

Regd. Off.: Sumashilp, 93/5A, Erandwane, Pune - 411004. (Maharashtra)

Aundh : 3rd Floor, Westend Icon, Westend Mall Extension,  
Aundh, Pune - 411007. (Maharashtra)

CIN No.: U72200PN2000PTC014900

T : +91 20 4013 0400 E : info@sumasoft.com

SS-ITRSM-2025/07/HCHABHAM1M2-001

Date: August 04, 2025

## API SECURITY TESTING (SAFE TO HOST) CERTIFICATE

**Organization Name** : Health Smarttech Private Limited  
**Full/Entire Application Security Tested** : No  
**M1,M2 APIs Tested** : Yes\*  
**API Name** : ABHA M1,M2 V3 APIs  
**Temporary APIs URL** : <https://qa.healthcarehms.com>  
**Security Testing Start & End Date** : July 11, 2025 to July 15, 2025  
**Audited By** : Kiran Mengawade (infosec@sumasoft.net / +91.20.40130400)

**\*Suma Soft did not test Full/Entire Application, This Vulnerability Assessment & Penetration Testing is limited to ABHA Milestone 1 (M1), Milestone 2 (M2) APIs Integration module and its related components only .**

**Observation:** Milestone 1 (M1), Milestone 2 (M2) V3 APIs only integrated into HealthCareHMS Web Application developed as part of the Ayushman Bharat Digital Mission (ABDM) , has undergone Vulnerability Assessment & Penetration Testing and has been certified to be safe from the known vulnerabilities.

The audited contents were based on the specified application and the URL provided above. This Vulnerability Assessment & Penetration Testing was conducted on the mentioned ABHA Milestone 1 (M1), Milestone 2 (M2), V3 APIs.

**Conclusion:** We have tested Milestone 1 (M1), Milestone 2 (M2), V3 APIs only integrated into HealthCareHMS Web Application developed by Health Smarttech Private Limited for OWASP Web Top Ten 2021 vulnerabilities based on the OWASP Testing Guide V4.2. The said APIs are free from OWASP Top Ten known vulnerabilities and is safe for hosting as on date of submission of the security certificate. The APIs have dynamic content meant to be available to authorized users only.

**MD5 for Backend Folder (Zip):** f5c672e3bff385235c09d6178e776fb3  
**MD5 for Frontend Folder (Zip):** afbd2a4bbf2f54825efd9df6dda83433

### Recommendations for Hosting the in Production:

1. The APIs may be hosted with limited privileges (Without Administrator/Root) of Read and Script Execution permissions.
2. Operating System, Web Server and Database Server hardening needs to be in place for the production server along with encrypted transport layer (SSL) protection.
3. Always use latest software technologies on production environments.

**Note** - The security certificate is valid for one year from the date of issuance, given that no dynamic changes are made to the APIs source code. If any alterations, such as modifications to the application code or system configuration, occur, the organization is required to conduct a subsequent VAPT/Security Testing specifically for the modified portion of the application.

**For Suma Soft Private Limited**

-----  
**Anil Waychal,**  
**CISA, ISO27001LA, ITIL, RHCE, Sun Solaris Admin**