

M183 Applikationssicherheit Implementieren

Tutorial zum Lab Self Signed Certificate for Apache Webserver

Version 1	19.12.2017	Jürg Nietlispach
-----------	------------	------------------

Contents

Idee	3
Herangehensweise Installation und Konfiguration.....	3

Idee

In diesem Lab soll ein self signed certificate erstellt werden und der Apache Webserver so konfiguriert werden, dass der http-Traffic verschlüsselt wird.

Herangehensweise Installation und Konfiguration

1. Apache Webserver downloaden (XAMPP)
2. Zertifikat erstellen
3. Server Konfigurieren

Als erstes soll der Apache Webserver lokal installiert werden. Auf der Download-Seite der Apachefriends wird man fündig: <https://www.apachefriends.org/de/download.html>

 **XAMPP für Windows 5.6.32, 7.0.26 & 7.1.12**

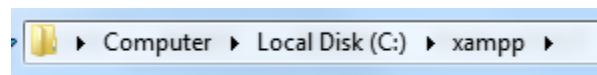
Version		Prüfsumme			Größe
5.6.32 / PHP 5.6.32	Was ist enthalten?	md5	sha1	Herunterladen (32 bit)	109 Mb
7.0.26 / PHP 7.0.26	Was ist enthalten?	md5	sha1	Herunterladen (32 bit)	120 Mb
7.1.12 / PHP 7.1.12	Was ist enthalten?	md5	sha1	Herunterladen (32 bit)	120 Mb

[Voraussetzungen](#) [Erweiterungen](#) [Weitere Downloads](#) »










































Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#).

Es kann das Package für die aktuellste PHP Version installiert werden (die PHP-Version spielt für die vorliegende Aufgabe keine Rolle).

Die Installation kann nun vorgenommen werden – xampp wird dann im Hauptverzeichnis installiert:



Innerhalb des apache-Ordners

Name	Date modified
 anonymous	19.12.2017 23:54
 apache	19.12.2017 23:54
 cgi-bin	19.12.2017 23:56
 contrib	19.12.2017 23:54
 FileZillaFTP	19.12.2017 23:56
 htdocs	19.12.2017 23:54
 img	19.12.2017 23:54
 install	19.12.2017 23:56
 licenses	19.12.2017 23:54
 locale	19.12.2017 23:54
 mailoutput	19.12.2017 23:54
 mailtodisk	19.12.2017 23:54
 MercuryMail	19.12.2017 23:56
 mysql	19.12.2017 23:55
 perl	19.12.2017 23:55
 php	19.12.2017 23:56
 phpMyAdmin	19.12.2017 23:56
 sendmail	19.12.2017 23:56
 src	19.12.2017 23:54
 tmp	19.12.2017 23:54
 tomcat	19.12.2017 23:55
 webalizer	19.12.2017 23:56
 webdav	19.12.2017 23:54
 apache_start.bat	07.06.2013 13:15
 apache_stop.bat	07.06.2013 13:15
 catalina_service.bat	30.03.2013 13:29
 catalina_start.bat	07.06.2013 13:15
 catalina_stop.bat	25.06.2013 15:36
 ctlscrip.bat	19.12.2017 23:54
 filezilla_setup.bat	30.03.2013 13:29
 filezilla_start.bat	07.06.2013 13:15
 filezilla_stop.bat	07.06.2013 13:15
 mercury_start.bat	07.06.2013 13:15
 mercury_stop.bat	07.06.2013 13:15
 mysql_start.bat	07.06.2013 13:15
 mysql_stop.bat	07.06.2013 13:15
 passwords.txt	13.03.2017 12:04
 properties.ini	19.12.2017 23:56
 readme_de.txt	14.12.2017 03:35
 readme_en.txt	14.12.2017 03:35
 RELEASENOTES	14.12.2017 03:35

Findet sich dann ein Batch-File, welches ein Zertifikat generiert:

Name	Date modifi
bin	19.12.2017 2
conf	19.12.2017 2
error	19.12.2017 2
icons	19.12.2017 2
include	19.12.2017 2
lib	19.12.2017 2
logs	19.12.2017 2
manual	19.12.2017 2
modules	19.12.2017 2
scripts	19.12.2017 2
ABOUT_APACHE.txt	16.04.2015 0
apache_installservice.bat	30.03.2013 1
apache_uninstallservice.bat	30.03.2013 1
CHANGES.txt	16.10.2017 1
INSTALL.txt	17.05.2016 2
LICENSE.txt	05.11.2017 1
makecert.bat	14.12.2017 0
NOTICE.txt	05.11.2017 1
OPENSSL-NEWS.txt	10.12.2017 1
OPENSSL-README.txt	10.12.2017 1
README.txt	23.01.2014 1

Schaut man sich das Batch File genauer an, sieht man, dass ein x509 Zertifikat generiert wird

```
@echo offset OPENSSL_CONF=./conf/openssl.cnfif not exist .\conf\ssl.crt mkdir .\conf\ssl.crtif not exist .\conf\ssl.key mkdir .\conf\ssl.keybin\openssl req -new -out server.csrbin\openssl rsa -in privkey.pem -out server.keybin\openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 365set OPENSSL_CONF=.del .rnde1 privkey.pemde1 server.csrmove /y server.crt .\conf\ssl.crtmove /y server.key .\conf\ssl.keyecho. echo -----echo Das Zertifikat wurde erstellt.echo The certificate was provided.echo.pause
```

Weitere Informationen zu diesem Zertifikatsstandard gibt es hier: <https://en.wikipedia.org/wiki/X.509>

Nun kann man das makecert- Batch-File ausführen. Als erstes muss man dann für den Private Key das Passwort eingeben:

```
C:\Windows\System32\cmd.exe
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
```

Und für die Verifizierung noch einmal

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Nun müssen verschiedene Informationen angegeben werden.

Z.B der Ländercode, innerhalb welchem das Zertifikat laufen soll: CH

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CH
```

State, z.B. Zug

```
Country Name (2 letter code) [AU]:CH
State or Province Name (full name) [Some-State]:Zug
```

Locality: z.B. Zug und Company: Gibz

```
Locality Name (eg, city) []:Zug
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gibz
```

Unit: Informatik

Und Server-Name z.B. testsystem.dev, der Domainname, unter welchem das Zertifikat dann aktiv werden soll:

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gibz
Organizational Unit Name (eg, section) []:Informatik
Common Name (e.g. server FQDN or YOUR name) []:testsystem.dev
```

Da wir lokal arbeiten müssen wir noch einen Virtuellen Host kreieren und eintragen. Dieser Host kann nun auch für das Zertifikat benutzt werden. Z.B

Email kann übersprungen werden.

Dann ein Passwort angeben

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

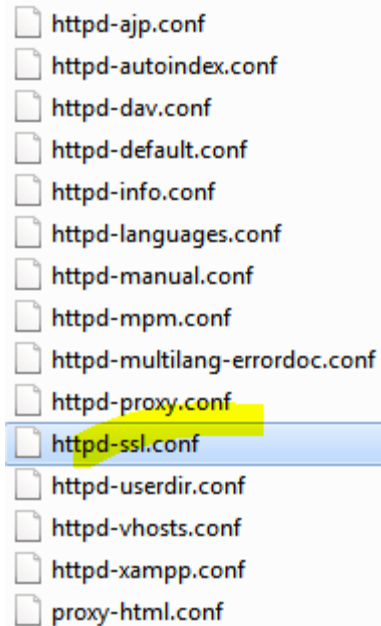
Dann am Schluss wieder das Passwort den Private Key (privkey.pem) eingeben – das Zertifikat wurde erstellt:

```
Enter pass phrase for privkey.pem:
writing RSA key
Signature ok
subject=/C=CH/ST=Zug/L=Zug/O=Gibz/OU=Informatik/CN=testsystem.dev
Getting Private key
    1 file(s) moved.
    1 file(s) moved.

-----
Das Zertifikat wurde erstellt.
The certificate was provided.

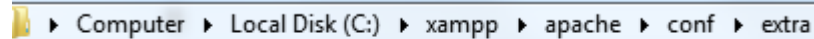
Press any key to continue . . .
```

Das Zertifikat wurde erstellt, nun muss Apache noch richtig konfiguriert werden. Hierzu muss im Dokument



- httpd-ajp.conf
- httpd-autoindex.conf
- httpd-dav.conf
- httpd-default.conf
- httpd-info.conf
- httpd-languages.conf
- httpd-manual.conf
- httpd-mpm.conf
- httpd-multilang-errordoc.conf
- httpd-proxy.conf
- httpd-ssl.conf**
- httpd-userdir.conf
- httpd-vhosts.conf
- httpd-xampp.conf
- proxy-html.conf

Welches unter



Computer > Local Disk (C:) > xampp > apache > conf > extra

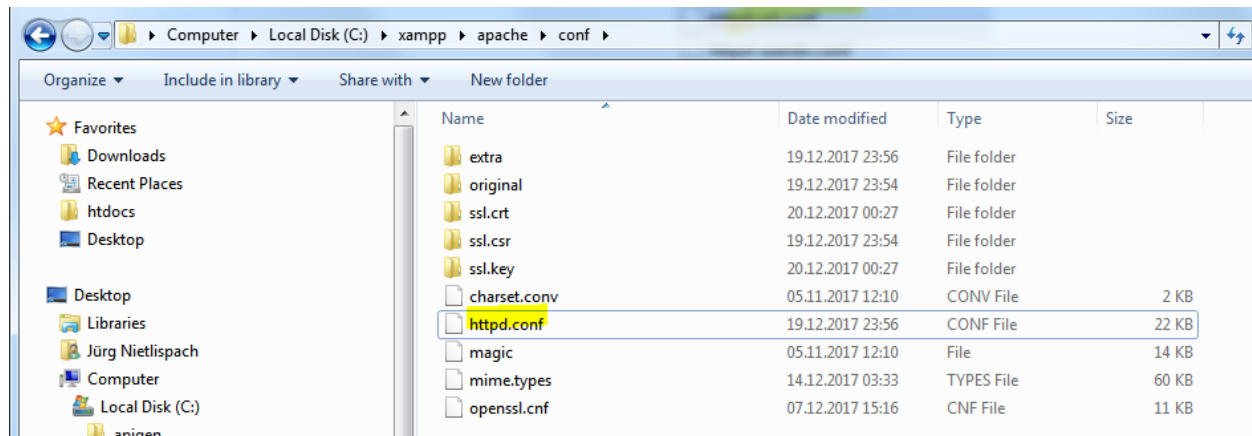
Zu finden ist, noch im Server Name folgender Eintrag angepasst werden:

```
<VirtualHost _default_:443>

#   General setup for the virtual host
DocumentRoot "C:/xampp/htdocs"
ServerName testsystem.dev:443
ServerAdmin admin@example.com
ErrorLog "C:/xampp/apache/logs/error.log"
TransferLog "C:/xampp/apache/logs/access.log"

#   SSL Engine Switch:
```

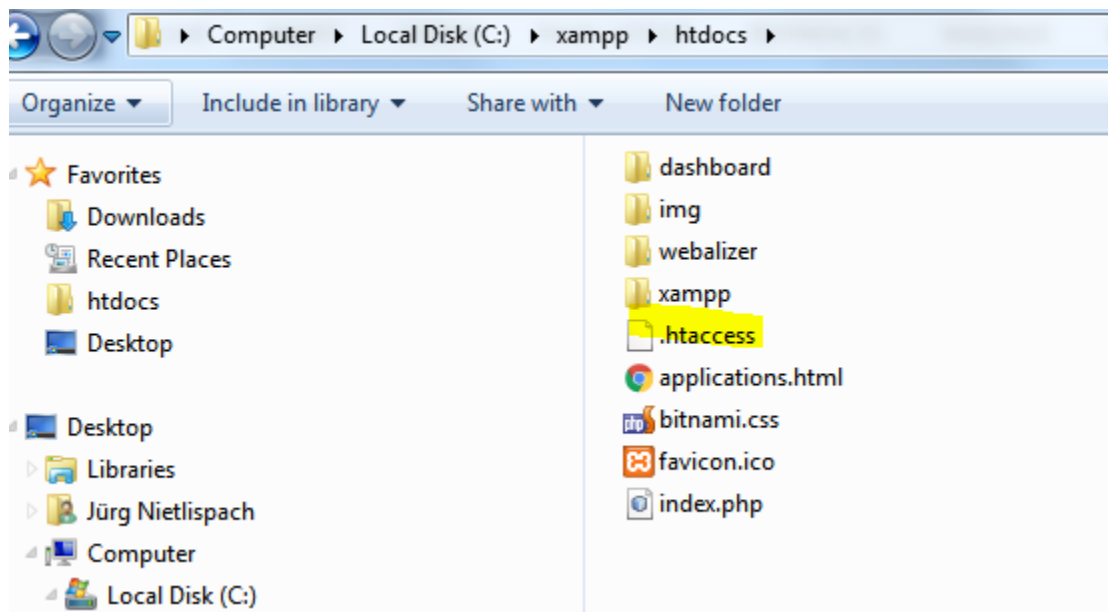
Nun müssen wir die Rewrite Engine starten, damit jede http-Anfrage auf https-Umgeleitet wird. Hierzu müssen wir folgendes File anpassen:



Es ist wichtig, dass das Rewrite Module enabled ist – also ohne #-Kommentarzeichen startet.

```
#LoadModule reqtimeout_module modules/mod_reqtimeout.so
LoadModule rewrite_module modules/mod_rewrite.so
#LoadModule sed module modules/mod_sed.so
```

Als nächstes kann im Webroot-Verzeichnis des Servers ein .htaccess-Dokument erstellt werden:



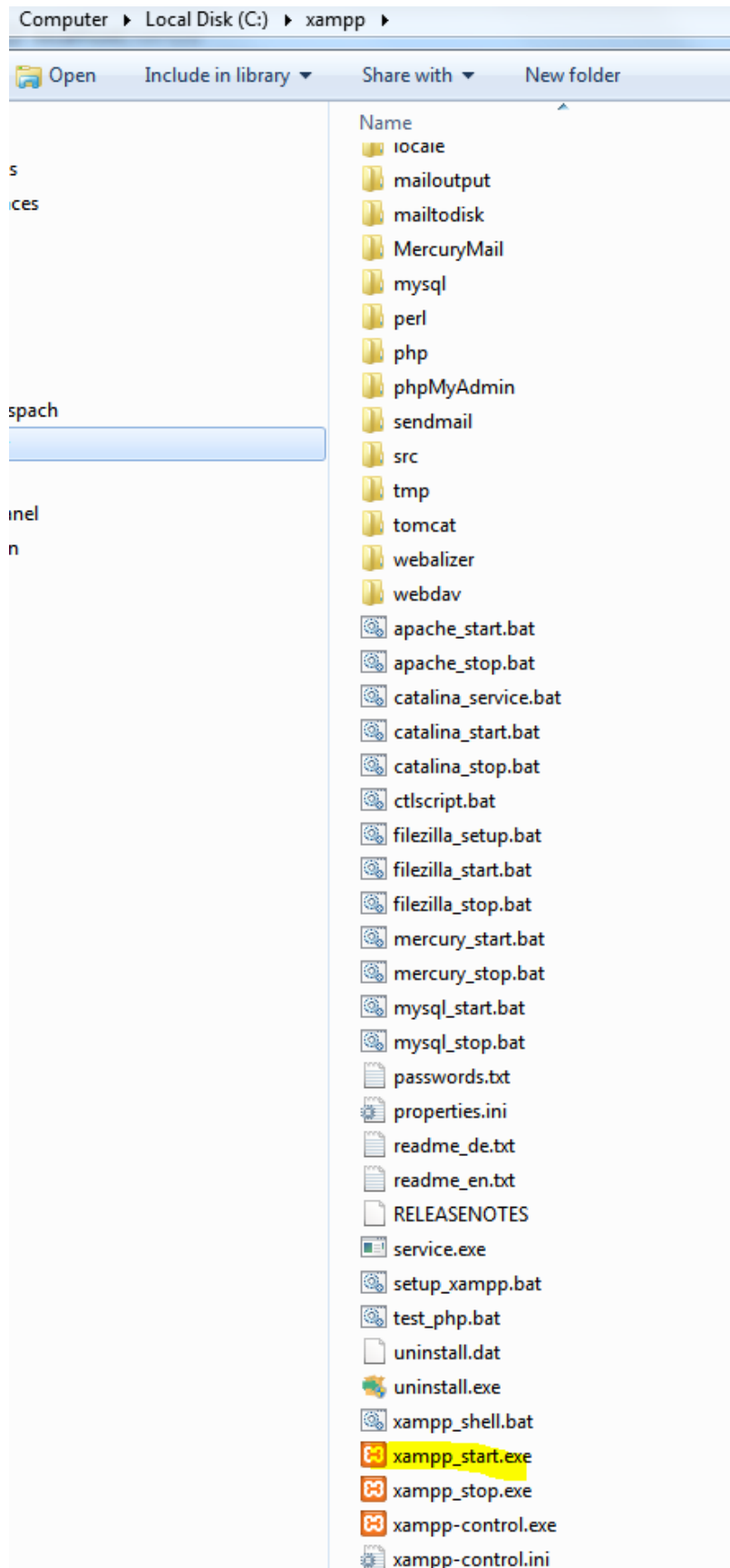
Folgender Inhalt muss angegeben werden:

```
<IfModule mod_rewrite.c>

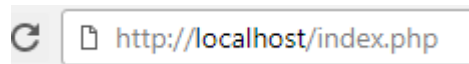
    RewriteEngine On
    RewriteCond %{SERVER_PORT} 80
    RewriteRule ^(.*) https://%{SERVER_NAME}/$1 [R,L]

</IfModule>
```

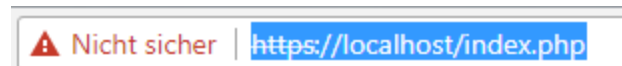
Nun kann der Webserver aufgestartet werden:



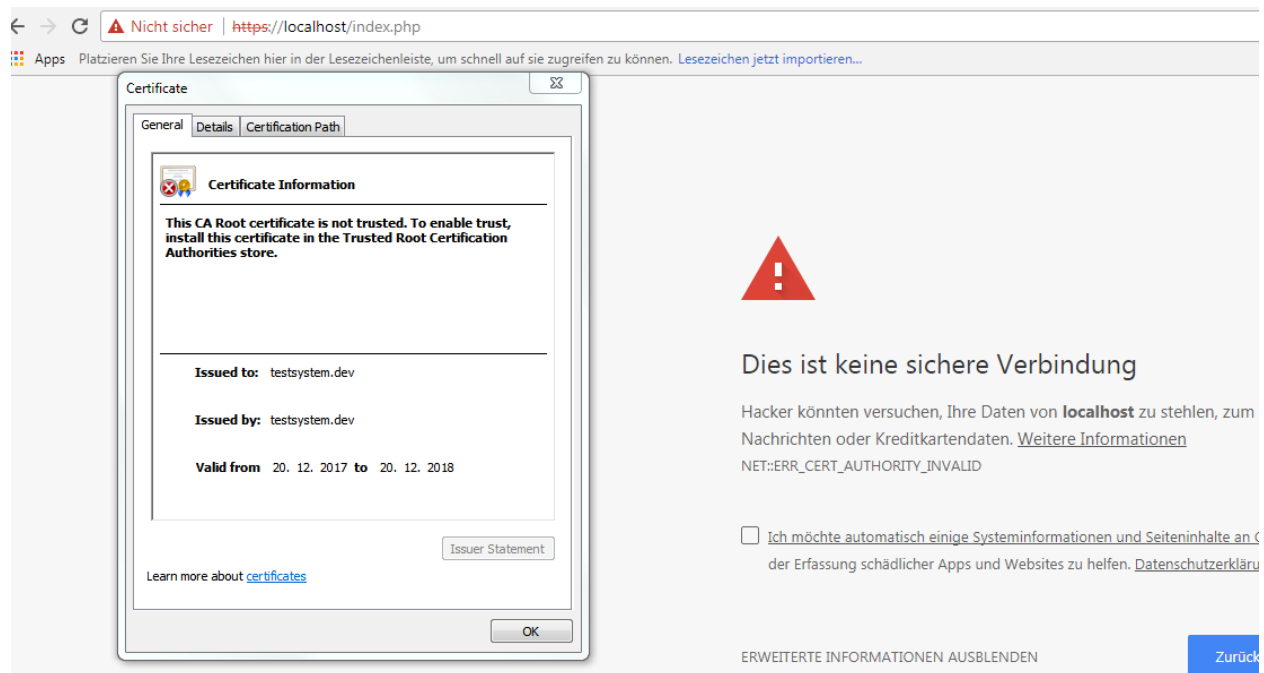
Die Weiterleitung http -> https funktioniert aber bereits:



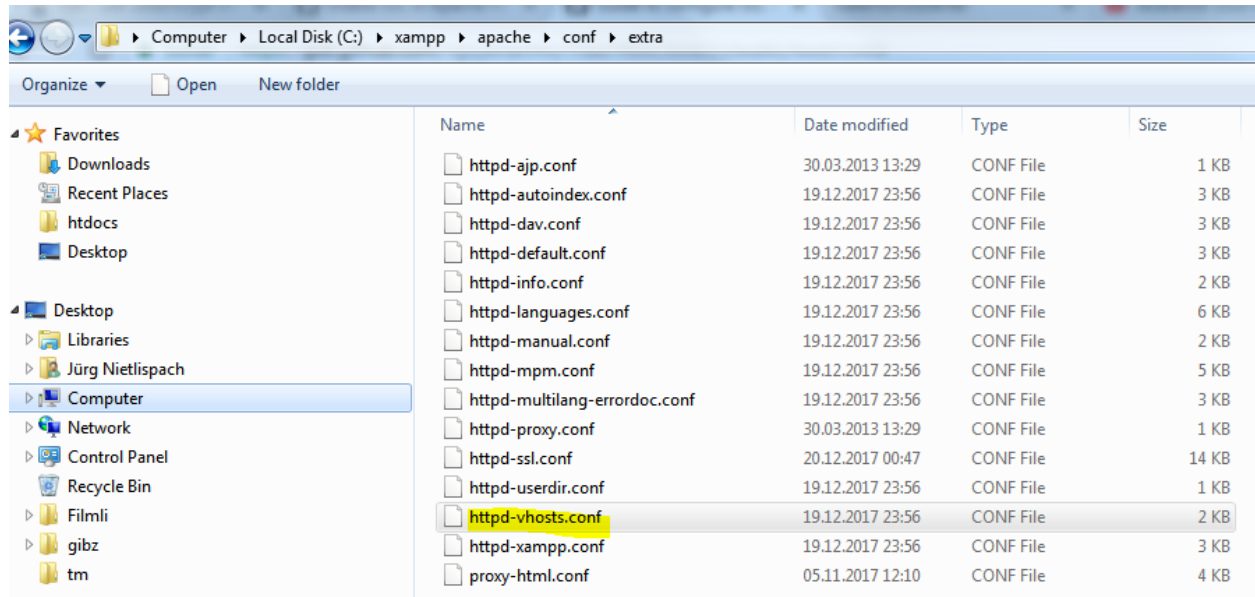
Wird wie gewünscht auf https umgeleitet



Nun wird das Zertifikat noch als unsicher eingestuft – ist klar, da wir das Zertifikat auf testsystem.dev ausgestellt haben:



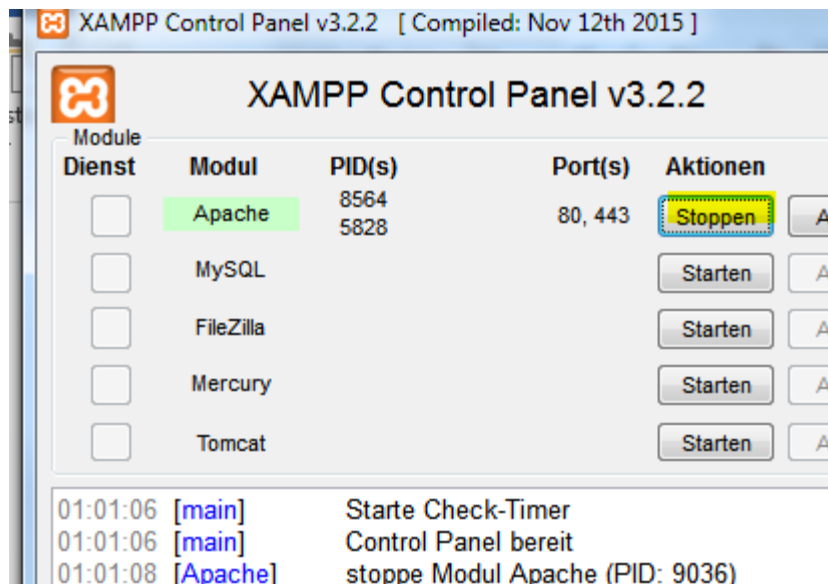
Wir müssen also noch den Virtuellen Host erstellen:



Folgender Eintrag muss noch gemacht werden.

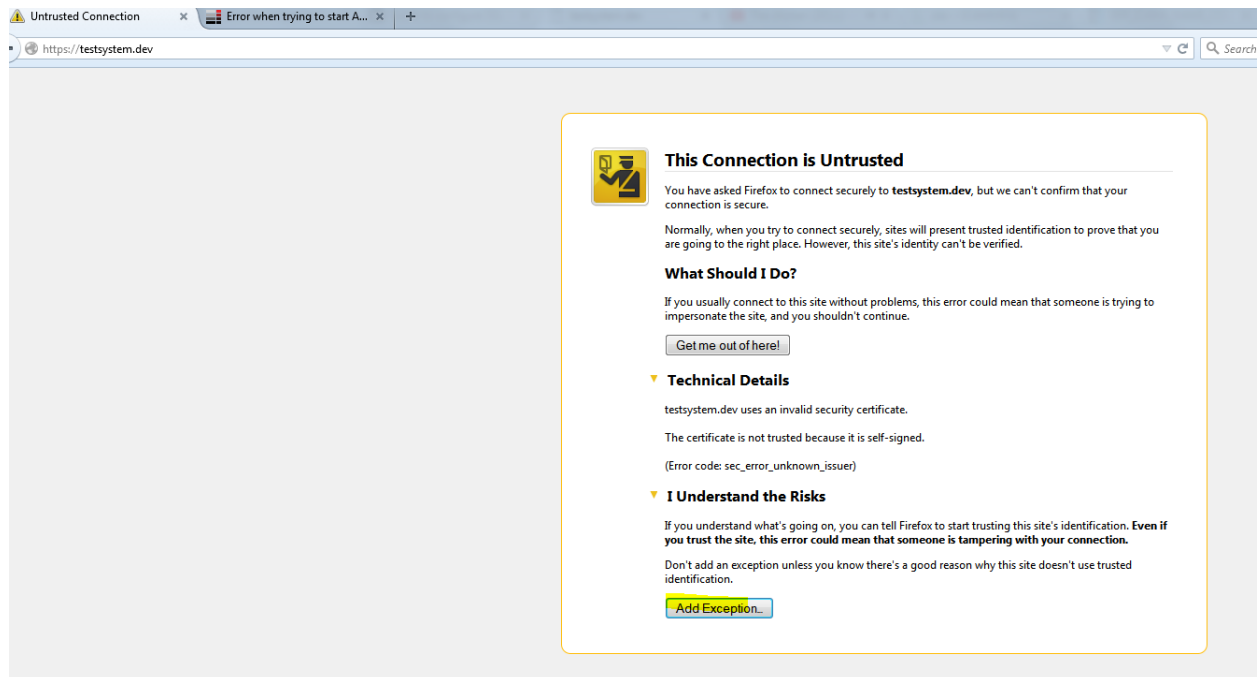
```
<VirtualHost *:443>
    DocumentRoot "C:/xampp/htdocs"
    ServerName testsystem.dev
    SSLEngine On
    SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "conf/ssl.key/server.key"
    ErrorLog "logs/testsystem.dev-error.log"
</VirtualHost>
```

Damit die Änderungen aktiv werden, muss der Server via Control-Panel neu gestartet werden.

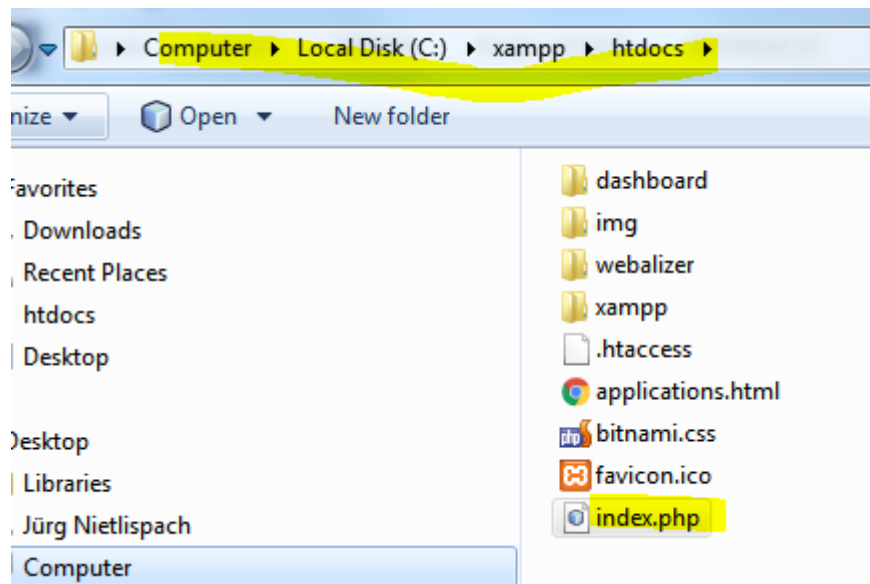


Nun ist es so, dass Google Chrome alle .dev-Toplevel-Domains „als Reserviert markiert“.

Wir können nun mit dem Firefox-Webbrowser aber auf die Domäne zugreifen. Indem wir bei Firefox die Ausnahme für Self-Signed Certificates hinzufügen:

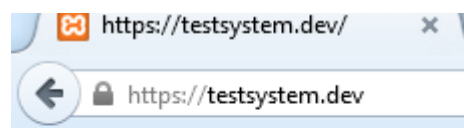


Erscheint dann das im Browser, wenn wir das index.php-File folgendermassen anpassen:



```
<?php
echo "Hello World!";

/*if (!empty($_SERVER['HTTPS']) && ('on' == $_SERVER['HTTPS'])) {
    $uri = 'https://';
} else {
    $uri = 'http://';
}
$uri .= $_SERVER['HTTP_HOST'];
header('Location: '.$uri.'/dashboard/');
exit;*/
?>
```



Hello World!