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

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

Project No. ES/EMBI/171814

5th December 2019

Web Application Security Audit

Application Name	: Website of High Commission of India, Lilongwe, Malawi
Customer's Address	: High Commission of India, Lilongwe, Malawi : Plot No.55, Area-9 : PO Box 1482, Lilongwe, Malawi
Site URL	: http://www.hcililongwe.gov.in
Temporary URL	: http://www.hcililongwe.in/ : http://www.hcililongwe.gov.in/
Audit Performed by	: STQC IT Services, Kolkata
Testing Date	: 23rdApril 2018 to 26th April 2018 (Stage-I) : 2nd July 2019 to 3rd July 2019 and 16th August 2019 (Stage-II)

Table 1: 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 web application may be hosted at http://www.hcililongwe.gov.in, with Read Only permission.
2. It is advisable to deploy SSL for the website (https://www.hcililongwe.gov.in) to ensure authenticity and trust of the website.
3. Hardening / proper secured configuration of the Web Server, including implementing 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.

Conclusion:

The Web Application is free from OWASP-Top 10 (2017) vulnerabilities and is safe for hosting.

Audited By: **Arpita Datta** 5/12/19
Scientist 'E'

Approved By: **Subhendu Das** 5/12/19
Scientist 'G' & Head, eSecurity Testing