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

5th January 2018

Application Security Audit

Application Name : Website of Raja Rammohun Roy Library Foundation

Organization Name : Raja Rammohun Roy Library Foundation
: Block DD-34, Sector-I, Salt Lake City, Kolkata - 700064

Site URL : http://rrrlf.gov.in

Temporary URL : http://rrrlf.nic.in/default.aspx

Audit Performed by : STQC IT Services, Kolkata

Testing Date : 8th March 2017 to 17th April 2017 (Cycle-1)
: 4th July 2017 to 18th July 2017 (Cycle-2)
: 20th September 2017 to 22nd September 2017 (Final verification)

Observation :

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	User credentials from the login page are transferred to the server over an unencrypted connection.	Login parameters should be transmitted over encrypted channel (Recommendation-2).
A7	Missing Function Level Access Control	No issues	--
A8	Cross-site Request Forgery	No issues	--
A9	Using Components with Known Vulnerabilities	No issues	--
A10	Unvalidated Redirects and Forwards	No issues	--

Recommendation:

1. The web application may be hosted at production URL http://rrrlf.gov.in, with Read & Script Execute permission.
2. The login modules in the production site, corresponding to the test site http://rrrlf.nic.in/TourDetails/Login.aspx and http://rrrlf.nic.in/Security/Login.aspx, are to be deployed over SSL.
3. 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 done at regular intervals.

Conclusion:

The Web Application is free from OWASP-Top 10 2013, except the issue related to Sensitive Data Exposure (A6). The issues should be taken care of in the production environment using SSL for the folders holding authentication modules.

5/1/2018

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

Approved By: **Subhendu Das**
Scientist-G & Head, IT Services