



## Government of West Bengal

This document having UDIN **25-G-GA001220-C-1746193294246** has been created by **WBEIDC - GSTIN : 19AAACW2411Q1Z1** with authorised person's Aadhaar no XXXXXXXX0487 on **07:11PM, May 02, 2025**.

This document is available at UDIN platform till 07:11PM, May 02, 2026.



Authorised Signatory  
(E-signed)  
Department of IT&E

## West Bengal Electronics Industry Development Corporation Limited

(A Government of West Bengal Undertaking)

Webel Bhavan, Block: EP & GP, Sector -V, Bidhannagar, Salt Lake, Kolkata: 700 091, West Bengal



# SAFE TO HOST CERTIFICATE

## WEB APPLICATION SECURITY COMPLIANCE REPORT

**Test Report ID:** WEBEL/G/CONSUMER AFFAIRS DEPARTMENT/2425/043

**Name of Test Laboratory:** West Bengal Electronics Industry Development Corporation Limited (WEBEL)

**Identification of the Web Application:** Online Consumer Grievance Lodging and Redressal System

**Organization Name:** Consumer Affairs Department, Govt. of West Bengal, 3rd Floor, Kreta Suraksha Bhawan, 11A, Mirza Ghalib Street, Kolkata - 700087

**Audited URL:** http://demowbconsumers.nic.in

**Production URL:** https://wbconsumers.gov.in

**Date of Testing:** 1<sup>st</sup> cycle completed on 13-11-2024, 2<sup>nd</sup> cycle completed on 27-12-2024, 3<sup>rd</sup> cycle completed on 24-04-2025

### Test Result Summary

OWASP Top 10	Web Application Vulnerabilities	Compliance	Remark
A01:2021	Broken Access Control	Satisfactory	
A02:2021	Cryptographic Failures	Satisfactory	
A03:2021	Injection	Satisfactory	
A04:2021	Insecure Design	Satisfactory	
A05:2021	Security Misconfiguration	Satisfactory	
A06:2021	Vulnerable and Outdated Components	Satisfactory	
A07:2021	Identification and Authentication Failures	Satisfactory	
A08:2021	Software and Data Integrity Failures	Satisfactory	
A09:2021	Security Logging and Monitoring Failures	Satisfactory	
A10:2021	Server-Side Request Forgery	Satisfactory	

### Recommendations

- The web application is recommended to be hosted at SDC
- Application should be deployed on a hardened server & operating system.
- SSL should be deployed before putting on the production server.
- Server-side issue should be taken care of by hosting provider.
- Conduct proactive testing periodically & ensure any new changes introduced in the application undergo security testing before they are published on the network.

### Conclusion

- This SAFE TO HOST CERTIFICATE is issued for the specific version of the Web Application.
- This SAFE TO HOST CERTIFICATE is valid for ONE YEAR from the date of issue or till any changes made in the code of the application or any new vulnerability is discovered whichever is earlier.
- This SAFE TO HOST CERTIFICATE will become 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 SAFE TO HOST CERTIFICATE will 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 on: 02-05-2025**

**Issued by: Vice President  
(Delivery & Execution)**

