■[1m
###
testssl.sh   2.9dev from ■[m■[1mhttps://testssl.sh/dev/■[m
■[1m
This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ ■[m■[1mhttps://testssl.sh/bugs/■[m
■[1m
###■[m

Using "OpenSSL 1.0.2-chacha (1.0.2i-dev)" [~183 ciphers]
on tejas:/home/tejas/dumpdemo/testssl/bin/openssl.Linux.x86_64
(built: "Jun 22 19:32:29 2016", platform: "linux-x86_64")

■[7m Start 2018-02-13 22:27:12   -->> 65.61.137.117:443 (testfire.net) <<--■[m

rDNS (65.61.137.117):   --
Service detected: HTTP

■[1m■[4m Testing vulnerabilities ■[m

■[1m Heartbleed■[m (CVE-2014-0160)   ■[1;32mnot vulnerable (OK)■[m, no heartbeat extension
■[1m CCS■[m (CVE-2014-0224)   ■[1;32mnot vulnerable (OK)■[m
■[1m Ticketbleed■[m (CVE-2016-9244), experiment. ■[1;32mnot vulnerable (OK)■[m, no session ticket exte
■[1m ROBOT   ■[m■[1;32mnot vulnerable (OK)■[m
■[1m Secure Renegotiation ■[m(CVE-2009-3555)   ■[1;32mnot vulnerable (OK)■[m
■[1m Secure Client-Initiated Renegotiation   ■[m■[0;32mnot vulnerable (OK)■[m
■[1m CRIME, TLS ■[m(CVE-2012-4929)   ■[0;32mnot vulnerable (OK)■[m
■[1m BREACH■[m (CVE-2013-3587)   ■[1;32mno HTTP compression (OK) ■[m - only supplied "/
■[1m POODLE, SSL■[m (CVE-2014-3566)   ■[0;31mVULNERABLE (NOT ok)■[m, uses SSLv3+CBC
■[1m TLS_FALLBACK_SCSV■[m (RFC 7507)   ■[0;31mDowngrade attack prevention NOT supported
■[1m SWEET32■[m (CVE-2016-2183, CVE-2016-6329)   ■[1;33mVULNERABLE■[m, uses 64 bit block ciph
■[1m FREAK■[m (CVE-2015-0204)   ■[1;32mnot vulnerable (OK)■[m
■[1m DROWN■[m (CVE-2016-0800, CVE-2016-0703)   ■[1;32mnot 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=4428215D816E528520C11CFD12A4CF84C14E0DDF56D47C6E56564E13ED6E451
■[1m LOGJAM■[m (CVE-2015-4000), experimental   ■[0;32mnot vulnerable (OK):■[m no DH EXPORT cip
■[1m BEAST■[m (CVE-2011-3389)   SSL3: ■[1;33mDES-CBC3-SHA ■[m
TLS1: ■[1;33mAES128-SHA AES256-SHA
DES-CBC3-SHA
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA ■[m
■[1;33mVULNERABLE■[m -- but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)
■[1m LUCKY13■[m (CVE-2013-0169), experimental   potentially ■[1;33mVULNERABLE■[m, uses cipher b
■[1m RC4■[m (CVE-2013-2566, CVE-2015-2808)   ■[0;31mVULNERABLE (NOT ok): ■[m■[0;31mRC4-S

■[7m Done 2018-02-13 22:28:56 [107s] -->> 65.61.137.117:443 (testfire.net) <<--■[m