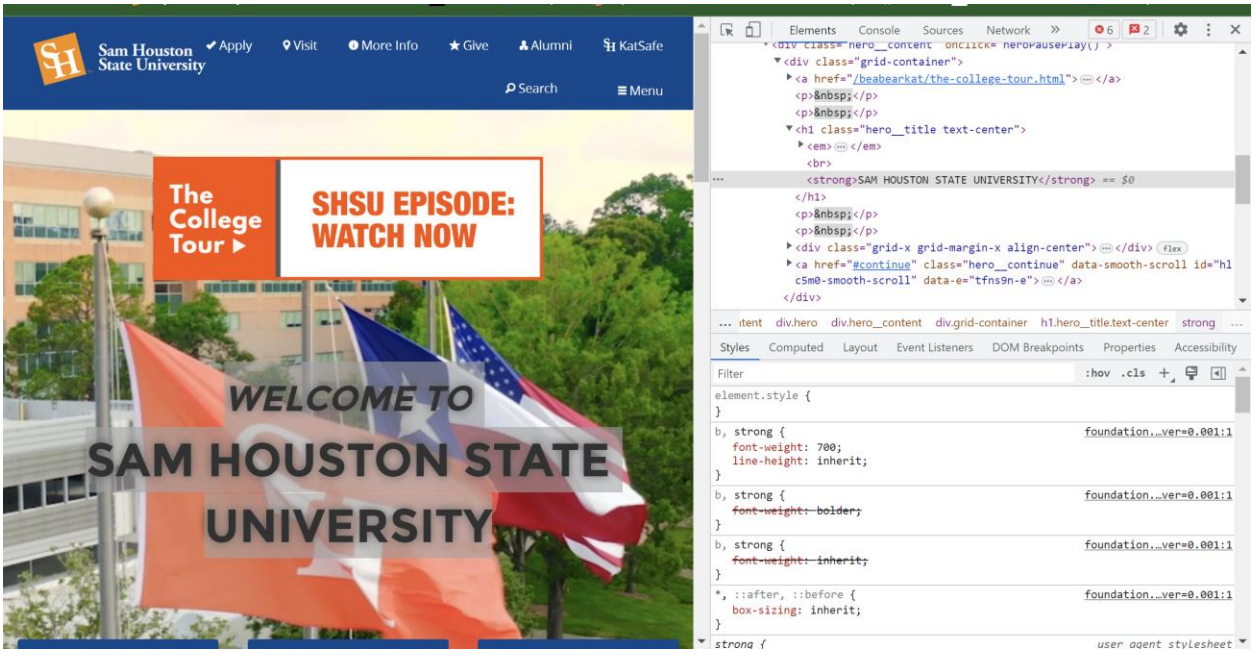
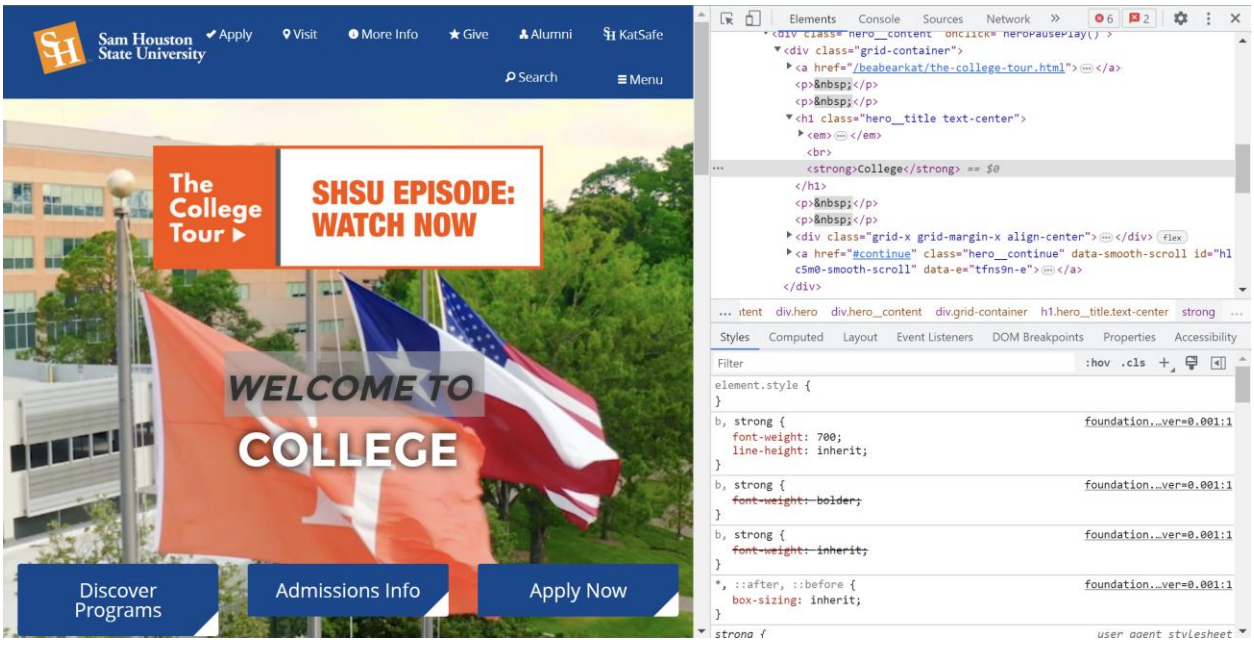
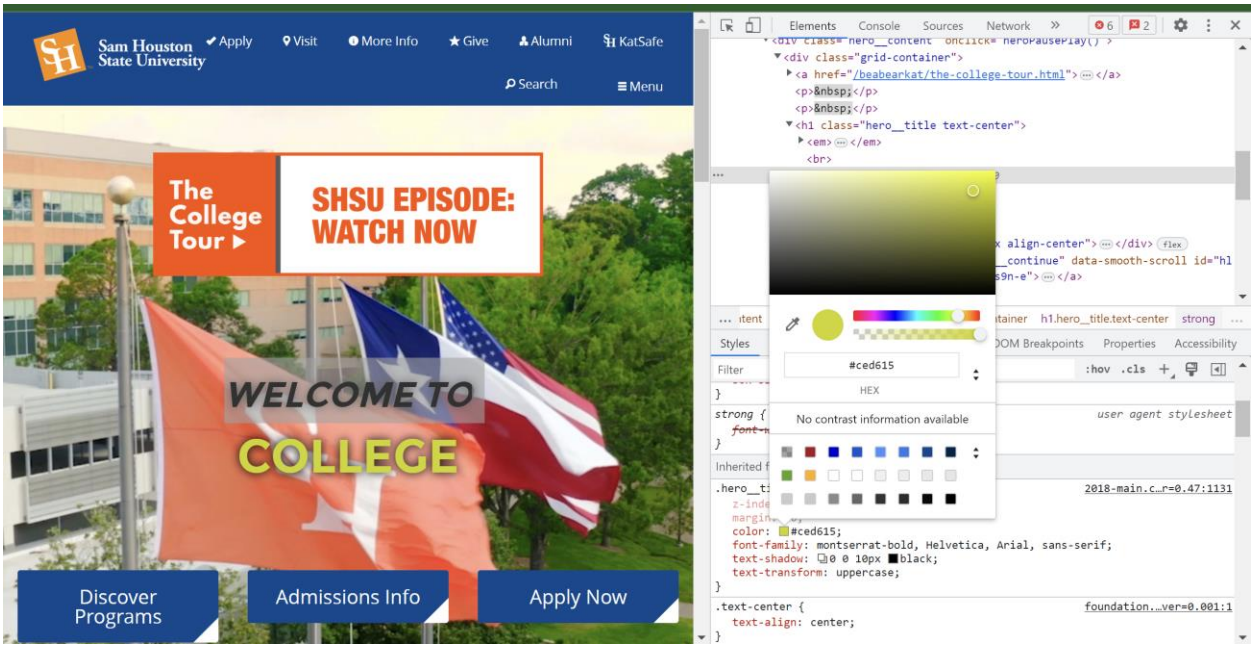
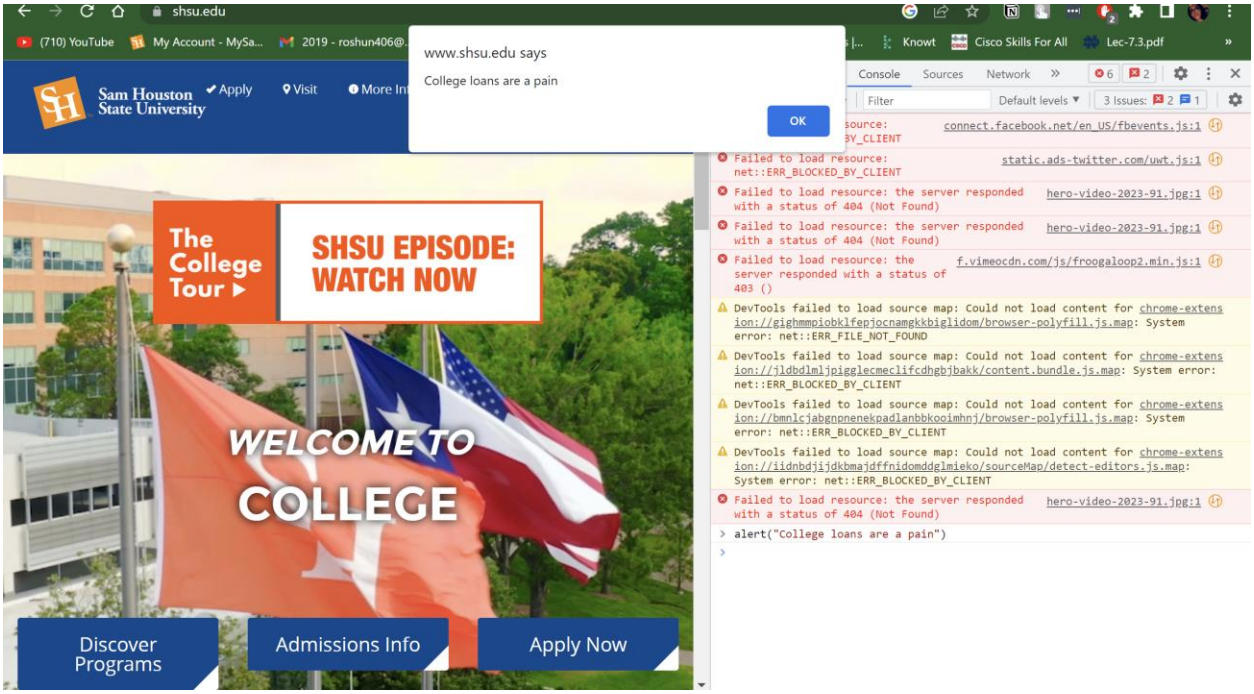
Task 1:


Sam Houston State University
Apply
Visit
More Info
Give
Alumni
KatSafe
Search
Menu
The College Tour
SHSU EPISODE: WATCH NOW
WELCOME TO
SAM HOUSTON STATE UNIVERSITY
Elements
Console
Sources
Network
SAM HOUSTON STATE UNIVERSITY == $0
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility


Sam Houston State University
Apply
Visit
More Info
Give
Alumni
KatSafe
Search
Menu
The College Tour
SHSU EPISODE: WATCH NOW
WELCOME TO
COLLEGE
Discover Programs
Admissions Info
Apply Now
Elements
Console
Sources
Network
College == $0
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility


Sam Houston State University
Apply
Visit
More Info
Give
Alumni
KatSafe
Search
Menu
The College Tour
SHSU EPISODE: WATCH NOW
WELCOME TO
COLLEGE
Discover Programs
Admissions Info
Apply Now
Elements
Console
Sources
Network
Styles
#ced615
HEX
No contrast information available
color: #ced615;
font-family: montserrat-bold, Helvetica, Arial, sans-serif;
text-shadow: 0 0 10px black;
text-transform: uppercase;
text-align: center;

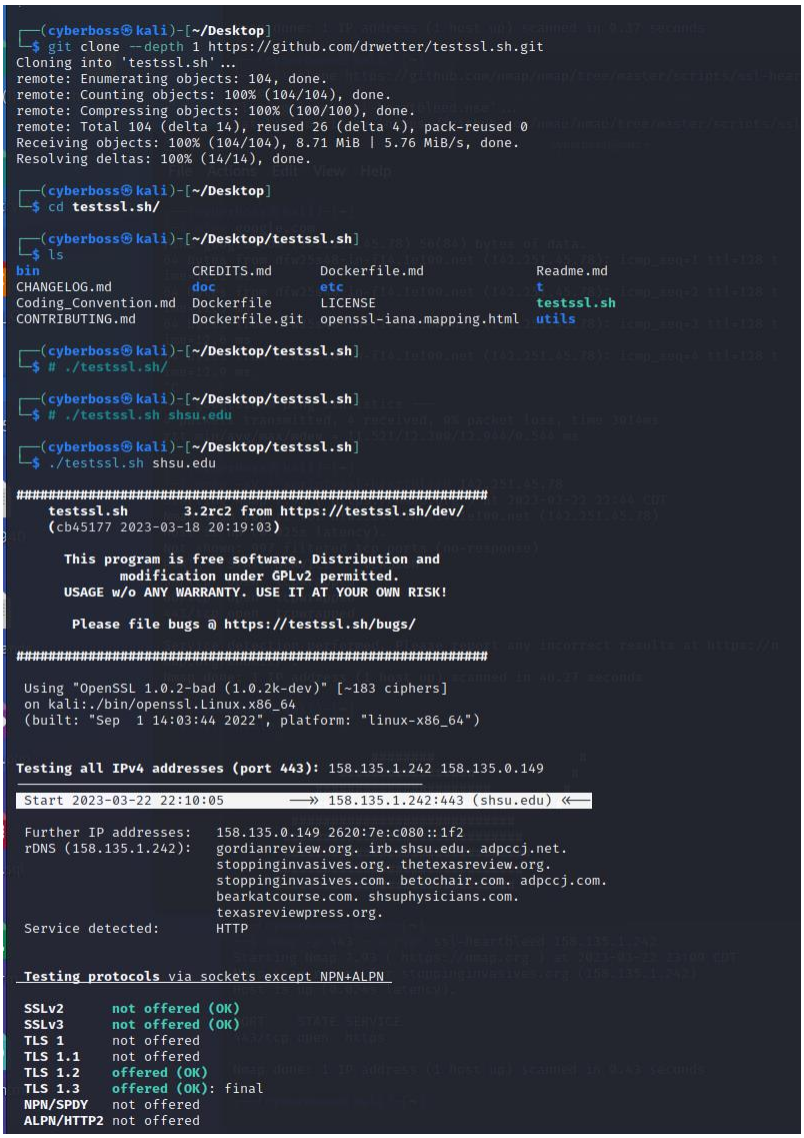

shsu.edu
www.shsu.edu says
College loans are a pain
OK
Sam Houston State University
The College Tour
SHSU EPISODE: WATCH NOW
WELCOME TO
COLLEGE
Discover Programs
Admissions Info
Apply Now
Console
Sources
Network
Failed to load resource: net::ERR_BLOCKED_BY_CLIENT
Failed to load resource: the server responded with a status of 404 (Not Found)
DevTools failed to load source map: Could not load content for chrome-extension://gighmmpiobklfepjocnamgkkbiglidom/browser-polyfill.js.map: System error: net::ERR_FILE_NOT_FOUND
DevTools failed to load source map: Could not load content for chrome-extension://jldbdlmljpigglecmeclifcdhgbjbakk/content.bundle.js.map: System error: net::ERR_BLOCKED_BY_CLIENT
DevTools failed to load source map: Could not load content for chrome-extension://bmnlcjabgnpnenekpadlanbbkooimhnj/browser-polyfill.js.map: System error: net::ERR_BLOCKED_BY_CLIENT
DevTools failed to load source map: Could not load content for chrome-extension://iidnbdjijdkbmajdffnidomddglmieko/sourceMap/detect-editors.js.map: System error: net::ERR_BLOCKED_BY_CLIENT
> alert("College loans are a pain")

SSL Heartbleed Detection

```
┌──(cyberboss㉿kali)-[~]
└─$ ping shsu.edu
PING shsu.edu (158.135.1.242) 56(84) bytes of data.
64 bytes from stoppinginvasives.org (158.135.1.242): icmp_seq=1 ttl=128 time=
18.4 ms
64 bytes from stoppinginvasives.org (158.135.1.242): icmp_seq=2 ttl=128 time=
17.7 ms
^C
── shsu.edu ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 17.681/18.026/18.371/0.345 ms
```

```
cyberboss@kali: ~
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 45.91 seconds

┌──(cyberboss㉿kali)-[~]
└─$ nmap -d --script ssl-heartbleed --script-args=vulns.showall -p 443 158.13
5.1.242
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-22 23:17 CDT
──────────── Timing report ────────────
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
──────────────────────────────────────
NSE: Using Lua 5.3.
NSE: Arguments from CLI: vulns.showall
NSE: Arguments parsed: vulns.showall
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating Ping Scan at 23:17
Scanning 158.135.1.242 [2 ports]
Completed Ping Scan at 23:17, 0.02s elapsed (1 total hosts)
Overall sending rates: 104.70 packets / s.
mass_rdns: Using DNS server 192.168.209.2
Initiating Parallel DNS resolution of 1 host. at 23:17
mass_rdns: 0.04s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 23:17, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, S
F: 0, TR: 1, CN: 0]
Initiating Connect Scan at 23:17
Scanning shsuphysicians.com (158.135.1.242) [1 port]
Discovered open port 443/tcp on 158.135.1.242
Completed Connect Scan at 23:17, 0.02s elapsed (1 total ports)
Overall sending rates: 55.92 packets / s.
NSE: Script scanning 158.135.1.242.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:17
NSE: Starting ssl-heartbleed against 158.135.1.242:443.
NSE: [ssl-heartbleed 158.135.1.242:443] Couldn't receive: EOF
NSE: [ssl-heartbleed 158.135.1.242:443] Couldn't receive: EOF
NSE: [ssl-heartbleed 158.135.1.242:443] we're done!
NSE: [ssl-heartbleed 158.135.1.242:443] Server does not support TLS Heartbeat
 Requests.
NSE: Finished ssl-heartbleed against 158.135.1.242:443.
Completed NSE at 23:17, 0.13s elapsed
Nmap scan report for shsuphysicians.com (158.135.1.242)
Host is up, received syn-ack (0.019s latency).
Scanned at 2023-03-22 23:17:06 CDT for 0s

PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-heartbleed:
|   NOT VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryp
tographic software library. It allows for stealing information intended to be
 protected by SSL/TLS encryption.
|     State: NOT VULNERABLE
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|       http://cvedetails.com/cve/2014-0160/
|_      http://www.openssl.org/news/secadv_20140407.txt
Final times for host: srtt: 18610 rttvar: 14361  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

TestSSL


┌──(cyberboss㉿kali)-[~/Desktop]
└─$ git clone --depth 1 https://github.com/drwetter/testssl.sh.git
Cloning into 'testssl.sh'...
remote: Enumerating objects: 104, done.
remote: Counting objects: 100% (104/104), done.
remote: Compressing objects: 100% (100/100), done.
remote: Total 104 (delta 14), reused 26 (delta 4), pack-reused 0
Receiving objects: 100% (104/104), 8.71 MiB | 5.76 MiB/s, done.
Resolving deltas: 100% (14/14), done.
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ cd testssl.sh/
┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ ls
bin CREDITS.md Dockerfile.md Readme.md
CHANGELOG.md doc etc t
Coding_Convention.md Dockerfile LICENSE testssl.sh
CONTRIBUTING.md Dockerfile.git openssl-iana.mapping.html utils
┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ # ./testssl.sh/
┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ # ./testssl.sh shsu.edu
┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ ./testssl.sh shsu.edu
testssl.sh 3.2rc2 from https://testssl.sh/dev/
(cb45177 2023-03-18 20:19:03)
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 @ https://testssl.sh/bugs/
Using "OpenSSL 1.0.2-bad (1.0.2k-dev)" [~183 ciphers]
on kali:./bin/openssl.Linux.x86_64
(built: "Sep 1 14:03:44 2022", platform: "linux-x86_64")
Testing all IPv4 addresses (port 443): 158.135.1.242 158.135.0.149
Start 2023-03-22 22:10:05 ⟶» 158.135.1.242:443 (shsu.edu) «⟵
Further IP addresses: 158.135.0.149 2620:7e:c080::1f2
rDNS (158.135.1.242): gordianreview.org. irb.shsu.edu. adpccj.net.
stoppinginvasives.org. thetexasreview.org.
stoppinginvasives.com. betochair.com. adpccj.com.
bearkatcourse.com. shsuphysicians.com.
texasreviewpress.org.
Service detected: HTTP
Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 not offered
TLS 1.1 not offered
TLS 1.2 offered (OK)
TLS 1.3 offered (OK): final
NPN/SPDY not offered
ALPN/HTTP2 not offered

```
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories

 NULL ciphers (no encryption)                  not offered (OK)
 Anonymous NULL Ciphers (no authentication)    not offered (OK)
 Export ciphers (w/o ADH+NULL)                 not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)  not offered (OK)
 Triple DES Ciphers / IDEA                     not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)        offered
 Strong encryption (AEAD ciphers) with no FS   not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Ci
pher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------
-----------------------------------------

SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256        ECDH 253   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256            ECDH 253   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384        ECDH 253   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384            ECDH 253   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305        ECDH 253   ChaCha20    256      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLSv1.3 (server order)
 x1301   TLS_AES_128_GCM_SHA256             ECDH 253   AESGCM      128      TLS_AES_128_GCM_SHA256
 x1302   TLS_AES_256_GCM_SHA384             ECDH 253   AESGCM      256      TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256       ECDH 253   ChaCha20    256      TLS_CHACHA20_POLY1305_SHA256

 Has server cipher order?     yes (OK) -- TLS 1.3 and below


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

 FS is offered (OK)           TLS_AES_256_GCM_SHA384
                              TLS_CHACHA20_POLY1305_SHA256
                              ECDHE-RSA-AES256-GCM-SHA384
                              ECDHE-RSA-AES256-SHA384
                              ECDHE-RSA-CHACHA20-POLY1305
                              TLS_AES_128_GCM_SHA256
                              ECDHE-RSA-AES128-GCM-SHA256
                              ECDHE-RSA-AES128-SHA256
 Elliptic curves offered:     prime256v1 secp384r1 X25519
 DH group offered:            ffdhe4096
 TLS 1.2 sig_algs offered:    RSA+SHA256 RSA+SHA384 RSA+SHA512
 TLS 1.3 sig_algs offered:    RSA-PSS+SHA256 RSA-PSS+SHA384 RSA-PSS+SHA512

 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281"
                              "EC point formats/#11" "key share/#51"
                              "supported versions/#43"
                              "extended master secret/#23"
 Session Ticket RFC 5077 hint no -- no lifetime advertised
 SSL Session ID support       yes
 Session Resumption           Tickets no, ID: yes
 TLS clock skew               Random values, no fingerprinting possible
```

```
TLS clock skew              Random values, no fingerprinting possible
Certificate Compression     none
Client Authentication       none
Signature Algorithm         SHA256 with RSA
Server key size             RSA 4096 bits (exponent is 65537)
Server key usage            Digital Signature, Key Encipherment
Server extended key usage   TLS Web Server Authentication, TLS Web Client Authentication
Serial                      14BD15A52F1F03AC5465919C (OK: length 12)
Fingerprints                SHA1 3ED72E001AF56E7D9C5F68FC64880D819C46E9DD
                            SHA256 51DCE03EFE443C2284216A3AE678B7DD38F8CDCCB09A2CC54D28BC23968FA667
Common Name (CN)            *.shsu.edu
subjectAltName (SAN)        *.shsu.edu shsu.edu
Trust (hostname)            Ok via SAN (same w/o SNI)
Chain of trust              Ok
EV cert (experimental)      no
Certificate Validity (UTC)  193 ≥ 60 days (2022-08-31 20:51 ⟶ 2023-10-02 20:51)
ETS/"eTLS", visibility info not present
Certificate Revocation List http://crl.globalsign.com/gsrsaovsslca2018.crl
OCSP URI                    http://ocsp.globalsign.com/gsrsaovsslca2018
OCSP stapling               not offered
OCSP must staple extension  --
DNS CAA RR (experimental)   available - please check for match with "Issuer" below: issue=globalsign.com
Certificate Transparency    yes (certificate extension)
Certificates provided       2
Issuer                      GlobalSign RSA OV SSL CA 2018 (GlobalSign nv-sa from BE)
Intermediate cert validity  #1: ok > 40 days (2028-11-21 00:00). GlobalSign RSA OV SSL CA 2018 ⟵ GlobalSign
Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

HTTP Status Code            302 Moved Temporarily, redirecting to "https://www.shsu.edu/"
HTTP clock skew             Got no HTTP time, maybe try different URL?
Strict Transport Security   not offered
Public Key Pinning          --
Server banner               BigIP
Application banner          --
Cookie(s)                   (none issued at "/") -- maybe better try target URL of 30x
Security headers            --
Reverse Proxy banner        --


 Testing vulnerabilities

Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
ROBOT                                     Server does not support any cipher suites that use RSA key transport
Secure Renegotiation (RFC 5746)           supported (OK)
Secure Client-Initiated Renegotiation     not vulnerable (OK) -- mitigated (disconnect within 6)
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression (OK)  - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
FREAK (CVE-2015-0204)                     not vulnerable (OK)
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, see
                                          https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=51DCE03EFE443C2284216A3AE678B7DD38F8CDCCB09A2CC54D2
8BC23968FA667
LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with ⩽ TLS 1.2
BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets

Browser                     Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
```

Running client simulations (HTTP) via sockets

Browser	Protocol	Cipher Suite Name (OpenSSL)	Forward Secrecy
Android 6.0	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Android 7.0 (native)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Android 8.1 (native)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	253 bit ECDH (X25519)
Android 9.0 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 10.0 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 11 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 12 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Chrome 79 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Chrome 101 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Firefox 66 (Win 8.1/10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Firefox 100 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
IE 6 XP	No connection		
IE 8 Win 7	No connection		
IE 8 XP	No connection		
IE 11 Win 7	TLSv1.2	ECDHE-RSA-AES128-SHA256	256 bit ECDH (P-256)
IE 11 Win 8.1	TLSv1.2	ECDHE-RSA-AES128-SHA256	256 bit ECDH (P-256)
IE 11 Win Phone 8.1	TLSv1.2	ECDHE-RSA-AES128-SHA256	256 bit ECDH (P-256)
IE 11 Win 10	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Edge 15 Win 10	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	253 bit ECDH (X25519)
Edge 101 Win 10 21H2	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Safari 12.1 (iOS 12.2)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Safari 13.0 (macOS 10.14.6)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Safari 15.4 (macOS 12.3.1)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Java 7u25	No connection		
Java 8u161	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK)	TLSv1.3	TLS_AES_128_GCM_SHA256	256 bit ECDH (P-256)
Java 17.0.3 (OpenJDK)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
go 1.17.8	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
LibreSSL 2.8.3 (Apple)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	253 bit ECDH (X25519)
OpenSSL 1.0.2e	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	253 bit ECDH (X25519)
OpenSSL 1.1.1d (Debian)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
OpenSSL 3.0.3 (git)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Apple Mail (16.0)	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	256 bit ECDH (P-256)
Thunderbird (91.9)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)

Rating (experimental)

Rating specs (not complete)	SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation	https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)	100 (30)
Key Exchange (weighted)	100 (30)
Cipher Strength (weighted)	90 (36)
Final Score	96
Overall Grade	A
Grade cap reasons	Grade capped to A. HSTS is not offered

Done 2023-03-22 22:11:24 [81s] ⟶» 158.135.1.242:443 (shsu.edu) «⟵

Start 2023-03-22 22:11:24 ⟶» 158.135.0.149:443 (shsu.edu) «⟵

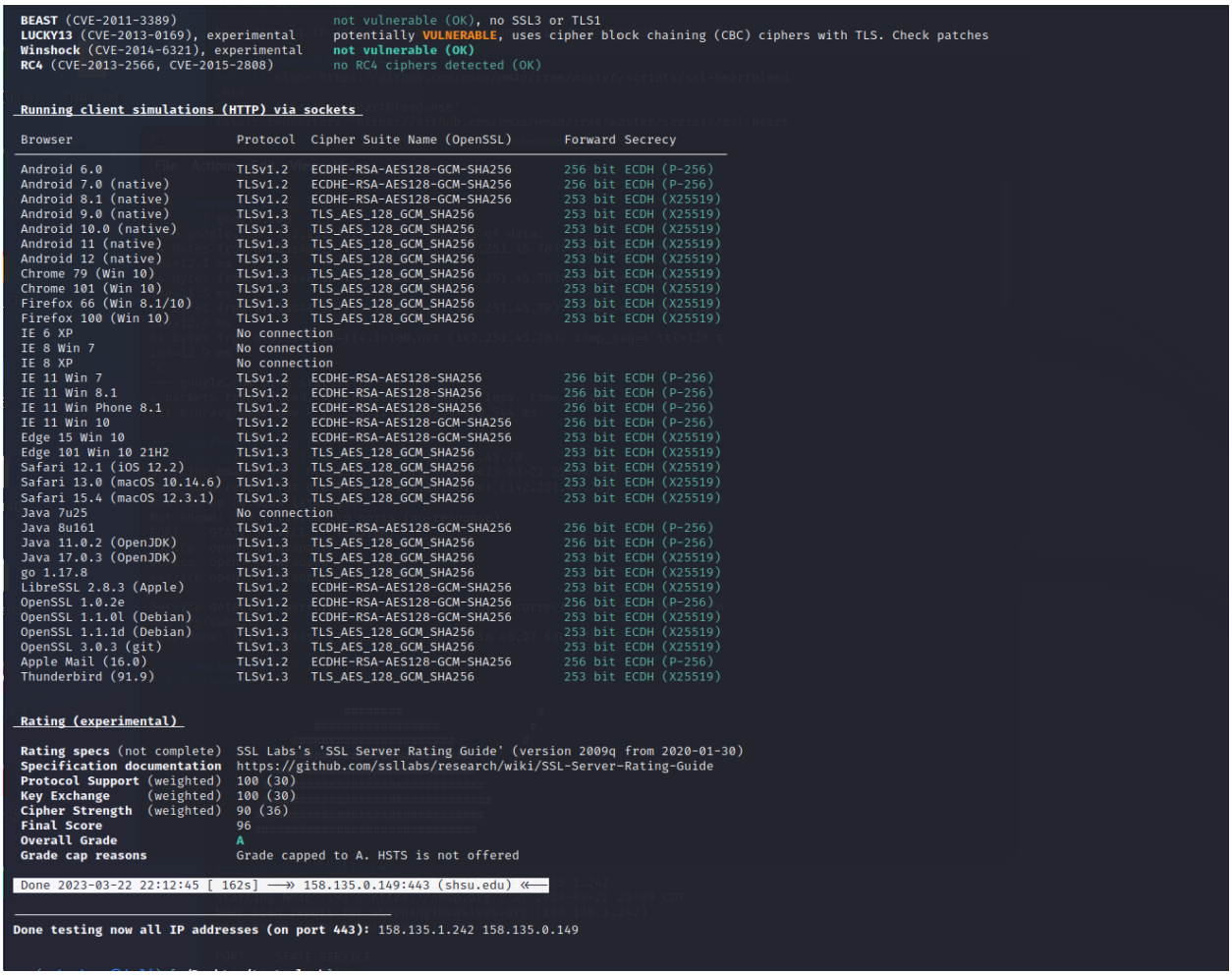
Further IP addresses: 158.135.1.242 2620:7e:c080::1f2
rDNS (158.135.0.149): bearkatcourse.com.
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2 **not offered (OK)**
SSLv3 **not offered (OK)**
TLS 1 not offered
TLS 1.1 not offered
TLS 1.2 **offered (OK)**

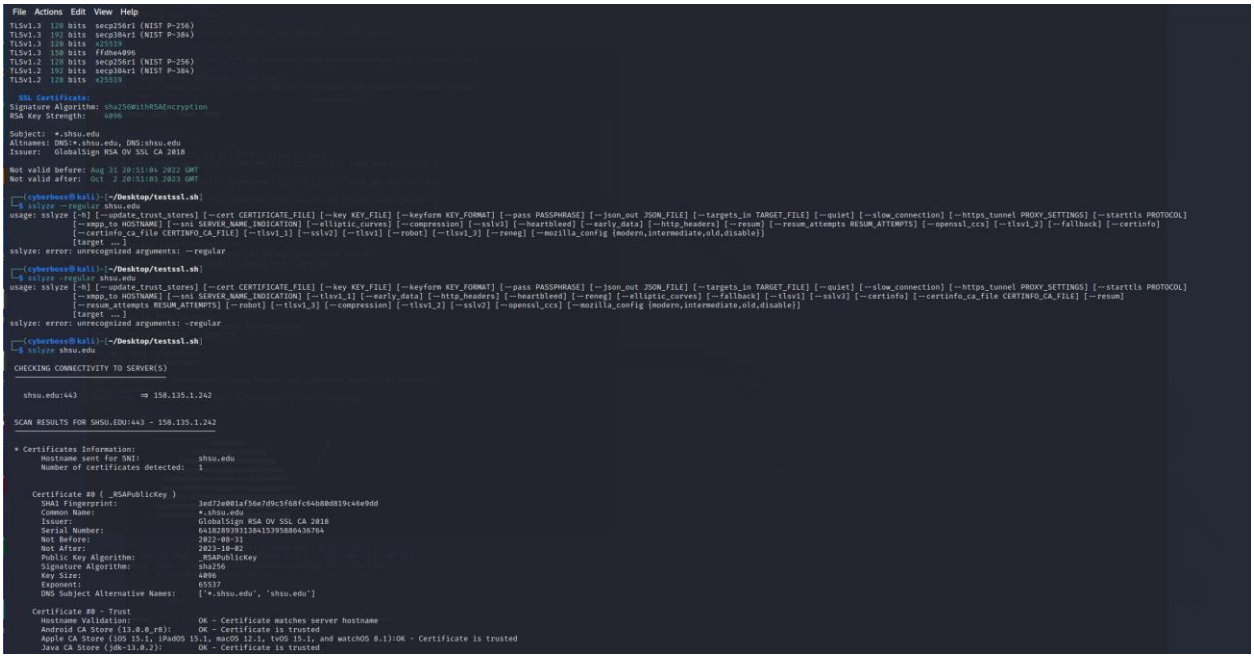
```
File  Actions  Edit  View  Help
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories

 NULL ciphers (no encryption)                   not offered (OK)
 Anonymous NULL Ciphers (no authentication)     not offered (OK)
 Export ciphers (w/o ADH+NULL)                  not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)   not offered (OK)
 Triple DES Ciphers / IDEA                      not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)         offered
 Strong encryption (AEAD ciphers) with no FS    not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 253   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 253   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20    256      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLSv1.3 (server order)
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128      TLS_AES_128_GCM_SHA256
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256      TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20    256      TLS_CHACHA20_POLY1305_SHA256

 Has server cipher order?     yes (OK) -- TLS 1.3 and below


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

 FS is offered (OK)           TLS_AES_256_GCM_SHA384
                              TLS_CHACHA20_POLY1305_SHA256
                              ECDHE-RSA-AES256-GCM-SHA384
                              ECDHE-RSA-AES256-SHA384
                              ECDHE-RSA-CHACHA20-POLY1305
                              TLS_AES_128_GCM_SHA256
                              ECDHE-RSA-AES128-GCM-SHA256
                              ECDHE-RSA-AES128-SHA256
 Elliptic curves offered:     prime256v1 secp384r1 X25519
 DH group offered:            ffdhe4096
 TLS 1.2 sig_algs offered:    RSA+SHA256 RSA+SHA384 RSA+SHA512
 TLS 1.3 sig_algs offered:    RSA-PSS+SHA256 RSA-PSS+SHA384 RSA-PSS+SHA512

 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281"
                              "EC point formats/#11" "key share/#51"
                              "supported versions/#43"
                              "extended master secret/#23"
 Session Ticket RFC 5077 hint no -- no lifetime advertised
 SSL Session ID support       yes
 Session Resumption           Tickets no, ID: yes
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      none
 Client Authentication        none
```

```
 TLS extensions (standard)    "renegotiation info/#65281"
                              "EC point formats/#11" "key share/#51"
                              "supported versions/#43"
                              "extended master secret/#23"
 Session Ticket RFC 5077 hint no -- no lifetime advertised
 SSL Session ID support       yes
 Session Resumption           Tickets no, ID: yes
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      none
 Client Authentication        none
 Signature Algorithm          SHA256 with RSA
 Server key size              RSA 4096 bits (exponent is 65537)
 Server key usage             Digital Signature, Key Encipherment
 Server extended key usage    TLS Web Server Authentication, TLS Web Client Authentication
 Serial                       14BD15A52F1F03AC5465919C (OK: length 12)
 Fingerprints                 SHA1 3ED72E001AF56E7D9C5F68FC64B80D819C46E9DD
                              SHA256 51DCE03EFE443C2284216A3AE678B7DD38F8CDCCB09A2CC54D28BC23968FA667
 Common Name (CN)             *.shsu.edu
 subjectAltName (SAN)         *.shsu.edu shsu.edu
 Trust (hostname)             Ok via SAN (same w/o SNI)
 Chain of trust               Ok
 EV cert (experimental)       no
 Certificate Validity (UTC)   193 ≥ 60 days (2022-08-31 20:51 ⟶ 2023-10-02 20:51)
 ETS/"eTLS", visibility info  not present
 Certificate Revocation List  http://crl.globalsign.com/gsrsaovsslca2018.crl
 OCSP URI                     http://ocsp.globalsign.com/gsrsaovsslca2018
 OCSP stapling                not offered
 OCSP must staple extension   --
 DNS CAA RR (experimental)    available - please check for match with "Issuer" below: issue=globalsign.com
 Certificate Transparency     yes (certificate extension)
 Certificates provided        2
 Issuer                       GlobalSign RSA OV SSL CA 2018 (GlobalSign nv-sa from BE)
 Intermediate cert validity   #1: ok > 40 days (2028-11-21 00:00). GlobalSign RSA OV SSL CA 2018 ⟵ GlobalSign
 Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code             302 Moved Temporarily, redirecting to "https://www.shsu.edu/"
 HTTP clock skew              Got no HTTP time, maybe try different URL?
 Strict Transport Security    not offered
 Public Key Pinning           --
 Server banner                BigIP
 Application banner           --
 Cookie(s)                    (none issued at "/") -- maybe better try target URL of 30x
 Security headers             --
 Reverse Proxy banner         --


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     Server does not support any cipher suites that use RSA key transport
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK) -- mitigated (disconnect within 6)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 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, see
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=51DCE03EFE443C2284216A3AE678B7DD38F8CDCCB09A2CC54D2
8BC23968FA667
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with ⩽ TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
```

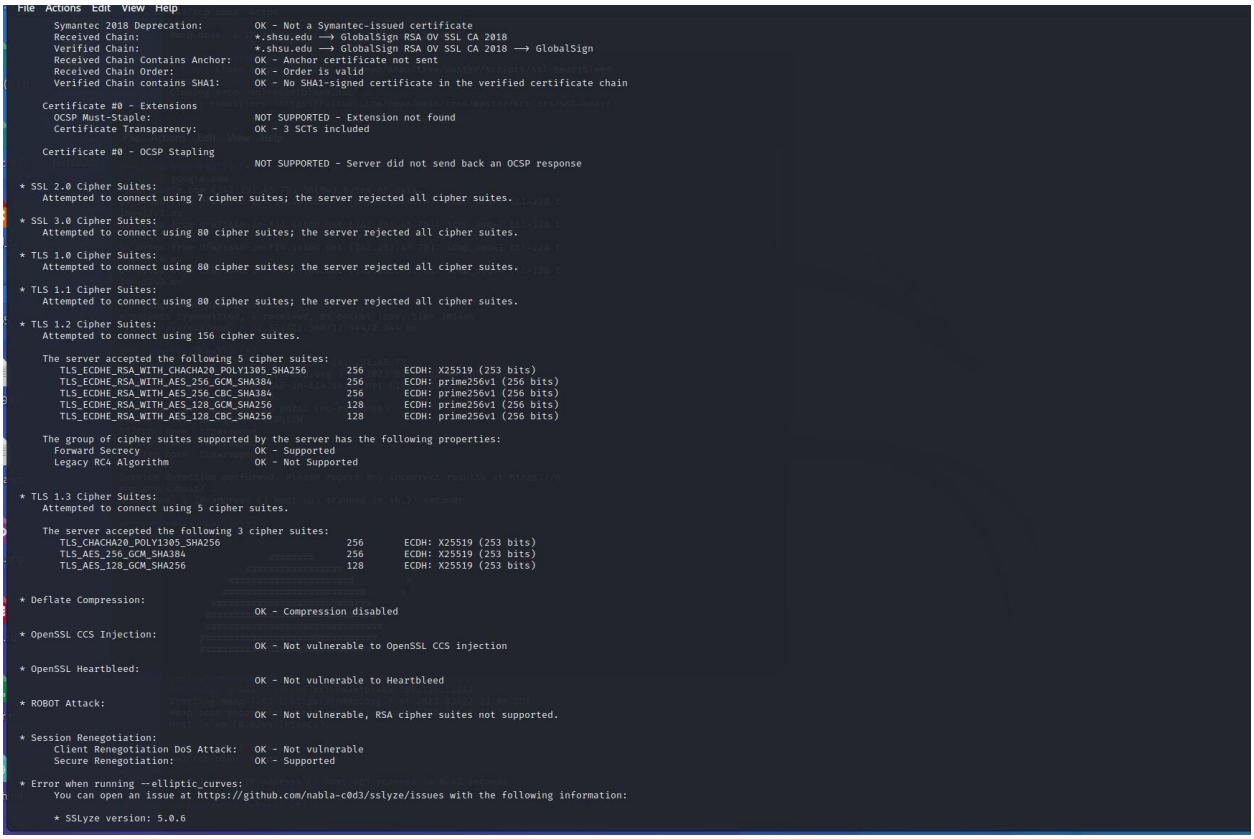


SSL Encryption Issue Detection

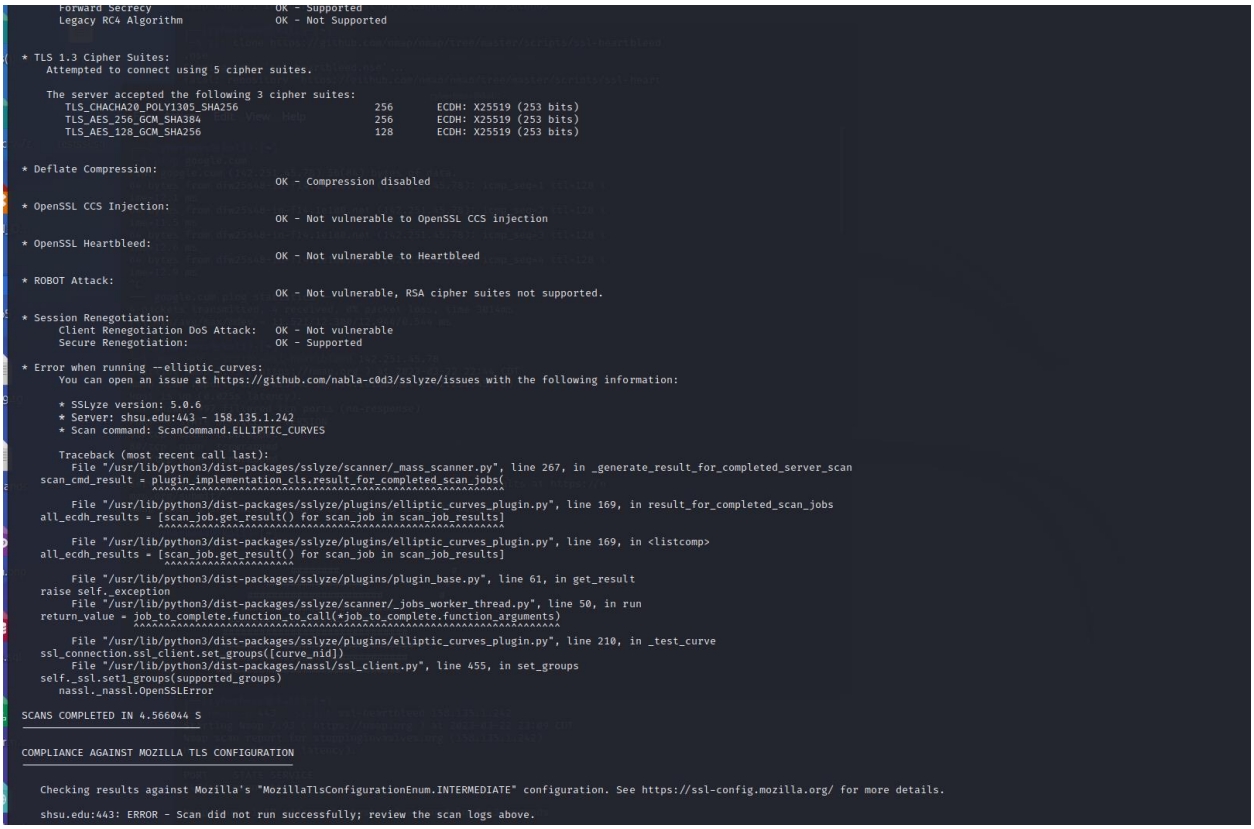
```
┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sudo apt install sslscan
[sudo] password for cyberboss:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
sslscan is already the newest version (2.0.15-0kali1).
sslscan set to manually installed.
The following packages were automatically installed and are no longer required:
  libpython3.10-dev python3.10 python3.10-dev python3.10-minimal
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1497 not upgraded.

┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sudo apt-get update
Get:1 https://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 https://kali.download/kali kali-rolling/main Sources [15.7 MB]
Get:3 https://kali.download/kali kali-rolling/non-free Sources [130 kB]
Get:4 https://kali.download/kali kali-rolling/contrib Sources [77.2 kB]
Get:5 https://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:6 https://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.0 MB]
Get:7 https://kali.download/kali kali-rolling/non-free amd64 Packages [217 kB]
Get:8 https://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [927 kB]
Get:9 https://kali.download/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:10 https://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [172 kB]
Fetched 81.8 MB in 2min 47s (491 kB/s)
Reading package lists ... Done

┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sslscan shsu.edu
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 158.135.0.149

Testing SSL server shsu.edu on port 443 using SNI name shsu.edu

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256         Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384         Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256   Curve 25519 DHE 253
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256    Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256        Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384    Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384        Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305    Curve 25519 DHE 253

  Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
```



```
File  Actions  Edit  View  Help
TLSv1.3  128 bits  secp256r1 (NIST P-256)
TLSv1.3  192 bits  secp384r1 (NIST P-384)
TLSv1.3  128 bits  x25519
TLSv1.3  158 bits  ffdhe4096
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  128 bits  x25519

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    4096

Subject:  *.shsu.edu
Altnames: DNS:*.shsu.edu, DNS:shsu.edu
Issuer:   GlobalSign RSA OV SSL CA 2018

Not valid before: Aug 31 20:51:04 2022 GMT
Not valid after:  Oct  2 20:51:03 2023 GMT

┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sslyze --regular shsu.edu
usage: sslyze [-h] [--update_trust_stores] [--cert CERTIFICATE_FILE] [--key KEY_FILE] [--keyform KEY_FORMAT] [--pass PASSPHRASE] [--json_out JSON_FILE] [--targets_in TARGET_FILE] [--quiet] [--slow_connection] [--https_tunnel PROXY_SETTINGS] [--starttls PROTOCOL]
              [--xmpp_to HOSTNAME] [--sni SERVER_NAME_INDICATION] [--elliptic_curves] [--compression] [--sslv3] [--heartbleed] [--early_data] [--http_headers] [--resum] [--resum_attempts RESUM_ATTEMPTS] [--openssl_ccs] [--tlsv1_2] [--fallback] [--certinfo]
              [--certinfo_ca_file CERTINFO_CA_FILE] [--tlsv1_1] [--sslv2] [--tlsv1] [--robot] [--tlsv1_3] [--reneg] [--mozilla_config {modern,intermediate,old,disable}]
              [target ...]
sslyze: error: unrecognized arguments: --regular

┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sslyze -regular shsu.edu
usage: sslyze [-h] [--update_trust_stores] [--cert CERTIFICATE_FILE] [--key KEY_FILE] [--keyform KEY_FORMAT] [--pass PASSPHRASE] [--json_out JSON_FILE] [--targets_in TARGET_FILE] [--quiet] [--slow_connection] [--https_tunnel PROXY_SETTINGS] [--starttls PROTOCOL]
              [--xmpp_to HOSTNAME] [--sni SERVER_NAME_INDICATION] [--tlsv1_1] [--early_data] [--http_headers] [--heartbleed] [--reneg] [--elliptic_curves] [--fallback] [--tlsv1] [--sslv3] [--certinfo] [--certinfo_ca_file CERTINFO_CA_FILE] [--resum]
              [--resum_attempts RESUM_ATTEMPTS] [--robot] [--tlsv1_3] [--compression] [--tlsv1_2] [--sslv2] [--openssl_ccs] [--mozilla_config {modern,intermediate,old,disable}]
              [target ...]
sslyze: error: unrecognized arguments: -regular

┌──(cyberboss㉿kali)-[~/Desktop/testssl.sh]
└─$ sslyze shsu.edu

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

  shsu.edu:443              => 158.135.1.242


 SCAN RESULTS FOR SHSU.EDU:443 - 158.135.1.242
 ---------------------------------------------

 * Certificates Information:
       Hostname sent for SNI:             shsu.edu
       Number of certificates detected:   1


     Certificate #0 ( _RSAPublicKey )
       SHA1 Fingerprint:                  3ed72e001af56e7d9c5f68fc64b80d819c46e9dd
       Common Name:                       *.shsu.edu
       Issuer:                            GlobalSign RSA OV SSL CA 2018
       Serial Number:                     64182893931384153958864636764
       Not Before:                        2022-08-31
       Not After:                         2023-10-02
       Public Key Algorithm:              _RSAPublicKey
       Signature Algorithm:               sha256
       Key Size:                          4096
       Exponent:                          65537
       DNS Subject Alternative Names:     ['*.shsu.edu', 'shsu.edu']

     Certificate #0 - Trust
       Hostname Validation:               OK - Certificate matches server hostname
       Android CA Store (13.0.0_r8):      OK - Certificate is trusted
       Apple CA Store (iOS 15.1, iPadOS 15.1, macOS 12.1, tvOS 15.1, and watchOS 8.1):OK - Certificate is trusted
       Java CA Store (jdk-13.0.2):        OK - Certificate is trusted
```



```
File  Actions  Edit  View  Help
       Symantec 2018 Deprecation:         OK - Not a Symantec-issued certificate
       Received Chain:                    *.shsu.edu --> GlobalSign RSA OV SSL CA 2018
       Verified Chain:                    *.shsu.edu --> GlobalSign RSA OV SSL CA 2018 --> GlobalSign
       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 #0 - Extensions
       OCSP Must-Staple:                  NOT SUPPORTED - Extension not found
       Certificate Transparency:          OK - 3 SCTs included

     Certificate #0 - 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 rejected all cipher suites.

 * TLS 1.1 Cipher Suites:
     Attempted to connect using 80 cipher suites; the server rejected all cipher suites.

 * TLS 1.2 Cipher Suites:
     Attempted to connect using 156 cipher suites.

     The server accepted the following 5 cipher suites:
       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256       256       ECDH: X25519 (253 bits)
       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH: prime256v1 (256 bits)
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             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


 * 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)


 * Deflate Compression:
                                          OK - Compression disabled

 * OpenSSL CCS Injection:
                                          OK - Not vulnerable to OpenSSL CCS injection

 * OpenSSL Heartbleed:
                                          OK - Not vulnerable to Heartbleed

 * ROBOT Attack:
                                          OK - Not vulnerable, RSA cipher suites not supported.

 * Session Renegotiation:
       Client Renegotiation DoS Attack:   OK - Not vulnerable
       Secure Renegotiation:              OK - Supported

 * Error when running --elliptic_curves:
       You can open an issue at https://github.com/nabla-c0d3/sslyze/issues with the following information:

       * SSLyze version: 5.0.6
```



When using the Heartbleed detection, the detection is used for if there is an error in an implementation that affects the SSL Library. Using Nmap for the detection I was able to not only find out that my target was not vulnerable, but that Nmap was able to discover an open port of 443/TCP with a service of https.

TestSSL offers many testing from protocol versions, cipher categories & preferences, and headers to vulnerabilities. I was able to observe that my target was not vulnerable but also had a cipher preference of TLS. I could also view the current sockets running under HTTP, and so much more.

With SSL Encryption Issue Detection, I was able to install and use the tool SSLyze. Using this tool, I was able to analyze the SSL configuration of a server. Though I was unable to receive a response in the beginning using -regular with the command, and removing the option I was able to receive an output. After scanning my target, I was able to observe that TLS v1.2 and TLS v1.3 were enabled while the rest of the protocols were disabled on the SSL server. As well as there

were many more advantages to this tool such as preferred server ciphers, gaining certificate information, cipher suites, etc.