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

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

22nd May 2015

Web Application Security Audit

Application Name	: Service Record Monitoring System (SRMS) for the Cadre Officers of Audit & Accounts Service,
Organization Name	: Finance Department, Government of West Bengal
Site URL	: http://wbaasprofile.gov.in
Test URL / Temporary URL	: http://wbdemo23.nic.in
Audit Performed by	: STQC IT Services, Kolkata
Testing Date	: 24th February to 9th April 2015 (Cycle-1) : 1st May 2015 to 12th May 2015 (Cycle-2)
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 of the application.	TRACE method, which is not necessary for a production application, is enabled in the staging server.
A6	Sensitive Data Exposure	Login parameters are transmitted over an unencrypted channel.	SSL may be deployed for transmitting login parameters.
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 the production URL http://wbaasprofile.gov.in with Read and Script Execute permission.
2. The entire website is 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.
4. There should be mechanism to ensure that there are no broken links (internal as well as external) or Page not found errors.

Conclusion:

The Web Application is free from OWASP-Top 10 2013 and any other known vulnerabilities, except the issue related to Sensitive Data Exposure (A6). The issues should be taken care of in the production environment using SSL for entire website.

22/5/2015

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

22/5/15

Approved By: **B.K. Mondal**
Scientist 'G' & Head, IT Services