Immer öfter Hört man von Sicherer Verschlüsselter Datenübertragung über SSL. Doch wie richtet man es ein und wie sicher ist SSL wirklich?

allgemeine Konfiguration

Zunächst sollte man dem Apache2 ein paar grundsätzliche Flausen abgewöhnen. Warum verrät er z.B. bei jeder Anfrage seine Versionsnummer und Patchstand?

Geschwätzigkeit abstellen

Bei falsch aufgerufenen Seiten (Error 404) verkündet der Apache, welche Version er und ein paar andere Programme hat.

Den Umfang der Auskünfte (Programmnamen, Versionsnummern) stellt man ab, indem man in der /etc/apache/conf.d/security folgendes setzt

```
ServerTokens Prod
```

Um die Anzeige komplett zu unterdrücken, setzt man den folgenden Wert

```
ServerSignature Off
```

Webroot absichern

man muss sicherstellen, dass alle Inhalte, die außerhalb des Web-roots liegen, nicht verbreitet werden. Dazu muss man in jedem virtuellen Host folgendes eintragen:

```
<Directory />
  Order Deny,Allow
  Deny from all
  Options None
  AllowOverride None
</Directory>
```

Optionen deaktivieren

Grundsätzlich sollte man in jedem virtuellen Host alle Optionen deaktivieren, wenn man sie nicht braucht.

```
Options none
```

Sollte man doch Optionen einschalten müssen, sollten diese auf ein Minimum reduziert werden.

Forward Secrecy

Wieder so eine Phrase, bei der kein Mensch weiß, um was es sich handelt aber jeder mitreden will.

Damit man nicht dumm stirbt, gibt es hier die Erklärung.

Doch wie bekommt man nun alle möglichen Schlüssel. Nachfolgend eine Tabelle, in der alle Kombinationen der Verschlüsselung aufgeführt sind.

Cipher-Tag	Protocol	Key Ex.	Auth.	Enc.	MAC	Type
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD	
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD	
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384	
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384	
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1	
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1	
SRP-DSS-AES-256-CBC-SHA	SSLv3	SRP	DSS	AES(256)	SHA1	
SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES(256)	SHA1	
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	DH	DSS	AESGCM(256)	AEAD	
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD	
DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256)	SHA256	
DHE-DSS-AES256-SHA256	TLSv1.2	DH	DSS	AES(256)	SHA256	
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES(256)	SHA1	
DHE-DSS-AES256-SHA	SSLv3	DH	DSS	AES(256)	SHA1	
DHE-RSA-CAMELLIA256-SHA	SSLv3	DH	RSA	Camellia(256)	SHA1	
DHE-DSS-CAMELLIA256-SHA	SSLv3	DH	DSS	Camellia(256)	SHA1	
AECDH-AES256-SHA	SSLv3	ECDH	None	AES(256)	SHA1	
SRP-AES-256-CBC-SHA	SSLv3	SRP	None	AES(256)	SHA1	
ADH-AES256-GCM-SHA384	TLSv1.2	DH	None	AESGCM(256)	AEAD	
ADH-AES256-SHA256	TLSv1.2	DH	None	AES(256)	SHA256	
ADH-AES256-SHA	SSLv3	DH	None	AES(256)	SHA1	
ADH-CAMELLIA256-SHA	SSLv3	DH	None	Camellia(256)	SHA1	
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM(256)	AEAD	
ECDH-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM(256)	AEAD	
ECDH-RSA-AES256-SHA384	TLSv1.2	ECDH/RSA	ECDH	AES(256)	SHA384	
ECDH-ECDSA-AES256-SHA384	TLSv1.2	ECDH/ECDSA	ECDH	AES(256)	SHA384	
ECDH-RSA-AES256-SHA	SSLv3	ECDH/RSA	ECDH	AES(256)	SHA1	
ECDH-ECDSA-AES256-SHA	SSLv3	ECDH/ECDSA	ECDH	AES(256)	SHA1	
AES256-GCM-SHA384	TLSv1.2	RSA	RSA	AESGCM(256)	AEAD	
AES256-SHA256	TLSv1.2	RSA	RSA	AES(256)	SHA256	
AES256-SHA	SSLv3	RSA	RSA	AES(256)	SHA1	
CAMELLIA256-SHA	SSLv3	RSA	RSA	Camellia(256)	SHA1	
PSK-AES256-CBC-SHA	SSLv3	PSK	PSK	AES(256)	SHA1	
ECDHE-RSA-DES-CBC3-SHA	SSLv3	ECDH	RSA	3DES(168)	SHA1	
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	ECDH	ECDSA	3DES(168)	SHA1	
SRP-DSS-3DES-EDE-CBC-SHA	SSLv3	SRP	DSS	3DES(168)	SHA1	

Cipher-Tag	Protocol	Key Ex.	Auth.	Enc.	MAC	Type
SRP-RSA-3DES-EDE-CBC-SHA	SSLv3	SRP	RSA	3DES(168)	SHA1	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168)	SHA1	
AECDH-DES-CBC3-SHA	SSLv3	ECDH	None	3DES(168)	SHA1	
SRP-3DES-EDE-CBC-SHA	SSLv3	SRP	None	3DES(168)	SHA1	
ADH-DES-CBC3-SHA	SSLv3	DH	None	3DES(168)	SHA1	
ECDH-RSA-DES-CBC3-SHA	SSLv3	ECDH/RSA	ECDH	3DES(168)	SHA1	
ECDH-ECDSA-DES-CBC3-SHA	SSLv3	ECDH/ECDSA	ECDH	3DES(168)	SHA1	
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168)	SHA1	
PSK-3DES-EDE-CBC-SHA	SSLv3	PSK	PSK	3DES(168)	SHA1	
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD	
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH	ECDSA	AESGCM(128)	AEAD	
ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256	
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	ECDH	ECDSA	AES(128)	SHA256	
ECDHE-RSA-AES128-SHA	SSLv3	ECDH	RSA	AES(128)	SHA1	
ECDHE-ECDSA-AES128-SHA	SSLv3	ECDH	ECDSA	AES(128)	SHA1	
SRP-DSS-AES-128-CBC-SHA	SSLv3	SRP	DSS	AES(128)	SHA1	
SRP-RSA-AES-128-CBC-SHA	SSLv3	SRP	RSA	AES(128)	SHA1	
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	DH	DSS	AESGCM(128)	AEAD	
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM(128)	AEAD	
DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES(128)	SHA256	
DHE-DSS-AES128-SHA256	TLSv1.2	DH	DSS	AES(128)	SHA256	
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES(128)	SHA1	
DHE-DSS-AES128-SHA	SSLv3	DH	DSS	AES(128)	SHA1	
DHE-RSA-SEED-SHA	SSLv3	DH	RSA	SEED(128)	SHA1	
DHE-DSS-SEED-SHA	SSLv3	DH	DSS	SEED(128)	SHA1	
DHE-RSA-CAMELLIA128-SHA	SSLv3	DH	RSA	Camellia(128)	SHA1	
DHE-DSS-CAMELLIA128-SHA	SSLv3	DH	DSS	Camellia(128)	SHA1	
AECDH-AES128-SHA	SSLv3	ECDH	None	AES(128)	SHA1	
SRP-AES-128-CBC-SHA	SSLv3	SRP	None	AES(128)	SHA1	
ADH-AES128-GCM-SHA256	TLSv1.2	DH	None	AESGCM(128)	AEAD	
ADH-AES128-SHA256	TLSv1.2	DH	None	AES(128)	SHA256	
ADH-AES128-SHA	SSLv3	DH	None	AES(128)	SHA1	
ADH-SEED-SHA	SSLv3	DH	None	SEED(128)	SHA1	
ADH-CAMELLIA128-SHA	SSLv3	DH	None	Camellia(128)	SHA1	
ECDH-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH/RSA	ECDH	AESGCM(128)	AEAD	
ECDH-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AESGCM(128)	AEAD	
ECDH-RSA-AES128-SHA256	TLSv1.2	ECDH/RSA	ECDH	AES(128)	SHA256	
ECDH-ECDSA-AES128-SHA256	TLSv1.2	ECDH/ECDSA	ECDH	AES(128)	SHA256	
ECDH-RSA-AES128-SHA	SSLv3	ECDH/RSA	ECDH	AES(128)	SHA1	
ECDH-ECDSA-AES128-SHA	SSLv3	ECDH/ECDSA	ECDH	AES(128)	SHA1	
AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM(128)	AEAD	
AES128-SHA256	TLSv1.2	RSA	RSA	AES(128)	SHA256	
AES128-SHA	SSLv3	RSA	RSA	AES(128)	SHA1	
SEED-SHA	SSLv3	RSA	RSA	SEED(128)	SHA1	

Cipher-Tag	Protocol	Key Ex.	Auth.	Enc.	MAC	Type
CAMELLIA128-SHA	SSLv3	RSA	RSA	Camellia(128)	SHA1	
PSK-AES128-CBC-SHA	SSLv3	PSK	PSK	AES(128)	SHA1	
ECDHE-RSA-RC4-SHA	SSLv3	ECDH	RSA	RC4(128)	SHA1	
ECDHE-ECDSA-RC4-SHA	SSLv3	ECDH	ECDSA	RC4(128)	SHA1	
AECDH-RC4-SHA	SSLv3	ECDH	None	RC4(128)	SHA1	
ADH-RC4-MD5	SSLv3	DH	None	RC4(128)	MD5	
ECDH-RSA-RC4-SHA	SSLv3	ECDH/RSA	ECDH	RC4(128)	SHA1	
ECDH-ECDSA-RC4-SHA	SSLv3	ECDH/ECDSA	ECDH	RC4(128)	SHA1	
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5	
PSK-RC4-SHA	SSLv3	PSK	PSK	RC4(128)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES(56)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES(56)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	None	DES(56)	SHA1	
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH(512)	RSA	DES(40)	SHA1	export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH(512)	DSS	DES(40)	SHA1	export
EXP-ADH-DES-CBC-SHA	SSLv3	DH(512)	None	DES(40)	SHA1	export
EXP-DES-CBC-SHA	SSLv3	RSA(512)	RSA	DES(40)	SHA1	export
EXP-RC2-CBC-MD5	SSLv3	RSA(512)	RSA	RC2(40)	MD5	export
EXP-ADH-RC4-MD5	SSLv3	DH(512)	None	RC4(40)	MD5	export
EXP-RC4-MD5	SSLv3	RSA(512)	RSA	RC4(40)	MD5	export

Umsetzung

Um die Verschlüsselung global zu setzen, muss man in der Datei /etc/apache2/mods-enabled/ssl.conf die folgendenen Zeilen eintragen / Ändern

Vorsicht:

In den <VirtualHost>-Anweisungen wird der Wert noch einmal gesetzt und damit überschrieben. Kommentiert ihn bei jedem vHost aus!!

```
SSLProtocol all -SSLv2
SSLHonorCipherOrder On
SSLCipherSuite EECDH+AES:EDH+AES:-SHA1:EECDH+RC4:EDH+RC4:RC4-
SHA:EECDH+AES256:EDH+AES256:AES256-SHA:!aNULL:!eNULL:!EXP:!LOW:!MD5
```

Nachtrag:

1. Leider Ist in der obigen Regel nicht der „anonyme Diffi-Hellmann Schlüsselaustausch“ inbegriffen. dieser sollte wenn mögliche auch abgeschalten werden. Ein `:!ADH` an die Zeile SSLCipherSuite angehängt und auch dieses Problem ist gelöst
2. RC4-Verschlüsselung gilt nicht mehr als sicher und kann mit `!:RC4` deaktiviert werden
3. Aufgrund von Inkompatibilität habe ich mich dazu entschieden, EDH-3DES und EECDH-3DES zu

aktivieren. Die Optimierte CipherSuite ist nun

```
SSLCipherSuite EECDH+AES:EDH+AES:-
SHA1:EECDH+AES256:EDH+AES256:EECDH+3DES:EDH+3DES:AES256-
SHA:!aNULL:!eNULL:!EXP:!LOW:!MD5:!ADH
```

4. Aufgrund von aktuellen Ereignissen (DH-Logjam Attacke) kann die obige CipherSuite auch nicht mehr als Maß aller Dinge betrachtet werden. Eine Beschreibung der zusätzlichen Absicherung sowie einer SSLCipherSuite ist hier beschrieben.

HTTP Strict Transport Security

Quellen

Allgemeine Konfiguration

- https://icertificate.eu/de/hilfe/anleitungen/perfect-forward-secrecy-apache.html
- http://www.petefreitag.com/item/505.cfm
- http://www.techrepublic.com/blog/10-things/10-things-you-should-do-to-secure-apache/477/

SSL

Forward-Secrecy

- http://blog.pregos.info/2013/09/05/howto-apache-ssl-and-perfect-forward-secrecy/
- https://blog.benny-baumann.de/?p=1446

HTTP Strict Transport Security

- http://blog.pregos.info/2014/01/31/hsts-was-es-ist-wie-es-funktioniert-und-wie-man-es-in-apache-einrichtet/

SSL Security test

- https://www.ssllabs.com/ssltest/

From:
https://wiki.da-checka.de/ - **PSwiki**

Permanent link:
https://wiki.da-checka.de/doku.php/wiki/sicherheit/apache2

Last update: **2015/10/23 10:32**