5:33 PM Ferry crash 'kind of shocking'
- 5:32 PM Manson to the fore again at rowing nationals
- 5:28 PM Centre Place up for sale
- 5:24 PM Three dead in crash
- 5:03 PM Bondage sex trial disturbs jury

editors' picks

- Kiwi tipped to pass A97 cents
- Recipe: Pea, feta & quinoa fritters
- Six Canterbury quake memorial designs
- Giants of tech world join Kiwi Webstock
- Top five reader comments
- Duchess gets behind mental health
- 8 best moments from SNL's 40th
- Crying foul over competition odds
- See inside Harry Potter's place

Contribute to Stuff Nation

most popular

- | viewed | shared | commented |
|---|--|---|
| | | |
| Car plunges into water in Northcote | As it happened: Black Caps survive late stumble to see off plucky Scotland | Live Cricket World Cup ODI 6: Black Caps vs Scotland - scorecard |
| Fugitives Paul Bennett and Simone Wright caught in Sydney | Armed police storm Barrington Mall | Ferry slams into Devonport Wharf |
| Hilary Barry and Perlina Lau join Paul Henry | Facebook booze brags sending wrong message | Live Cricket World Cup ODI 6: Black Caps vs Scotland - commentary |
| Celia Lashlie dies | | |



		Inspector	Console	Debugger	Style Editor	Performance	Timeline	Network				
✓	Method	File	Domain	Type	Size	0 ms	1.36 min	2.73 min	4.09 min	5.46 min	6.82 min	
● 200	GET	socialize.js?apiKey=3_9JitkeW_HE...	cdns.gigya.com	js	136.43 KB	→ 593 ms						
● 200	GET	brand?form=cse-search-box&lang...	www.google.com	js	2.45 KB	→ 52 ms						
● 200	GET	omniture.min.js	www.stuff.co.nz	js	5.48 KB	→ 77 ms						
● 200	GET	nielsen.min.v60.js	www.stuff.co.nz	js	11.06 KB	→ 77 ms						
● 200	GET	mystuff-1.0.js?_=1424149113990	cdn-my.stuff.co.nz	js	9.49 KB	→ 28 ms						
● 200	GET	jwpsrv.js	p.jwpcdn.com	js	12.48 KB	→ 279 ms						
● 200	GET	googima.js	p.jwpcdn.com	js	29.21 KB	→ 280 ms						
● 200	GET	comments.getTopStreams?categor...	comments.us1.gigya.com	js	6.01 KB	→ 700 ms						
● 200	GET	jquery.min.js	ajax.googleapis.com	js	90.38 KB	→ 568 ms						
● 200	GET	underscore-min.js	cdnjs.cloudflare.com	js	15.26 KB	→ 58 ms						
● 200	GET	jquery.min.js	cdnjs.cloudflare.com	js	90.45 KB	→ 89 ms						
● 200	GET	gscounters.sendReport?reports=[{...	gscounters.us1.gigya.com	js	0.15 KB	→ 1037 ms						
● 200	GET	clientlibs-all.min.clientlibversion.98...	www.stuff.co.nz	js	238.68 KB	→ 116 ms						
● 200	GET	jwplayer.min.clientlibversion.53da6...	www.stuff.co.nz	js	61.71 KB	→ 293 ms						
● 200	GET	mobile-redirect.min.clientlibversion....	www.stuff.co.nz	js	4.16 KB	→ 53 ms						
● 200	GET	Stuff_Tag_Container.js	www.adobetag.com	js	119.33 KB	→ 443 ms						
● 200	GET	jquery.easing.1.3.js	dynamic.pulselive.com	js	8.10 KB	→ 389 ms						
● 200	GET	jquery.json-2.2.min.js	dynamic.pulselive.com	js	2.22 KB	→ 867 ms						
● 200	GET	jquery.jsonp-2.4.0.min.js	dynamic.pulselive.com	js	2.01 KB	→ 386 ms						
● 200	GET	TimeController.js	dynamic.pulselive.com	js	4.80 KB	→ 385 ms						
● 200	GET	FlipCounterCell.js	dynamic.pulselive.com	js	3.41 KB	→ 386 ms						
● 200	GET	FlipCounter.js	dynamic.pulselive.com	js	0.90 KB	→ 385 ms						
● 200	GET	CounterController.js	dynamic.pulselive.com	js	3.10 KB	→ 577 ms						
● 200	GET	CountdownController.js	dynamic.pulselive.com	js	2.17 KB	→ 577 ms						
● 200	GET	pulse-lib.js	dynamic.pulselive.com	js	743.47 KB	→ 3139 ms						
● 200	GET	css-example.js	dynamic.pulselive.com	js	2.65 KB	→ 576 ms						
● 200	GET	TextController.js	dynamic.pulselive.com	js	1.09 KB	→ 577 ms						
● 200	GET	widget.js	dynamic.pulselive.com	js	2.02 KB	→ 769 ms						
● 200	GET	matchSchedule2.js?_1424149118...	dynamic.pulselive.com	js	28.33 KB	→ 190 ms						
● 200	GET	matchSchedule2.js?_1424149178...	dynamic.pulselive.com	js	28.33 KB	→ 0 ms						
● 200	GET	matchSchedule2.js?_1424149239...	dynamic.pulselive.com	js	28.33 KB	→ 379 ms						
● 200	GET	matchSchedule2.js?_1424149299...	dynamic.pulselive.com	js	28.33 KB	→ 381 ms						
● 200	GET	matchSchedule2.js?_1424149360...	dynamic.pulselive.com	js	28.33 KB	→ 379 ms						
● 200	GET	matchSchedule2.js?_1424149420...	dynamic.pulselive.com	js	28.33 KB	→ 570 ms						
● 200	GET	matchSchedule2.js?_1424149481...	dynamic.pulselive.com	js	28.33 KB	→ 379 ms						

`https://ajax.googleapis.com
/ajax/libs/jquery/1.8.0/
jquery.min.js`

what would happen if that
server were **compromised**?



Bad Things™

steal sessions

leak confidential data

redirect to phishing sites

enlist DDoS zombies

simple solution

instead of this:

```
<script  
  src="https://ajax.googleapis.com...">
```


do this:

```
<script
```

```
  src="https://ajax.googleapis.com..."
```

```
  integrity="sha256-1z4uG/+cVbhShP..."
```

```
  crossorigin="anonymous">
```

guarantee:

script won't change

or it'll be **blocked**

security

for sysadmins

HTTPS

if you're not using it, now is the time to start :)

Mozilla Security Blog



Deprecating Non-Secure HTTP



rbarnes

288

Today we are announcing our intent to phase out non-secure HTTP.

There's pretty broad agreement that HTTPS is the way forward for the web. In recent months, there have been statements from [IETF](#), [IAB](#) (even the [other IAB](#)), [W3C](#), and the [US Government](#) calling for universal use of encryption by Internet applications, which in the case of the web means HTTPS.

After a [robust discussion](#) on our community mailing list, Mozilla is committing to focus new development efforts on the secure web, and start removing capabilities from the non-secure web. There are two broad elements of this plan:



rbarnes

More

Cate

Anno

Conf

Firefo

Firefo

Musin

Press



mass surveillance of
all Internet traffic
is no longer theoretical

strong encryption of
all Internet traffic
is no longer optional

“If we only use encryption when we're working with important data, then **encryption signals that data's importance**. If only dissidents use encryption in a country, that country's authorities have an easy way of identifying them. But **if everyone uses it all of the time, encryption ceases to be a signal**. The government can't tell the dissidents from the rest of the population. Every time you use encryption, you're **protecting someone who needs to use it to stay alive.**”

-Bruce Schneier



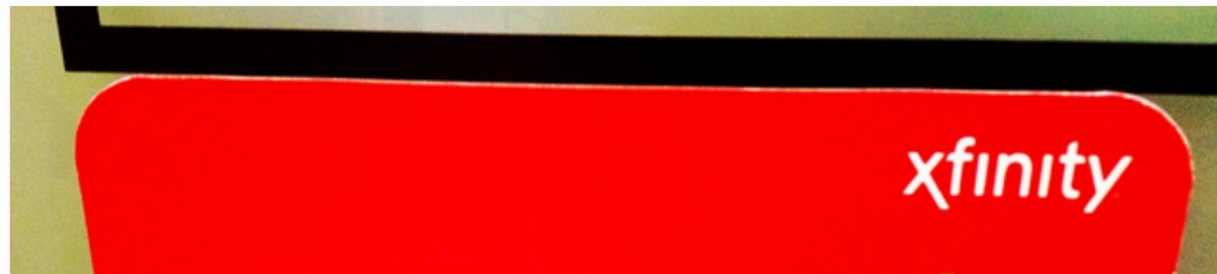
LAW & DISORDER / CIVILIZATION & DISCONTENTS

Comcast Wi-Fi serving self-promotional ads via JavaScript injection

The practice raises security, net neutrality issues as FCC mulls Internet reforms.

by David Kravets - Sep 8, 2014 5:00am PDT

[Share](#) [Tweet](#) 196



LATEST FEATURE STORY



FEATURE STORY (2 PAGES)

Remembering Nuon, the gaming chip that nearly changed the world—but didn't

How DVD players and game consoles nearly combined to rock consumer electronics in the

Don't let AT&T mislead you about its \$29 "privacy fee"

by Stacey Higginbotham [Twitter](#) Feb. 19, 2015 - 11:26 AM PDT

17 Comments



MUST READ **73 PERCENT OF COMPANIES PLAN TO ADOPT WINDOWS 10 WITHIN TWO YEARS OF ITS RELEASE**

Optus hands over customers' numbers to websites

Optus has admitted that it hands over the mobile phone numbers of customers to websites that have a commercial relationship with the company, without its customers' knowledge.



By [Josh Taylor](#) | June 24, 2015 -- 01:19 GMT (18:19 PDT) | Topic: [Telcos](#)



ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS P

NOVEMBER 3, 2014 | BY [JACOB HOFFMAN-ANDREWS](#)



Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls

Verizon users might want to start looking for another provider. In an effort to **better serve advertisers**, Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device. It allows third-party advertisers and websites to assemble a deep, permanent profile of visitors' web browsing habits without their consent.

Verizon apparently created this mechanism to expand **their advertising programs**, but it has privacy



Let's Encrypt

```
$ apt-get install letsencrypt
```

```
$ letsencrypt example.com
```

automatically prove domain ownership

automatically prove domain ownership

download a free-as-in-beer certificate

automatically prove domain ownership

download a free-as-in-beer certificate

monitor and renew it before it expires

HTTPS is not enough

you need to do it properly

RC4

RC4

SHA-1

RC4

1024-bit certificates

SHA-1

RC4 weak DH parameters

1024-bit certificates SHA-1

Security/Server Side TLS

< Security

The goal of this document is to help operational teams with the configuration of TLS on servers. All Mozilla recommendations below.

The Operations Security (OpSec) team maintains this document as a reference guide to navigate the TLS landscape, protocols, known issues and vulnerabilities, configuration examples and testing tools. Changes are reviewed and broadcasted to the various Operational teams.

Contents [\[hide\]](#)

- 1 Recommended configurations
 - 1.1 **Modern** compatibility
 - 1.2 **Intermediate** compatibility (default)
 - 1.3 **Old** backward compatibility
- 2 Prioritization logic
- 3 Mandatory discards
- 4 Forward Secrecy
 - 4.1 DHE handshake and dhparam
 - 4.2 Pre-defined DHE groups
 - 4.3 DHE and ECDHE support
 - 4.4 DHE and Java
- 5 OCSP Stapling
- 6 Session Resumption
- 7 HSTS: HTTP Strict Transport Security
- 8 HPKP: Public Key Pinning Extension for HTTP



- Main page
- Product releases
- New pages
- Recent changes
- Recent uploads
- Popular pages
- Random page
- Help

- How to Contribute
 - All-hands meeting
 - Other meetings
 - Contribute to Mozilla
 - Mozilla Reps
 - Student Ambassadors
- MozillaWiki
- Around Mozilla
- Tools

Mozilla SSL Configuration Generator

- Apache
- Nginx
- HAProxy
- AWS ELB

- Modern
- Intermediate
- Old

Server Version

OpenSSL Version

HSTS Enabled

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | [link](#)

Oldest compatible clients : Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

```
<VirtualHost *:443>
...
SSLEngine on
SSLCertificateFile      /path/to/signed_certificate
SSLCertificateChainFile /path/to/intermediate_certificate
SSLCertificateKeyFile   /path/to/private/key
SSLCACertificateFile    /path/to/all_ca_certs

# intermediate configuration, tweak to your needs
SSLProtocol              all -SSLv2 -SSLv3
SSLCipherSuite           ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECI
SSLHonorCipherOrder     on

# HSTS (mod_headers is required) (15768000 seconds = 6 months)
Header always set Strict-Transport-Security "max-age=15768000"
...
</VirtualHost>
```

[More details on these security profiles](#) - [Report issues, submit pull requests and fork code here](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.linuxfestnorthwest.org](#)

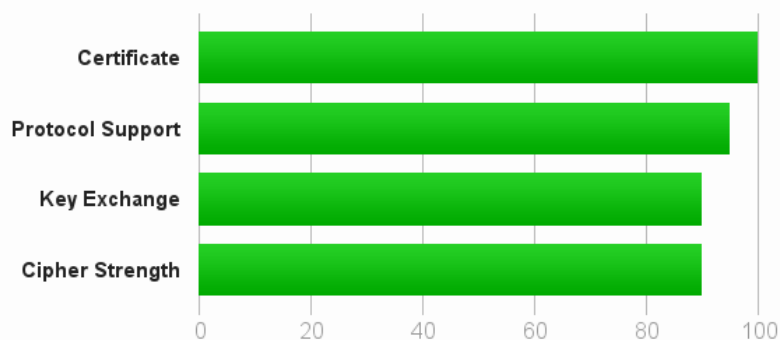
SSL Report: [www.linuxfestnorthwest.org](#) (54.186.134.147)

Assessed on: Mon, 18 Apr 2016 22:54:56 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

Authentication



Server Key and Certificate #1



Subject

[www.linuxfestnorthwest.org](#)

Fingerprint SHA1: 9e2676d434685d4040dfb3082c4f6ebc1e06d866

Pip SHA256: iNRddwAFn1OC5MKJlJ0ahL5lIaEvh0NHRTUfE1mPmVA=



Mixed Content

Editor's Draft, 24 June 2015

This version:

<https://w3c.github.io/webappsec/specs/mixedcontent/>

Latest version:

<http://www.w3.org/TR/mixed-content/>

Previous Versions:

<http://www.w3.org/TR/2015/CR-mixed-content-20150317/>

<http://www.w3.org/TR/2014/WD-mixed-content-20141113/>

<http://www.w3.org/TR/2014/WD-mixed-content-20140916/>

<http://www.w3.org/TR/2014/WD-mixed-content-20140722/>

Version History:

<https://github.com/w3c/webappsec/commits/master/specs/mixedcontent>

Feedback:

public-webappsec@w3.org with subject line "[mixed-content] ... message"

Issue Tracking:

[GitHub](#)

Editor:

[Mike West](#) (Google Inc.)

<https://people.mozilla.org/~fmarier/mixed-content.html>

```
<html>
<head>
  <script
    src="http://people.mozilla.org/~fmarier/mixed-content.js">
  </script>
</head>
<body>
  
</body>
</html>
```

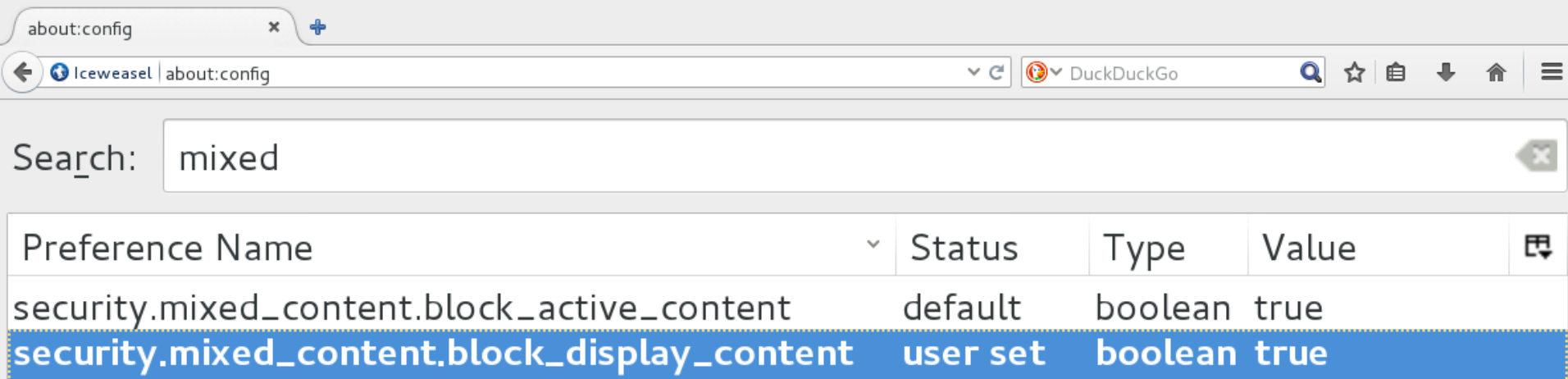


Con... Inspe... Debu... Style E... Pro... Net...

Net CSS JS Security Logging Clear Filter output

- Blocked loading mixed active content "http://people.mozilla.org/~fmarier/mixed-content.js" [Learn More] 2 mixed-content.h...
- Loading mixed (insecure) display content on a secure page "http://fmarier.org/img/francois_marier.jpg" [Learn More] 2 mixed-content.h...

turn on full mixed-content blocking in development



The screenshot shows a web browser window with the address bar set to 'about:config'. The search bar contains the text 'mixed'. Below the search bar, a table lists configuration preferences. The table has five columns: Preference Name, Status, Type, Value, and an icon. The second row is highlighted in blue.

Preference Name	Status	Type	Value	
security.mixed_content.block_active_content	default	boolean	true	
security.mixed_content.block_display_content	user set	boolean	true	

privacy

privacy

for users

cricket world cup

DRAMATIC RESCUE

Frantic effort to rescue woman

5:05 PM Police plunge into water and use rocks to save a woman trapped in a sinking car.

Three dead in crash

5:24 PM Three people die and one is critically injured after a logging truck crash in Tokoroa.

NZ stumble to three-wicket win

4:44 PM Black Caps go two-from-two in World Cup, but not before losing seven wickets.

Fugitive in court

Man who was on the run from sex and fraud allegations enters no plea in Sydney court.

Ferry crash 'kind of shocking'

15 min ago Seventeen people hurt as an Auckland harbour ferry crashes into a wharf.

Proposal to outsource NZ Post jobs

5:03 PM Staff at New Zealand Post are told of proposal to outsource 24 financial support jobs to the Philippines.

Labour leader broke law - Greens

Paul Henry's co-hosts named

Ad Feedback

Keep up with NZ's No. 1 news site. LIKE US ON FACEBOOK

latest news headlines

- 5:44 PM Ford NZ recalls 1485 vehicles
- 5:33 PM Labour and Greens: Unhappily ever after?
- 5:33 PM Ferry crash 'kind of shocking'
- 5:32 PM Manson to the fore again at rowing nationals
- 5:28 PM Centre Place up for sale
- 5:24 PM Three dead in crash
- 5:03 PM Bondage sex trial disturbs jury

editors' picks

- Kiwi tipped to pass A97 cents
- Recipe: Pea, feta & quinoa fritters
- Six Canterbury quake memorial designs
- Giants of tech world join Kiwi Webstock
- Top five reader comments
- Duchess gets behind mental health
- 8 best moments from SNL's 40th
- Crying foul over competition odds
- See inside Harry Potter's place

most popular

- | viewed | shared | commented |
|--|--------|-----------|
| | | |
| Car plunges into water in Northcote | | |
| As it happened: Black Caps survive late stumble to see off plucky Scotland | | |
| Live Cricket World Cup ODI 6: Black Caps vs Scotland - scorecard | | |
| Fugitives Paul Bennett and Simone Wright caught in Sydney | | |
| Armed police storm Barrington Mall | | |
| Ferry slams into Devonport Wharf | | |
| Hilary Barry and Perlina Lau join Paul Henry | | |
| Facebook booze brags sending wrong message | | |
| Live Cricket World Cup ODI 6: Black Caps vs Scotland - commentary | | |
| Celia Lashlie dies | | |

Contribute to Stuff Nation



		Inspector	Console	Debugger	Style Editor	Performance	Timeline	Network				
✓	Method	File	Domain	Type	Size	0 ms	1.36 min	2.73 min	4.09 min	5.46 min	6.82 min	
●	200 GET	socialize.js?apiKey=3_9JitkeW_HE...	cdns.gigya.com	js	136.43 KB	→ 593 ms						
●	200 GET	brand?form=cse-search-box&lang...	www.google.com	js	2.45 KB	→ 52 ms						
●	200 GET	omniture.min.js	www.stuff.co.nz	js	5.48 KB	→ 77 ms						
●	200 GET	nielsen.min.v60.js	www.stuff.co.nz	js	11.06 KB	→ 77 ms						
●	200 GET	mystuff-1.0.js?_=1424149113990	cdn-my.stuff.co.nz	js	9.49 KB	→ 28 ms						
●	200 GET	jwpsrv.js	p.jwpcdn.com	js	12.48 KB	→ 279 ms						
●	200 GET	googima.js	p.jwpcdn.com	js	29.21 KB	→ 280 ms						
●	200 GET	comments.getTopStreams?categor...	comments.us1.gigya.com	js	6.01 KB	→ 700 ms						
●	200 GET	jquery.min.js	ajax.googleapis.com	js	90.38 KB	→ 568 ms						
●	200 GET	underscore-min.js	cdnjs.cloudflare.com	js	15.26 KB	→ 58 ms						
●	200 GET	jquery.min.js	cdnjs.cloudflare.com	js	90.45 KB	→ 89 ms						
●	200 GET	gscounters.sendReport?reports=[{...	gscounters.us1.gigya.com	js	0.15 KB	→ 1037 ms						
●	200 GET	clientlibs-all.min.clientlibversion.98...	www.stuff.co.nz	js	238.68 KB	→ 116 ms						
●	200 GET	jwplayer.min.clientlibversion.53da6...	www.stuff.co.nz	js	61.71 KB	→ 293 ms						
●	200 GET	mobile-redirect.min.clientlibversion....	www.stuff.co.nz	js	4.16 KB	→ 53 ms						
●	200 GET	Stuff_Tag_Container.js	www.adobetag.com	js	119.33 KB	→ 443 ms						
●	200 GET	jquery.easing.1.3.js	dynamic.pulselive.com	js	8.10 KB	→ 389 ms						
●	200 GET	jquery.json-2.2.min.js	dynamic.pulselive.com	js	2.22 KB	→ 867 ms						
●	200 GET	jquery.jsonp-2.4.0.min.js	dynamic.pulselive.com	js	2.01 KB	→ 386 ms						
●	200 GET	TimeController.js	dynamic.pulselive.com	js	4.80 KB	→ 385 ms						
●	200 GET	FlipCounterCell.js	dynamic.pulselive.com	js	3.41 KB	→ 386 ms						
●	200 GET	FlipCounter.js	dynamic.pulselive.com	js	0.90 KB	→ 385 ms						
●	200 GET	CounterController.js	dynamic.pulselive.com	js	3.10 KB	→ 577 ms						
●	200 GET	CountdownController.js	dynamic.pulselive.com	js	2.17 KB	→ 577 ms						
●	200 GET	pulse-lib.js	dynamic.pulselive.com	js	743.47 KB	→ 3139 ms						
●	200 GET	css-example.js	dynamic.pulselive.com	js	2.65 KB	→ 576 ms						
●	200 GET	TextController.js	dynamic.pulselive.com	js	1.09 KB	→ 577 ms						
●	200 GET	widget.js	dynamic.pulselive.com	js	2.02 KB	→ 769 ms						
●	200 GET	matchSchedule2.js?_1424149118...	dynamic.pulselive.com	js	28.33 KB	→ 190 ms						
●	GET	matchSchedule2.js?_1424149178...	dynamic.pulselive.com	js	28.33 KB	→ 0 ms						
●	200 GET	matchSchedule2.js?_1424149239...	dynamic.pulselive.com	js	28.33 KB		→ 379 ms					
●	200 GET	matchSchedule2.js?_1424149299...	dynamic.pulselive.com	js	28.33 KB			→ 381 ms				
●	200 GET	matchSchedule2.js?_1424149360...	dynamic.pulselive.com	js	28.33 KB				→ 379 ms			
●	200 GET	matchSchedule2.js?_1424149420...	dynamic.pulselive.com	js	28.33 KB					→ 570 ms		
●	200 GET	matchSchedule2.js?_1424149481...	dynamic.pulselive.com	js	28.33 KB						→ 379 ms	

- VISUALIZATION
- Graph
 - List
- DATA
- Save Data
 - Reset Data
- Give Us Feedback
mozilla.org/lightbeam

Daily

GRAPH VIEW



> stuff.co.nz

? FIRST ACCESS Tue, Feb 17, 2015 5:50PM
LAST ACCESS Tue, Feb 17, 2015 5:50PM

i

Block Site

Server Location



Connected to **18 sites** since first access.

- google.com
- googletagservices.com
- gigya.com
- googlesyndication.com
- imrworldwide.com
- googleadservices.com
- jwpcdn.com
- adobetag.com
- pulselive.com
- doubleclick.net
- 2mdn.net
- ajax.googleapis.com
- demdex.net
- google-analytics.com
- facebook.net
- scorecardresearch.com
- rubiconproject.com
- facebook.com

TOGGLE CONTROLS

- Visited Sites
- Watched Sites
- Third Party Sites
- Blocked Sites
- Connections
- Cookies

FILTER

Hide

- Recent Site
- Last 10 Sites
- Daily
- Weekly



about:config

network.cookie.lifetimePolicy = 3

network.cookie.lifetime.days = 5

network.cookie.thirdparty.sessionOnly = true

<https://feeding.cloud.geek.nz/posts/tweaking-cookies-for-privacy-in-firefox/>

Tracking Protection



based on Safe Browsing

pre-downloaded list of full hashes

(no server lookups)

1. is this resource coming from a third-party server?
2. is it on Disconnect's list of trackers?
3. is it actually a third-party or
does it belong to the same org?

Q: What does it do?

A: It blocks network loads!

No cookies

No fingerprinting

No wasted bandwidth

No performance hit

about:config

privacy.trackingprotection.pbmode.enabled

about:config

privacy.trackingprotection.enabled

<https://feeding.cloud.geek.nz/posts/how-tracking-protection-works-in-firefox/>

privacy

for developers



Referrer Policy

Editor's Draft 11 May 2015

This version:

<https://w3c.github.io/webappsec/specs/referrer-policy/>

Latest version:

<http://www.w3.org/TR/referrer-policy/>

Version History:

<https://github.com/w3c/webappsec/commits/master/spec>

Feedback:

public-webappsec@w3.org with subject line “[REFERRE”

Issue Tracking:

[Inline In Spec](#)

Editors:

[Jochen Eisinger](#) (Google Inc.)

[Mike West](#) (Google Inc.)



⚙ ➤ Console 🔍 Inspector ⏸ Debugger ✍ Style Editor 🕒 Profiler **📡 Network**

Method	File	Domain	Headers	Cookies	Params	Response
200 GET	mixed-content.html	people.mozilla.org	Request URL: https://people.mozilla.org/~fmarier Request method: GET Status code: 200 OK			
200 GET	francois_marier.jpg	fmarier.org				

🔍 Filter headers

- ⊕ Response headers (0.356 KB)
- ⊖ Request headers (0.452 KB)

Host: "people.mozilla.org"

User-Agent: "Mozilla/5.0 (X11; Linux x86_6...Fir"

Accept: "text/html,application/xhtml+xml,application/javascript;q=0.9,*/*;q=0.8"

Accept-Language: "en-US,en;q=0.5"

Accept-Encoding: "gzip, deflate"

Referer: "https://people.mozilla.org/~fmarier/"

Cookie: "_ga=GA1.2.1405561007.143441803"

Connection: "keep-alive"

Pragma: "no-cache"

http://example.com/search?q=serious+medical+condition

Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla.

Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla. Bla bla bla, bla bla, bla bla bla bla.

[Click here for
the cheapest
insurance
around!](#)



SEARCH

JANUARY 20, 2015 | BY COOPER QUINTIN



HealthCare.gov Sends Personal Data to Dozens of Tracking Websites

The Associated Press reports that healthcare.gov—the flagship site of the Affordable Care Act, where millions of Americans have signed up to receive health care—is quietly sending personal health information to a number of third party websites. The information being sent includes one's zip code, income level, smoking status, pregnancy status and more.

event?a=166688199&d=166688199&y=false&src=js&x2219631051=2229360796&s171652904=false&s171674651=none&s171946972=gc&s172159083=direct&s269684250=true... 166688199.log.optimizely.com	GET	200 OK	166688199.log.optimizely.com	application/json
activity;src=4037109;type=20142003;cat=201420;ord=4567172936304;--oref=https%3A%2F%2Fwww.healthcare.gov%2Fsee-plans%2F85001%2Fresults%2F%3Fcounty%3D040... 4037109.fl.s.doubleclick.net	GET	200 OK	4037109.fl.s.doubleclick.net	text/html
?random=1421466406378&cv=7&fst=1421466406378&num=1&fmt=1&guid=ON&u_h=900&u_w=1600&u_ah=... googleads.g.doubleclick.net/pagead/viewthroughconversion/977299465		302 Found	https://4037109.fl.s.doubleclick.net/activity;src=4037109;type... googleads.g.doubleclick.net	text/html
ping?h=healthcare.gov&p=%2Fsee-plans%2F85001%2Fresults%2F%3Fcounty%3D04013%26age%3D38%26smoker%3D1%26parent%3D0%26pregnant%3D1%26mec%3D%26zi... ping.chartbeat.net	GET	200 OK	ping.chartbeat.net	image/gif

An example of personal health data being sent to third parties from healthcare.gov

EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled **Do Not Track**. The information is sent via the referrer header, which contains the URL of the page requesting a third party resource.

The referrer header is an essential part of the HTTP protocol, and is sent for every request that is made on the web. The referrer header lets the requested resource know what URL the request came from. This

No Referrer

No Referrer

No Referrer When Downgrade

No Referrer

No Referrer When Downgrade

Origin Only

No Referrer

No Referrer When Downgrade

Origin Only

Origin When Cross Origin

No Referrer

No Referrer When Downgrade

Origin Only

Origin When Cross Origin

Unsafe URL

Referrer-Policy: origin

Referrer-Policy: origin

```
<meta name="referrer" content="origin">
```

Referrer-Policy: origin

```
<meta name="referrer" content="origin">
```

```
<a href="http://example.com"  
  referrerPolicy="origin">
```

recommendations

for users

network.cookie.lifetimePolicy = 3

network.cookie.lifetime.days = 5

network.cookie.thirdparty.sessionOnly = true

network.http.referer.spoofSource = true

privacy.trackingprotection.enabled = true

security.pki.sha1_enforcement_level = 2

security.ssl.errorReporting.automatic = true

Install the EFF's **HTTPS Everywhere** add-on

<https://github.com/pyllyukko/user.js>

recommendations

for developers

Use **SRI** for your external scripts

Set a more restrictive **Referrer** policy

Consider enabling **CSP**

Watch out for **mixed content**

Test your site with **Tracking Protection**

recommendations

for sysadmins

Enable **HTTPS** and **HSTS** on all your sites

Use our **recommended TLS config**

Test your site **periodically** using SSL Labs

Questions?

feedback:

francois@mozilla.com

mozilla.dev.security

public-webappsec@w3.org



© 2016 François Marier <francois@mozilla.com>

This work is licensed under a

[Creative Commons Attribution-ShareAlike 4.0](https://creativecommons.org/licenses/by-sa/4.0/) License.

photo credits:

cookie: <https://secure.flickr.com/photos/jamisonjudd/4810986199/>

explosion: <https://www.flickr.com/photos/-cavin-/2313239884/>

snowden: <https://www.flickr.com/photos/gageskidmore/16526354372>