

# Security and Privacy on the Web in 2015



François Marier @fmarier

**mozilla**



# Firefox

## Security & Privacy

Platform

# Web Platform

# Content Security Policy

## aka *CSP*

# 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 you<script>  
alert('p0wned');  
</script>!
```

**Tweet!**



**without CSP**

---

John Doe - just moments ago

Hi yo

p0wned

---

Ok











**with CSP**

---

John Doe - just moments ago

# Hi you!

---

  Cons...  Inspec...  Debug...  Style Edi...  Prof...  Netw...   

☐ Net

☒ CSS


☐ JS

☒ Security

☐ Logging

Clear

Filter output

 Content Security Policy: The page's settings blocked the loading of a resource: [csp-block](#)  
An attempt to execute inline scripts has been blocked

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

inline scripts are **blocked** unless  
`unsafe-inline` is specified

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

# violation reports:

```
$ curl --head https://twitter.com
HTTP/1.1 200 OK
content-length: 58347
content-security-policy: ...
report-uri https://twitter.com/csp_report
```



```
"csp-report": {  
  "document-uri":  
    "http://example.org/page.html",  
  "referrer":  
    "http://evil.example.com/haxor.html",  
  "blocked-uri":  
    "http://evil.example.com/image.png",  
  "violated-directive": "default-src 'self'",  
  "effective-directive": "img-src",  
  "original-policy":  
    "default-src 'self';  
    report-uri http://example.org/..."  
}
```



# Content Security Policy Level 2

W3C Candidate Recommendation, 19 February 2015

**This version:**

<http://www.w3.org/TR/2015/CR-CSP2-20150219/>

**Latest version:**

<http://www.w3.org/TR/CSP2/>

**Editor's Draft:**

<https://w3c.github.io/webappsec/specs/CSP2/>

**Previous Versions:**

support for inline scripts

Content-Security-Policy:

script-src 'sha256-YWIZ0W...'



iOS

# Strict Transport Security aka *HSTS*

# Strict Transport Security aka *HSTS*

mechanism for preventing  
HTTPS to HTTP downgrades

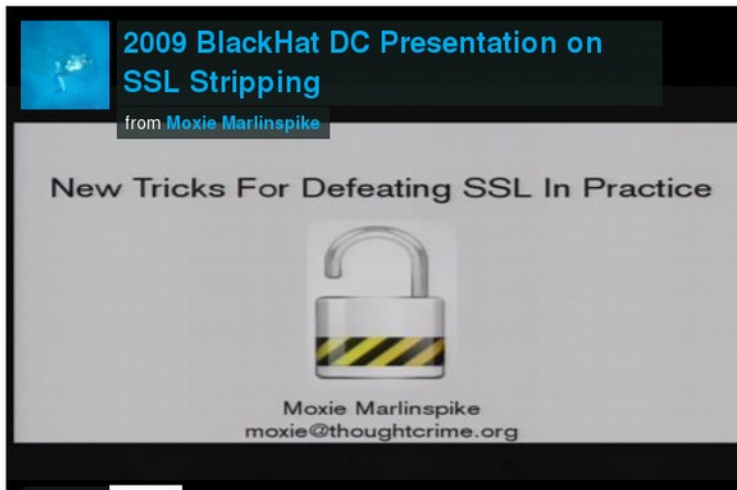
telling the browser that your site  
should **never be reached** over HTTP



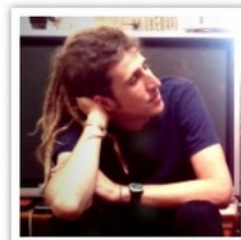
## Software >> sslstrip

[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](mailto:moxie.website@moxie.org)[@moxie](https://twitter.com/moxie)[GPG Key](#)



no HSTS, no sslstrip

GET banque.fr → 301

GET https://banque.fr → 200

no HSTS, **with** sslstrip

GET banque.fr → 200

what does HSTS look like?

```
$ curl -i https://example.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://banque.fr> → 200

silent client-side redirects

HTTP → HTTPS

**no** HTTP traffic for  
sslstrip to tamper with

except for the very  
**first** connection



# https://hstspreload.appspot.com/

**Domain to include in HSTS list:**

This form is used to submit domains for inclusion in Chrome's [HTTP Strict Transport Security \(HSTS\)](#) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only. [Firefox](#), Safari and [a future IE version](#) also have HSTS preload lists which include the Chrome list. (See the [HSTS compatibility matrix](#).)

In order to be included on the HSTS preload list, your site must:



iOS

coming up in 2015



# 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.

## 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



**stuff.co.nz**  
 News for the world you live in

## 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 Perina Lau join Paul Henry
- Facebook booze brags sending wrong message
- Live Cricket World Cup ODI 6: Black Caps vs Scotland - commentary
- Cela Lashie 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								

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

how common is this?





# Search

[Repositories](#)

8

[Code](#)

2,487,059

[Issues](#)

2,373

[Users](#)

## We've found 2,487,059 code results

Sort: **Best match** ▾[phpzoom/FastCode – jQuery](#)

Showing the top seven matches. Last indexed on 23 Jul 2014.

```
1 http://ajax . googleapis . com / ajax / libs / jquery / 1.7.2 / jquery . min . js
```

[spautz/appointments-app – https.js](#)

JavaScript

Showing the top seven matches. Last indexed on 2 Aug 2014.

```
1 steal('https://ajax . googleapis . com / ajax / libs / jquery / 1.4.4 / jquery . js');
```

[npmcomponent/DamonOehlman-bedazzle – jquery.min.js](#)

JavaScript

Showing the top seven matches. Last indexed on 31 Jul 2014.

```
1 //= http://ajax . googleapis . com / ajax / libs / jquery / 1.7.1 / jquery . min . js
```

[pascalbeyeler/PhysicsEngine – https.js](#)

JavaScript

Showing the top seven matches. Last indexed on 21 Jul 2014.

```
1 steal('https://ajax . googleapis . com / ajax / libs / jquery / 1.4.4 / jquery . js');
```

## Languages

HTML 1,935,382

PHP 203,152

JavaScript 33,920

HTML+ERB 26,701

Java Server Pages 26,005

Markdown 23,161

Jade 12,705

Haml 6,012

Python 4,244

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...">
```

guarantee:

script won't change

or it'll be **blocked**



limitation:

won't work for scripts

that **change all the time**

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

there's a little something missing...

complete example:

```
<script  
  src="https://ajax.googleapis.com..."  
  integrity="sha256-1z4uG/+cVbhShP..."  
  crossorigin="anonymous">
```



# Cross-Origin Resource Sharing

W3C Recommendation 16 January 2014

## **This Version:**

<http://www.w3.org/TR/2014/REC-cors-20140116/>

## **Latest Version:**

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

## **Previous Versions:**

<http://www.w3.org/TR/2013/PR-cors-20131205/>

<http://www.w3.org/TR/2013/CR-cors-20130129/>

<http://www.w3.org/TR/2012/WD-cors-20120403/>

<http://www.w3.org/TR/2010/WD-cors-20100727/>

<http://www.w3.org/TR/2009/WD-cors-20090317/>

<http://www.w3.org/TR/2008/WD-access-control-20080912/>

<http://www.w3.org/TR/2008/WD-access-control-20080214/>

<http://www.w3.org/TR/2007/WD-access-control-20071126/>

<http://www.w3.org/TR/2007/WD-access-control-20071001/>

<http://www.w3.org/TR/2007/WD-access-control-20070618/>

<http://www.w3.org/TR/2007/WD-access-control-20070215/>

<http://www.w3.org/TR/2006/WD-access-control-20060517/>

<http://www.w3.org/TR/2005/NOTE-access-control-20050613/>

## **Editor:**

[Anne van Kesteren](#) (formerly of [Opera Software ASA](#)) <[annevk@annevk.nl](mailto:annevk@annevk.nl)>

Please note there may be [errata](#) for this document.

The English version of this specification is the only normative version. Non-normative [translations](#) may also be available.

# same-origin policy

“a web browser permits scripts contained in a first web page to access data in a second web page, but **only if both web pages have the same origin**”

`example.com/index.html`

`example.com/index.html`

A black arrow originates from the bottom right corner of the first box and points towards the top left corner of the second box.

`example.com/data.js:`

`var secret = 42;`



`example.com/index.html`



A large rectangular box on the left contains the text 'example.com/index.html'. From the right side of this box, two arrows originate. The top arrow points diagonally upwards and to the right, ending at the top-left corner of the first box on the right. The bottom arrow points diagonally downwards and to the right, ending at the top-left corner of the second box on the right.

`example.com/data.js:`

```
var secret = 42;
```

`evil.net/widget.js:`

```
exfiltrate(secret);
```

example.com/index.html



```
graph LR; A[example.com/index.html] --> B[example.com/data.js: var secret = 42;]; A --> C[evil.net/widget.js: exfiltrate(secret);];
```

example.com/data.js:

```
var secret = 42;
```

evil.net/widget.js:

```
exfiltrate(seXet);
```

on the **server**:

`Access-Control-Allow-Origin: *`

on the **server**:

```
Access-Control-Allow-Origin: *
```

on the **client**:

```
crossorigin="anonymous"
```

complete example:

```
<script
```

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

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

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

complete example:

```
<link rel="stylesheet"  
      href="style.css"  
      integrity="sha256-PgMdguwx/0..."  
      crossorigin="anonymous">
```

SRIhash.org

# SRI Hash Generator

Enter the URL of the resource you wish to use:

Hash!

```
<script src="https://code.jquery.com/jquery-1.8.0.min.js" integrity="sha256-DpuJI2KWjyuDwynH9NpMNutHejNcFPor91XKLMihYhc=" crossorigin="anonymous"></script>
```

## What is Sub-resource integrity?

SRI is a new [W3C specification](#) that allows web developers to ensure that resources hosted on third-party servers have not been tampered with. Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

---





# 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/specs/referrer-policy/index.src.html>

**Feedback:**

[public-webappsec@w3.org](mailto:public-webappsec@w3.org) with subject line “[REFERRER] ... *message topic* ...” ([archives](#))

**Issue Tracking:**

[Inline In Spec](#)

**Editors:**

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

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

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



⚙ Console Inspector Debugger Style Editor Profiler Network

✓	Method	File	Domain	Headers	Cookies	Params	Response	Timings	Preview
● 200	GET	mixed-content.html	people.mozilla.org	<div>Request URL: https://people.mozilla.org/~fmarier/mixed-content.html Request method: GET Status code: ● 200 OK <span>Edit and Resend</span></div> <div>Filter headers</div> <div>Response headers (0.356 KB)</div> <div>Request headers (0.452 KB)</div> <div>Host: "people.mozilla.org"</div> <div>User-Agent: "Mozilla/5.0 (X11; Linux x86_6...Firefox/31.0 Icedove/31.7.0"</div> <div>Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"</div> <div>Accept-Language: "en-US,en;q=0.5"</div> <div>Accept-Encoding: "gzip, deflate"</div> <div>Referer: "https://people.mozilla.org/~fmarier/"</div> <div>Cookie: "_ga=GA1.2.1405561007.1434418036"</div> <div>Connection: "keep-alive"</div>					
● 200	GET	francois_marier.jpg	fmarier.org						

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!](#)



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&x=2219631051=2229360796&s171652904=false&s171674651=none&s171946972=gc&s172159083=direct&s269684250=true...	GET	200 OK	166688199.log.optimizely.com	application/json
	activity?src=4037109&type=20142003&cat=20142003&ord=4567172936304~oref=https%3A%2F%2Fwww.healthcare.gov%2Fsee-plans%2F85001%2Fresults%2F%3Fcounty%3D040...	GET	200 OK	4037109.flis.doubleclick.net	text/html
	?random=1421466406378&cv=7&fst=1421466406378&num=1&fmt=ON&u_h=900&u_w=1600&u_ah=fhttps://4037109.flis.doubleclick.net/activity?src=4037109;type=...		302 Found	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...	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

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

Content-Security-Policy:referrer origin;

Content-Security-Policy:referrer origin;

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

Content-Security-Policy:referrer origin;

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

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



(initial implementations)

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 from Richard »](#)

### Categories

[Announcements](#)

[Conferences](#)

[Firefox](#)

[Firefox OS](#)

[Musings](#)

[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.

LATEST FEATURE STORY



GIGAOM RESEARCH

<https://gigaom.com/2015/02/19/dont-let-att-mislead-you-about-its-29-privacy-fee/>

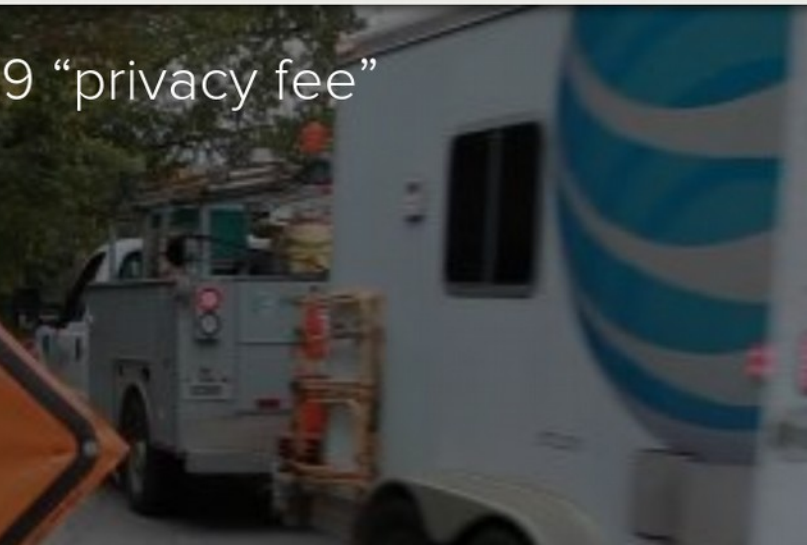
[Apple](#) [Cloud](#) [Data](#) [Media](#) [Mobile](#) [Science & Energy](#) [Social & Web](#) [Podcasts](#)

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

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

17 Comments

UTILITY  
WORK



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 that 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 implications far beyond those programs. Indeed, while we're concerned about Verizon's own use of the header, we're even more worried about what it allows *others* to find out about Verizon users. The X-UIDH header effectively reinvents the cookie, but does so in a way that is shockingly insecure and dangerous to your privacy. Worse still, Verizon doesn't let users turn off this "feature." In fact, it functions even if you use a private browsing mode or clear your cookies. You can test whether the header is injected in your traffic by visiting [lessonslearned.org/sniff](http://lessonslearned.org/sniff) or [amibeingtracked.com](http://amibeingtracked.com) over a cell data connection.

### How X-UIDH Works, and Why It's a Problem

Like a cookie, this header uniquely identifies users to the websites they visit. Verizon adds the header at the network level, between the user's device and the servers with which the user interacts. Unlike a cookie, the header is tied to a data plan, so anyone who browses the web through a hotspot, or sh







# 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 sites and deployment should follow the recommendations below.

The Operations Security (OpSec) team maintains this document as a reference guide to navigate the TLS landscape. It contains information on protocols, known issues and vulnerabilities, configuration examples and testing tools. Changes are reviewed and merged by the OpSec team and then 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



- [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:EC
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](#) > 2015.rml.info

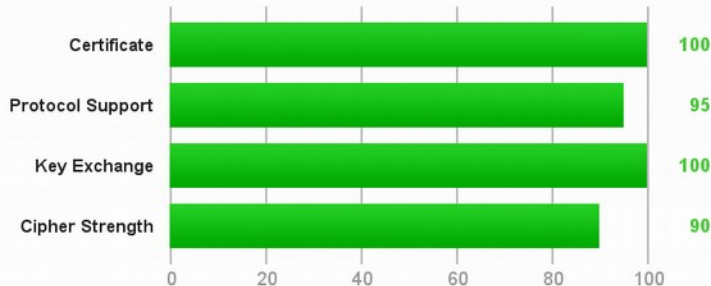
## SSL Report: 2015.rml.info (80.67.169.71)

Assessed on: Tue, 30 Jun 2015 03:53:04 UTC | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



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

This server uses RC4 with modern browsers. Grade capped to C.

This server supports TLS\_FALLBACK\_SCSV to prevent protocol downgrade attacks.



# 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/index.src.html>

**Feedback:**

[public-webappsec@w3.org](mailto:public-webappsec@w3.org) with subject line “[mixed-content] ... *message topic* ...” ([archives](#))

**Issue Tracking:**

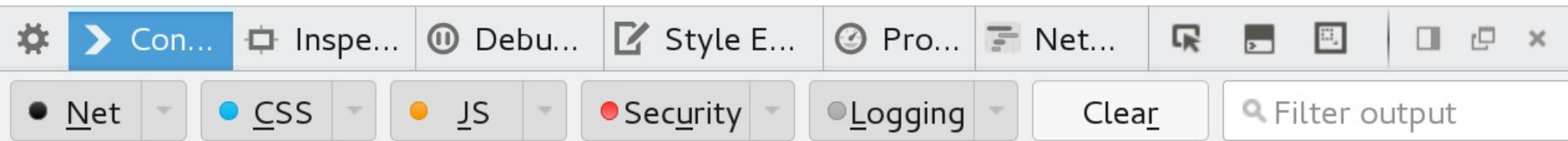
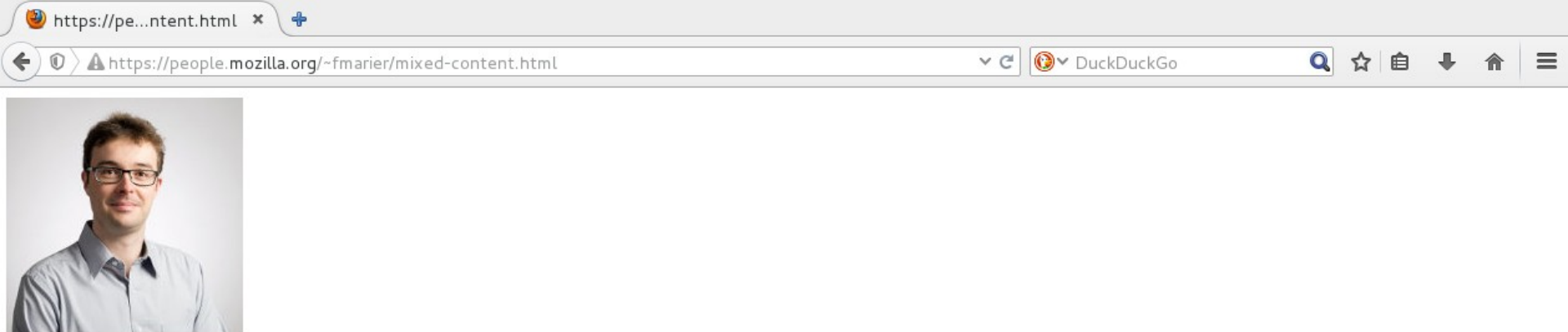
[GitHub](#)

**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>
```



✖ 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

about:config

Iceweasel | about:config

DuckDuckGo

Search: mixed

Preference Name	Status	Type	Value
security.mixed_content.block_active_content	default	boolean	true
<b>security.mixed_content.block_display_content</b>	<b>user set</b>	<b>boolean</b>	<b>true</b>

Start by enabling **HTTPS** and **HSTS**

Use **SRI** for your external scripts

Set a more restrictive **Referrer** policy

Consider enabling **CSP**

Watch out for **mixed content**

# Questions?

feedback:

[francois@mozilla.com](mailto:francois@mozilla.com)

[mozilla.dev.security](https://mozilla.dev.security)

[public-webappsec@w3.org](mailto:public-webappsec@w3.org)



© 2015 François Marier <[francois@mozilla.com](mailto: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:

tinfoil: <https://www.flickr.com/photos/laurelrusswurm/15129449047>

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

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