



**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.:** ITB/g/WAS(TR)-1/14980722

**Dated:**

25/07/2022

**Identification of the Web Application:** NAAC- Online Assessment and Accreditation Process

**Organization Name:** M/s National Assessment and Accreditation Council (NAAC)

**Test / Staging URL:** <http://218.248.45.210/naacfeb7/public/index.php>

**Production URL:** <https://assessmentonline.naac.gov.in>

**Test Laboratory:** STQC IT Services, STQC Directorate, ETDC Bangalore

**Date of Testing:** Start Date: 18-02-2022, Completion Date: 14-07-2022

**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:**

1. The web application is recommended to be hosted at **STPI Data Centre, Bengaluru** with 'Read Only permission'.
2. Security hardening / secured configuration of the Web Server, Network devices and Operating System are recommended for the hosting environment.
3. Regular security vulnerability assessment of the hosting It infrastructure (servers and network devices) are recommended
4. All the sensitive data must be suitably protected using TLS ver1.2 or higher.
5. User access log & transaction log of the Web application should be enabled and stored on a separate secure server.

**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.



Issued By:

S P Thares Kumar