

RakhaMaulana

REPORTS

OWASP® Top 10

- Summary
- Intended use
- Continuous Code Health
- About DeepSource

REPOSITORY

Bismillah\_TA

OWASP® Top 10 report

Created on Aug 13, 2025

Summary

The Open Web Application Security Project Foundation, or OWASP® Foundation, is a non-profit foundation dedicated to improving software security. The foundation is community-driven and helps organizations build secure software through open-source tools, resources, and research. The OWASP® Top 10 is a recommendation framework maintained by the OWASP® Foundation since 2003. The list is a collection of security recommendations that helps organizations to write more secure code. It is updated periodically to accommodate for the advancements and developments in application security. More information on OWASP® Top 10 can be found [here](#).

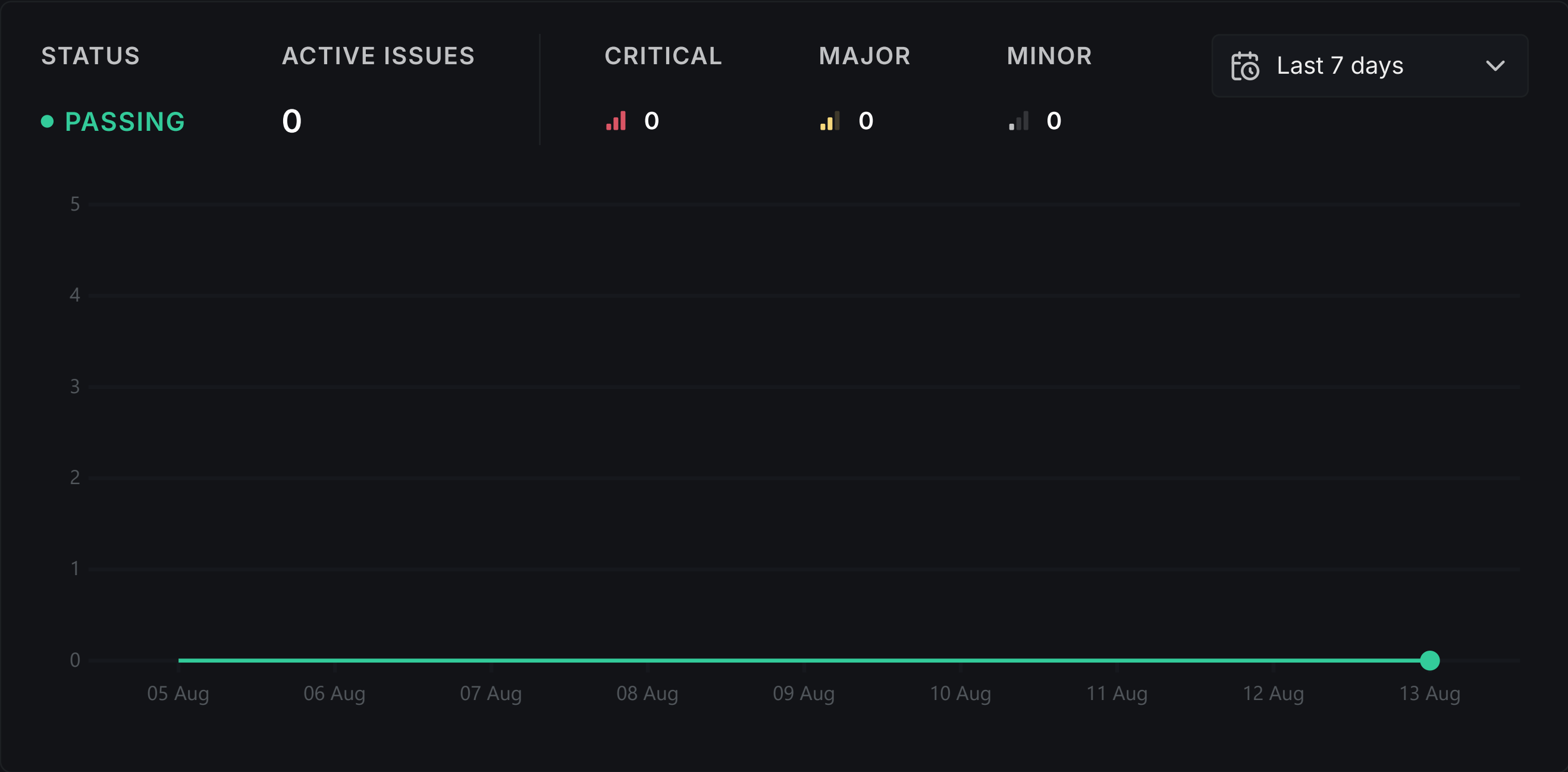
DeepSource continuously scans RakhaMaulana’s source code to detect violations of OWASP® Top 10 recommendations and provides guidance to correct them. This report provides the current, as well as a historical snapshot of the presence of such vulnerabilities in RakhaMaulana's source code, limited to the repositories, tracked on DeepSource.

Intended use of this report

This report can be used by the RakhaMaulana team to identify and remediate violations of OWASP® Top 10 recommendations in their source code. The report can also be used by key stakeholders within the organization and interested external stakeholders to understand the source code security posture of RakhaMaulana.

Continuous Code Health

DeepSource integrates with RakhaMaulana’s software development workflows to provide developers and key stakeholders a way to identify and fix code health issues continuously and proactively. This report is dynamic. As RakhaMaulana’s team improves its source code security posture, the changes will be reflected in this report.



CURRENT	1 MONTH AGO	3 MONTHS AGO	6 MONTHS AGO	12 MONTHS AGO
0	0	0	0	N/A

ID	NAME	OCCURRENCES
A01	Broken Access Control	0
A02	Cryptographic Failures	0
A03	Injection	0
A04	Insecure Design	0
A05	Security Misconfiguration	0
A06	Vulnerable and Outdate components	0
A07	Identification and Authentication Failures	0
A08	Software and Data Integrity Failures	0
A09	Security Logging and Monitoring Failures	0
A10	Server-Side Request Forgery (SSRF)	0

About DeepSource

DeepSource is a technology company that builds tools for developers. It provides a set of tools that fit into a developer’s workflow. Our cloud-based technology scans code in multiple languages and detects flaws in the codebase including, but not restricted to security and performance issues, bug risks, and anti-patterns.

DeepSource is based in San Francisco, California and Bengaluru, India.