Ref. No. : STQC IT-ERTL (N)/EVoting/Right2vote/AS/02/2019/Cert-02   Dated: 11.02.2019

Application Security Test Certificate

Web Site Tested:	Right2Vote Web application
Test URL:	https://right2vote.org/
Host URL :	https://right2vote.in/
Test /Audit Agency:	STQC IT Services, ERTL (North) New Delhi
Testing/ Audit Date(s):	I Cycle: 12th December 2018 to 4th January 2019, II Cycle: 28th January 2019 to 1st February 2019, III Cycle : 7th February 2019 to 8th February 2019

Test/ Audit Result Summary:

OWASP Top 10 (2017)	Web Application Vulnerabilities	Compliance	Remark
A1	Injection	Satisfactory	Nil
A2	Broken Authentication	Satisfactory	Nil
A3	Sensitive Data Exposure	Satisfactory	Nil
A4	XML External Entities (XXE)	Satisfactory	Nil
A5	Broken Access Control	Satisfactory	Nil
A6	Security Misconfiguration	Satisfactory	Nil
A7	Cross-Site Scripting (XSS)	Satisfactory	Nil
A8	Insecure Deserialization	Satisfactory	Nil
A9	Using Components with Known Vulnerabilities	Satisfactory	Nil
A10	Insufficient Logging & Monitoring	Satisfactory	Nil

Note: For details please refer Security Test Report Ref. NO. STQC IT-ERTL (N)/EVoting/Right2vote/AS/TR/02/2019/37, dated 11th February, 2019.

Recommendations:

1. Auditing for Right2Vote web application of Right2Vote was done from 12th December 2018 to 04th January 2019, as per the OWASP Top 10 2017 by STQC IT, ERTL (N). The follow-up testing/ auditing was done from 28th January to 1st February 2019, then from 07th to 08th February (Final Cycle) and there is no pending nonconformity w.r.t OWASP Top 10 2017 as on 11th February 2019.
2. This is a PHP based application. It can be hosted with Read permissions only.
3. Sensitive data must be suitably protected using TLS ver1.2.
4. User access log & transaction log of the Web application should be enabled and stored on a separate secure server.
5. Before deploying the Website in the production environment, the hardening of IT infrastructure (Network, Hosts and OS) must be ensured.
6. **This Certificate is valid for one year from the date of issue or till any change in the code of the application or any new vulnerability is discovered whichever is earlier.**

Conclusion:

The Web application is free from OWASP Top 10, 2017 (and any other known) vulnerabilities and is safe for hosting.

Tested by:

Charupriya 11/02/19

Charupriya Bisht, Scientist "B"

Pinky 11/02/2019

Pinky Bai, Scientist "B"

Approved by:

Sanjeev Kumar 11/02/19

Sanjeev Kumar, Scientist "F"