Certificate No.: ITO/SH2023/10010
Issuing Date : 18/10/2023
Valid till : 17/10/2024

Safe-to-host Certificate

Issued to	**Finance Department, Government of West Bengal**
Test URL (In Scope)	**http://172.25.151.111/ridf/Page/login.aspx**
Production URL	**https://finance.wb.gov.in**
Product Name	**NA**
Scope of Audit	**Web Application Security Assessment**
Auditor	**Debjyoti Chowdhury**
Audit Dates	**1st Round of Testing: 9-Sep-2023 to 15-Sep-2023** **Final Round of Testing: 5-Oct-2023 to 12-Oct-2023**

Conclusion

Auditing for Web application of **Finance Department, Government of West** was done from 9-Sep-2023 to 12-Oct-2023 as per the CERT-In Web application Audit guidelines, by ITOrizin Technology Solutions Pvt. Ltd. as per the scope. As on 12-Oct-2023, there are no pending nonconformity w.r.t Web Application Audit.

The Web application is free from OWASP (and any other Known) vulnerabilities and is safe for hosting.

The clearance for the above site is given taking into consideration that the OWASP (and any other Known) vulnerabilities do not exist in the web Application. Any unapproved changes to the web Application will void the certificate.

Hosting Permission

Web Application may be considered safe for hosting with read permission only for general public.

Debjyoti Chowdhury

Audited by
ITOrizin Technology Solutions Pvt. Ltd.

ITORIZIN TECHNOLOGY SOLUTIONS PRIVATE LIMITED
Kolkata
700 078

Gangopadhyay

Authorised Signatory
ITOrizin Technology Solutions Pvt. Ltd.

Validate Certificate

Safe-to-host Certificate

Test/Audit Result Summary

OWASP Top 10 (2021)	Web Application Vulnerabilities	Compliance	Remark
1	Broken Access Control	Satisfactory	Nil
2	Cryptographic Failures	Satisfactory	3 Residual Risk
3	Injection	Satisfactory	Nil
4	Insecure Design	Satisfactory	Nil
5	Security Misconfiguration	Satisfactory	Nil
6	Vulnerable & Outdated Components	Satisfactory	Nil
7	Identification & Authentication Failures	Satisfactory	Nil
8	Software & Data Integrity Failures	Satisfactory	Nil
9	Security Logging & Monitoring Failures	Satisfactory	Nil
10	Server-Side Request Forgery (SSRF)	Satisfactory	Nil

The residual risk given in “Test/Audit Result Summary” above pertain to three (3) vulnerabilities as given below:

Residual Risk/Observation

SR. No.	Web Application Vulnerabilities	Remark
1	Weak Cryptography.	The vulnerability will be mitigated in the production URL.
2	SSL not implemented.	The vulnerability will be mitigated in the production URL.
3	Cookie not set to secure	The vulnerability will be mitigated in the production URL.

Recommendations

I. Web Server SSL Digital certificate, web server and OS level hardening need to be in place for the production server before making the web application live.
II. Web Application audit should be done at least once a year or when there is any change in the web Application.
III. No new web pages are to be added without proper security audit.
IV. Server-side issue should be taken care by hosting provider

Debjyoti Chowdhury

Audited by
ITOrizin Technology Solutions Pvt. Ltd.

ITORIZIN TECHNOLOGY SOLUTIONS PRIVATE LIMITED ★ Kolkata 700 078

Gangopadhyay

Authorised Signatory
ITOrizin Technology Solutions Pvt. Ltd.

Validate Certificate