



**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.:**

**Dated:**

**Identification of the Web Application:**

**Organization Name:**

**Test / Staging URL:**

**Production URL:**

**Test Laboratory:**

**Date of Testing:**

**TEST RESULT SUMMARY:**

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

**RECOMMENDATIONS:**

1. The web application is recommended to be hosted at \_\_\_\_\_ 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

**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: