Friday, 2nd May 2025

Audit Certificate

Certificate Number	: 569/24-25/1425-2
Organization Name	: Consulate General of India,Hambantota, Sri Lanka
Address	: No. 107 B, New Road, Hambantota, Sri Lanka
Application Name	: Website of Consulate General of India-Hambantota, Sri Lanka
Production URL	: https://www.cgihambantota.gov.in/
Audit Period	: 4th April 2024 to 30th April 2025
Compliance Verification Date	: 30th April 2025
Hash Value	:b433217gcaejf362c1fc1495fece8ba3a01bc50b7fe128c0f1566afbba9y65d3
Path	: D:\xampp\htdocs\cgihambantota.gov.in\new
Certificate Validity	: 1 year (Valid till 29-04-2026)

The above web application has undergone through IT (Cyber) Security Audit by our organization through provided Production URL as per guidelines, advisories, white papers and vulnerability notes issued by Indian Computer Emergency Response Team (CERT-In). We also tested the web application against various Web Security Standards like Open Web Application Security Project (OWASP) Comprehensive Framework, Directions by CERT-In under Section 70B, Information Technology Act 2000, Guidelines for Secure Application Design, Development, Implementation & Operations SANS Top 25 Software Errors, Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), The Web Application Security Consortium (WASC) and Web Content Accessibility Guidelines (WCAG) etc. The audit was conducted on the given staging environment, not in production environment.

Conclusion: On the basis of audit outcomes, it is certified that the above application is safe from any known vulnerabilities as on date except Out-of-Band Resource Load & Host Header Injection vulnerabilities were not patched by the auditee as risk accepted.

The Certificate shall be deemed invalid if the underlying IT infrastructure of the web application gets modified after compliance audit.

Other Recommendations:

1. Web Server Security and the OS hardening need to be in place for the production server.
2. Web Application should comply with Guidelines for Secure Application Design, Development, Implementation & Operations issued by CERT-In.
3. Organization must comply with the Directions issued by CERT-In (Notification No. 20(3)/2022-CERT-In) dated 28 April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
4. The Developer Team must follow the Technical Guidelines on Software Bill of Materials (SBOM) issued by CERT-In dated 03.10.2024.

Prepared & Verified By
DRCBS-22-017 & DRCBS-24-045

Dr. CB SHARMA IPS (R)
Certified Lead Auditor ISMS (ISO/IEC 27001: 2013)
Founder & CEO