Tuesday, 19th May 2026

Audit Certificate

Certificate Number	: 051/26-27/2381
Organization Name	: Embassy of India, Sofia, Bulgaria
Address	: 4 Alfred Nobel Street,Geo Milev, Sofia 1113,Bulgaria
Application Name	: Official Website of the Embassy of India, Sofia, Bulgaria
Testing URL	: https://www.indembsofia.gov.in/
Production URL	: https://www.indembsofia.gov.in/
Audit Period	: 27th April 2026 to 19th May 2026
Compliance Verification Date	: 19th May 2026
Hash Value	:bf3d8538da5b57766bc3c5e0590653bd74a238f7482681c89a255defece8575 88da20cc03d9cee7e2ae6bb89702c888a
Path	: D:\xampp\htdocs\indembsofia.gov.in
Certificate Validity	: 1 year (18th May 2027)

The above web application has undergone Vulnerability Assessment & Penetration Testing, by our organization through provided testing URL as per guidelines, advisories, white papers and vulnerability notes, directions issued by CERT-In. We also tested the web application against various Web Security Standards like OWASP Application Security Verification Standard (ASVS), Open Source Security Testing Methodology Manual (OSSTMM3), Common Weakness Enumeration (CWE), Common Vulnerabilities Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), SANS Top 25 Software Errors.

The audit was conducted on the given production environment, not in staging environment.

Conclusion: Based on the audit outcomes, it is certified that the above application is free from any known vulnerabilities as of the audit date. However, the Host Header Injection vulnerability remains unresolved at this time and is pending remediation at the server level. Accordingly, the Audit Certificate is being issued based on the current assessment with this noted exception. The auditee assumes full responsibility for any potential risks, impacts, or security incidents and the audit team shall not be held liable for any consequences until the issue is fully remediated and verified.

The assessment represents the security posture of the application at the time of testing only. Any changes to application code, configuration, infrastructure, deployment architecture or security controls after the assessment period may invalidate this certificate. The certificate is valid only for the explicitly defined scope.

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. Auditee should also follow the Technical Guidelines on SBOM | QBOM & CBOM | AIBOM | HBOM | Version 2.0 issued by CERT-In dated 03.10.2025.

VANSH DAVE 19/05/2026

Prepared & Verified By
DRCBS-25-066 & DRCBS-24-048

19/5/2026

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

Dr. C. B. Sharma IPS R.
Founder & CEO

DR CBS CYBER SECURITY SERVICES LLP JAIPUR