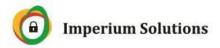


Web Application Security Audit Certificate

Certificate No: IMS/2025-2026/0237

Audit Details

Audit Firm	:	IMPERIUM SOLUTIONS		
CertIN Empanelment	:	3(15)/2004-CERT-In (Vol. XIII)		
Reference				
Client Name	:	Ascentech Information Technology Private Limited		
Scope of activity	:	Web Application Vulnerability Assessment and Penetration Testing (VAPT)		
Application	:	Parbhani Municipal Corporation		
Production URL	:	http://pcmcparbhani.org/		
Tested URL	:	http://pcmcparbhani.org/		
Audit Duration	:	23 rd September 2025 – 30th September 2025		
SHA256 Hash	:	Not available		
Audit Methodology	:	OWASP, SANS, Cert-IN Advisory, OSSTMM, PTES, ISSAF		
A 1'' D : '1		M O B		
Auditor Details	:	Mr. Om Pagar		
ContiConto Incon		04ct 0 -4 -1 2025		
Certificate Issue	:	01st October 2025		
Date				
Certificate Validity	:	This certificate is valid till there are no changes in the		
certificate valuity	•	application		



Conclusion

parbhani 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	Missing Security Headers (Content-Security-Policy, Permission-Policy, X-Content-Type-Option)	Medium	Closed
2	Out-of-date Version (J Query)	Medium	Closed
3	Out-of-date Version (Bootstrap)	Medium	Closed
4	Swiper out- of date	Medium	Closed
5	Version Discloser(J Query)	Low	Closed
6	Version Disclosure (Bootstrap)	Low	Closed
7	Cookie Without Same Site Attribute	Low	Closed
8	Information Disclosure	Low	Closed
9	Stack Disclosure (PHP)	Low	Closed
10	Swiper Version Disclosure	Low	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: 1st October 2025