Contemporary Webserver Configuration

A serving suggestion

Contemporary Webserver Configuration

A serving suggestion

Protocols

HTTP

HTTP 0.9

1991

HTTP/1.0

1996

SSLv3

1996

HTTP/1.1

1999

TLS 1.0

1999

TLS 1.1

2006

TLS 1.2

2008

SPDY

2009

HTTP/2

2012 .. 2015

HTTP/2

2012 .. 2015

Scenarios for implementing HTTP/2

with modern TLS

Your motivation?

2016

really gross food
sts at State Fair of

rre fast foods you have
e to believe

6 6-foot-9-inch fish found on shore of Lake Champlain

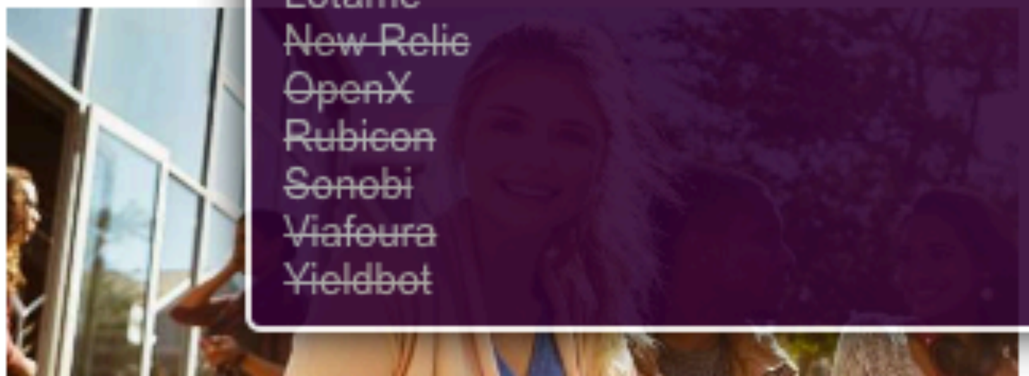
7 Raw footage purportedly shows moment El Chapo's son was...

8 Super-fast flip in Ingleside sees 1951 home bought, renovated...

9 Regularly going to concerts and dancing with friends makes you...

10 The cor... people ...

DON'T ...



~~Amazon Associates~~
~~Catchpoint~~
~~ChartBeat~~
~~Ensighten~~
~~Facebook Connect~~
~~Google Publisher Tags~~
~~Index Exchange (Formerly Casale Media)~~
~~Lotame~~
~~New Relic~~
~~OpenX~~
~~Rubicon~~
~~Sonobi~~
~~Viafoura~~
~~Yieldbot~~

Subscribe Sign In Register

Adblade
AdGear
Adify
Admeta
AdScale
adsnative
ADTECH
Amazon Associates
AppNexus
BidSwitch
BlueKai
Bounce Exchange
Burt
Catchpoint
Chango
ChartBeat
Connexity
Crazy Egg
Criteo
DataXu
Digilant
Dotomi
DoubleClick
DoubleVerify
Dstillery
eBay Stats
Ensighten
EQ Advertising
Facebook Connect
Google Adsense
Google Analytics
gumgum
iCrossing
Index Exchange (Formerly Casale Media)
Integral Ad Science
Krux Digital
LiveRamp
Lotame
Magnetic
Media Innovation Group
Media Optimizer (Adobe)
MediaMath
Moat
Nativo
NDN Player Suite
Ohana Advertising Network
OpenX
OwnerIQ
Proximic
PubMatic
PulsePoint
Quantcast
Rich
Rubicon
Simpli.fi
SiteScout
Sonobi
Taboola
TradeDesk
Veruta
Viafoura
Videology
Yashi
Yieldbot
Zedo

Some really gross food finalists at State Fair of Texas

- Bizarre fast foods you have to see to believe

6 6-foot-9-inch fish found on shore of Lake Champlain

7 Raw footage purportedly shows moment El Chapo's son was...

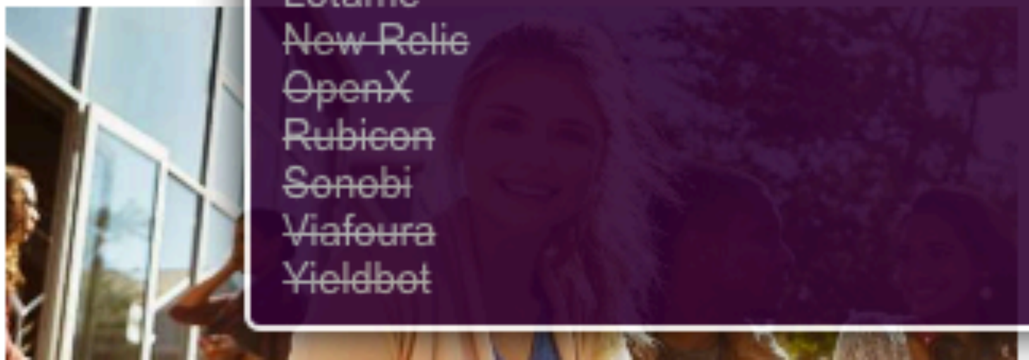
8 Super-fast flip in Ingleside sees 1951 home bought, renovated...

9 Regularly going to concerts and dancing with friends makes you...

10 The cor... people ...

~~Amazon Associates~~
~~Catchpoint~~
~~ChartBeat~~
~~Ensighten~~
~~Facebook Connect~~
~~Google Publisher Tags~~
~~Index Exchange (Formerly Casale Media)~~
~~Lotame~~
~~New Relic~~
~~OpenX~~
~~Rubicon~~
~~Sonobi~~
~~Viafoura~~
~~Yieldbot~~

DON'T



www.httpvshttps.com

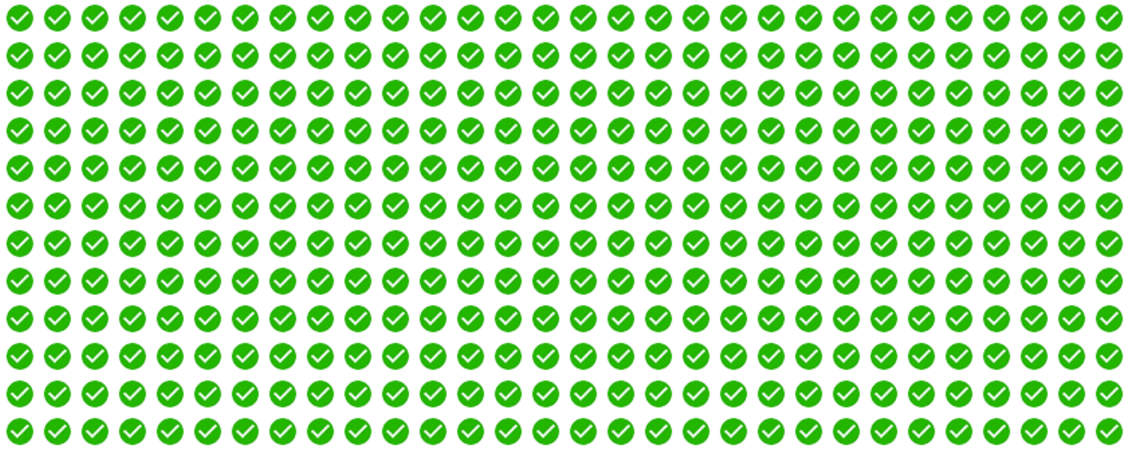
HTTP vs HTTPS Test

HTTP HTTPS

Encrypted Websites Protect Our Privacy and are Significantly Faster
Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

9.017 s

135% slower than HTTPS



Only full, end-end encryption ensures complete privacy. Cloudflare and MaxCDN SSL encryption services compromise privacy by using interceptive middle proxy servers. HTTPS means "Secure HTTP". Plaintext HTTP/1.1 is compared against encrypted HTTP/2 HTTPS on a non-caching, nginx server with a direct, non-proxied connection.

Let's Encrypt

Free TLS Certificate provided by Let's Encrypt.

Server location: Dallas, USA. Contact me below if you're getting slow results from Europe or Japan.

https://www.httpvshttps.com

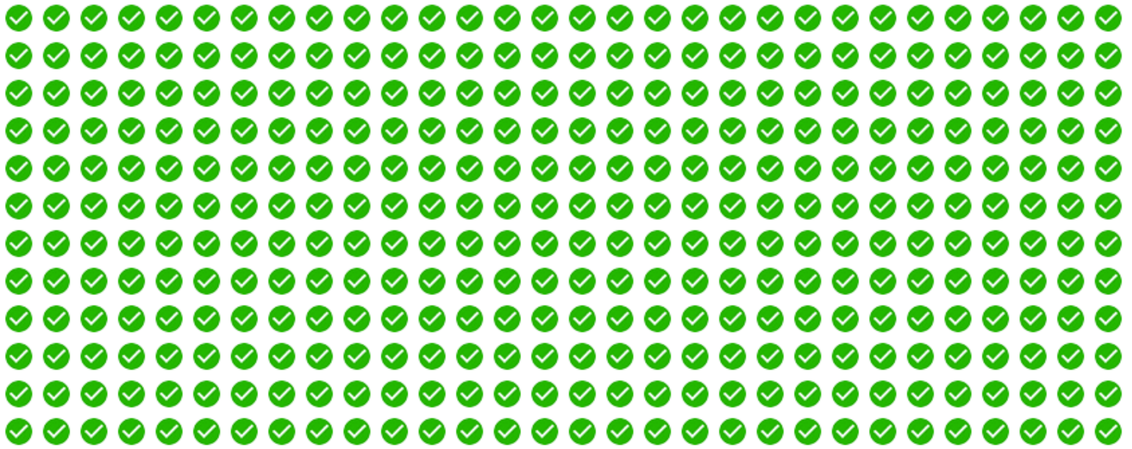
HTTP vs HTTPS Test

HTTP HTTPS

Encrypted Websites Protect Our Privacy and are Significantly Faster
Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

3.344 s

67% faster than HTTP



Only full, end-end encryption ensures complete privacy. Cloudflare and MaxCDN SSL encryption services compromise privacy by using interceptive middle proxy servers. HTTPS means "Secure HTTP". Plaintext HTTP/1.1 is compared against encrypted HTTP/2 HTTPS on a non-caching, nginx server with a direct, non-proxied connection.

Let's Encrypt

Free TLS Certificate provided by Let's Encrypt.

Server location: Dallas, USA. Contact me below if you're getting slow results from Europe or Japan.

Status Quo

SSLLabs

https://www.ssllabs.com/

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: camp.hsbp.org Submit

Do not show the results on the boards

Recently Seen	
torrentfreak.com	
fate.fr.nf	
www.gdrzine.com	Err
sociallyuncensored.com	Err
www.santander.com	A
prosecureone.propath.com	A
bitreactor.net	Err
prosesecureone.propath.com	F
www.googledrive.com	A
rates-globalmarkets.bnpparib ...	A

Recent Best	
psylab.cc	A+
syntra-staging.weopendata.co ...	A+
gamesplanet.com	A+
prosecureone.propath.com	A
www.santander.com	A
www.googledrive.com	A
animexico-online.com	A
prosecurethree.propath.com	A
go.microsoft.com	A
umfrage.klagemauer.tv	B

Recent Worst	
prosesecureone.propath.com	F
seagate.com	T
repanier.be	F
c90.itliteclient.ru	T
www.credit-pret-en-ligne.fr	F
dev1.newlist.com	T
4smart.cz	F
apps.facevaluetechnologies.c ...	F
itsupport247.net	F
klapperbox.marius-gawenda.ne ...	T

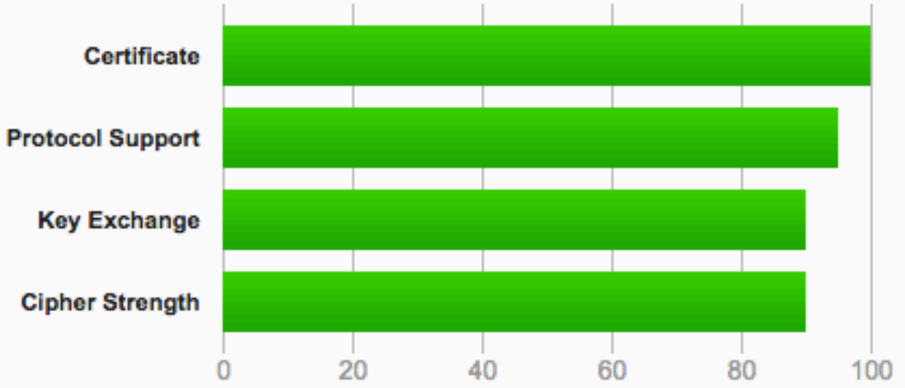
SSL Report v1.23.50

SSL Report: camp.hsbp.org (2a01:270:2016:0:0:0:0:1)

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Public Key Pinning (HPKP) deployed on this server. Yay!

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	zerobin.hsbp.org Fingerprint SHA1: 7b2218c948331044d3a0bd80b3124fd9671dca3b Pin SHA256: GDsPiknRjmuM06cdPPSNnQ1ViZEQIky2LJ0N0Rk0LTo=
Common names	zerobin.hsbp.org
Alternative names	apps.daydreamer.hu aproka.eu blog.aproka.eu camp.hsbp.org frab.hsbp.org hsbp.org hspbp.org media.aproka.eu nominatim.vsza.hu openhort.hsbp.org techblog.vsza.hu ticket.hsbp.org vsza.hu www.aproka.eu www.hsbp.org www.hspbp.org www.vsza.hu zerobin.hsbp.org
Valid from	Wed, 22 Jun 2016 11:14:00 UTC
Valid until	Tue, 20 Sep 2016 11:14:00 UTC (expires in 1 month and 13 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org/
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	2 (2978 bytes)
Chain issues	None

#2

Subject	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=
Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 4 years and 7 months)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted PIN

1	Sent by server	zerobin.hsbp.org PIN Fingerprint SHA1: 7b2218c948331044d3a0bd80b3124fd9671dca3b Pin SHA256: GDsPiknRjmuM06cdPPSNnQ1ViZEQIky2LJ0N0Rk0LTo= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	Let's Encrypt Authority X3 Fingerprint SHA1: e6a3b45b062d509b3382282d196efe97d5956ccb Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DST Root CA X3 Self-signed Fingerprint SHA1: dac9024f54d8f6df94935fb1732638ca6ad77c13 Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Transport Layer Security

TLS 1.3

TLS 1.2

TLS 1.1

TLS 1.0

~~*SSLv3*~~

~~*SSLv2*~~

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits FS	256

Handshake Simulation

Android 2.3.7 No SNI [2]	Server sent fatal alert: handshake_failure					
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS	
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
Android 6.0	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS	
Chrome 51 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS	
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
Firefox 46 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
Googlebot Feb 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS	
IE 6 / XP No FS [1] No SNI [2]	Server closed connection					
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
IE 8 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure					
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DH 4096	FS	

Edge 13 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 6u45 No SNI [2]	Server sent fatal alert: handshake_failure			
Java 7u25	Server sent fatal alert: handshake_failure			
Java 8u31	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 4096 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2e R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 6 / iOS 6.0.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes

Miscellaneous

Test date	Sat, 06 Aug 2016 18:40:01 UTC
Test duration	149.885 seconds
HTTP status code	200
HTTP server signature	Apache/2.4.10 (Debian)
Server hostname	faszkorbacs.hu

SSL Report v1.23.50

SSL Report: camp.hsbp.org

Assessed on: Sat, 06 Aug 2016 18:22:54 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	2a01:270:2016:0:0:0:0:1 faszkorbacs.hu Ready	Sat, 06 Aug 2016 18:18:00 UTC **Duration:** 146.658 sec	A+
2	88.151.101.208 vsza.hu Ready	Sat, 06 Aug 2016 18:20:26 UTC **Duration:** 147.445 sec	A+

SSL Report v1.23.50

SSL Report: outlook.com

Assessed on: Wed Oct 15 18:04:10 UTC 2014 | **HIDDEN** | Clear cache

Scan Another >>

	Server	Domain(s)	Test time	Grade
1	157.56.243.11 Ready	outlook.com	Wed Oct 15 17:53:13 UTC 2014 **Duration:** 45.631 sec	F
2	157.56.244.38 outlook.com Ready	www.outlook.com	Wed Oct 15 17:53:58 UTC 2014 **Duration:** 42.575 sec	F
3	132.245.6.134 Ready	www.outlook.com	Wed Oct 15 17:54:41 UTC 2014 **Duration:** 45.848 sec	F
4	157.56.242.123 Ready	outlook.com	Wed Oct 15 17:55:27 UTC 2014 **Duration:** 45.719 sec	F
5	157.56.237.102 outlook.com Ready	www.outlook.com	Wed Oct 15 17:56:13 UTC 2014 **Duration:** 54.714 sec	F
6	132.245.89.171 Ready	outlook.com	Wed Oct 15 17:57:07 UTC 2014 **Duration:** 52.702 sec	F
7	132.245.3.187 Ready	outlook.com	Wed Oct 15 17:58:00 UTC 2014 **Duration:** 45.697 sec	F
8	132.245.6.235 Ready	outlook.com	Wed Oct 15 17:58:46 UTC 2014 **Duration:** 46.554 sec	F
9	157.56.233.251 Ready	outlook.com	Wed Oct 15 17:59:32 UTC 2014 **Duration:** 45.700 sec	F
10	157.56.240.102 bl2prd0510.outlook.com Ready	www.outlook.com	Wed Oct 15 18:00:18 UTC 2014 **Duration:** 46.25 sec	F

SSL Report: outlook.com

Assessed on: Sun, 07 Aug 2016 13:19:01 UTC | **HIDDEN** | Clear cache

Scan Another >>

	Server	Test time	Grade
1	132.245.92.194 Ready	Sun, 07 Aug 2016 13:08:53 UTC **Duration:** 68.478 sec	B
2	132.245.17.34 Ready	Sun, 07 Aug 2016 13:10:01 UTC **Duration:** 75.988 sec	B
3	132.245.23.242 Ready	Sun, 07 Aug 2016 13:11:17 UTC **Duration:** 73.176 sec	B
4	132.245.13.210 Ready	Sun, 07 Aug 2016 13:12:30 UTC **Duration:** 75.701 sec	B
5	132.245.113.194 Ready	Sun, 07 Aug 2016 13:13:46 UTC **Duration:** 65.985 sec	B
6	157.56.237.242 Ready	Sun, 07 Aug 2016 13:14:52 UTC **Duration:** 53.388 sec	B
7	132.245.21.82 Ready	Sun, 07 Aug 2016 13:15:46 UTC **Duration:** 66.871 sec	B
8	132.245.81.130 Ready	Sun, 07 Aug 2016 13:16:52 UTC **Duration:** 53.247 sec	B
9	157.56.242.98 Ready	Sun, 07 Aug 2016 13:17:46 UTC **Duration:** 75.584 sec	B

SSL Report: openbsd.org (129.128.5.194)

Assessed on: Fri, 29 Apr 2016 15:49:34 UTC | **HIDDEN** | Clear cache

Scan Another »

Assessment failed: Unable to connect to the server

Known Problems

There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- **No secure protocols supported** - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- **no more data allowed for version 1 certificate** - the certificate is invalid; it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- **Failed to obtain certificate** and **Internal Error** - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- **NetScaler issues** - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- **Unexpected failure** - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers behind the same IP address. In such cases we can't provide accurate results, which is why we fail.

Common Error Messages

SSL Report: www.openbsd.org (129.128.5.194)

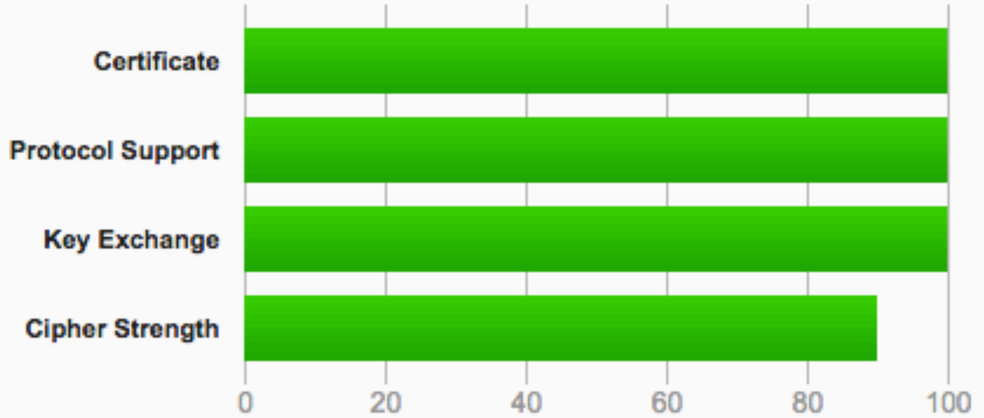
Assessed on: Sun, 07 Aug 2016 13:35:26 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

SSL Report: [redacted].gv.at (78.41.148.117)

Assessed on: Sun, 07 Aug 2016 13:40:46 UTC | **HIDDEN** | Clear cache

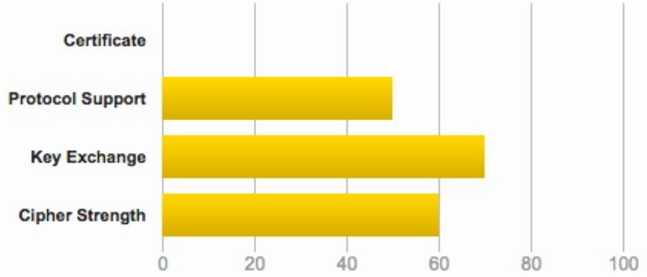
Scan Another »

Summary

Overall Rating

T

If trust issues are ignored: C



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

The server private key is not strong enough. Grade capped to B.

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	[redacted].gv.at Fingerprint SHA1: [redacted] Pin SHA256: [redacted]
Common names	[redacted]gv.at **MISMATCH**
Alternative names	-
Valid from	Mon, 26 Nov 2007 14:52:01 UTC
Valid until	Tue, 25 Nov 2008 14:52:01 UTC (expired 7 years and 8 months ago) **EXPIRED**
Key	RSA 1024 bits (Exponent 65537) **WEAK**
Weak key (Debian)	No
Issuer	[redacted].gv.at Self-signed
Signature algorithm	SHA1withRSA **WEAK**
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
Trusted	No **NOT TRUSTED** (Why?)

Additional Certificates (if supplied)

Certificates provided	1 (1042 bytes)
Chain issues	**Contains anchor**

Certification Paths

Path #1: Not trusted (path does not chain to a trusted anchor)

1	Sent by server Not in trust store	[redacted].gv.at Self-signed Fingerprint SHA1: fcc979e0dd8a12076014bba7f22927500354170f Pin SHA256: aN5tDiTgq7aloa7UW+UdfNTF3A+N1YAgu0mW1SgjfNo= RSA 1024 bits (e 65537) / SHA1withRSA Valid until: Tue, 25 Nov 2008 14:52:01 UTC **EXPIRED** **WEAK KEY** Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

Cipher Suites (sorted by strength as the server has no preference; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits FS **WEAK**	56
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS **WEAK**	112
TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256

HTTP Response Header

Security Headers

https://securityheaders.io

securityheaders.io

Home About

Scan your site now

camp.hsbp.org

Scan

Hide results Follow redirects

Grand Totals

A+	75,117
A	100,536
B	65,922
C	3,135
D	54,502
E	349,960
F	296,467
R	191,850
Total	1,137,489

Recent Scans

bpttest.andrick.ho...	A
www.eurobahnm.com	F
www.24option.com	F
www.jayharris.ca	A+
www.ieeess12.com	F
www.ieee.org.bd	F
ghyadk.com	F
groovycarrot.co.uk	E
www.lloydsbank.com	F

Hall of Fame

www.jayharris.ca	A+
www.facebook.com	A
paragonie.com	A
bpttest.andrick.ho...	A
www.tobymackenzie....	A+
www.ghcif.de	A
securityheaders.io	A+
pi.duuu.ch	A
shahab.tadkar.com	A

Hall of Shame

www.24option.com	F
www.lloydsbank.com	F
www.eurobahnm.com	F
calific.com	F
bernardi.be	F
example.com	F
ghyadk.com	F
www.anekdot.ru	F
www.ieeess12.com	F

http://camp.hsbp.org

Scan

Hide results Follow redirects

Security Report Summary

R

Redirect:	Click here to follow the redirect to https://camp.hsbp.org/.
Site:	http://camp.hsbp.org/ - (Scan again over https)
IP Address:	2a01:270:2016::1
Report Time:	07 Aug 2016 14:26:46 UTC
Report Short URL:	https://schd.io/1Hn
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-XSS-Protection ✖ X-Content-Type-Options

Raw Headers

HTTP/1.1	302 Found
Date	Sun, 07 Aug 2016 14:26:46 GMT
Server	Apache/2.4.10 (Debian)
Strict-Transport-Security	max-age=23328000; preload
Location	https://camp.hsbp.org/
Content-Length	285

securityheaders.io

Home About

Scan your site now

https://camp.hsbp.org

Scan

Hide results Follow redirects

Security Report Summary

A

Site:	https://camp.hsbp.org/2016/pp7e0/
IP Address:	2a01:270:2016::1
Report Time:	07 Aug 2016 14:19:48 UTC
Report Short URL:	https://schd.io/1Hm
Headers:	✔ X-Frame-Options ✔ Strict-Transport-Security ✔ Public-Key-Pins ✔ X-Content-Type-Options ✔ X-XSS-Protection ✘ Content-Security-Policy

Raw Headers

HTTP/1.1	200 OK
Date	Sun, 07 Aug 2016 14:19:48 GMT

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
```

Raw Headers

HTTP/1.1	200 OK
Date	Sun, 07 Aug 2016 14:37:22 GMT
Server	Apache/2.4.10 (Debian)
X-Frame-Options	DENY
Strict-Transport-Security	max-age=23328000; preload
Public-Key-Pins	pin-sha256="GDsPiknRjmuM06cdPPSNnQ1ViZEQIky2LJ0N0Rk0LTo="; pin-sha256="i4QA+Qa4W5c896qTMTsdD1G4IkjNt2cWIEGRmKnIaFo="; max-age=2592000
Last-Modified	Mon, 25 Jan 2016 09:41:30 GMT
ETag	"c01-52a255f9f8680"
Accept-Ranges	bytes
Content-Length	3073
X-Content-Type-Options	nosniff
X-XSS-Protection	1; mode=block
Content-Type	text/html; charset=UTF-8

Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
Public-Key-Pins	HTTP Public Key Pinning protects your site from MiTM attacks using rogue X.509 certificates. By whitelisting only the identities that the browser should trust, your users are protected in the event a certificate authority is compromised. Analyse this policy in more detail.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filters built into most browsers. The best configuration is "X-XSS-Protection: 1; mode=block".

```
# CSP
content-security-policy: default-src 'self'
'unsafe-inline' 'unsafe-eval' ; connect-src
'none' ; object-src 'none' ; frame-ancestors
'none' ; form-action 'none' ; upgrade-
insecure-requests; block-all-mixed-content;
reflected-xss block; referrer no-referrer;
```

CSP Generator

https://report-uri.io/home/generate

Here is your Policy!

Content-Security-Policy: default-src 'self' ; script-src 'self' 'unsafe-inline' 'unsafe-eval' ;

Import a policy

Enter your domain

Content-Security-Policy

Import

Build your CSP

1) Default Source
2) Script Source
3) Style Source
4) Image Source
5) Font Source
6) Connect Source
7) Media Source
8) Object Source

Default Source View Info

- [ ] None
- [ ] All
- [x] Self
- [ ] Data
- [ ] Unsafe Inline
- [ ] Unsafe Eval

Space separated list of hosts.

```
# HSTS
Strict-Transport-Security: max-age=23328000; preload

# HPKP
Public-Key-Pins "pin-sha256=\"YOUR_HASH=\"; pin-sha256=
\"YOUR_BACKUP_HASH=\"; max-age=7776000; report-uri=\"https://
YOUR.REPORT.URL\""
```

hpkp-gen

https://github.com//hannob/hpkp

```
curl -I https://camp.hsbp.org/
```

[-4|-6]

```
$ curl -I https://camp.hsbp.org/2016/pp7e0/

HTTP/1.1 200 OK
Date: Sun, 07 Aug 2016 15:06:35 GMT
Server: Apache/2.4.10 (Debian)
X-Frame-Options: DENY
Strict-Transport-Security: max-age=23328000; preload
Public-Key-Pins: pin-sha256="GDsPiknRjmuM06cdPPSNnQ1ViZEQIky2LJ0N0Rk0LTo=";
pin-sha256="i4QA+Qa4W5c896qTMTsdD1G4IkjNt2cWlEGRmKnIaFo="; max-age=2592000
Last-Modified: Mon, 25 Jan 2016 09:41:30 GMT
ETag: "c01-52a255f9f8680"
Accept-Ranges: bytes
Content-Length: 3073
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Type: text/html; charset=UTF-8
```

```
wget -S -O/dev/null https://camp.hsbp.org/2016/pp7e0/
```

[-4|-6]

```
$ wget -S -O/dev/null https://camp.hsbp.org/2016/pp7e0/

 --2016-08-07 17:08:34--  https://camp.hsbp.org/2016/pp7e0/
Resolving camp.hsbp.org (camp.hsbp.org)... 88.151.101.208, 2a01:270:2016::1
Connecting to camp.hsbp.org (camp.hsbp.org)|88.151.101.208|:443... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Date: Sun, 07 Aug 2016 15:08:34 GMT
  Server: Apache/2.4.10 (Debian)
  X-Frame-Options: DENY
  Strict-Transport-Security: max-age=23328000; preload
  Public-Key-Pins: pin-sha256="GDsPiknRjmuM06cdPPSNnQ1ViZEQIky2LJ0N0Rk0LTo="; pin-sha256="i4QA
+Qa4W5c896qTMTsdD1G4IkjNt2cWlEGRmKnIaFo="; max-age=2592000
  Last-Modified: Mon, 25 Jan 2016 09:41:30 GMT
  ETag: "c01-52a255f9f8680"
  Accept-Ranges: bytes
  Content-Length: 3073
  X-Content-Type-Options: nosniff
  X-XSS-Protection: 1; mode=block
  Keep-Alive: timeout=15, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=UTF-8
Length: 3073 (3.0K) [text/html]
Saving to: ‘/dev/null’

/dev/null                     100%[=============================================================>]   3.00K  --.-KB/s
in 0.002s

2016-08-07 17:08:34 (1.88 MB/s) - ‘/dev/null’ saved [3073/3073]
```

High Tech Bridge

https://www.htbridge.com/ssl/

Geneva: +41 (22) 723 2424 | San Francisco: +1 (415) 659 1861 | sales@htbridge.com

Summary of camp.hsbp.org SSL/TLS Security Test

FINAL GRADE

A+

COMPLIANT WITH

PCI DSS

HOST

SERVER IP : PORT
88.151.101.208:443

DATE OF TEST
August 7th 2016, 17:18 CEST

OPTIONS

Download PDF

Refresh results

The server configuration seems to be good, but is not entirely compliant with NIST guidelines — Information

The server prefers cipher suites supporting Perfect-Forward-Secrecy — Good configuration

The server provides HTTP Strict Transport Security — Good configuration

Browser

Qualys SSLLabs

https://www.ssllabs.com/ssltest/viewMyClient.html

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2683.0 Safari/537.36

Protocol Features

Protocols

TLS 1.2	Yes*
TLS 1.1	Yes*
TLS 1.0	Yes*
SSL 3	Yes*
SSL 2	No

Cipher Suites (in order of preference)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) Forward Secrecy	256

Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA512/RSA, SHA512/ECDSA, SHA384/RSA, SHA384/ECDSA, SHA256/RSA, SHA256/ECDSA, SHA1/RSA, SHA1/ECDSA
Elliptic curves	x25519, secp256r1, secp384r1
Next Protocol Negotiation	Yes
Application Layer Protocol Negotiation	Yes h2 spdy/3.1 http/1.1
SSL 2 handshake compatibility	No

about:config

chrome://net-internals/

Webserver Configuration

https://bettercrypto.org/

httpd 2.4

mod_ssl
mod_header

mod_h2

HTTP/2

```
/etc/apache2/httpd.conf
  NameVirtualHost *:443
  # Linux / Windows
  # AcceptFilter http data
  AcceptFilter https data

  # FreeBSD
  # AcceptFilter http httpready
  # AcceptFilter https dataready

/etc/apache2/ports.conf
  Listen 443
```

```
<VirtualHost *:443>
  ServerName www.yoursite.com
  DocumentRoot /var/www/site
  SSLEngine on
  Protocols h2 http/1.1

  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
  SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

  SSLProtocol All -SSLv2 -SSLv3
  SSLCipherSuite 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH
+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!
LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-
SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA'
```

```
    SSLHonorCipherOrder On
    SSLCompression off

    # TLS_DHE_
    SSLDHParametersFile /etc/ssl/dh4096.pem

</VirtualHost>
```

Security Header

```
# For HTTPS only

  # HSTS
  Header always set strict-transport-security "max-
age=15768000"

  # HPKP
  Header always set Public-Key-Pins "pin-sha256=\"YOUR_HASH=
\"; pin-sha256=\"YOUR_BACKUP_HASH=\"; max-age=7776000;
report-uri=\"https://YOUR.REPORT.URL\""
```

```
# For HTTPS and HTTP

    # CSP
    Header always set Content-Security-Policy "default-src
https: data: 'unsafe-inline' 'unsafe-eval'" always; upgrade-
insecure-requests"


    Header setifempty  X-Frame-Options DENY
    Header always set  X-Content-Type-Options "nosniff"
    Header always set  X-XSS-Protection "1; mode=block"
```

HTTP → HTTPS

301

```
# mod_rewrite syntax
<VirtualHost camp.hsbp.org:80>
  RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>

# mod_alias syntax
<VirtualHost camp.hsbp.org:80>
  Redirect permanent / https://%{SERVER_NAME}/
</VirtualHost>
```

ServerTokens Prod[uctOnly]

Server: Apache

```
# For HTTPS and HTTP

    add_header  X-Clacks-Overhead "GNU Terry Pratchett";
```

nginx 1.10 stable / 1.11 mainline

```
--with-http_ssl_module
```

--with-http_v2_module

HTTP/2

```
server {
  # Tux
  # listen [2a01:270:2016::1]:443 ssl http2 deferred;

  # FreeBSD
  listen [2a01:270:2016::1]:443 ssl http2 accept_filter=dataready;

  server_name camp.hsbp.org;

  ssl_certificate_key /etc/nginx/certificates/camp.hsbp.org.key;
  ssl_certificate /etc/nginx/certificates/camp.hsbp.org_chained.pem;

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

  ssl_ciphers EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA
+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!
MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!IDEA:!ECDSA:kEDH:CAMELLIA256-SHA:AES256-
SHA:CAMELLIA128-SHA:AES128-SHA;
```

```
  ssl_prefer_server_ciphers on;

  # TLS_DHE_
  ssl_dhparam /etc/nginx/dhparam/dh4096.pem;

  # TLS compression is automatically turned OFF in
  # nginx 1.1.6+/1.0.9+ (if OpenSSL 1.0.0+ used)
  # nginx 1.3.2+/1.2.2+ (if older OpenSSL).
  # spdy_headers_comp 0; # SPDY Header Compression off

  ssl_ecdh_curve          secp384r1;

  # Speed improvements to first byte for smaller files.
  ssl_buffer_size 4k;
}
```

Security Header

```
# For HTTPS only

  # HSTS
  add_header strict-transport-security "max-age=31104000;
includeSubDomains; preload" always;

  # HPKP
  add_header Public-Key-Pins 'max-age=2592000; pin-
sha256="rFfvG6DIxgDwHy4qfCVEnDKoFJ2XG3szxQHeeaRv9g8=";pin-
sha256="gXaQqXAAR+AjznLZGRlBAYOabhv/II5Bc+CL9e7Kpmg=";pin-
sha256="5noWBr53rhdxeVxcQagM3hqYu+Cw0m34VjrBo1Cu5Ag="' always;
```

```
# For HTTPS and HTTP

    # CSP
    add_header Content-Security-Policy "default-src https: data:
'unsafe-inline' 'unsafe-eval' upgrade-insecure-requests" always;

    add_header  X-Frame-Options DENY always;
    add_header  X-Content-Type-Options "nosniff" always;
    add_header  X-XSS-Protection "1; mode=block" always;
```

HTTP → HTTPS

301

```
server {
    listen [2a01:270:2016::1]:80;
    server_name camp.hsbp.org;
    server_name www.camp.hsbp.org;
    server_name [2a01:270:2016::1];

    return 301 https://$server_name$request_uri;
}
```

```
server_tokens off;
```

Server: nginx

```
# For HTTPS and HTTP

    add_header  X-Clacks-Overhead "GNU Terry Pratchett";
```

Think about Security Headers

Web Application Firewalls

mod_security

Apache, nginx

naxsi

nginx


On Fire


A

Questions?

Thanks!

@leyrer
@MacLemon

$ testing

$ openssl

Ja, wirklich

```
$ openssl version

OpenSSL 1.0.2g  1 Mar 2016
```

```
$ openssl version
```

```
OpenSSL 0.9.8zg 14 July 2015
```

```
openssl ciphers \
'ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH'
```

```
DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-
SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-
SHA:DES-CBC3-SHA:DHE-RSA-SEED-SHA:DHE-DSS-
SEED-SHA:SEED-SHA:DHE-RSA-AES128-SHA:DHE-DSS-
AES128-SHA:AES128-SHA:RC4-SHA
```

Bettercrypto cipherstring B

```
EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH
+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SS
Lv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!
DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-
SHA:CAMELLIA128-SHA:AES128-SHA
```

openssl 0.9.8

AES256-SHA:AES128-SHA

openssl 1.0.2g

DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA256-SHA:DHE-RSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA:ECDHE-RSA-AES128-SHA:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA

openssl 1.1.0-pre5

ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-AES256-CCM:DHE-RSA-AES256-CCM8:DHE-RSA-AES256-CCM:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:DHE-RSA-CAMELLIA256-SHA256:DHE-DSS-CAMELLIA256-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:AECDH-AES256-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CHACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:DHE-PSK-AES256-CCM8:DHE-PSK-AES256-CCM:AES256-GCM-SHA384:AES256-CCM8:AES256-CCM:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:PSK-AES256-CCM8:PSK-AES256-CCM:AES256-SHA256:CAMELLIA256-SHA256:ECDHE-PSK-AES256-CBC-SHA384:ECDHE-PSK-AES256-CBC-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-SHA:DHE-PSK-AES256-CBC-SHA:ECDHE-PSK-CAMELLIA256-SHA384:RSA-PSK-CAMELLIA256-SHA384:DHE-PSK-CAMELLIA256-SHA384:AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:PSK-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM8:ECDHE-ECDSA-AES128-CCM:DHE-RSA-AES128-CCM8:DHE-RSA-AES128-CCM:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-DSS-CAMELLIA128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:AECDH-AES128-SHA:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-CCM8:DHE-PSK-AES128-CCM:AES128-GCM-SHA256:AES128-CCM8:AES128-CCM:PSK-AES128-GCM-SHA256:PSK-AES128-CCM8:PSK-AES128-CCM:AES128-SHA256:CAMELLIA128-SHA256:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES128-CBC-SHA:ECDHE-PSK-CAMELLIA128-SHA256:RSA-PSK-CAMELLIA128-SHA256:DHE-PSK-CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA:PSK-CAMELLIA128-SHA256:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:DHE-RSA-DES-CBC3-SHA:DHE-DSS-DES-CBC3-SHA:AECDH-DES-CBC3-SHA:ECDHE-PSK-3DES-EDE-CBC-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:SRP-3DES-EDE-CBC-SHA:RSA-PSK-3DES-EDE-CBC-SHA:DHE-PSK-3DES-EDE-CBC-SHA:DES-CBC3-SHA:PSK-3DES-EDE-CBC-SHA

$ cipherscan

https://github.com/jvehent/cipherscan

```
$ ./cipherscan example.com
```

prio	ciphersuite	protocols	pfs	curves
1	ECDHE-RSA-CHACHA20-POLY1305	TLSv1.2	ECDH,P-256,256bits	prime256v1
2	ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH,P-256,256bits	prime256v1
3	ECDHE-RSA-AES128-SHA	TLSv1.1,TLSv1.2	ECDH,P-256,256bits	prime256v1
4	ECDHE-RSA-RC4-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	ECDH,P-256,256bits	prime256v1
5	AES128-GCM-SHA256	TLSv1.2	None	None
6	AES128-SHA256	TLSv1.2	None	None
7	AES128-SHA	TLSv1.1,TLSv1.2	None	None
8	RC4-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	None	None
9	RC4-MD5	SSLv3,TLSv1,TLSv1.1,TLSv1.2	None	None
10	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH,P-256,256bits	prime256v1
11	ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH,P-256,256bits	prime256v1
12	ECDHE-RSA-AES256-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	ECDH,P-256,256bits	prime256v1
13	AES256-GCM-SHA384	TLSv1.2	None	None
14	AES256-SHA256	TLSv1.2	None	None
15	AES256-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	None	None
16	ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH,P-256,256bits	prime256v1
17	ECDHE-RSA-DES-CBC3-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	ECDH,P-256,256bits	prime256v1
18	DES-CBC3-SHA	SSLv3,TLSv1,TLSv1.1,TLSv1.2	None	None

Certificate: trusted, 2048 bit, sha1WithRSAEncryption signature
TLS ticket lifetime hint: 100800
OCSP stapling: not supported
Cipher ordering: server

```
$ nmap
```

```
nmap --script \
  ssl-cert,ssl-enum-ciphers \
  -p 443 example.com
```

nmap

```
Starting Nmap 7.10 ( https://nmap.org ) at 2016-03-27 18:53 CEST
Nmap scan report for maclemon.at (86.59.70.21)
Host is up (0.084s latency).
Other addresses for maclemon.at (not scanned): 2001:470:6f:4ca:9a26:fb93:ba1c:e29a
rDNS record for 86.59.70.21: pandora.maclemon.at
PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=www.maclemon.at/countryName=AT
| Issuer: commonName=StartCom Class 1 Primary Intermediate Server CA/organizationName=StartCom Ltd./countryName=IL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-05-11T02:19:06
| Not valid after:  2016-05-11T10:30:02
| MD5:   327b 2139 db86 8ba7 3b54 2f8f 1d8f 73c9
|_SHA-1: ceec 5e21 879d 16de 4064 cd34 e525 802d 22ce 4c40
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 4096) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 4096) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 4096) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp384r1) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 4096) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 4096) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 4096) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 4096) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
```

```
$ telnet
```

LOL NOPE

```
$ openssl s_client
```

```
openssl s_client -connect \
  webmail.example.com:443 \
  -servername webmail.example.com
```

OCSP stapling

```
openssl s_client -connect \
  example.com:443 -tls1 \
  -tlsextdebug -status \
  < /dev/null | grep OCSP
```

OCSP stapling

```
depth=1 C = US, O = DigiCert Inc, OU = www.digicert.com, CN =
DigiCert High Assurance CA-3
verify error:num=20:unable to get local issuer certificate
verify return:0
DONE
OCSP response:
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
```

$ testssl.sh

https://testssl.sh/

```
 Start 2016-08-07 19:03:14    -->> 88.151.101.208:443 (camp.hsbp.org) <<--

 further IP addresses:   2a01:270:2016::1
 rDNS (88.151.101.208):  vsza.hu.
 Service detected:       HTTP


 Testing protocols (via sockets except TLS 1.2, SPDY+HTTP2)

 SSLv2                   not offered (OK)
 SSLv3                   not offered (OK)
 TLS 1                   offered
 TLS 1.1                 offered
 TLS 1.2                 offered (OK)
 Version tolerance       downgraded to TLSv1.2 (OK)
 SPDY/NPN                not offered
 HTTP2/ALPN              not offered

 Testing ~standard cipher lists

 Null Ciphers                 not offered (OK)
 Anonymous NULL Ciphers       not offered (OK)
 Anonymous DH Ciphers         not offered (OK)
 40 Bit encryption            Local problem: No 40 Bit encryption  configured in /usr/local/maclemon/bin/openssl
 56 Bit encryption            Local problem: No 56 Bit encryption  configured in /usr/local/maclemon/bin/openssl
 Export Ciphers (general)     Local problem: No Export Ciphers (general) configured in /usr/local/maclemon/bin/openssl
 Low (<=64 Bit)               Local problem: No Low (<=64 Bit) configured in /usr/local/maclemon/bin/openssl
 DES Ciphers                  Local problem: No DES Ciphers  configured in /usr/local/maclemon/bin/openssl
 Medium grade encryption      Local problem: No Medium grade encryption  configured in /usr/local/maclemon/bin/openssl
 Triple DES Ciphers           not offered (OK)
 High grade encryption        offered (OK)


 Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption as well as 3DES and RC4 here

 PFS is offered (OK)          DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-
RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA
 Elliptic curves offered:     prime256v1
```

SSLyze

https://github.com/iSECPartners/sslyze