

# Safe to Host Certificate

**Dated:** 06<sup>th</sup> May 2026

**Cert No.:** CNPL26-27080426086

|                                |  |
|--------------------------------|--|
| <b>Client Name:</b>            | CSIR-Human Resource Development Group  |
| <b>Client Address:</b>         | CSIR Complex, Library Avenue, Pusa, New Delhi – 110012, India  |
| <b>Application Name:</b>       | CSIR-Human Resource Development Group Web Application  |
| <b>Purpose of Application:</b> | The CSIR-HRDG website provides authoritative information on HRDG schemes, programs, and activities, serving as the official digital platform for communication, resources, and public engagement |
| <b>Application Version:</b>    | v1.0   |
| <b>Hosting URL:</b>            | <a href="https://csirhrdg.res.in/">https://csirhrdg.res.in/</a>  |
| <b>Testing URL:</b>            | <a href="http://192.168.250.140:84/">http://192.168.250.140:84/</a>  |
| <b>Audit Methodology:</b>      | OWASP Top 10 & OWASP Web Security Testing Guide (WSTG)   |
| <b>Tool Used:</b>              | Nessus Professional, Burpsuite Professional, Nmap & NSE, Exploit DB Database OSINT Tools, Manual Test Methodologies  |
| <b>Current Version Hash:</b>   | E48BC0AA8825866DB53479FBD981B43D9C5D96345A81D6527CE867C45B6E84B2   |
| <b>Hash Algorithm:</b>         | SHA256   |
| <b>Testing Dates:</b>          | 14 <sup>th</sup> March 2026 till 08 <sup>th</sup> April 2026   |
| <b>Name of Audit Company:</b>  | Codec Networks Private Limited   |
| <b>Audit Team Members:</b>     | Mr. Gaurav Pant, Mr. Gulshan Chauhan   |
| <b>Reviewed By:</b>            | Mr. Piyush Mittal, Head – Projects (Email: <a href="mailto:piyush@codecnetworks.com">piyush@codecnetworks.com</a> )  |

## To Whomsoever It May Concern

This is to certify that the tested application hosted of the current version is audited by Codec Networks Private Limited (A CERT-In Empaneled Organization Wide Letter No: 3(15)/2004-CERT-In (Vol. XIV)-RE20 dated 01.01.2025) and it is free from OWASP vulnerabilities, and any known severe web vulnerability/threat.

Respectively it is safe for hosting and carrying out transactions.

The application has passed Critical / High / Medium vulnerabilities for application security assessment tests.


For detailed description of vulnerabilities and other security assessment related details, please refer to the audit report shared with the respective client.

It is also recommended that the application may be hosted with read and script execution permission for the public with an exact replica of the audited URL in the production environment.

**Certificate Validity:** The maximum validity of the certificate is One Year from the date of issue.

**Note:** Our opinion is valid for the period during which the changes are not made in the source of tested application thus any changes in the system will require to re-audit of application's new version. Projections of any conclusions based on our current findings will not be applicable and has to be altered for future periods and the application of new versions is subject to any risks because of changes made to the application or system. Also, we recommend that Web Server and OS level hardening need to be in place for the production server.

**Thanks & Regards,**

**Piyush Mittal**

**Project Manager; Codec Networks Private Limited**