

Project Name	Version	Last Analysis Date
Aspose.PDF for C++	25.9	2025-09-25

OWASP Vulnerabilities

0

OWASP Rating

A

OWASP TOP 10 (2021) Application Security Risks

		Category Rating	Vulnerabilities
A1	Broken Access Control Improperly enforced access restrictions allow attackers to bypass authentication and access unauthorized data or functions.	A	0
A2	Cryptographic Failures Weak encryption or improper handling of sensitive data (e.g., passwords, credit card details) can lead to data leaks.	A	0
A3	Injection 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 Poor application design choices, such as missing security controls, increase vulnerability risks.	A	0
A5	Security Misconfiguration Default settings, exposed error messages, or unnecessary services can create security gaps.	A	0
A6	Vulnerable and Outdated Components Using outdated software, libraries, or frameworks with known vulnerabilities can lead to exploits.	A	0
A7	Identification and Authentication Failures Weak authentication mechanisms, such as poor password policies or missing multi-factor authentication (MFA), can lead to unauthorized access.	A	0
A8	Software and Data Integrity Failures Untrusted or malicious updates, dependencies, or CI/CD pipelines can lead to compromised systems.	A	0
A9	Security Logging and Monitoring Failures Lack of proper logging and alerting mechanisms delays detection and response to security incidents.	A	0
A10	Server-Side Request Forgery (SSRF) Attackers manipulate web applications to make unauthorized requests to internal or external services.	A	0

Security ratings

 - no vulnerabilities
  - at least one minor vulnerability
  - at least one major vulnerability
  - at least one critical vulnerability
  - at least one blocker vulnerability