SSL/TLS vulnerability scan of the Chameleon website

By

Usman Tariq

S217034263

&

Kartik Kaushik

We used 2 tools for this demonstration first one is sslyze tool and second is NMAP.

Using sslyze tool

Target: https://sit-chameleon-website-0bc2323.ts.r.appspot.com/

I used the following options with **sslyze** command as shown in screenshot below. sslyze –sslv3 **sit-chameleon-website-0bc2323.ts.r.appspot.com:443**

1. --sslv3: Test a server for SSL 3.0 support.
2. --tlsv1: Test a server for TLS 1.0 support.
3. --tlsv1_1: Test a server for TLS 1.1 support.
4. --tlsv1_2: Test a server for TLS 1.2 support.
5. --tlsv1_3: Test a server for TLS 1.3 support.
6. --fallback: Test a server for the TLS_FALLBACK_SCSV mechanism to prevent downgrade attacks.
7. --heartbleed: Test a server for the OpenSSL Heartbleed vulnerability.
8. --resum: Test a server for TLS 1.2 session resumption support using session IDs and TLS tickets.
9. --resum_attempts RESUM_ATTEMPTS: Specify the number of session resumptions SSLyze should attempt.
10. --reneg: Test a server for insecure TLS renegotiation and client-initiated renegotiation.
11. --robot: Test a server for the ROBOT vulnerability.

12. --compression: Test a server for TLS compression support, which can be leveraged to perform a CRIME attack.

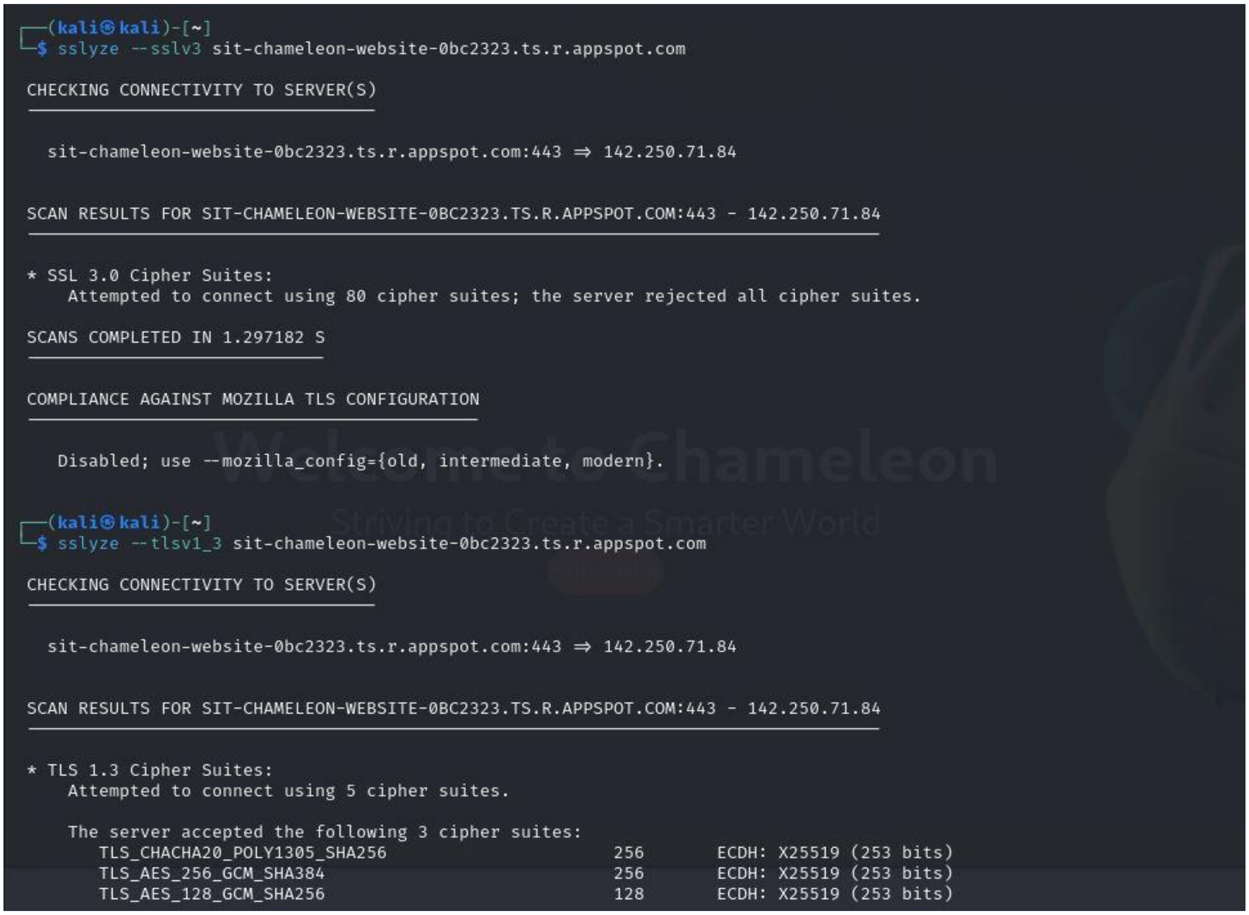
13. --http_headers: Test a server for the presence of security-related HTTP headers.

14. --certinfo: Retrieve and analyze a server's certificate(s) to verify its validity.

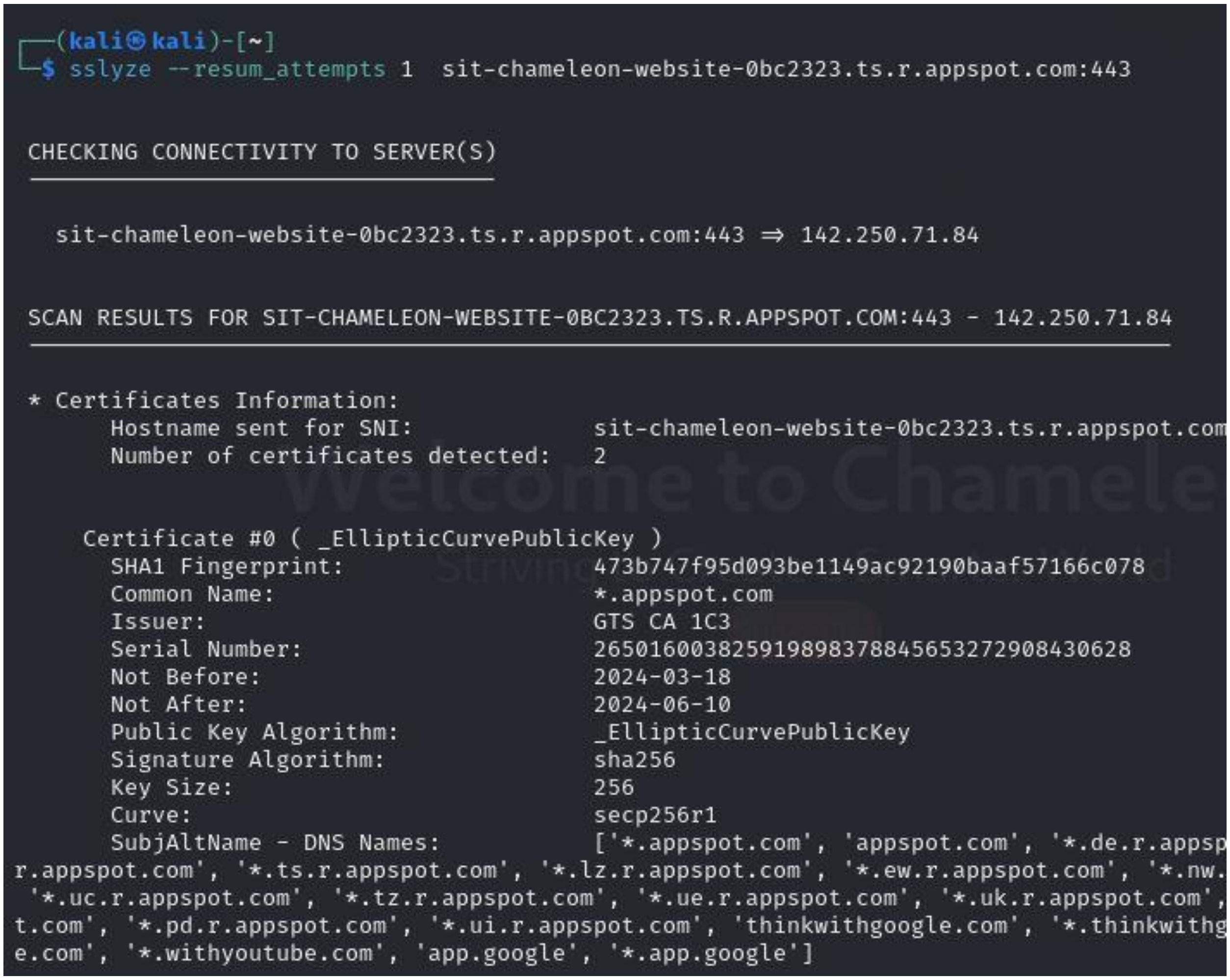
15. --openssl_ccs: Test a server for the OpenSSL CCS Injection vulnerability (CVE-2014-0224).

16. --early_data: Test a server for TLS 1.3 early data support.

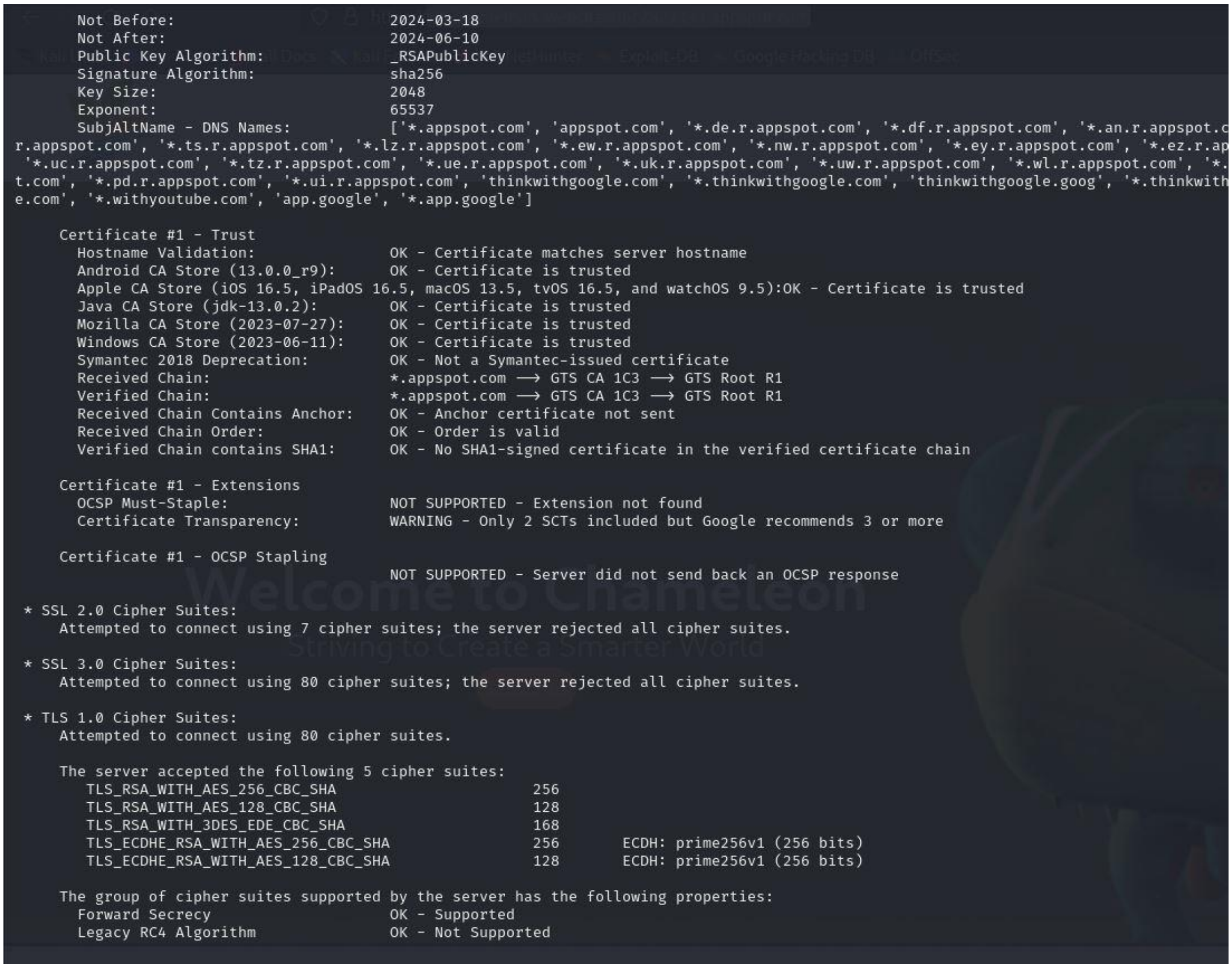
17. --elliptic_curves: Test a server for supported elliptic curves.



```
┌──(kali㉿kali)-[~]
└─$ sslyze --sslv3 sit-chameleon-website-0bc2323.ts.r.appspot.com

 CHECKING CONNECTIVITY TO SERVER(S)
 ----------------------------------

   sit-chameleon-website-0bc2323.ts.r.appspot.com:443 ⇒ 142.250.71.84


 SCAN RESULTS FOR SIT-CHAMELEON-WEBSITE-0BC2323.TS.R.APPSPOT.COM:443 - 142.250.71.84
 ----------------------------------------------------------------------------------

 * SSL 3.0 Cipher Suites:
     Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 SCANS COMPLETED IN 1.297182 S
 -----------------------------

 COMPLIANCE AGAINST MOZILLA TLS CONFIGURATION
 --------------------------------------------

    Disabled; use --mozilla_config={old, intermediate, modern}.

┌──(kali㉿kali)-[~]
└─$ sslyze --tlsv1_3 sit-chameleon-website-0bc2323.ts.r.appspot.com

 CHECKING CONNECTIVITY TO SERVER(S)
 ----------------------------------

   sit-chameleon-website-0bc2323.ts.r.appspot.com:443 ⇒ 142.250.71.84


 SCAN RESULTS FOR SIT-CHAMELEON-WEBSITE-0BC2323.TS.R.APPSPOT.COM:443 - 142.250.71.84
 ----------------------------------------------------------------------------------

 * TLS 1.3 Cipher Suites:
     Attempted to connect using 5 cipher suites.

     The server accepted the following 3 cipher suites:
        TLS_CHACHA20_POLY1305_SHA256                      256       ECDH: X25519 (253 bits)
        TLS_AES_256_GCM_SHA384                            256       ECDH: X25519 (253 bits)
        TLS_AES_128_GCM_SHA256                            128       ECDH: X25519 (253 bits)
```



```
┌──(kali㉿kali)-[~]
└─$ sslyze --resum_attempts 1  sit-chameleon-website-0bc2323.ts.r.appspot.com:443

 CHECKING CONNECTIVITY TO SERVER(S)
 ─────────────────────────────────

   sit-chameleon-website-0bc2323.ts.r.appspot.com:443 ⇒ 142.250.71.84

 SCAN RESULTS FOR SIT-CHAMELEON-WEBSITE-0BC2323.TS.R.APPSPOT.COM:443 - 142.250.71.84
 ──────────────────────────────────────────────────────────────────────────────────

 * Certificates Information:
       Hostname sent for SNI:             sit-chameleon-website-0bc2323.ts.r.appspot.com
       Number of certificates detected:   2


     Certificate #0 ( _EllipticCurvePublicKey )
       SHA1 Fingerprint:                  473b747f95d093be1149ac92190baaf57166c078
       Common Name:                       *.appspot.com
       Issuer:                            GTS CA 1C3
       Serial Number:                     265016003825919898378845653272908430628
       Not Before:                        2024-03-18
       Not After:                         2024-06-10
       Public Key Algorithm:              _EllipticCurvePublicKey
       Signature Algorithm:               sha256
       Key Size:                          256
       Curve:                             secp256r1
       SubjAltName - DNS Names:           ['*.appspot.com', 'appspot.com', '*.de.r.appsp
r.appspot.com', '*.ts.r.appspot.com', '*.lz.r.appspot.com', '*.ew.r.appspot.com', '*.nw.
 '*.uc.r.appspot.com', '*.tz.r.appspot.com', '*.ue.r.appspot.com', '*.uk.r.appspot.com',
t.com', '*.pd.r.appspot.com', '*.ui.r.appspot.com', 'thinkwithgoogle.com', '*.thinkwithg
e.com', '*.withyoutube.com', 'app.google', '*.app.google']
```



```
       Not Before:                    2024-03-18
       Not After:                     2024-06-10
       Public Key Algorithm:          _RSAPublicKey
       Signature Algorithm:           sha256
       Key Size:                      2048
       Exponent:                      65537
       SubjAltName - DNS Names:       ['*.appspot.com', 'appspot.com', '*.de.r.appspot.com', '*.df.r.appspot.com', '*.an.r.appspot.c
 r.appspot.com', '*.ts.r.appspot.com', '*.lz.r.appspot.com', '*.ew.r.appspot.com', '*.nw.r.appspot.com', '*.ey.r.appspot.com', '*.ez.r.ap
  '*.uc.r.appspot.com', '*.tz.r.appspot.com', '*.ue.r.appspot.com', '*.uk.r.appspot.com', '*.uw.r.appspot.com', '*.wl.r.appspot.com', '*.
 t.com', '*.pd.r.appspot.com', '*.ui.r.appspot.com', 'thinkwithgoogle.com', '*.thinkwithgoogle.com', 'thinkwithgoogle.goog', '*.thinkwith
 e.com', '*.withyoutube.com', 'app.google', '*.app.google']

     Certificate #1 - Trust
       Hostname Validation:           OK - Certificate matches server hostname
       Android CA Store (13.0.0_r9):      OK - Certificate is trusted
       Apple CA Store (iOS 16.5, iPadOS 16.5, macOS 13.5, tvOS 16.5, and watchOS 9.5):OK - Certificate is trusted
       Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
       Mozilla CA Store (2023-07-27):     OK - Certificate is trusted
       Windows CA Store (2023-06-11):     OK - Certificate is trusted
       Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
       Received Chain:                    *.appspot.com --> GTS CA 1C3 --> GTS Root R1
       Verified Chain:                    *.appspot.com --> GTS CA 1C3 --> GTS Root R1
       Received Chain Contains Anchor:    OK - Anchor certificate not sent
       Received Chain Order:              OK - Order is valid
       Verified Chain contains SHA1:      OK - No SHA1-signed certificate in the verified certificate chain

     Certificate #1 - Extensions
       OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
       Certificate Transparency:          WARNING - Only 2 SCTs included but Google recommends 3 or more

     Certificate #1 - OCSP Stapling
                                          NOT SUPPORTED - Server did not send back an OCSP response

 * SSL 2.0 Cipher Suites:
     Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

 * SSL 3.0 Cipher Suites:
     Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * TLS 1.0 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 5 cipher suites:
        TLS_RSA_WITH_AES_256_CBC_SHA                      256
        TLS_RSA_WITH_AES_128_CBC_SHA                      128
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                     168
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1 (256 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               OK - Not Supported
```

The server rejects all SSL 3.0 cipher suites.
The server supported TLS 1.0 cipher suites, including 3DES encryption, which is deemed weak.
TLS 1.1 Cipher Suites: Like TLS 1.0, the server allowed 3DES cipher suites.
TLS 1.2 Cipher Suites: The server supported a variety of cipher suites, including AES-GCM.
The server supported TLS 1.3 cipher suites, which are regarded secure.
Deflate compression was deactivated, a recommended security practice to prevent attacks like CRIME.
Session Renegotiation: The server supports secure renegotiation and is not vulnerable to DoS attacks performed by clients.

ROBOT Attack: The server is not vulnerable to this attack.
HTTP Security Headers: The server did not return the appropriate Strict-Transport-Security header for enforcing HTTPS.
Certificate Information: The server issued two certificates in the chain, both from GTS CA 1C3. The certificates are trusted by key systems.
The server supports key exchange using the X25519 and prime256v1 elliptic curves.

The server did not comply with Mozilla's intermediate TLS setup as it supported TLS 1.0 and 1.1 and accepted weak or deprecated cypher suites.

Based on these observations, the server may improve its security posture by:

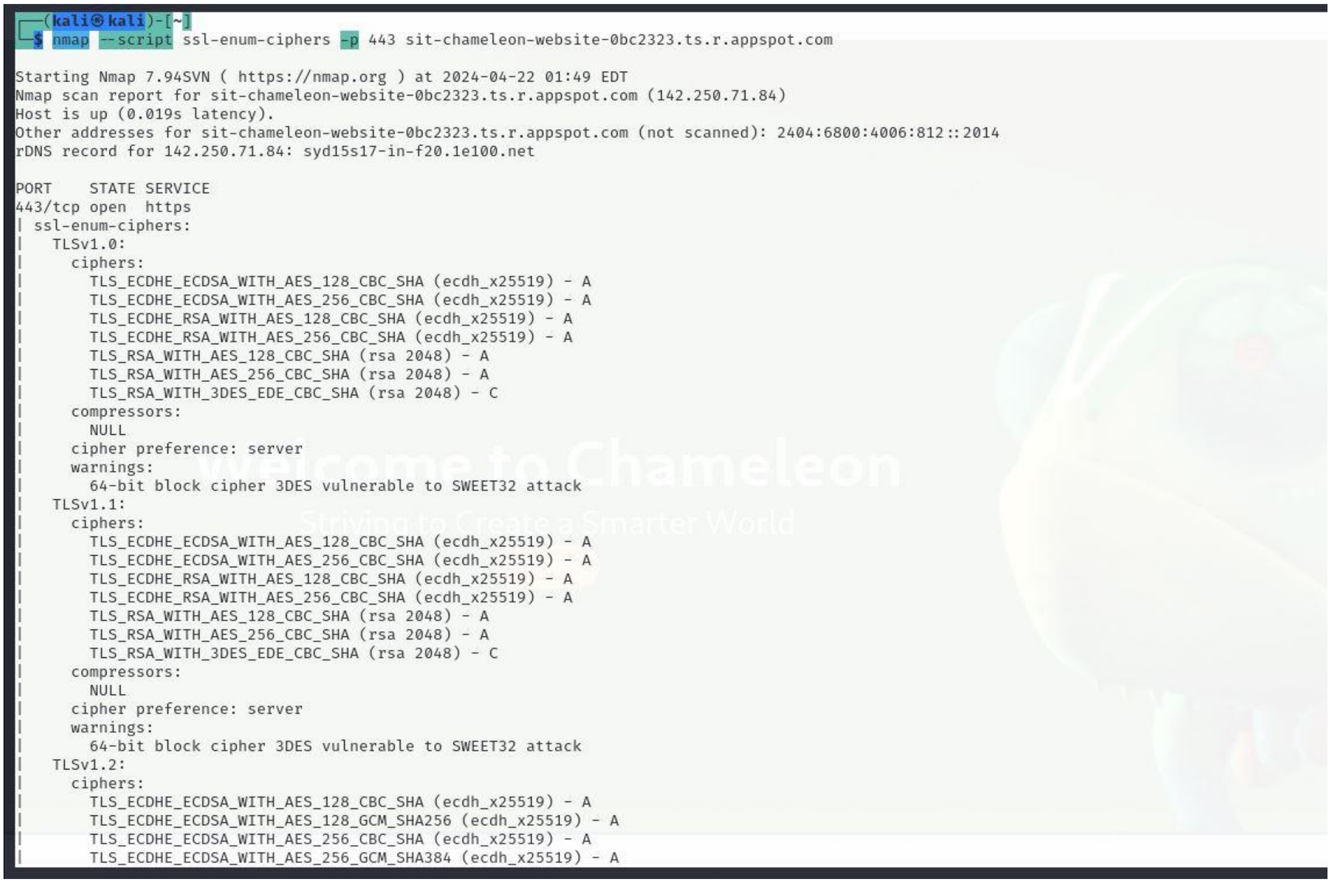
To address vulnerabilities related with these protocols, disable support for SSL 3.0, TLS 1.0, and TLS 1.1.
Removing cipher suites using 3DES encryption.
To enforce HTTPS, enable the Strict-Transport-Security header.
Ensuring adherence to specified TLS setups, such as Mozilla's intermediate configuration.

Findings:
Overall, while the server supports contemporary TLS 1.2 and TLS 1.3 cypher suites, as well as safe renegotiation, there is room for improvement in terms of security posture and compliance with best practices.

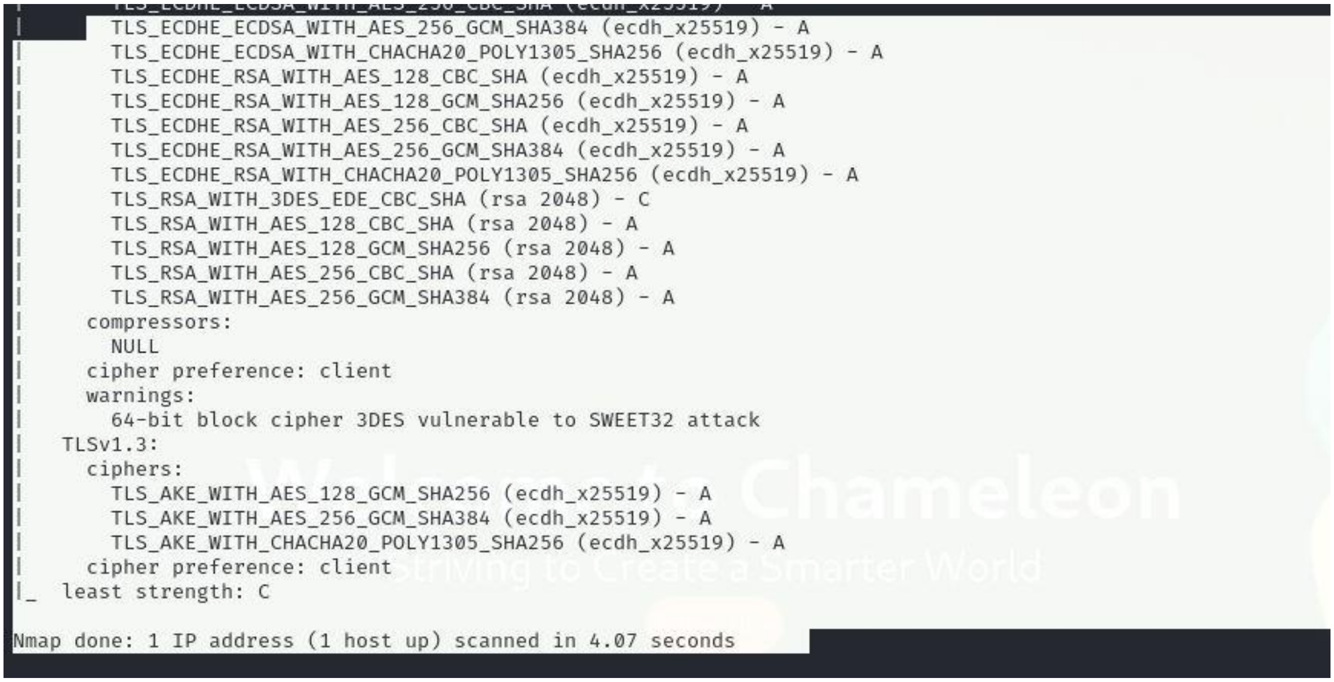
Using NMAP

Target: https://sit-chameleon-website-0bc2323.ts.r.appspot.com/

I used this command with NMAP: **nmap --script ssl-enum-ciphers -p 443 sit-chameleon-website-0bc2323.ts.r.appspot.com**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script ssl-enum-ciphers -p 443 sit-chameleon-website-0bc2323.ts.r.appspot.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 01:49 EDT
Nmap scan report for sit-chameleon-website-0bc2323.ts.r.appspot.com (142.250.71.84)
Host is up (0.019s latency).
Other addresses for sit-chameleon-website-0bc2323.ts.r.appspot.com (not scanned): 2404:6800:4006:812::2014
rDNS record for 142.250.71.84: syd15s17-in-f20.1e100.net

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
```



```
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.3:
|     ciphers:
|       TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|     cipher preference: client
|_  least strength: C

Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds
```

TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 Support:

TLS versions 1.0, 1.1, 1.2, and 1.3. The server supports several TLS protocol versions, including TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3. This is generally a good practice because it allows clients to negotiate the maximum version of TLS that they support.

Cipher Suites:

The server supports multiple cipher suites for each TLS version. Each cipher suite is a collection of cryptographic algorithms designed for safe communication.

3DES Vulnerability:

The warning warns that the server uses the Triple Data Encryption Standard (3DES) cypher, which is known to be susceptible to the SWEET32 attack. This issue stems from 3DES' usage of a 64-bit block size, which makes it vulnerable to specific attacks when a large quantity of data is encrypted using the same key. Due to this weakness, it is suggested that you avoid using 3DES.

Findings:

Overall, the server supports a diverse set of SSL/TLS protocols and cypher suites; nevertheless, the inclusion of 3DES cypher suites offers a security risk due to the SWEET32 vulnerability. It is best to disable 3DES and prioritise the usage of more secure cypher suites. In addition, regular updates and monitoring of SSL/TLS configurations are needed to ensure server security.