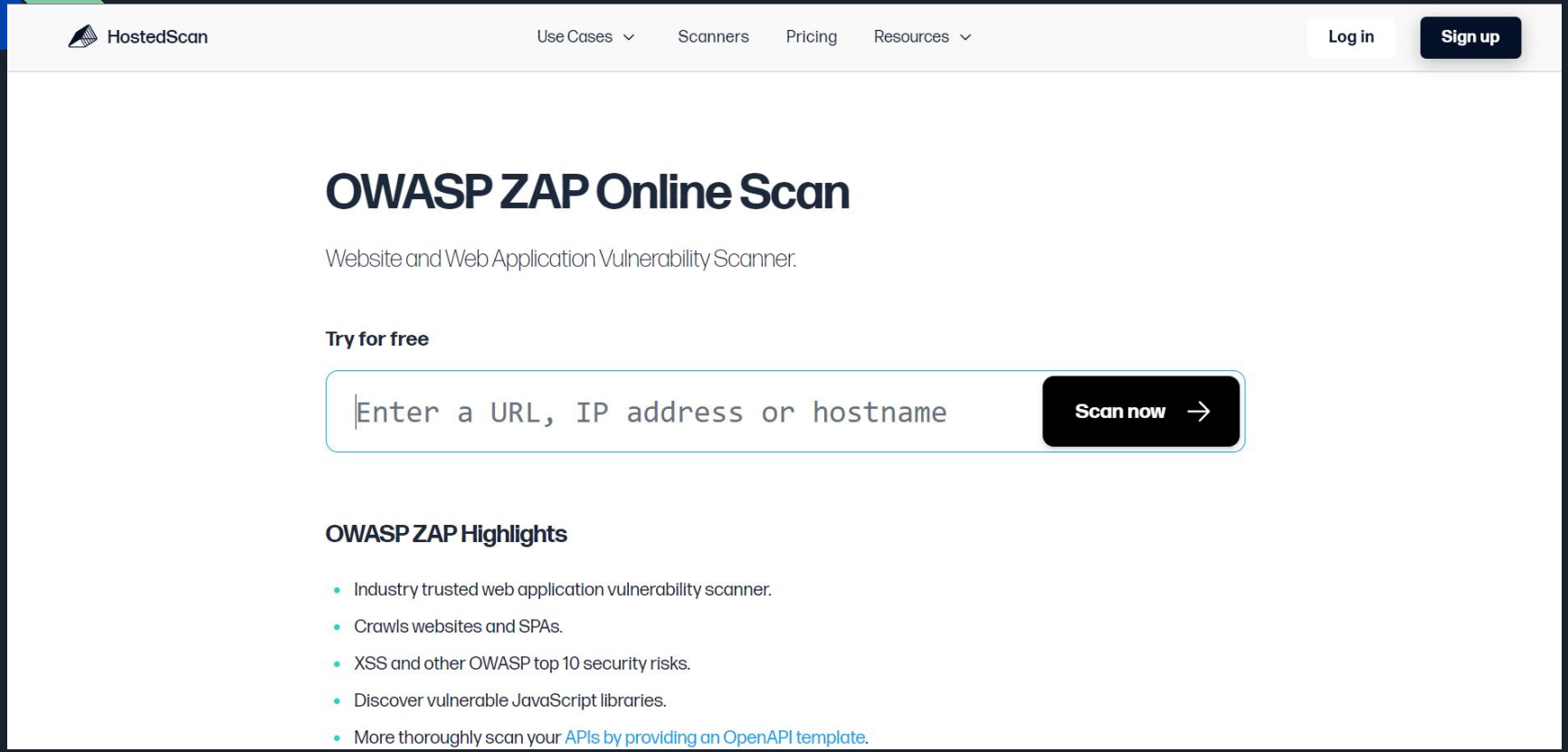
ZAP

SOFTWARE TESTING TOOL

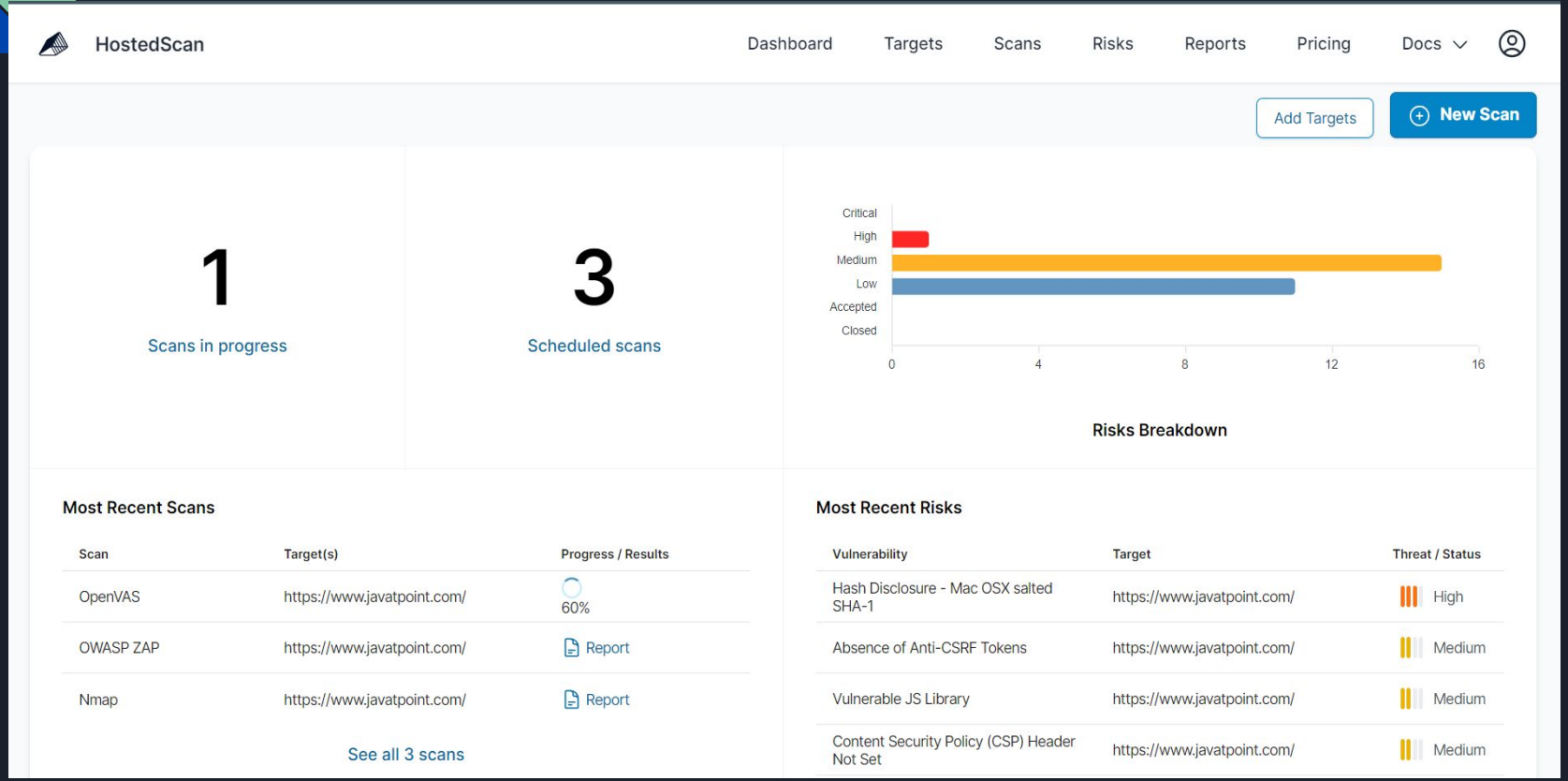
INTRODUCTION

ZAP (short for Zed Attack Proxy), formerly known as OWASP ZAP, is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.

INTERFACE FOR ZAP

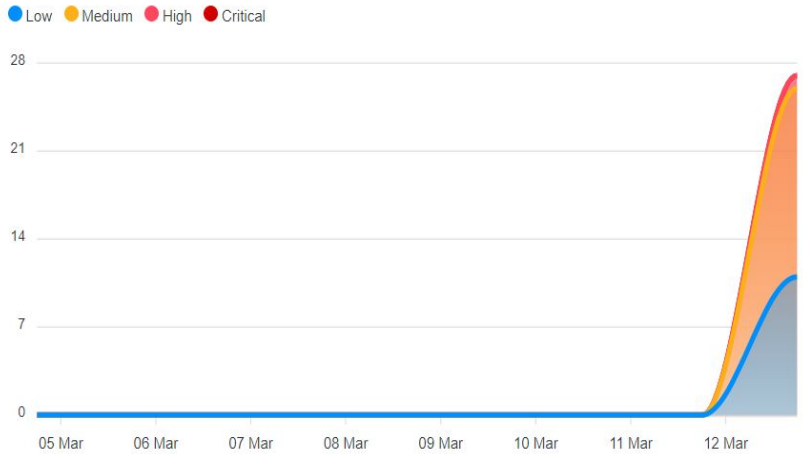


DASHBOARD

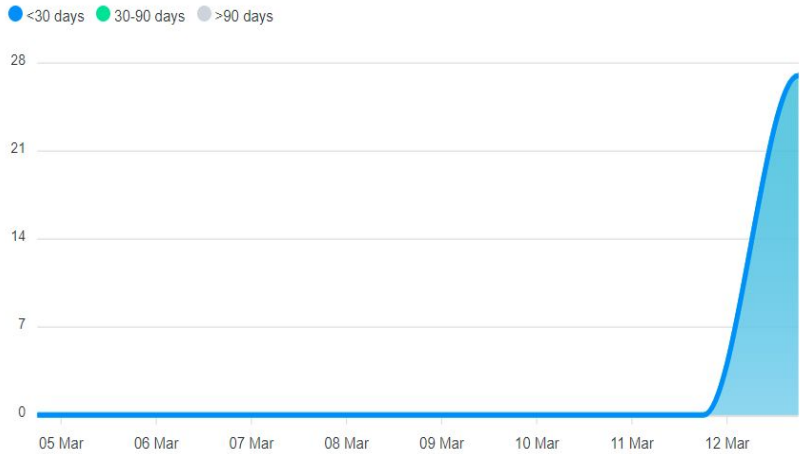

HostedScan
Dashboard
Targets
Scans
Risks
Reports
Pricing
Docs
Add Targets
New Scan
1
Scans in progress
3
Scheduled scans
Critical
High
Medium
Low
Accepted
Closed
0
4
8
12
16
Risks Breakdown
Most Recent Scans
Scan
Target(s)
Progress / Results
OpenVAS
https://www.javatpoint.com/
60%
OWASP ZAP
https://www.javatpoint.com/
Report
Nmap
https://www.javatpoint.com/
Report
See all 3 scans
Most Recent Risks
Vulnerability
Target
Threat / Status
Hash Disclosure - Mac OSX salted SHA-1
https://www.javatpoint.com/
High
Absence of Anti-CSRF Tokens
https://www.javatpoint.com/
Medium
Vulnerable JS Library
https://www.javatpoint.com/
Medium
Content Security Policy (CSP) Header Not Set
https://www.javatpoint.com/
Medium

Security Over Time

1 Week | 1 Month | 1 Year | Filters



Open Risks



Exposure Window

ADVANTAGES

Open Source: ZAP is freely available and open-source, allowing anyone to use, modify, and contribute to its development. This makes it accessible to developers and organizations of all sizes without requiring significant financial investment.

Comprehensive Testing: ZAP supports a wide range of automated and manual security testing techniques, including but not limited to, scanning for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms.

Automation: ZAP provides automation features that allow security tests to be integrated into the continuous integration/continuous deployment (CI/CD) pipeline. This enables organizations to incorporate security testing into their development workflows and identify vulnerabilities early in the software development lifecycle.

DISADVANTAGES

False Positives: Like any automated security testing tool, ZAP may produce false positives, flagging issues that are not actual vulnerabilities. This can result in wasted time and effort spent investigating and remedying non-existent security issues.

Limited Reporting: While ZAP provides basic reporting capabilities, its built-in reporting functionality may be insufficient for organizations with more advanced reporting requirements. Users may need to export scan results to external tools or formats for further analysis and documentation.

Lack of Support: As an open-source tool, ZAP does not offer formal support agreements or service-level agreements (SLAs) like commercial security testing solutions. Users may need to rely on community resources or forums for assistance with troubleshooting and resolving issues.

THANK YOU