Apache Grundinstallation und Absicherung mit SSL und mod_php

> Diese Anleitung wurde für Debian Jessie geschrieben.

In diesem Artikel geht es darum Apache mit PHP (mod_php) zu installieren und grundlegend sicher zu konfigurieren.

Folgendes soll erreicht werden (Stand 11.12.2015):

- Keine Ausgabe von Versionsinformationen bei Apache und PHP
- Verwendung sicherer Ciphers und Hashingalgorithmen bei SSL
- Versteckte Dateien sollen nicht abrufbar sein (z.B. .git- oder .svn-Verzeichnisse)
- DocumentRoots sicher machen

Nach Änderungen an den Konfigurationsdateien die Apache-Syntax testen und neu laden:

```
# apache2ctl configtest
Syntax OK
# systemctl restart apache2.service
```

Installation von apache2.4 mit PHP und SSL

```
aptitude install apache2 libapache2-mod-php5 php5
```

Apache 2.4 absichern

Ausgabe von Versionsinformationen bei Apache deaktivieren

/etc/apache2/conf-available/security.conf

```
ServerTokens Prod
ServerSignature Off
```

ggf. zusätzliche Header mitsenden (mod_headers aktivieren: „a2enmod headers“)

/etc/apache2/conf-available/security.conf

```
# prevent MSIE from interpreting files as something else than declared by HTTP headers
Header set X-Content-Type-Options: "nosniff"
# disable loading pages from this site as frames
Header set X-Frame-Options: "sameorigin"
```

Zugriff auf Verzeichnisse von Versionskontrollsystemen wie Git und SVN unterbinden. Aktivieren mit „a2enconf cvs-deny“

/etc/apache2/conf-available/cvs-deny.conf

```
RedirectMatch 403 (?i)\.git
RedirectMatch 403 (?i)\.svn
```

ggf. Zugriff auf alle versteckten Verzeichnisse unterbinden (kann auch Probleme machen). Aktivieren mit „a2enconf hidden-deny“

/etc/apache2/conf-available/hidden-deny.conf

```
RedirectMatch 404 (?i)/\..+
```

SSL soll möglichst sicher konfiguriert (soweit die alten SSL-Libs bei Debian es erlauben) werden. Wie man SSL mit modernen Ciphers sicher konfiguriert steht in diesem Artikel.

Ggf. mod_security installieren, ein Filter und IDS gegen verschiedene Angriffe auf den Webserver (XSS, SQL injection):

```
# aptitude install libapache2-mod-security2
# cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

ein sicherer Apache default-Vhost (auch als Vorlage für weitere Vhosts verwendbar)

/etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
    ServerName www.FQDN
    ServerAlias FQDN
    ServerAdmin webmaster@FQDN
    DocumentRoot /var/www/FQDN

    LogLevel info
    ErrorLog ${APACHE_LOG_DIR}/FQDN-error.log
    CustomLog ${APACHE_LOG_DIR}/FQDN-access.log combined
</VirtualHost>

<VirtualHost _default_:443>
    ServerName www.FQDN
    ServerAlias FQDN
    ServerAdmin webmaster@FQDN
    DocumentRoot /var/www/FQDN
```

```
    LogLevel info ssl:warn
    ErrorLog ${APACHE_LOG_DIR}/FQDN-error.log
    CustomLog ${APACHE_LOG_DIR}/FQDN-access.log combined

    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/FQDN.pem    # contains the domain certificate and
intermediate certificates
    SSLCertificateKeyFile /etc/apache2/ssl/FQDN.key
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

PHP absichern

Ausgabe von Versionsinformationen bei PHP deaktivieren

/etc/php5/apache2/php.ini

```
expose_php=Off
```

bei Bedarf können weitere Sicherungsmaßnahmen getroffen werden

/etc/php5/apache2/php.ini

```
# ggf. Dateiuploads deaktivieren
file_uploads=Off

# Ausführung von entferntem Code unterbinden
allow_url_fopen=Off
allow_url_include=Off

# Zugriff auf das Dateisystem einschränken
open_basedir="/var/www/html/"
```

Revision #2
Created 2021-05-05 07:22:20 UTC by magenbrot
Updated 2021-05-05 07:25:56 UTC by magenbrot