



Awwwwwww

Advanced Wibbly-Wobbly World Wide Webserver Wizardry

Awwwwwww

Advanced Wibbly-Wobbly World Wide Webserver Wizardry

#lww17



@leyrer



@MacLemon

Awwwwwww

Advanced Wibbly-Wobbly World Wide Webserver Wizardry

Status Quo

NGINX

1.13 mainline



httpd 2.4

LibreSSL

OpenSSL

HTTP/2

Transportverschlüsselung

TLS 1.3

TLS 1.2

TLS 1.1

TLS 1.0

~~SSLv3~~

~~SSLv2~~

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > linuxwochen.at

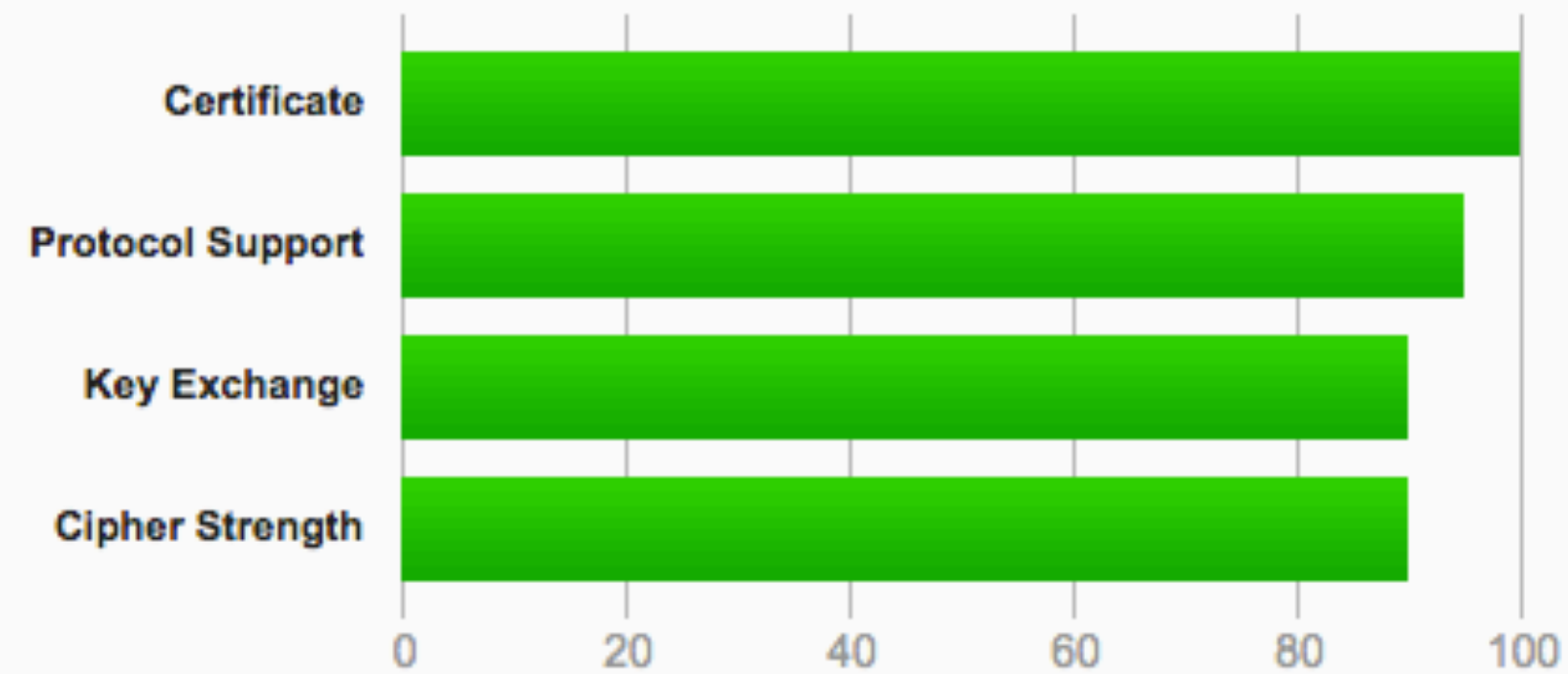
SSL Report: linuxwochen.at (195.230.168.88)

Assessed on: Fri, 05 May 2017 09:15:22 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](#).

This server is vulnerable to the DROWN attack. Grade set to F. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This site works only in browsers with SNI support.

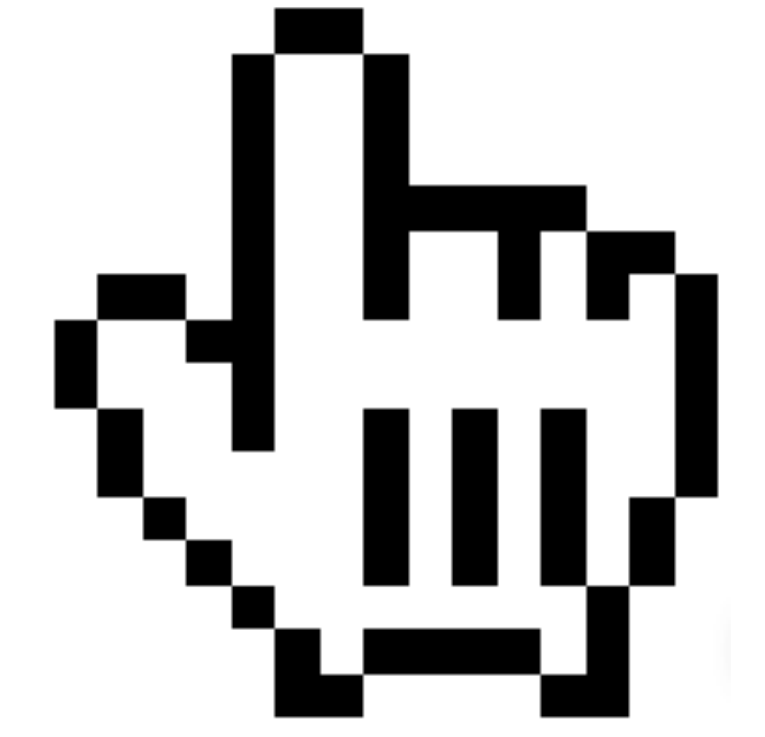


Modulare Config

/ Status Quo

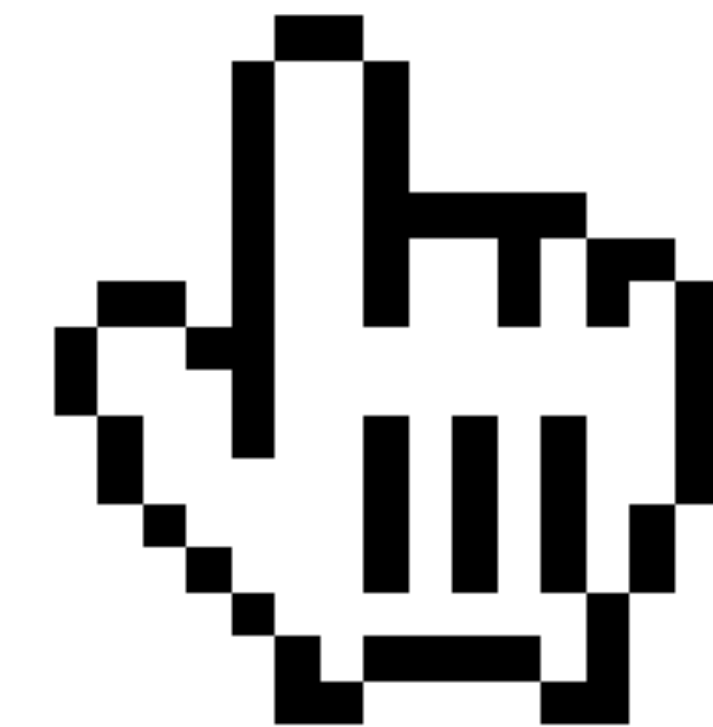
Sichere Transportverschlüsselung

Ist TLS schnell?



Ist TLS schnell?

Ja!



Ist *Dein* TLS schnell?

```
seq 10 |
```

```
xargs -I@ -n1
```

```
curl -kso /dev/null -w "tcp:%{time_connect},  
ssldone:%{time_appconnect}\n"
```

```
https://linuxwochen.at/
```

tcp:0.055579, sslDone:0.115298
tcp:0.015132, sslDone:0.079048
tcp:0.015066, sslDone:0.078038
tcp:0.015576, sslDone:0.073277
tcp:0.015558, sslDone:0.085817
tcp:0.014850, sslDone:0.072564
tcp:0.014518, sslDone:0.071202
tcp:0.016096, sslDone:0.073199
tcp:0.017248, sslDone:0.074969
tcp:0.016756, sslDone:0.071830

TLS Session Tickets

NGINX


```
common/tls_tickets.conf
```

```
keepalive_timeout      70;  
ssl_session_tickets    on;  
ssl_session_cache      shared:SSL:10m;  
ssl_session_timeout    10m;  
ssl_buffer_size        2k;
```



```
$ sudo a2enmod socache_shmcb
```

```
/etc/apache2/mods-enabled/ssl.conf
```

```
...
```

```
SSLSessionCache shmcb:$
```

```
  {APACHE_RUN_DIR}/ssl_scache(512000)
```

```
SSLSessionCacheTimeout 300
```

Reconnect Test

```
openssl s_client -connect linuxwochen.at:443  
-reconnect 2>&1 </dev/null  
| egrep -i "(new|reused|conn)"
```

CONNECTED(0000003)

New, TLSv1/SSLv3,

Cipher is ECDHE-RSA-AES256-GCM-SHA384

drop connection and then reconnect

CONNECTED(0000003)

Reused, TLSv1/SSLv3,

Cipher is ECDHE-RSA-AES256-GCM-SHA384

drop connection and then reconnect

Lifetime?


```
openssl s_client -connect linuxwochen.at:443  
-tlsextdebug -status  
< /dev/null 2>/dev/null  
| grep lifetime
```

TLS session ticket lifetime hint: 300 (seconds)

Lifetime Test

```
openssl s_client -connect linuxwochen.at:443  
-sess_out /tmp/ssl_s </dev/null 2>/dev/null  
| egrep -i "(new|reused|conn)" ;
```

```
sleep 298 ;
```

```
openssl s_client -connect linuxwochen.at:443  
-sess_in /tmp/ssl_s </dev/null 2>/dev/null  
| egrep -i "(new|reused|conn)"
```

CONNECTED(00000003)

New, TLSv1/SSLv3,

Cipher is ECDHE-RSA-AES256-GCM-SHA384

CONNECTED(00000003)

Reused, TLSv1/SSLv3,

Cipher is ECDHE-RSA-AES256-GCM-SHA384

Revocation

OCSP Stapling

```
common/letsencrypt_ocsp.conf
```

```
ssl_stapling on;
```

```
ssl_stapling_verify on;
```

```
ssl_trusted_certificate \
    trusted_CAs.pem;
```



```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
SSLUseStapling on
```

```
# Optional
```

```
SSLStaplingResponderTimeout 5
```

```
SSLStaplingReturnResponderErrors off
```

SSLStaplingCache

shmcb:/var/run/ocsp(128000)

```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
<IfModule mod_ssl.c>
```

```
    # Specify cached response location (must be  
    outside <VirtualHost>)
```

```
    SSLStaplingCache shmcb: /var/run/ocsp(128000)
```

```
<VirtualHost *:443>
```

```
    ServerAdmin admin@example.com
```

```
    ServerName example.com
```

```
    DocumentRoot /var/www
```

```
# Enable SSL & OCSP Stapling
```

```
SSLEngine on
```

```
SSLUseStapling on
```

```
# Configure Stapling Options
```

```
SSLStaplingResponderTimeout 5
```

```
SSLStaplingReturnResponderErrors off
```

OCSP Test

```
openssl s_client  
-connect linuxwochen.at:443  
-tlsextdebug -status  
< /dev/null 2>/dev/null  
  
| egrep "(OCSP|Cert Status)"
```

OCSP response: no response sent

OCSP response:

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Cert Status: good

/ TLS Session Tickets

Content Compression

common/compression.conf

```
gzip on;  
gzip_http_version 1.0;  
gzip_vary on;  
gzip_comp_level 1;  
gzip_min_length 50;  
gzip_buffers 16 8k;  
gzip_proxied any;
```

```
common/compression.conf
```

```
gzip_types text/plain text/css
```

```
application/json application/x-javascript
```

```
text/xml application/xml
```

```
application/xml+rss text/javascript
```

```
application/javascript text/x-jsi
```

```
image/svg+xml;
```

```
common/compression.conf
```

```
# --with-http_gzip_static_module  
gzip_static on;
```

```
apachectl -t -D DUMP_MODULES | grep deflate
```

```
sudo a2enmod deflate
```

```
sudo a2enmod headers
```

```
sudo a2enmod rewrite
```

```
sudo a2enmod filter
```

```
/etc/apache2/mods-enabled/deflate.conf
```

```
DeflateCompressionLevel 1
```

```
DeflateMemLevel 8
```

```
DeflateWindowSize 15
```



```
/etc/apache2/mods-enabled/deflate.conf
```

```
<IfModule mod_deflate.c>  
  <IfModule mod_filter.c>
```

```
# these are known to be safe with MSIE 6
```

```
AddOutputFilterByType DEFLATE text/html text/plain text/xml
```

```
# everything else may cause problems with MSIE 6
```

```
AddOutputFilterByType DEFLATE text/css
```

```
AddOutputFilterByType DEFLATE application/x-javascript  
                        application/javascript application/ecmascript
```

```
AddOutputFilterByType DEFLATE application/rss+xml
```

```
AddOutputFilterByType DEFLATE application/xml
```

```
</IfModule>
```

```
</IfModule>
```

AddOutputFilterByType	DEFLATE	application/atom+xml
AddOutputFilterByType	DEFLATE	application/atomcat+xml
AddOutputFilterByType	DEFLATE	application/javascript
AddOutputFilterByType	DEFLATE	application/json
AddOutputFilterByType	DEFLATE	application/octet-stream
AddOutputFilterByType	DEFLATE	application/x-javascript
AddOutputFilterByType	DEFLATE	application/xhtml+xml
AddOutputFilterByType	DEFLATE	application/xml
AddOutputFilterByType	DEFLATE	text/css
AddOutputFilterByType	DEFLATE	text/html
AddOutputFilterByType	DEFLATE	text/javascript
AddOutputFilterByType	DEFLATE	text/plain
AddOutputFilterByType	DEFLATE	text/xml
AddOutputFilterByType	DEFLATE	text/xsl

```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
# AddEncoding allows you to have certain browsers  
uncompress information on the fly.
```

```
AddEncoding gzip .gz
```

```
RewriteEngine on
```

```
#Serve gzip compressed CSS files if they exist and  
the client accepts gzip.
```

```
RewriteCond %{HTTP:Accept-encoding} gzip
```

```
RewriteCond %{REQUEST_FILENAME}\.gz -s
```

```
RewriteRule ^(.*)\.css $1\.css\.gz [QSA]
```

```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
# Serve gzip compressed JS files if they exist and  
the client accepts gzip.
```

```
    RewriteCond %{HTTP:Accept-encoding} gzip
```

```
    RewriteCond %{REQUEST_FILENAME}\.gz -s
```

```
    RewriteRule ^(.*)\.js $1\.js\.gz [QSA]
```

```
# Serve correct content types, and prevent  
mod_deflate double gzip.
```

```
    RewriteRule \.css\.gz$ - [T=text/css,E=no-gzip:1]
```

```
    RewriteRule \.js\.gz$ - [T=text/javascript,E=no-gzip:1]
```

/ Content Compression

Client Caching

ETag
Expires
Cache-Control

```
common/caching.conf
```

```
location ~* \.(?:jpg|jpeg|gif|png|ico|  
gz|svg|svgz|mp4|mp3|ogg|ogv|webm|woff|  
eot)$ {  
    expires 7d;  
    add_header Cache-Control "public";  
}
```



```
common/caching.conf
```

```
# Web Feeds
```

```
location ~* \.(?:rss|atom)$ {  
    expires 1h;  
    add_header Cache-Control "public";  
}
```

```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
<Directory /var/www>  
    FileETag MTime Size  
</Directory>
```

FileETag

INode

MTime

Size

All

None

```
sudo a2enmod expires
```

```
sudo a2enmod headers
```

```
/etc/apache2/sites-enabled/example.com-ssl.conf
```

```
<VirtualHost *:443>
```

```
    ServerAdmin admin@example.com
```

```
    ServerName example.com
```

```
    DocumentRoot /var/www
```

```
<Location />
```

```
    ExpiresActive on
```

```
    ExpiresDefault "modification plus 2 weeks 3 days 1 hour"
```

```
    ExpiresByType image/png "modification plus 7"
```

```
    Header merge Cache-Control public
```

```
</Location>
```

Cache Tests

```
curl -sI https://linuxwochen.at/css/  
lightbox.css  
| egrep -i "(etag|cache|expires)"
```

ETag: "f22-5177952f7b380"


```
curl -sI https://linuxwochen.at/css/  
lightbox.css  
--header 'If-None-Match:  
"f22-5177952f7b380"'
```

HTTP/1.1 304 Not Modified

ETag: "f22-5177952f7b380"

Date: Fri, 05 May 2017 14:44:07 GMT

Server: Apache/2.4.10 (Debian) PHP/

5.6.27-0+deb8u1 mod_python/3.3.1 Python/2.7.9

OpenSSL/1.0.1t

etag: "590252f9-444"

expires: Sun, 28 May 2017 00:38:27 GMT

cache-control: max-age=2592000

cache-control: public

/ Client Caching

Security Headers

Simpel

HTTPS und HTTP

```
# For HTTPS and HTTP
```

```
add_header X-Frame-Options DENY always;
```

```
add_header X-Content-Type-Options "nosniff" always;
```

```
add_header X-XSS-Protection "1; mode=block" always;
```

```
# For HTTPS and HTTP
```

```
Header always set X-Frame-Options DENY
```

```
Header always set X-Content-Type-Options "nosniff"
```

```
Header always set X-XSS-Protection "1; mode=block"
```


HSTS

HTTPS

```
# HSTS
```

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

```
# HSTS
```

```
Header always set
```

```
strict-transport-security
```

```
"max-age=15768000"
```

Content-Security-Policy

HTTPS und HTTP

```
add_header Content-Security-Policy
"default-src none; upgrade-insecure-
requests; block-all-mixed-content;
reflected-xss block;referrer no-
referrer;" always;
```

```
add_header Content-Security-Policy "default-src  
'self' 'unsafe-inline' 'unsafe-eval'; script-src  
'self' 'unsafe-inline' 'unsafe-eval'; style-src  
'self' 'unsafe-inline'; img  
-src 'self'; font-src 'self'; connect-src 'self';  
media-src 'self' blob:; object-src 'none'; child-  
src 'self' blob:; frame-src 'self' blob:; worker-  
src 'none'; frame-ancestors 'non  
e'; form-action 'self'; upgrade-insecure-  
requests; block-all-mixed-content; reflected-xss  
block;referrer no-referrer;" always;
```

Header always set Content-Security-Policy "default-src 'self' https://www.goodreads.com; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://www.goodreads.com/; object-src 'none'; style-src 'self' 'unsafe-inline'; media-src 'self'; child-src 'self' https://www.youtube.com; connect-src 'self' https://www.youtube.com/"

CSP Generator


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

Generate your CSP

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

info@report-uri.io

Log In Register



Home Tools CSP Builder

Import a policy

https://privacyweek.at/ Content-Security-Policy Import

Build your CSP

- 1) Default Source
- 2) Script Source
- 3) Style Source
- 4) Image Source**
- 5) Font Source

Image Source [View Info](#)

- None
- All
- Self
- Data

Testen...

Testen... Testen...

Mehr Testen...

und noch mehr testen...

Navigation bar with tabs: Insp..., Co..., Deb..., Style ..., Perfor..., Me..., Net... and a filter input field labeled "Filter output".

- ⚠ Content Security Policy: Directive 'frame-src' has been deprecated. Please use directive 'child-src' (unknown) instead.
- ⚠ Content Security Policy: Couldn't process unknown directive 'worker-src' (unknown)
- ⚠ Content Security Policy: Not supporting directive 'reflected-xss'. Directive and values will be ignored. (unknown)
- ⚠ Content Security Policy: Referrer Directive 'no-referrer' has been deprecated. Please use the Referrer-Policy header instead. (unknown)
- ✖ Content Security Policy: The page's settings blocked the loading of a resource at <https://releases.flowplayer.org/swf/flowplayer-3.2.1.swf> ("object-src 'none'"). (unknown)

/ Security Headers

The Future...

TLS 1.3

OCSP Expect-Staple

OCSP Must-Staple

DNS CAA RR

Expect-CT Extension for HTTP

/ The Future...

Fragen?

#lww17



@leyrer



@MacLemon

Danke