



Web Application Security Audit Certificate

Certificate No: IMS/2025-2026/0225

Audit Details

Audit Firm	:	IMPERIUM SOLUTIONS
CertIN Empanelment Reference	:	3(15)/2004-CERT-In (Vol. XIII)
Client Name	:	ASCENTech Information Technology Private Limited
Scope of activity	:	Web Application Vulnerability Assessment and Penetration Testing (VAPT)
Application	:	Amravati Corporation
Production URL	:	https://amravaticorporation.in/
Tested URL	:	https://amravaticorporation.in/
Audit Duration	:	17th September 2025 – 25th September 2025
SHA256 Hash	:	Not available
Audit Methodology	:	OWASP, SANS, Cert-IN Advisory, OSSTMM, PTES, ISSAF
Auditor Details	:	Mr. Om Pagar
Certificate Issue Date	:	25 th September 2025
Certificate Validity	:	This certificate is valid till there are no changes in the application

Conclusion

Amravati corporation Web Application was in the scope of the activity. It was observed that ASCENTech has currently resolved all previously identified vulnerabilities.

Sr. No.	Vulnerability Name	Severity	Final Status
1	Out-of-date Version (Bootstrap)	Medium	Closed
2	Missing Security Headers	Medium	Closed
3	Version Disclosure (Apache)	Low	Closed
4	Cookie Not Marked as Secure	Low	Closed
5	Cookie Not Marked as Httponly	Low	Closed
6	Cookie Without SameSite Attribute	Low	Closed
7	Missing X-Frame-Options Header	Low	Closed
8	Version Disclosure (jQuery)	Info	Closed
9	Version Discloser (Bootstrap)	Info	Closed

The application can be hosted in the production environment after implementing the compensatory controls.

General Recommendations

Production Hosting Environment

1. Deploy a Web Application Firewall ahead of your application facing the Internet and allow only relevant traffic to flow to your web server.
2. Fine tune the firewall rules such that only specific ports and IP addresses are allowed access to your application.
3. Enable, capture and retain application logs so as to be able to trace a security incident, in case it becomes necessary to do so.
4. Utilise services of 3rd party vendors to check for malicious activities like web defacement, etc.
5. Ensure that the Operating system, database and application is hardened.
6. Ensure that the Operating Systems, Database and applications is the latest stable version.

7. Application should undergo security testing annually or whenever any changes are implemented in the application functionality, whichever is earlier.
8. Ensure that all vulnerabilities, irrespective of their criticality, are resolved asap.

For Imperium Solutions,

Ms. Tasneam P
CISA (Certification No – 0977475)

Dated: 25th September 2025