Sri Lanka Institute of Information Technology

Bug Bounty Report - 01

Module: IE2062

Web Security

Year 2, Semester 2

Aazaf Ritha. J – IT23151710

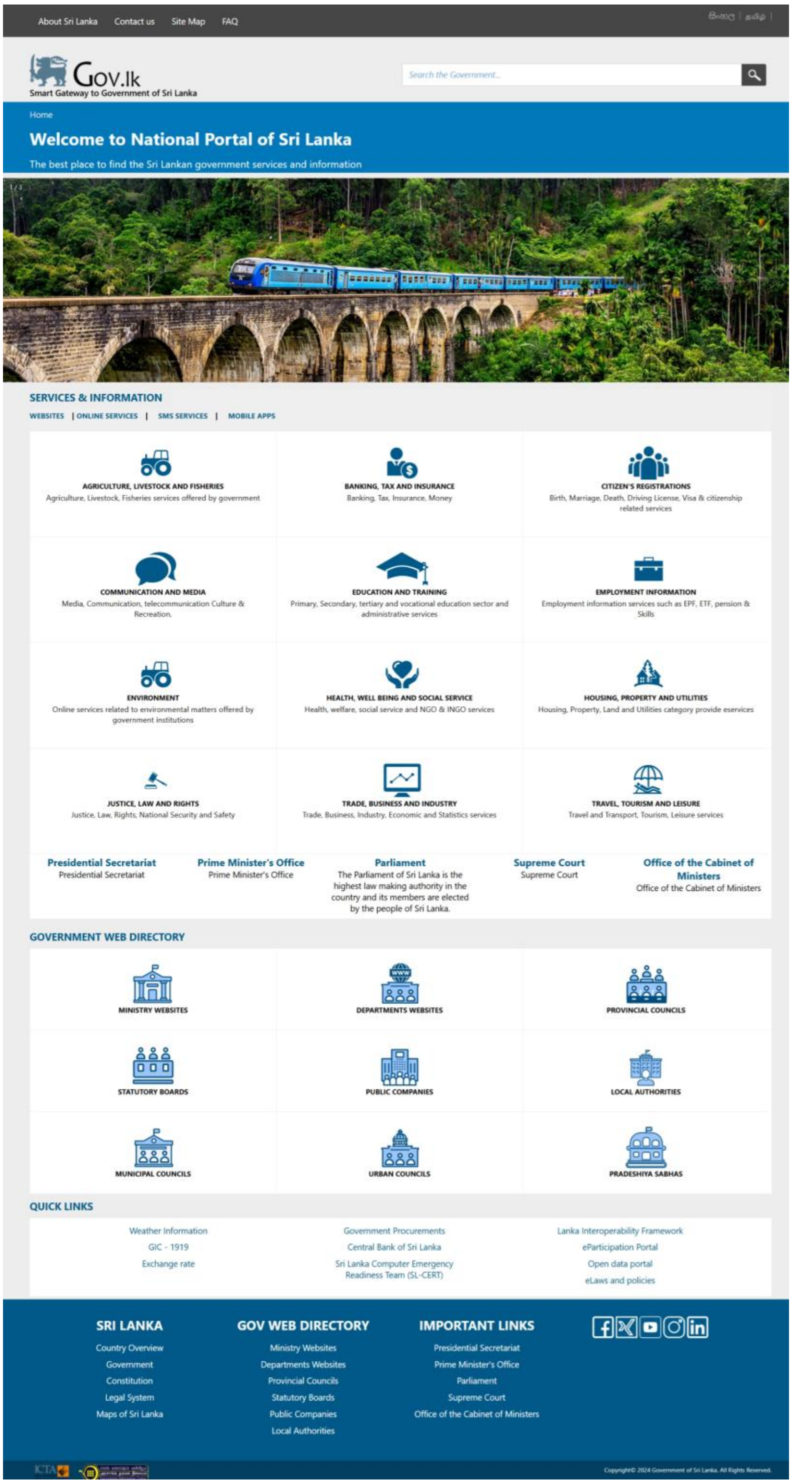
B.Sc. (Hons) in Information Technology

Specialized in Cyber Security

Table of Contents

Introduction

This report documents a critical **cryptographic vulnerability** found on the official www.gov.lk website. During SSL/TLS configuration analysis, multiple weaknesses were discovered, potentially allowing attackers to intercept, decrypt, and manipulate secure communications.



About Sri Lanka Contact us Site Map FAQ

සිංහල | தமிழ் |

Gov.lk
Smart Gateway to Government of Sri Lanka

Search the Government...

Home

Welcome to National Portal of Sri Lanka

The best place to find the Sri Lankan government services and information

SERVICES & INFORMATION

WEBSITES | ONLINE SERVICES | SMS SERVICES | MOBILE APPS

AGRICULTURE, LIVESTOCK AND FISHERIES
Agriculture, Livestock, Fisheries services offered by government

BANKING, TAX AND INSURANCE
Banking, Tax, Insurance, Money

CITIZEN'S REGISTRATIONS
Birth, Marriage, Death, Driving License, Visa & citizenship related services

COMMUNICATION AND MEDIA
Media, Communication, telecommunication Culture & Recreation.

EDUCATION AND TRAINING
Primary, Secondary, tertiary and vocational education sector and administrative services

EMPLOYMENT INFORMATION
Employment information services such as EPF, ETF, pension & Skills

ENVIRONMENT
Online services related to environmental matters offered by government institutions

HEALTH, WELL BEING AND SOCIAL SERVICE
Health, welfare, social service and NGO & INGO services

HOUSING, PROPERTY AND UTILITIES
Housing, Property, Land and Utilities category provide eservices

JUSTICE, LAW AND RIGHTS
Justice, Law, Rights, National Security and Safety

TRADE, BUSINESS AND INDUSTRY
Trade, Business, Industry, Economic and Statistics services

TRAVEL, TOURISM AND LEISURE
Travel and Transport, Tourism, Leisure services

Presidential Secretariat
Presidential Secretariat

Prime Minister's Office
Prime Minister's Office

Parliament
The Parliament of Sri Lanka is the highest law making authority in the country and its members are elected by the people of Sri Lanka.

Supreme Court
Supreme Court

Office of the Cabinet of Ministers
Office of the Cabinet of Ministers

GOVERNMENT WEB DIRECTORY

MINISTRY WEBSITES
DEPARTMENTS WEBSITES
PROVINCIAL COUNCILS
STATUTORY BOARDS
PUBLIC COMPANIES
LOCAL AUTHORITIES
MUNICIPAL COUNCILS
URBAN COUNCILS
PRADESHIYA SABHAS

QUICK LINKS

Weather Information
GIC - 1919
Exchange rate

Government Procurements
Central Bank of Sri Lanka
Sri Lanka Computer Emergency Readiness Team (SL-CERT)

Lanka Interoperability Framework
eParticipation Portal
Open data portal
eLaws and policies

SRI LANKA
Country Overview
Government
Constitution
Legal System
Maps of Sri Lanka

GOV WEB DIRECTORY
Ministry Websites
Departments Websites
Provincial Councils
Statutory Boards
Public Companies
Local Authorities

IMPORTANT LINKS
Presidential Secretariat
Prime Minister's Office
Parliament
Supreme Court
Office of the Cabinet of Ministers

ICTA

Copyright© 2024 Government of Sri Lanka. All Rights Reserved.

Vulnerability Title

Title - Cryptographic Failures in SSL/TLS Configuration

Risk Level- High

Domain - https://www.gov.lk/

Description

The target server (https://www.gov.lk/) exhibits multiple cryptographic weaknesses within its SSL/TLS configuration. It supports outdated and insecure protocols (TLS 1.0 and TLS 1.1), uses weak Diffie-Hellman (DH) parameters (1024-bit), and enables vulnerable cipher suites, including RSA-based key exchanges without forward secrecy. Additionally, the server allows compression (NULL compression), exposing it to **CRIME attacks**, and uses AES-CBC cipher modes that are susceptible to padding oracle attacks.

These weaknesses collectively compromise the confidentiality and integrity of secure communications, making it possible for an attacker to intercept, decrypt, or manipulate sensitive information. This vulnerability aligns with the OWASP Top 10 category **A02:2021 – Cryptographic Failures**, which highlights risks due to weak, outdated, or improperly configured cryptographic protections.

The issues include:

- Support for **TLS 1.0** and **TLS 1.1** (outdated protocols).
- Use of **1024-bit Diffie-Hellman** key exchange, which is weak.
- Lack of **forward secrecy** (via RSA key exchange).
- Vulnerability to **CRIME** due to **NULL compression**.
- Use of **AES-CBC** mode which is vulnerable to **padding oracle attacks**.

Exploiting these flaws could enable attacks such as man-in-the-middle interception, session hijacking, information leakage through compression side-channels, and ciphertext manipulation.

Affected Component

SSL/TLS Configuration: The affected component is the SSL/TLS protocol stacked on the server, which governs secure communication over HTTPS (port 443).

Diffie-Hellman Key Exchange: The server's cryptographic mechanism for establishing a shared secret key is vulnerable due to the use of weak 1024-bit DH parameters.

RSA Cipher Suites: The use of **RSA-based cipher suites** makes the server prone to lack of forward secrecy.

Compression Mechanism: The use of **NULL compression** enables the possibility of **CRIME** attacks.

Encryption Modes: The use of **AES-CBC** cipher suites exposes the server to padding oracle attacks.

Impact Assessment

Man-in-the-Middle (MITM) Attacks: Outdated protocols (TLS 1.0 and TLS 1.1) increase the risk of MITM attacks where an attacker could intercept and potentially decrypt or modify traffic.

Key Compromise: The weak Diffie-Hellman parameters (1024-bit) expose the server to the possibility of **key recovery** attacks, where an attacker can compute the shared secret key and decrypt the communication.

Loss of Confidentiality: The lack of forward secrecy (due to RSA key exchange) means that if the server's private RSA key is compromised in the future, past communications can be decrypted.

Information Disclosure: NULL compression enables **CRIME** attack, potentially leaking sensitive information like session cookies.

Integrity Vulnerability: AES-CBC's vulnerability to padding oracle attacks allows an attacker to manipulate the ciphertext, potentially modifying or decrypting encrypted data without access to the key.

Overall Impact: The server is highly vulnerable to cryptographic attacks, potentially leading to **data breaches**, **session hijacking**, and **eavesdropping** on encrypted communications.

Steps to Reproduce

Step 1: Perform SSL/TLS Enumeration with Nmap

Run the following ssl-enum-ciphers with Nmap command to enumerate supported SSL/TLS protocols and cipher suites:

```
nmap --script ssl-enum-ciphers -p 443 gov.lk
```

Observation:

TLS 1.0 and TLS 1.1 are still enabled.

Weak cipher suites and 1024-bit Diffie-Hellman key exchange parameters are identified.

Step 2: Deep SSL Scan using testssl.sh

Use the open-source tool testssl.sh for detailed analysis:

```
./testssl.sh gov.lk
```

Observation:

Confirms outdated protocols, weak key exchanges, vulnerable cipher modes (AES-CBC), and NULL compression support.

Step 3: Verify Protocol and Cipher Grades on SSL Org

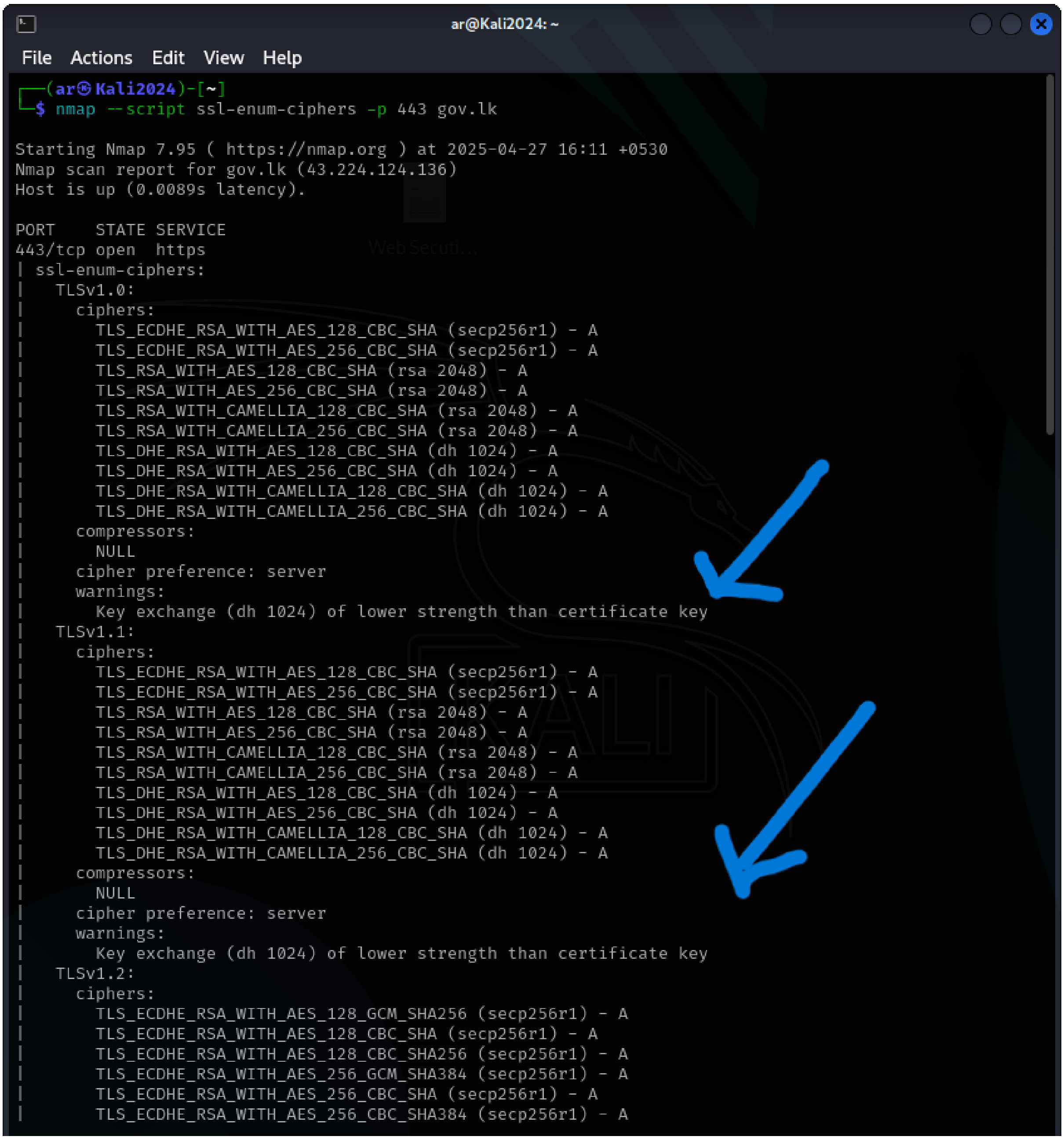
Visit https://www.ssl.org/, enter the target domain, and click "Submit".

Expected SSL Org Results:

- Protocol support for deprecated versions (TLS 1.0, 1.1)
- Overall Grade (A-F)

Proof of Concept (Screenshots or video link)

Nmap SSL/TLS Cipher Suite Enumeration

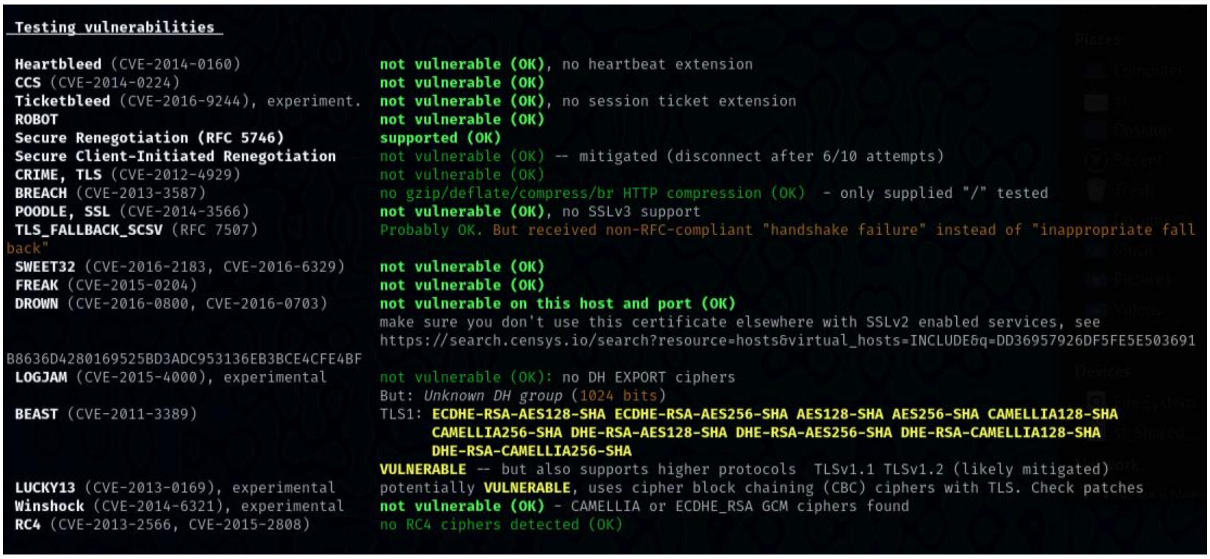


```
┌──(ar㉿Kali2024)-[~]
└─$ nmap --script ssl-enum-ciphers -p 443 gov.lk

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 16:11 +0530
Nmap scan report for gov.lk (43.224.124.136)
Host is up (0.0089s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Key exchange (dh 1024) of lower strength than certificate key
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Key exchange (dh 1024) of lower strength than certificate key
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
```

TestSSL.sh Security Assessment



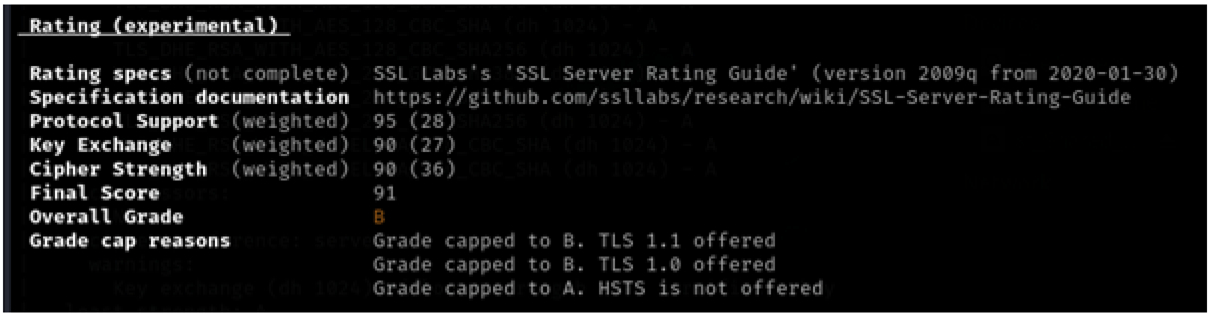
```
 Testing vulnerabilities 

 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                                         not vulnerable (OK)
 Secure Renegotiation (RFC 5746)               supported (OK)
 Secure Client-Initiated Renegotiation         not vulnerable (OK) -- mitigated (disconnect after 6/10 attempts)
 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)                  Probably OK. But received non-RFC-compliant "handshake failure" instead of "inappropriate fall
back"
 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=DD36957926DF5FE5E503691
B8636D4280169525BD3ADC953136EB3BCE4CFE4BF
 LOGJAM (CVE-2015-4000), experimental          not vulnerable (OK): no DH EXPORT ciphers
                                               But: Unknown DH group (1024 bits)
 BEAST (CVE-2011-3389)                         TLS1: ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-SHA AES256-SHA CAMELLIA128-SHA
                                                     CAMELLIA256-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA128-SHA
                                                     DHE-RSA-CAMELLIA256-SHA
                                               VULNERABLE -- but also supports higher protocols  TLSv1.1 TLSv1.2 (likely mitigated)
 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) - CAMELLIA or ECDHE_RSA GCM ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)            no RC4 ciphers detected (OK)
```

Summary of **www.gov.lk:443**, IP:**43.224.124.136**

Expiration	Oct 24, 2025 (180 days from today)
Certificate Trusted	**Yes**
Name Matches Domain	Yes
OCSP Revocation Check	**Good**
Certificate Type	Domain Validation (Single Domain)
Issuer	Sectigo Limited, GB
Issued To	
Common Name	www.gov.lk
Subject Alternative Names	Total SAN count: 1 www.gov.lk
Algorithm / Key Type & Size	sha256 / RSA 2048 bits
HSTS Supported	No
Supported TLS Versions	**TLSv1.0** , **TLSv1.1** , **TLSv1.2**
Certificate Chain Order	**Valid**
Chain Completeness	**Complete**

Overall Grade



```
 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)  95 (28)
 Key Exchange     (weighted)  90 (27)
 Cipher Strength  (weighted)  90 (36)
 Final Score                  91
 Overall Grade                B
 Grade cap reasons            Grade capped to B. TLS 1.1 offered
                              Grade capped to B. TLS 1.0 offered
                              Grade capped to A. HSTS is not offered
```

Proposed Mitigation or Fix

Disable TLS 1.0 and TLS 1.1:

Modify the server's SSL/TLS configuration to **only support TLS 1.2 and TLS 1.3**, as these protocols are secure and have mitigated the vulnerabilities present in older versions.

Upgrade Diffie-Hellman Key Exchange:

Use **2048-bit DH** parameters or switch to **ECDHE** (Elliptic Curve Diffie-Hellman Ephemeral) for key exchange.

Enable Forward Secrecy:

Prioritize **ECDHE cipher suites** over RSA cipher suites to ensure **forward secrecy**.

Disable Compression:

Disable **NULL compression** to prevent **CRIME** attacks.

Switch to AES-GCM:

Replace **AES-CBC** cipher suites **AES-GCM**, which provides both encryption and integrity, and is resistant to padding oracle attacks.

Testing and Validation:

After making changes, re-scan the server using tools like **SSL Labs** or **Nmap** to ensure that only secure protocols and ciphers are in use. Verify that **forward secrecy** is enabled, TLS 1.0 and 1.1 are disabled, and AES-GCM is being used.

Conclusion

The assessment of gov.lk revealed significant cryptographic weaknesses in the SSL/TLS configuration, including support for outdated protocols (TLS 1.0 and TLS 1.1), weak Diffie-Hellman key exchange parameters (1024-bit), lack of forward secrecy, vulnerable cipher suites (AES-CBC), and enabled compression (NULL compression), making the server susceptible to various cryptographic attacks such as Man-in-the-Middle (MITM), CRIME, and Padding Oracle attacks.

Immediate remediation is necessary to strengthen the server's security posture by disabling outdated protocols, upgrading cryptographic parameters, enabling forward secrecy, and switching to secure cipher modes (e.g., AES-GCM). Proper cryptographic configurations are critical to ensuring the confidentiality, integrity, and authenticity of sensitive user communications.

The identified vulnerabilities align with the OWASP Top 10 category **A02:2021 – Cryptographic Failures**, emphasizing the importance of securing encryption protocols and mechanisms against modern attack vectors.