Forum:Hack Forums

Thread: CONNECT Method for SSL Handshake

v.e.n.o.m - *April 24, 2018, 5:27 pm*

Hello guys,
I'am trying to send a httpwebrequest to CONNECT with a website.

I'am trying using fiddler and i can successfully connect with that website. Can anyone know how to use that code in VB.NET (HttpWebRequest)

The RAW code is

Code CONNECT s.chatp.net:9091 HTTP/1.1
Host: s.chatp.net:9091
User-Agent: USER_AGENT
Connection: Keep-Alive

A SSLv3-compatible ClientHello handshake was found. Fiddler extracted the parameters below.

Version: 3.1 (TLS/1.0)
Random: 5A DF BE D1 34 56 B2 27 33 88 A6 23 04 87 14 51 7A FB D3 29 09 71 27 87 FB 8E C6 94 68 6C F6 50
"Time": 05-07-2081 6.49.22 PM
SessionID: 37 4B 00 00 72 23 BF D5 28 FC 11 4B 7B 54 72 CB 9D FB 2C C0 E2 A9 3A EB 94 E3 27 2D 95 2C 56 E7
Extensions:
    server_name   s.chatp.net
    ec_point_formats   uncompressed [0x0], ansiX962_compressed_prime [0x1], ansiX962_compressed_char2 [0x2]
    elliptic_curves   sect571r1 [0xE], sect571k1 [0xD], secp521r1 [0x19], sect409k1 [0xB], sect409r1 [0xC], secp384r1 [0x18], sect283k1 [0x9], sect283r1 [0xA], secp256k1 [0x16], secp256r1 [0x17], sect239k1 [0x8], sect233k1 [0x6], sect233r1 [0x7], secp224k1 [0x14], secp224r1 [0x15], sect193r1 [0x4], sect193r2 [0x5], secp192k1 [0x12], secp192r1 [0x13], sect163k1 [0x1], sect163r1 [0x2], sect163r2 [0x3], secp160k1 [0xF], secp160r1 [0x10], secp160r2 [0x11]
    SessionTicket   empty
Ciphers:
    [0004]   SSL_RSA_WITH_RC4_128_MD5
    [0005]   SSL_RSA_WITH_RC4_128_SHA
    [002F]   TLS_RSA_AES_128_SHA
    [0035]   TLS_RSA_AES_256_SHA
    [C002]   TLS_ECDH_ECDSA_WITH_RC4_128_SHA
    [C004]   TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
    [C005]   TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
    [C00C]   TLS_ECDH_RSA_WITH_RC4_128_SHA
    [C00E]   TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
    [C00F]   TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
    [C007]   TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
    [C009]   TLS1_CK_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    [C00A]   TLS1_CK_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

[C011] TLS_ECDHE_RSA_WITH_RC4_128_SHA
[C013] TLS1_CK_ECDHE_RSA_WITH_AES_128_CBC_SHA
[C014] TLS1_CK_ECDHE_RSA_WITH_AES_256_CBC_SHA
[0033] TLS_DHE_RSA_WITH_AES_128_SHA
[0039] TLS_DHE_RSA_WITH_AES_256_SHA
[0032] TLS_DHE_DSS_WITH_AES_128_SHA
[0038] TLS_DHE_DSS_WITH_AES_256_SHA
[000A] SSL_RSA_WITH_3DES_EDE_SHA
[C003] TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
[C00D] TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
[C008] TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
[C012] TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
[0016] SSL_DHE_RSA_WITH_3DES_EDE_SHA
[0013] SSL_DHE_DSS_WITH_3DES_EDE_SHA
[0009] SSL_RSA_WITH_DES_SHA
[0015] SSL_DHE_RSA_WITH_DES_SHA
[0012] SSL_DHE_DSS_WITH_DES_SHA
[0003] SSL_RSA_EXPORT_WITH_RC4_40_MD5
[0008] SSL_RSA_EXPORT_WITH_DES40_SHA
[0014] SSL_DHE_RSA_EXPORT_WITH_DES40_SHA
[0011] SSL_DHE_DSS_EXPORT_WITH_DES40_SHA
[00FF] TLS_EMPTY_RENEGOTIATION_INFO_SCSV

Compression:
[00] NO_COMPRESSION

Zettabit - *April 24, 2018, 9:19 pm*
What exactly are you trying to accomplish? I might be able to help you better if I know what it is you’re trying to do.

v.e.n.o.m - *April 25, 2018, 3:52 am*
(Apr 24, 2018 09:19 PM)Zettabit Wrote: *[CITE]* What exactly are you trying to accomplish? I might be able to help you better if I know what it is you’re trying to do.
Please check your private message.

Dalvik - *April 25, 2018, 6:16 am*
Why would you connect to a website? The WebRequest can already handle SSL. You can just skip the handshake and send the request you wish.