testssl.sh

Wann kann’s

(Aktive) Überprüfung serverseitiger Verschlüsselung

- Plain TLS/SSL-verschlüsselte TCP-Ports
  - HTTPS
  - SMTP/587, RDP/3389, IMAPS/993, POP3D/995,…
    - (agnostisch f. darunter liegende Protokolle)
  - Tunneln über Proxy (CONNECT)

- Diverse STARTTLS-Protokolle
  - → Plaintext-Handshake vor Verschlüsselung
  - FTP, IMAP, POP, SMTP, LMTP, XMPP,
  - PostgreSQL, MySQL, LDAP.

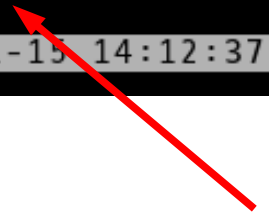
Wann kann’s

Aktive Überprüfung serverseitiger Verschlüsselung

- IPv4, IPv6 (switch -6 erforderlich)
- Protokolle: SSLv2 - TLS 1.3 (Drafts ab 18 bis Final)
- Cipher: 370
  - (eingetragen als Hexcode in externer Datei)
- Kurven (DH, ECDHE, x448, x25519)
- Verwundbarkeiten
  - Sockets: Heartbleed, Ticketbleed, ROBOT, CCS, …
  - Cipher u.a: POODLE (SSL), Renegotiation, BEAST BREACH, LOGJAM, DROWN, …
- TLS Extensions

Protokolle

```
dirks@laptop:~|130% testssl.sh -q --ip=one -p -6 testssl.net

 Start 2018-11-15 14:12:23        -->> [2606:4700:30::6812:2251]:443 (testssl.net) <<--

 Further IP addresses:             104.18.35.81 104.18.34.81 2606:4700:30::6812:2351
 AAAA record via:                  supplied IP "2606:4700:30::6812:2251"
 rDNS (2606:4700:30::6812:2251):   --
 Service detected:                 HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered
 TLS 1.1    offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): draft 28, draft 23, final
 NPN/SPDY   h2, http/1.1 (advertised)
 ALPN/HTTP2 h2, http/1.1 (offered)

 Done 2018-11-15 14:12:37 [  24s] -->> [2606:4700:30::6812:2251]:443 (testssl.net) <<--
```



HTTP2

Protokolle in schlecht+Verwundbarkeiten (STARTTLS SMTP)

```
dirks@laptop:~|7% testssl.sh -p  -q --vulnerable --starttls smtp  borken:25

 Start 2018-11-15 14:16:24        -->> [redacted]:25 ([redacted]) <<--

 rDNS ([redacted]):
 Service set:            STARTTLS via SMTP

 Testing protocols via sockets

 SSLv2      not offered (OK)
 SSLv3      offered (NOT ok)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    not offered
 TLS 1.3    not offered

 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                VULNERABLE (NOT ok)
 CCS (CVE-2014-0224)                       likely VULNERABLE (NOT ok), suspicious "bad_record_mac" (14)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (CVE-2009-3555)      not vulnerable (OK)
 Secure Client-Initiated Renegotiation     VULNERABLE (NOT ok), potential DoS threat
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK) (not using HTTP anyway)
 POODLE, SSL (CVE-2014-3566)               VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible, SSLv3 is the only protocol
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
 FREAK (CVE-2015-0204)                     VULNERABLE (NOT ok), uses EXPORT RSA ciphers
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://censys.io/ipv4?q=A3ADE2897CDBFD642665512ECF2DCF95A19F30E9BCD3DD60B61CE939468B0A21
 could help you to find out
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): uses DH EXPORT ciphers
                                           VULNERABLE (NOT ok): common prime Postfix detected (1024 bits)
 BEAST (CVE-2011-3389)                     SSL3: ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA AECDH-AES256-SHA
                                                 ADH-AES256-SHA ADH-CAMELLIA256-SHA AES256-SHA CAMELLIA256-SHA ECDHE-RSA-AES128-SHA
                                                 DHE-RSA-AES128-SHA DHE-RSA-SEED-SHA DHE-RSA-CAMELLIA128-SHA AECDH-AES128-SHA
                                                 ADH-AES128-SHA ADH-SEED-SHA ADH-CAMELLIA128-SHA AES128-SHA SEED-SHA
                                                 CAMELLIA128-SHA ECDHE-RSA-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA AECDH-DES-CBC3-SHA
                                                 ADH-DES-CBC3-SHA DES-CBC3-SHA EDH-RSA-DES-CBC-SHA ADH-DES-CBC-SHA DES-CBC-SHA
                                                 EXP-EDH-RSA-DES-CBC-SHA EXP-ADH-DES-CBC-SHA EXP-DES-CBC-SHA EXP-RC2-CBC-MD5
                                           VULNERABLE -- and no higher protocols as mitigation supported
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): ECDHE-RSA-RC4-SHA AECDH-RC4-SHA ADH-RC4-MD5 RC4-SHA RC4-MD5
                                                                EXP-ADH-RC4-MD5 EXP-RC4-MD5

 Done 2018-11-15 14:17:00 [  38s] -->> [redacted]:25 ([redacted]) <<--
```

Schlüsselaustausch

(Elliptische Kurven und Diffie-Hellman)

```
dirks@laptop:~|130% testssl.sh -q --pfs owasp.org

 Start 2018-11-15 14:26:11        -->> 104.130.219.202:443 (owasp.org) <<--

 Further IP addresses:   2001:4801:7828:101:be76:4eff:fe10:4f89
 rDNS (104.130.219.202): --
 Service detected:       HTTP


 Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4

 PFS is offered (OK)          ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384
                              DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
                              ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA
 Elliptic curves offered:     sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 secp256k1 prime256v1 secp384r1 secp521r1
                              brainpoolP256r1 brainpoolP384r1 brainpoolP512r1
 DH group offered:            RFC3526/Oakley Group 14 (2048 bits)

 Done 2018-11-15 14:26:26 [  17s] -->> 104.130.219.202:443 (owasp.org) <<--
```

Wann kann’s

Aktive Überprüfung serverseitiger Verschlüsselung

- Server- oder Client-Cipher-Order?
- Bestimmung Cipher-Reihenfolge Server

Server-Order, gut:

```
dirks@laptop:~|0% testssl.sh -q -P testssl.sh

 Start 2018-11-15 14:32:01        -->> 81.169.199.25:443 (testssl.sh) <<--

 rDNS (81.169.199.25):   testssl.sh.
 Service detected:       HTTP


 Testing server preferences

 Has server cipher order?     yes (OK)
 Negotiated protocol          TLSv1.2
 Negotiated cipher            ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
 Cipher order
    TLSv1:     DHE-RSA-CAMELLIA256-SHA DHE-RSA-CAMELLIA128-SHA ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES256-SHA
               DHE-RSA-AES128-SHA AES256-SHA
    TLSv1.1:   DHE-RSA-CAMELLIA256-SHA DHE-RSA-CAMELLIA128-SHA ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES256-SHA
               DHE-RSA-AES128-SHA AES256-SHA
    TLSv1.2:   ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256
               DHE-RSA-CAMELLIA256-SHA DHE-RSA-CAMELLIA128-SHA ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA25
               ECDHE-RSA-AES128-SHA DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA
               AES256-GCM-SHA384 AES128-GCM-SHA256 AES256-SHA256 AES256-SHA


 Done 2018-11-15 14:32:08 [   9s] -->> 81.169.199.25:443 (testssl.sh) <<--
```

Server-Order, gut (anderer Ansatz):

```
dirks@laptop:~/projekte/ssltester|0% testssl.sh -q -E testssl.sh

 Start 2018-11-15 15:00:31        -->> 81.169.199.25:443 (testssl.sh) <<--

 rDNS (81.169.199.25):   testssl.sh.
 Service detected:       HTTP


 Testing ciphers per protocol via OpenSSL plus sockets against the server, ordered by encryption strength

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
------------------------------------------------------------------------------------------------------------------------------
SSLv2
SSLv3
TLS 1
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x39     DHE-RSA-AES256-SHA                DH 2048    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 x88     DHE-RSA-CAMELLIA256-SHA           DH 2048    Camellia    256      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x33     DHE-RSA-AES128-SHA                DH 2048    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 x45     DHE-RSA-CAMELLIA128-SHA           DH 2048    Camellia    128      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS 1.1
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x39     DHE-RSA-AES256-SHA                DH 2048    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 x88     DHE-RSA-CAMELLIA256-SHA           DH 2048    Camellia    256      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x33     DHE-RSA-AES128-SHA                DH 2048    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 x45     DHE-RSA-CAMELLIA128-SHA           DH 2048    Camellia    128      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS 1.2
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 256   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9f     DHE-RSA-AES256-GCM-SHA384         DH 2048    AESGCM      256      TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 x6b     DHE-RSA-AES256-SHA256             DH 2048    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 x39     DHE-RSA-AES256-SHA                DH 2048    AES         256      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
 x88     DHE-RSA-CAMELLIA256-SHA           DH 2048    Camellia    256      TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
 x9d     AES256-GCM-SHA384                 RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384
 x3d     AES256-SHA256                     RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA256
 x35     AES256-SHA                        RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 256   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9e     DHE-RSA-AES128-GCM-SHA256         DH 2048    AESGCM      128      TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
 x67     DHE-RSA-AES128-SHA256             DH 2048    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
 x33     DHE-RSA-AES128-SHA                DH 2048    AES         128      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
 x45     DHE-RSA-CAMELLIA128-SHA           DH 2048    Camellia    128      TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
 x9c     AES128-GCM-SHA256                 RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256
TLS 1.3

 Done 2018-11-15 15:00:44 [  15s] -->> 81.169.199.25:443 (testssl.sh) <<--
```

Server-Order, nicht. so. gut.

```
dirks@laptop:~|0% testssl.sh -q -P --mx owasp.de

Testing all MX records (on port 25): 2014.serverle.info
----------------------------------------------------------------------------
 Start 2018-11-15 14:55:41        -->> 85.214.55.68:25 (2014.serverle.info) <<--

 rDNS (85.214.55.68):    www.serverle.info.
 Service set:            STARTTLS via SMTP

 Testing server preferences

 Has server cipher order?     nope (NOT ok)
 Negotiated protocol          TLSv1.2
 Negotiated cipher            ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256) (limited sense as client wi
ll pick)
 Negotiated cipher per proto  (limited sense as client will pick)
     ECDHE-RSA-AES256-SHA:          TLSv1, TLSv1.1
     ECDHE-RSA-AES256-GCM-SHA384:   TLSv1.2
 No further cipher order check has been done as order is determined by the client


 Done 2018-11-15 14:55:46 [  15s] -->> 85.214.55.68:25 (2014.serverle.info) <<--

----------------------------------------------------------------------------
Done testing all MX records (on port 25): 2014.serverle.info
```

Wann kann’s

Aktive Überprüfung serverseitiger Verschlüsselung

- Client-Simulation: *Welcher Client vereinbart welchen Cipher und welche Kurve?*
- Clients: viele Browser, OpenSSL, Java
- Mail-Clients z.B. fehlen

- Daten (mit Erlaubnis) von SSLlabs API
  - Leider ohne Android >7, iOS >10, Edge >15

Client Simulation (default nur letzte Versionen)

```
 Start 2018-11-15 15:06:34        -->> 104.18.35.81:443 (testssl.net) <<--

 Further IP addresses:   104.18.34.81 2606:4700:30::6812:2251 2606:4700:30::6812:2351
 A record via:           supplied IP "104.18.35.81"
 rDNS (104.18.35.81):    --
 Service detected:       HTTP


 Running client simulations (HTTP) via sockets

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
--------------------------------------------------------------------------------------------
 Android 4.2.2                TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 Android 4.4.2                TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Android 5.0.0                TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305-OLD 256 bit ECDH (P-256)
 Android 6.0                  TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305-OLD 256 bit ECDH (P-256)
 Android 7.0                  TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305     253 bit ECDH (X25519)
 Chrome 65 Win 7              TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Chrome 70 Win 10             TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Firefox 59 Win 7             TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Firefox 62 Win 7             TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 IE 6 XP                      No connection
 IE 7 Vista                   TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 IE 8 Win 7                   TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 IE 8 XP                      No connection
 IE 11 Win 7                  TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win 8.1                TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win Phone 8.1          TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win 10                 TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Edge 13 Win 10               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Edge 13 Win Phone 10         TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Edge 15 Win 10               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     253 bit ECDH (X25519)
 Opera 17 Win 7               TLSv1.2   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 Safari 9 iOS 9               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Safari 9 OS X 10.11          TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Safari 10 OS X 10.12         TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Apple ATS 9 iOS 9            TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Tor 17.0.9 Win 7             TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 Java 6u45                    No connection
 Java 7u25                    TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 Java 8u161                   TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Java 9.0.4                   TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 OpenSSL 1.0.1l               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 OpenSSL 1.0.2e               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)

 Done 2018-11-15 15:06:51 [  25s] -->> 104.18.35.81:443 (testssl.net) <<--
```

Wann kann’s

Serverzertifikat

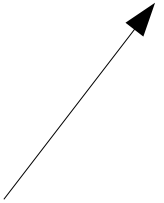
- Trust
  - Expiration
  - Match: SAN (CN), auch Wildcards
  - Stores:
    - Apple, Linux, Windows, Mozilla
    - Eigene Root-CAs
    - ToDo: Symantec-Rauswurf
  - Revocation Checks: OCSP, CRL (extra Flag: --phone-out)
  - DNS: CAA
  - CT

Alles rund ums Serverzertifikat (und TLS Extensions)

```
dirks@laptop:~|0% testssl.sh -q -S expired.badssl.com

 Start 2018-11-15 15:43:10        -->> 104.154.89.105:443 (expired.badssl.com) <<--

 rDNS (104.154.89.105):  105.89.154.104.bc.googleusercontent.com.
 Service detected:       HTTP


 Testing server defaults (Server Hello)

 TLS extensions (standard)    "server name/#0" "renegotiation info/#65281" "EC point formats/#11" "session ticket/#35"
                              "heartbeat/#15" "next protocol/#13172" "application layer protocol negotiation/#16"
 Session Ticket RFC 5077 hint 300 seconds, session tickets keys seems to be rotated < daily
 SSL Session ID support       yes
 Session Resumption           Tickets: yes, ID: no
 TLS clock skew               Random values, no fingerprinting possible
 Signature Algorithm          SHA256 with RSA
 Server key size              RSA 2048 bits
 Server key usage             Digital Signature, Key Encipherment
 Server extended key usage    TLS Web Server Authentication, TLS Web Client Authentication
 Serial / Fingerprints        4AE79549FA9ABE3F100F17A478E16909 / SHA1 404BBD2F1F4CC2FDEEF13AABDD523EF61F1C71F3
                              SHA256 BA105CE02BAC76888ECEE47CD4EB7941653E9AC993B61B2EB3DCC82014D21B4F
 Common Name (CN)             *.badssl.com (CN in response to request w/o SNI: badssl-fallback-unknown-subdomain-or-no-sni)
 subjectAltName (SAN)         *.badssl.com badssl.com
 Issuer                       COMODO RSA Domain Validation Secure Server CA (COMODO CA Limited from GB)
 Trust (hostname)             Ok via SAN wildcard and CN wildcard (SNI mandatory)
 Chain of trust               NOT ok (expired)
 EV cert (experimental)       no
 Certificate Validity (UTC)   expired (2015-04-09 02:00 --> 2015-04-13 01:59)
 # of certificates provided   3
 Certificate Revocation List  http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl
 OCSP URI                     http://ocsp.comodoca.com
 OCSP stapling                not offered
 OCSP must staple extension   --
 DNS CAA RR (experimental)    not offered
 Certificate Transparency     --


 Done 2018-11-15 15:43:27 [  20s] -->> 104.154.89.105:443 (expired.badssl.com) <<--
```

Alles rund ums Serverzertifikat (und TLS Extensions)

```
testssl.sh -q --server-defaults --phone-out web.de
```



```
--phone-out instructs testssl.sh to query external -- in a sense of the
current run -- URLs or URIs. This is needed for checking  revoked  cer-
tificates  via  CRL and OCSP. By using this switch you acknowledge that
the check might could  have  privacy  issues,  a  download  of  several
megabytes  (CRL  file) may happen and there may be network connectivity
problems while contacting CA which testssl.sh doesn´t handle.
```

```
 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281" "server name/#0" "EC point formats/#11" "extended master secret/#23"
 Session Ticket RFC 5077 hint (no lifetime advertised)
 SSL Session ID support       yes
 Session Resumption           Tickets: yes, ID: yes
 TLS clock skew               Random values, no fingerprinting possible

  Server Certificate #1
   Signature Algorithm          SHA256 with RSA
   Server key size              RSA 2048 bits
   Server key usage             Digital Signature, Key Encipherment
   Server extended key usage    TLS Web Client Authentication, TLS Web Server Authentication
   Serial / Fingerprints        21DD14CE55C5F92102F4F95E545CF525 / SHA1 BC9AE646CB1F999E66B191848B041A81B198595F
                                SHA256 7C8454AE4C8818E00D3DF70641EFD2D6577ADC08355283334287CB51988D8684
   Common Name (CN)             *.web.de (CN in response to request w/o SNI: web.de)
   subjectAltName (SAN)         *.web.de web.de
   Issuer                       TeleSec ServerPass DE-2 (T-Systems International GmbH from DE)
   Trust (hostname)             Ok via SAN (works w/o SNI)
   Chain of trust               Ok
   EV cert (experimental)       no
   Certificate Validity (UTC)   69 >= 60 days (2018-01-18 13:33 --> 2019-01-24 00:59)
   # of certificates provided   2
   Certificate Revocation List  http://crl.serverpass.telesec.de/rl/TeleSec_ServerPass_DE-2.crl, not revoked
                                ldap://ldap.serverpass.telesec.de/cn=TeleSec%%20ServerPass%%20DE-2,ou=T-Systems%%20Trust%%20Center,o
=T-Systems%%20International%%20GmbH,c=de?certificateRevocationlist?base?certificateRevocationlist=*, not revoked
   OCSP URI                     http://ocsp.serverpass.telesec.de/ocspr, not revoked
   OCSP stapling                not offered
   OCSP must staple extension   --
   DNS CAA RR (experimental)    available - please check for match with "Issuer" above
                                issue=Digicert.com, issue=telesec.de
   Certificate Transparency     --

  Server Certificate #2 (in response to request w/o SNI)
   Signature Algorithm          SHA256 with RSA
   Server key size              RSA 2048 bits
   Server key usage             Digital Signature, Key Encipherment
   Server extended key usage    TLS Web Client Authentication, TLS Web Server Authentication
   Serial / Fingerprints        8A18ECF934E2A41D / SHA1 F42F6D37BF8B75CB6934E69892FE1A9BD449E5C2
                                SHA256 6699CEE7617F50988CFE114980832E175C8564C74A51BC0677E1A8CC9F59D230
   Common Name (CN)             web.de
   subjectAltName (SAN)         web.de
   Issuer                       TeleSec ServerPass DE-2 (T-Systems International GmbH from DE)
   Trust (hostname)             Ok via SAN and CN
   Chain of trust               Ok
   EV cert (experimental)       no
   Certificate Validity (UTC)   116 >= 60 days (2017-03-06 13:26 --> 2019-03-12 00:59)
   # of certificates provided   3
   Certificate Revocation List  http://crl.serverpass.telesec.de/rl/TeleSec_ServerPass_DE-2.crl, not revoked
                                ldap://ldap.serverpass.telesec.de/cn=TeleSec%%20ServerPass%%20DE-2,ou=T-Systems%%20Trust%%20Center,o
=T-Systems%%20International%%20GmbH,c=de?certificateRevocationlist?base?certificateRevocationlist=*, not revoked
   OCSP URI                     http://ocsp.serverpass.telesec.de/ocspr, not revoked
   OCSP stapling                not offered
   OCSP must staple extension   --
   DNS CAA RR (experimental)    available - please check for match with "Issuer" above
                                issue=Digicert.com, issue=telesec.de
   Certificate Transparency     --
```

Wann kann’s

Bonus

- HTTP HEADER
  - Server-Banner (App, Proxy)
  - CSP, HPKP, HSTS
  - Weitere Security Header
  - Cookies
    - Goodie: F5 cookie decoder, außer AES ;-)

HTTP Header

```
dirks@laptop:~|0% testssl.sh -q --header https://www.owasp.org/index.php/Main_Page

 Start 2018-11-15 15:59:38        -->> 104.130.219.202:443 (www.owasp.org) <<--

 Further IP addresses:   2001:4801:7828:101:be76:4eff:fe10:4f89
 rDNS (104.130.219.202): --
 Service detected:       HTTP


 Testing HTTP header response @ "/index.php/Main_Page"

 HTTP Status Code             200 OK
 HTTP clock skew              0 sec from localtime
 Strict Transport Security    not offered
 Public Key Pinning           --
 Server banner                Apache
 Application banner           --
 Cookie(s)                    (none issued at "/index.php/Main_Page")
 Security headers             X-Frame-Options DENY
                              X-XSS-Protection 1; mode=block
                              X-Content-Type-Options nosniff
                              X-UA-Compatible IE=Edge
 Reverse Proxy banner         --


 Done 2018-11-15 15:59:45 [  10s] -->> 104.130.219.202:443 (www.owasp.org) <<--
```

HTTP Header (F5 BigIP)

```
Testing HTTP header response @ "/"

HTTP Status Code               302 Found, redirecting to "http://www.mastercard.com/index.html" -- Redirect to insecure URL (NOT ok)
HTTP clock skew                0 sec from localtime
Strict Transport Security      not offered
Public Key Pinning             --
Server banner                  (no "Server" line in header, interesting!)
Application banner             --
Cookie(s)                      2 issued: 2/2 secure, 2/2 HttpOnly -- maybe better try target URL of 30x
                               Encrypted F5 cookie named LB1 detected
Security headers               --
Reverse Proxy banner           --


Done 2018-11-15 15:21:12 [  11s] -->> 216.119.216.188:443 (mastercard.com) <<--
```

```
Testing HTTP header response @ "/"

HTTP Status Code               200 OK
HTTP clock skew                +3 (± 1.5) sec from localtime
Strict Transport Security      --
Public Key Pinning             --
Server banner                  Lotus-Domino
Application banner             --
Cookie(s)                      1 issued: NOT secure, NOT HttpOnly
                               F5 cookie (IPv4 pool in routed domain 2): BIGipServer~RD-DMZ~LOTUSWEBMAIL-HTTP 172.16.40.194:80
Security headers               --
Reverse Proxy banner           --
```

Wann kann’s

Ausgaben

- Mensch: Farbe
  - ANSI: Color-based rating
    - Auch Farbenblinde
  - HTML
- Maschine
  - CSV
  - JSON (flach, nicht flach)
  - Ausgabe nur maximaler „severities“

Wann kann’s

Mehr

- Datei als Input
  - Kommandos, Kommentare erlaubt
  - Parser für NMAP-Ausgabe
- Mass Testing
  - Seriell
  - Parallel (mit Bildschirmausgabe)

Wann kann’s

Einstieg

- `testssl.sh (mit oder ohne –help)`
- `testssl.sh <host> oder <host:port>`

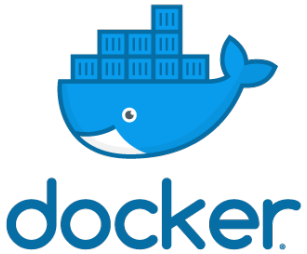
→ macht Default-Lauf, ohne Logging, nur Bildschirm

```
dirks@laptop:~/git.testssl.sh|0% cd doc && ls -1
testssl.1
testssl.1.html
testssl.1.md
dirks@laptop:~/git.testssl.sh/doc|0%
```

Was brauche ich?

- **Voraussetzungen**
  - `/bin/bash`
  - Basis-Tools Linux (GNU) oder BSD
  - OpenSSL nur als Helfer
  - Servertests: Sockets

  → läuft ohne weitere Installation
    - nativ unter Linux, BSDs, Mac OSX
    - WSL, Cygwin, MSYS2 (langsamer)
    - `docker pull drwetter/testssl.sh`



Wer?

Dirk Wetter
- Initiator, Maintainer, Contributor

David Cooper (NIST)
- Sockets ausgebaut, parallel mass testing, ROBOT, ..

Weitere
- JSON, CSV, Client Handshakes, Unit tests, ..

Wo

(oder)