

ImmuniWeb[®]
AI for Application Security

API Security Scanning

Run unlimited scans of your APIs and microservices for OWASP API Top 10 vulnerabilities with [ImmuniWeb[®] Neuron](#) premium security scanning



www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

Why Investing in API Security Scanning

88%

of companies now consider cybersecurity a critical business risk

Gartner

\$4.45M

is the average cost of a data breach in 2024, a 15% surge in just three years

IBM

100+

countries have laws imposing a personal liability on executives for a data breach

ImmuniWeb

APIs are prime targets for attackers. Just like any system, APIs can have vulnerabilities, and without scanning, these weaknesses remain hidden. API Security Scanning acts as a proactive shield, identifying these vulnerabilities before attackers exploit them. This prevents data breaches, unauthorized access, and potential regulatory issues, ultimately safeguarding your valuable information and building trust with users.

API Security Scanning with ImmuniWeb® Neuron

[+ CREATE NEW PROJECT](#)
Discovery 5
Neuron 1
Neuron Mobile 1
On-Demand 1
MobileSuite 2
Continuous 1

Your ImmuniWeb® Neuron Projects User Manual API & User Access

Neuron:Project #3138898 Subscription Valid Until July 1, 2025 | Targets Left: 44 (View History)

[Notifications](#)
[My Tasks](#)
[IP Ranges](#)

Charts are currently hidden. [Unfold this panel to see charts.](#) [Show charts](#)

[New](#) 10
 [GDPR](#) 12
 [PCI DSS](#) 23

[Search and Filters](#)
[Tags](#)
[Add Target](#)
[Import Targets](#)
[CI/CD Integrations](#)

Target	Scan Status	Vulnerabilities	Actions
home.example.com [93.184.216.34] AuthenticationNone Next scan: Unscheduled Last scan: Jul 4 2023, 15:35 CEST	Status: Finished New Events: 2	1 0 3 0	[Stop] [Refresh] [Scan] [Screenshot] [Export]
marketing24.example.com [93.184.216.39] AuthenticationNone Next scan: Unscheduled Last scan: Never	Status: Unscheduled New Events: 0	0 4 0 0	[Start] [Refresh] [Scan] [Screenshot] [Export]
promotional.example.com [93.184.216.99] AuthenticationNone Next scan: Unscheduled Last scan: Mar 14 2024, 19:39 CEST	Status: Error New Events: 2	2 3 0 3	[Stop] [Refresh] [Scan] [Screenshot] [Export]
developers5.example.com [93.184.216.56] AuthenticationWeb Next scan: Unscheduled Last scan: Feb 4 2024, 17:34 CEST	Status: Finished New Events: 1	7 4 0 2	[Start] [Refresh] [Scan] [Screenshot] [Export]
pov.example.com [93.184.216.22] AuthenticationNone Next scan: Unscheduled Last scan: Jan 4 2024, 02:30 CEST	Status: Stopped New Events: 2	0 0 0 0	[Stop] [Refresh] [Scan] [Screenshot] [Export]
delegate.example.com [93.184.216.34] AuthenticationNone Next scan: Unscheduled Last scan: Jan 7 2024, 11:38 CEST	Status: Finished New Events: 2	0 0 0 0	[Start] [Refresh] [Scan] [Screenshot] [Export]

portal.example.com Vulnerability Risk Level Remember current settings

Table of Contents

- ImmuniWeb® Neuron Scan History
- Vulnerability Coverage
- Scan Scope and Testing Statistics
- Detected Vulnerabilities Statistics
- Website Screenshot
- Critical Risk Web Application Vulnerabilities [0]
- High Risk Web Application Vulnerabilities [0]
- Medium Risk Web Application Vulnerabilities [0]
- Low Risk Web Application Vulnerabilities [0]
- Security Warnings [3]
 - 10.1 Cookies without "HttpOnly" Attribute
 - 10.2 Cookies without "SameSite" Attribute
 - 10.3 Cookies without "Secure" Attribute
- Useful Links

4. Detected Vulnerabilities Statistics

Low Risk & Warnings 4
 Medium Risk 3
 High Risk 1
 Critical Risk 2

Aggregated Risk

Diagram 1: Number of vulnerabilities in your web application grouped by risk levels

Diagram 2: Vulnerabilities and weaknesses in your web application grouped by the CWE classification

- CWE-78: OS Command Injection (1)
- CWE-89: SQL Injection (2)
- CWE-284: Improper Access Control (3)
- CWE-287: Improper Authentication (4)
- CWE-352: Cross-Site Request Forgery (2)
- CWE-79: Cross-Site Scripting (2)
- CWE-200: Information Exposure (3)
- CWE-601: Open Redirect (4)

Efficient. Simple. Cost-Effective.

Customize your API security scanning requirements and authentication including SSO and MFA. Schedule recurrent API scans in a few clicks and configure email notifications about completed API scans.

Our API security scanning is provided with a contractual zero SLA. If there false positive in your API security scanning testing report, you get the money back. Additionally, our award-winning Machine Learning technology provides better vulnerability detection and coverage rate compared to traditional software scanners that rely solely on heuristic vulnerability detection algorithms.





















The API scanning reports are available via a multiuser dashboard with flexible RBAC access permissions. Our turnkey CI/CD integrations enable 100% automation of your web and API security testing within your CI/CD pipeline, both in a cloud environment and on premise. Our 24/7 technical support is at your service may your software developers have questions or need assistance during API security scanning.

Trusted by 1,000+ Global Customers



Looking for Something Else?

Explore 20 use cases we have for you

-  API Penetration Testing
-  Continuous Automated Red Teaming
-  Continuous Penetration Testing
-  Phishing Websites Takedown
-  API Security Scanning
-  Mobile Penetration Testing
-  Cyber Threat Intelligence
-  Red Teaming Exercise
-  Attack Surface Management
-  Mobile Security Scanning
-  Cybersecurity Compliance
-  Third-Party Risk Management
-  Cloud Penetration Testing
-  Network Security Assessment
-  Dark Web Monitoring
-  Web Penetration Testing
-  Cloud Security Posture Management
-  Continuous Breach and Attack Simulation
-  Digital Brand Protection
-  Web Security Scanning





www.immuniweb.com



“ ImmuniWeb outperformed IBM Watson for Cybersecurity and won in the **“Best Usage of Machine Learning and AI”** category



One Platform. All Needs.