



Government of India

Ministry of Electronics & Information Technology
Standardisation, Testing & Quality Certification
Directorate

Electronics Niketan, 6 CGO Complex,
Lodhi Road, New Delhi-110003.

सत्यमेव जयते

भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
मानकीकरण, परीक्षण एवं गुणवत्ता प्रमाणन निदेशालय
इलेक्ट्रॉनिक्स निकेतन, 6, सीजीओ कॉम्प्लेक्स,
लोधी रोड, नई दिल्ली - 110003

WEB APPLICATION SECURITY COMPLIANCE STATUS

Ref. Test Report No.: STQC IT-ERTL(N)/DoT/AS/TR/07/2022/222

Dated: 05/07/2022

Identification of the Web Application: DoT website

Organization Name: Department of Telecommunication

Test / Staging URL: http://10.247.19.221

Production URL: http://www.dot.gov.in

Test Laboratory: STQC IT-ERTL (N), New Delhi

Date of Testing: 11.05.2022 - 05.07.2022

TEST RESULT SUMMARY:

OWASP Top10	Web Application Vulnerabilities	Compliance	Remark
A1	Injection	Satisfactory	
A2	Broken Authentication	Satisfactory	
A3	Sensitive Data Exposure	Satisfactory	
A4	XML External Entities (XXE)	Satisfactory	
A5	Broken Access Control	Satisfactory	
A6	Security Misconfiguration	Satisfactory	
A7	Cross-Site Scripting (XSS)	Satisfactory	
A8	Insecure Deserialization	Satisfactory	
A9	Using Components with Known Vulnerabilities	Satisfactory	
A10	Insufficient Logging & Monitoring	Satisfactory	

RECOMMENDATIONS:

- The web application is recommended to be hosted at <http://www.dot.gov.in> with 'Read Only permission'.
- Security hardening / secured configuration of the Web Server, Network devices and Operating System are recommended for the hosting environment.
- Regular security vulnerability assessment of the hosting It infrastructure (servers and network devices) are recommended
- Sensitive data must be suitably protected using TLS ver1.2 or above and use the proper server certificate.
- SSL should be enforced on the production server (as specified in Section 4.1 Sr. No. 13)

CONCLUSION:

This statement of compliance is issued for the specific version of the Web Application and remains valid for two years from the date of issue. This Statement of compliance becomes null and void, if changes are made to the Application code related to the security architecture & security mechanisms for handling inputs, user Access Control, user Authentication & Authorization, Session Management, handling sensitive data, Data encryption at Rest & in Motion, handling of runtime errors & external resources. This statement of compliance state is also become null and void if there is any change in underlying IT infrastructure or their configuration, hosting the Web Application and if any new vulnerabilities are discovered.

The Web application is free from OWASP Top 10, 2017 and any other known vulnerability and is safe for hosting based on the fulfillment of the recommendations mentioned above.

Manish Selal

Digitally signed by Manish Selal
DN: C=IN, OU=IT, O=STQC,
CN=Manish Selal,
E=manishselal@stqc.gov.in
Reason: I attest to the accuracy
and integrity of this document
Location: ERTL(N)
Date: 2022.07.29 10:42:
44+05'30'
Foxit Reader Version: 10.1.0

Issued By:

Manish Selal