भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
एस. टी. क्यू. सी. निदेशालय
इलेक्ट्रॉनिकी क्षेत्रीय परीक्षण प्रयोगशाला (पूर्व)
कोलकाता

सत्यमेव जयते

Government of India
Ministry of Electronics & Information Technology
STQC Directorate
ELECTRONICS REGIONAL TEST LABORATORY (EAST)
Kolkata

Project No. ES/EMBI/192009 23rd March 2021

# Web Application Security Audit

**Application Name** : **Website of Consulate General of India, St. Petersburg**

**Customer's Address** : Consulate General of India
35 Ryleeva Street, St. Petersburg, Leningrad Oblast
Russia, 191123

**Site URL** : https://www.cgispburg.gov.in

**Temporary URL** : https://www.cgispburg.gov.in

**Audit Performed by** : STQC IT Services, Kolkata

**Testing Date** : 27th July 2019 to 27th September 2019 (Stage-I)
23rd December 2019 to 2nd January 2020 and 7th February 2020 to 9th September 2020 and 22nd March 2021 (Stage-II)

## OWASP Top 10 (2017) Vulnerabilities

| Sl. No | Web Application Vulnerabilities | Observation | Remarks |
|---|---|---|---|
| A1 | Injection | No issues | -- |
| A2 | Broken Authentication | No issues | -- |
| A3 | Sensitive Data Exposure | No issues | -- |
| A4 | XML External Entities | No issues | -- |
| A5 | Broken Access Control | No issues | -- |
| A6 | Security Misconfiguration | No issues | -- |
| A7 | Cross-Site Scripting | No issues | -- |
| A8 | Insecure Deserialization | No issues | -- |
| A9 | Using Components with Known Vulnerabilities | No issues | -- |
| A10 | Insufficient Logging and Monitoring | No issues | -- |

## Recommendation:

1. The website may be hosted at https://www.cgispburg.gov.in,with Read Only permission.
2. Hardening / proper secured configuration of the Web Server, including implementation of HTTP security headers, disabling unnecessary HTTP methods, denying directory browsing etc. and Operating System need to be done in the production environment where the application will be hosted. Vulnerability assessment of the critical servers and perimeter devices should be done at regular intervals.
3. Source code of the website may be audited in Phase-II.

## Conclusion:

The Web Application is free from OWASP-Top 10 (2017) vulnerabilities and is safe for hosting, if configured as recommended.

ARPITA DATTA Digitally signed by ARPITA DATTA
Date: 2021.03.23 14:19:06 +05'30'

SUBHENDU DAS Digitally signed by SUBHENDU DAS
Date: 2021.03.23 14:24:17 +05'30'

Audited By: **Arpita Datta**
Scientist 'E'

Approved By: **Subhendu Das**
Scientist 'G' & Head, eSecurity Testing