



Project Name Version

Aspose OMR for .NET 25.8

Last Analysis Date

2025-08-28

OWASP Vulnerabilities

0

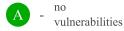
OWASP Rating



OWASP. TOP 10 (2021) Application Security Risks

		Category Rating	Vulnerabilities
A 4	Broken Access Control		
AI	Improperly enforced access restrictions allow attackers to bypass authentication and access unauthorized data or functions.	A	0
A2	Cryptographic Failures		0
	Weak encryption or improper handling of sensitive data (e.g., passwords, credit card details) can lead to data leaks.	A	0
4.3	Injection		0
A3	Malicious input (e.g., SQL, NoSQL, OS command injection) is improperly handled, allowing attackers to manipulate databases or execute unintended commands.	A	0
A4	Insecure Design	A	0
	Poor application design choices, such as missing security controls, increase vulnerability risks.		U
A5	Security Misconfiguration	A	0
	Default settings, exposed error messages, or unnecessary services can create security gaps.		U
A6	Vulnerable and Outdated Components	A	0
	Using outdated software, libraries, or frameworks with known vulnerabilities can lead to exploits.		
A 77	Identification and Authentication Failures		0
A '/	Weak authentication mechanisms, such as poor password policies or missing multi-factor authentication (MFA), can lead to unauthorized access.	A	0
AQ	Software and Data Integrity Failures		0
Ao	Untrusted or malicious updates, dependencies, or CI/CD pipelines can lead to compromised systems.		U
A O	Security Logging and Monitoring Failures	A	0
A	Lack of proper logging and alerting mechanisms delays detection and response to security incidents.		U
A1 0	Server-Side Request Forgery (SSRF)	A	0
AIU	Attackers manipulate web applications to make unauthorized requests to internal or external services.		U

Security ratings





at least one minor vulnerability



at least one major vulnerability



at least one
- critical
vulnerability



at least one
blocker
vulnerability