HTTPS but without S

date 24.10.2021

solved post time of CTF

category Web Exploitation score none

Description

Analyze HTTPS certificate file.

Attached files

- cert.cer (DER Encoded binary X.509)
- cert2.cer (Base64 Encoded X.509)

Summary

Extract SSL certificate & analyze.

Flag

```
HOLOGY4.0{SoMe_BaSiC_S5L_mIsTAkE}
```

Detailed solution

1. Extract SSL certificate from browser.
2. Analyze with openssl `openssl x509 -in cert2.cer -text -noout`

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0f:fc:dc:34:fe:b3:6d:59:d4:2b:f0:b2:33:ee:ef:42:97:6d:87:59
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = DE, ST = Thuringia, L = Erfurt, O = Poros UB, OU = Team Foo,
CN = Poros UB
        Validity
            Not Before: Oct 22 20:01:55 2021 GMT
            Not After : Oct 20 20:01:55 2031 GMT
        Subject: C = DE, ST = Thuringia, L = Erfurt, O = Poros UB, OU = Team Foo,
CN = Poros UB
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:dd:9e:41:d8:c3:d5:00:32:fe:91:ea:83:10:33:
```

```
                    9e:81:d5:7b:c8:e6:d3:ea:bd:bb:af:03:96:00:5a:
                    01:b4:37:4f:43:2d:ec:96:b7:20:9a:20:79:d7:a3:
                    32:45:6c:a3:ea:46:43:c6:e5:ad:ee:db:a2:96:7e:
                    11:cb:41:57:69:a0:75:cd:3b:86:41:16:59:0a:f5:
                    e0:08:f8:05:1b:fb:e8:8c:bb:1d:46:8d:4d:9b:a0:
                    87:07:85:61:7d:b3:64:61:98:de:25:fc:d0:7a:fd:
                    11:a5:b6:bb:3d:37:61:17:01:45:09:83:5c:d5:25:
                    fd:e1:60:27:f6:d6:ef:7e:9b:41:ed:89:36:79:cc:
                    a2:2d:79:d8:fe:f5:d4:6d:f1:0f:b2:4a:65:32:50:
                    99:85:ea:cf:cb:f8:d2:83:24:9a:40:52:32:c8:e4:
                    32:ba:6f:59:98:67:0b:3e:f4:ea:3c:2f:89:3b:ed:
                    ec:5b:ff:cf:37:d0:f8:11:06:a7:0b:5e:5d:c1:3a:
                    69:9d:9a:87:d6:45:4a:84:2b:12:76:3e:db:5f:1c:
                    b1:64:77:e2:86:c8:cd:71:39:a7:d2:a6:60:28:3e:
                    16:d2:36:81:cd:a2:cf:6f:3c:d3:2b:54:2e:7f:da:
                    c1:76:30:99:27:79:43:20:04:ab:ab:2d:f4:e8:da:
                    79:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:the flag is in here, DNS:/theflaghere
    Signature Algorithm: sha256WithRSAEncryption
         70:e3:46:92:2e:79:bd:82:ce:e3:3e:7a:6a:fc:56:6c:43:a3:
         28:89:51:fc:42:2c:4c:f8:f3:eb:ff:e3:aa:8c:fe:a0:fc:41:
         c5:ec:fa:16:86:b2:32:d3:55:47:27:d2:fc:d2:7d:26:f9:80:
         c4:7f:cc:0d:13:7a:17:dc:32:bb:cf:e0:25:83:85:c3:12:55:
         1c:89:8f:9d:4b:af:90:f0:55:81:a1:85:3f:88:ed:2e:e6:67:
         e7:25:80:e6:72:4c:4a:70:43:00:ec:3d:77:a9:79:d0:0c:17:
         43:ba:19:2e:cc:ce:e7:10:c9:cd:37:bb:94:b8:ab:76:4f:b5:
         c0:0d:b6:af:19:b0:63:45:b0:f9:28:c4:43:9e:9a:0c:c4:ca:
         3e:14:e3:a6:e5:65:34:96:3b:28:8d:81:39:ff:ce:04:f8:02:
         d4:f4:94:65:0f:1e:a1:15:fe:97:e6:4c:3b:4c:11:f6:75:a1:
         34:a8:8a:c0:54:c2:8b:d2:cf:cc:2c:c9:50:05:22:6d:2e:fa:
         67:58:a0:9a:6a:46:72:4b:a2:69:02:06:52:d1:bd:0f:38:ed:
         e4:73:b0:7d:12:e7:46:57:88:8e:24:f2:de:a5:cf:76:d3:bc:
         6a:4d:9a:01:63:e7:8c:01:47:44:90:ed:e7:ad:a8:83:e0:eb:
         17:47:56:b7
```

3. Flag location `/theflaghere`

Another solutions

none.