Imperium Solutions

Web Application Security Certificate

Certificate No: IMS/2024-2025/0360

Audit Details

Audit Firm	**:**	401, 4th Floor, Maruti Bhavan, Ram Maruti Road, Thane (W) 400602 www.imperiumsolution.com email: info@imperiumsolution.com
CertIN Empanelment Reference	**:**	3(15)/2004-CERT-In (Vol. XIII)
Client Name	**:**	Mira Bhayandar Municipal Corporation
Scope of activity	**:**	Web Application Audit
Application	**:**	MBMC Website
Production Application URL	**:**	https://www.mbmc.gov.in/
Audit Duration	**:**	05th January 2026 - 06th January 2026
Audit Methodology	**:**	OWASP, SANS, Cert-IN Advisory, OSSTMM, PTES, ISSAF
Auditor Details	**:**	Ms. Tanushree Khairnar
Certificate Issue Date	**:**	06th January 2026
Certificate Validity	**:**	This certificate is valid till there are no changes in the application

Conclusion

The MBMC Web Application was in the scope of the activity. It was observed that MBMC has taken exceptions for all the identified vulnerabilities.

Sr.no	Vulnerability Name	Severity	Final Status
1	Out-Of- Date Version (jQuery)	Medium	Exception taken
2	Out-Of- Date Version (Swiper)	Medium	Exception taken
3	Missing Security Headers	Medium	Exception taken
4	Weak Ciphers	Medium	Exception taken
5	Version Disclosure (BootStrap)	Low	Exception taken
6	Version Disclosure (jQuery)	Low	Exception taken
7	Version Disclosure (Swiper)	Low	Exception taken
8	Cookie Without HttpOnly Attribute	Low	Exception taken
9	Cookie without SameSite Attribute	Low	Exception taken
10	Cookie Not Marked as Secure Attribute	Low	Exception taken

This vulnerability which requires a complete overhaul of the application and which cannot be addressed without re-writing the application, as per the client communication. The application can be hosted in the production environment after implementing the compensatory controls.

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,

Jude Michael Dcosta

Digitally signed by Jude Michael Dcosta
DN: C=IN, O=Personal, T=7466, OID.2.5.4.65=dd3978672a4340b98eefd2e852e9366f, Phone=08d947c5c06c8a3835adbee625572b7ae400d84c46ee887Be0036f821529c65b, PostalCode=401202, S=Maharashtra, SERIALNUMBER=61db6fa8f5c5ad71bca535eabb0260f54574eab42dfb2e69a93d3e7fcf051a2a, CN=Jude Michael Dcosta
Reason: I am approving this document
Location: Thane
Date: 2026-01-06 18:16:32
Foxit PhantomPDF Version: 9.6.0

Mr. Jude Dcosta
Dated: 06th January 2026