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/WFIN/171802

9th August 2019

Web Application Security Audit

Application Name : Web Portal of NRI Cell

Organization Name : Finance Department, Govt. of West Bengal
: 11th Floor, Room No: 1102, NABANNA, MANDIRTALA
: 325, S.C Chatterjee Road, Howrah - 712225

Production URL : http://www.cmo.wb.gov.in

Temporary URL : http://nriwestbengal.gov.in

Audit Performed by : STQC IT Services, Kolkata

Testing Date : 29th January 2018 to 1st February 2018 (Cycle-1)
: 20th February to 21st February 2018 (Cycle-2)
: 10th July 2018 (Verification of Cycle-2)

Table 1: OWASP Top 10 Vulnerabilities (2013)

Sl. No	Web Application Vulnerabilities	Observation	Remarks
A1	Injection	No issues	--
A2	Broken Authentication and Session Management	No issues	--
A3	Cross-site Scripting	No issues	--
A4	Insecure Direct Object Reference	No issues	--
A5	Security Misconfiguration	No issues	--
A6	Sensitive Data Exposure	Login parameters are transmitted over an unencrypted channel.	SSL should be implemented in production server and login parameters should be transmitted over SSL (Recommendation-2).
A7	Missing Function Level Access Control	No issues	--
A8	Cross-site Request Forgery	No issues	--
A9	Using Components with Known Vulnerabilities	Version of jQuery (1.3.2) is vulnerable to reported security issues.	jQuery may be upgraded to the latest secure version (Recommendation-3).
A10	Unvalidated Redirects and Forwards	No issues	--

Recommendation:

1. The web application may be hosted at http://www.cmo.wb.gov.in,with Read Only permission.
2. The /HCM folder, which holds authentication module, may be deployed over SSL.
3. jQuery may be upgraded to the latest secure version.
4. Hardening / proper secured configuration of the Web Server 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 conducted at regular intervals.

Conclusion:

The Web Application is free from OWASP-Top 10 (2013) vulnerabilities, and is safe for hosting, if configured as recommended.

9/8/2019
Prepared By: **Arpita Datta**
Scientist 'E'

9/8/2019
Approved By: **Subhendu Das**
Scientist 'G' and Head, eSecurity