



Services absichern

Common Practice

*Aleksander Paravac
watz@nerd2nerd.org*

#cn4n



1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen



- 1 Motivation
- 2 Services
 - Apache HTTP und HTTPS
 - Postfix
 - Dovecot
 - Ejabberd
 - Unrealircd
- 3 Anmerkungen



Motivation

Es gibt solche Webseiten ...

QUALYS SSL LABS Home Projects Groups View Contact

Report Name: [SSL - \[Redacted\]](#) > [SSL Report](#)

SSL Report: [Redacted] [Scan Another](#)

Downloaded on: Mon, 27 Apr 2016 13:43:17 UTC (GMT+02:00)

Summary

Overall Rating: **C**

Conditions: [Green bar]

Protocol Support: [Green bar]

Key Exchange: [Green bar]

Cipher Strength: [Yellow bar]

View our [documentation](#) for more information, configuration guides, and tools. Please browse our [documented bugs](#).

This server uses TLS 1.2 with modern protocols. Grade support is C.

This server does not support a cipher or protocol with the [strongest](#) strength.

Authentication

[View Key and Certificate](#) [Redacted]

securityheaders.io Home About

Scan your site now

[Redacted] [Enter URL](#)

Security Report Summary

Grade: **F**

URL: [Redacted]

IP Address: [Redacted]

Report Time: [Redacted]

Weaknesses: [HTTP Strict Transport Security](#) [Content Security Policy](#) [X-Frame-Options](#) [X-Content-Type-Options](#)

Raw Headers

HTTP/1.1	200 OK
Date	Mon, 27 Apr 2016 13:43:16 GMT
Server	Apache/2.4.18
Content-Length	21038
Content-Type	text/html
Set-Cookie	[Redacted]





1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen



1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen



Extra Header für mehr Sicherheit

- **X-Frame-Options**
Bietet Schutz gegen Clickjacking Attacken
- **X-Content-Type-Options**
Verhindert MIME-Type sniffing
- **X-Xss-Protection**
Aktiviert den in modernen Browsern eingebauten XSS Schutz
- **X-Content-Type-Options**
Regelt woher Objekte (CSS, Bilder, Skripte, etc.) nachgeladen werden dürfen



Apache 2.4

```
Header always set X-Frame-Options "SAMEORIGIN"  
Header always set X-Content-Type-Options "nosniff"  
Header always set X-Xss-Protection "1; mode=block"
```

X-Frame-Options

- DENY
- SAMEORIGIN
- ALLOW-FROM
https://example.com

X-Xss-Protection

- 0 # Aus
- 1; mode=block



Obacht!





Content-Security-Policy

```
Header always set Content-Security-Policy \  
"default-src 'self' https://*.nerd2nerd.org; \  
script-src 'self' https://*.nerd2nerd.org '\'  
unsafe-inline' 'unsafe-eval; \  
img-src 'self' https://*.nerd2nerd.org; \  
frame-src 'self' https://*.nerd2nerd.org; \  
font-src 'self' \  
style-src 'self'\  
object-src 'none'"
```

Debug: Content-Security-Policy-Report-Only



Content-Security-Policy



Abbildung: Debug der Optionen¹ für Content-Security-Policy.

¹Liste der Optionen bei Scott Helme





HTTPS

Beast



Logjam



Poodle





HTTP-Header, die zweite. SSL only!

- **Strict-Transport-Security**
User Agent dazu zwingen TLS zu benutzen
- **Public-Key-Pins**
Versucht SSL MiTM Attacken zu verhindern



Strict-Transport-Security

```
Header always set Strict-Transport-Security \  
"max-age=31536000; includeSubDomains; preload"
```



Obacht!





Public-Key-Pins

```
Header always set Public-Key-Pins '\
pin-sha256="X3pGTS0uJeEVw989IJ/...="; \
pin-sha256="MHJYVThihUrJcxW6wcq...="; \
pin-sha256="isi41AizREkLvvt0IR...="; \
max-age=10';
```

Debug: Public-Key-Pins-Report-Only

Fingerprint über:

```
openssl req -pubkey < yourcert.pem |
openssl pkey -pubin -outform der |
openssl dgst -sha256 -binary | base64
```





Apache 2.4

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCompression off

SSLDHParametersFile /path/to/dh.pem

SSLCipherSuite "ECDH+AESGCM:DH+AESGCM:ECDH+AES256:\
DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:\
RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS"
```





1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen





Postfix

```
# Enable TLS/SSL
smtpd_use_tls = yes
[...]
```



```
# Select strong ciphers
smtpd_tls_loglevel = 0
smtpd_tls_dh1024_param_file =
    /etc/postfix/ssl/dh_2048.pem
smtpd_tls_dh512_param_file =
    /etc/postfix/ssl/dh_512.pem
smtpd_tls_eecdh_grade = strong
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3
smtpd_tls_mandatory_ciphers = high
tls_ssl_options = NO_COMPRESSION
```



Postfix Cipher List

```
tls_preempt_cipherlist = yes
tls_high_cipherlist = 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-AES
```



Postfix und DANE

```
# Enable DANE
smtp_dns_support_level = dnssec
smtp_tls_security_level = dane
smtp_tls_loglevel = 1
```



Postfix und SASL Auth

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
```

Weitere DNS Geschichten

- DKIM (DomainKey Identified Mail)
- SPF (Sender Policy Framework)



1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen





Dovecot SSL

```
ssl = yes
ssl_protocols = !SSLv3 !SSLv2
ssl_dh_parameters_length = 2048
ssl_options = no_compression

ssl_cert = </etc/ssl/private/yourcert.pem
ssl_key = </etc/ssl/private/yourkey.key

ssl_cipher_list = EDH+CAMELLIA:EDH+aRSA:\
EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:\
EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:\
+AES256:+CAMELLIA128:+AES128:!SSLv2:\
!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:\
!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-SHA:\
CAMELLIA128-SHA:AES128-AES
```



1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen





ejabberd.yml - Client to Server

```
listen:  
- port: 5222  
  module: ejabberd_c2s  
  ciphers: "[...]"  
  starttls: true  
  starttls_required: true  
  certfile: "/etc/ssl/ejabberd/jabber.pem"  
  dhfile: "/etc/ssl/ejabberd/jabber.pem.dh"  
  tls_compression: false  
  protocol_options:  
    - "no_sslv3"  
    - "no_tlsv1"  
    - "cipher_server_preference"
```





ejabberd.yml - Server to Server

```
-  
  port: 5269  
  module: ejabberd_s2s_in  
  s2s_use_starttls: required_trusted  
  s2s_certfile: "/etc/ssl/ejabberd/jabber.pem"  
  s2s_dhfile: "/etc/ssl/ejabberd/jabber.pem.dh"  
  s2s_protocol_options:  
  - "no_sslv3"  
  - "no_tlsv1"  
  - "cipher_server_preference"  
  s2s_ciphers: "[...]"
```





Übersicht

1 Motivation

2 Services

Apache HTTP und HTTPS

Postfix

Dovecot

Ejabberd

Unrealircd

3 Anmerkungen





Unrealircd

```
set {
  ssl {
    certificate yourcert.crt;
    key yourkey.key;
    trusted-ca-file ca_chain.pem;
    renegotiate-bytes "64m";
    renegotiate-time "10h";
    server-cipher-list "[...]";
  };
};
```





Übersicht

- 1 Motivation
- 2 Services
 - Apache HTTP und HTTPS
 - Postfix
 - Dovecot
 - Ejabberd
 - Unrealircd
- 3 Anmerkungen





Updates - Updates und Updates

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Forthcoming OpenSSL releases

=====

The OpenSSL project team would like to announce the forthcoming release of OpenSSL versions 1.0.2h, 1.0.1t.

These releases will be made available [on 3rd May 2016](#) between approximately 1200-1500 UTC. They will fix several security defects with maximum severity "high".

[Abbildung: OpenSSL Update¹](#).

¹Matthew Green auf [Twitter](#)





Empfohlene Cipher Liste

```
SSLCipherSuite "EDH+CAMELLIA:EDH+aRSA:\nEECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:\n+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:\n!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:\n!IDEA:!ECDSA:kEDH:CAMELLIA128-SHA:AES128-SHA"
```





Cipher - Cipher - Cipher

Diff

```
> TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
> TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
> TLS_RSA_WITH_3DES_EDE_CBC_SHA
> TLS_RSA_WITH_AES_128_CBC_SHA256
> TLS_RSA_WITH_AES_128_GCM_SHA256
> TLS_RSA_WITH_AES_256_CBC_SHA
> TLS_RSA_WITH_AES_256_CBC_SHA256
> TLS_RSA_WITH_AES_256_GCM_SHA384
< TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
< TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
< TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
```





Danke an

- <https://bettercrypto.org/>
- <https://www.ssllabs.com/>
- <https://securityheaders.io/>
- Scott Helme