



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

इलेक्ट्रॉनिक्स 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(Kol)/ES/NWDA/212202/1284

Dated: 25/07/2022

Identification of the Web Application: Departmental website of NWDA

Organization Name: National Water Development Agency, Ministry of Jal Shakti, Govt. of India, New Delhi

Test / Staging URL: http://nwda.gov.in/nwda_upgrade/content <https://demoarea.1akal.in/NWDA/content/index.php>

Production URL: <http://nwda.gov.in>

Test Laboratory: STQC IT Services, ERTL (East), Kolkata

Date of Testing: 02-Dec-21 to 15-Feb-22 (Assessment); 21-Mar-22 to 22-Jul-22 (Closure Verification)

TEST RESULT SUMMARY:

OWASP Top10	Web Application Vulnerabilities	Compliance	Remark
A1	Injection	Satisfactory	
A2	Broken Authentication	Satisfactory	
A3	Sensitive Data Exposure	Satisfactory	If configured as Recommendation-4.
A4	XML External Entities (XXE)	Satisfactory	
A5	Broken Access Control	Satisfactory	
A6	Security Misconfiguration	Satisfactory	If configured as Recommendation-5.
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://nwda.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.
- Entire site should be deployed over SSL (HTTPS) to ensure better data security.
- As security headers are not configured properly or missing, production server should be configured with proper security headers.

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.

TAPAS
BANDYOPADHYAY

Digitally signed by TAPAS
BANDYOPADHYAY
Date: 2022.07.25 14:28:46 +05'30'

Issued By:

Tapas Bandyopadhyay Sc F