INDUSFACE™

API Scan Coverage for OWASP Top 10

What is API Security?

API security is a process of implementing multiple practices and techniques to protect the APIs.

The process involves three steps.

1. Discovering the API Resources
2. Inspection
3. Mitigation of security risks of APIs

Why is API security crucial?

APIs job is to serve as gateways to sensitive data and system resources. If APIs are not secured properly, it can lead to unauthorized access, data breaches, malicious activity, stealing data, disrupted services, and so on.

OWASP API Security Top 10 2023

Since APIs play a vital role in modern application architecture, it's important to educate those involved in API Development and maintenance.

Walk through the following checklist to get a better understanding of how AppTrana enhances the API Security.

OWASP API Security Top 10 (2023)	Tests Recommended by OWASP	Detected by Automated Scans
API 1: Broken Object Level Authorization	Possible Physical Path Disclosure	Yes
	Remote File Inclusion (RFI)	Yes
	Email Address Disclosure	Yes
	Internal IP Address Disclosure	Yes
	Web Server Info Disclosure	Yes
	Robots.txt File Detected	Yes
	Programming Language and Version Information Disclosure	Yes
	Predictable Resource Location	Yes
	Missing Account Lockout Policy	Yes
	ASP.NET Version Disclosure	Yes
	Insecure Direct Object References	Yes
	Sensitive Information Disclosure Through URL	Yes
	Reveals Sensitive Information- low severity	Yes
	Reveals Sensitive Information	Yes
API2: Broken Authentication	SQL Injection Authentication Bypass	Yes
	Password found in server response	Yes
	Credential found in token	Yes
API3: Broken Object Property Level Authorization	Session ID In URL	Yes
	Weak Session IDs	Yes
	Possible Social Security Number Found	Yes
	Incorrect Session Timeout	Yes
	JWT misconfiguration	Yes
	Improper Session Management	Yes

API4: Unrestricted Resource Consumption	Possible Slow Response Time Detected	Yes
	Apache Range Denial of Service	Yes
API5: Broken Function Level Authorization	WebDAV Extensions Are Enabled	Yes
	Sensitive Form Data Submitted in Cleartext	Yes
API7: Server-Side Request Forgery	AWS Metadata Server-Side Request Forgery	Yes
	Server-Side Request Forgery Local File Inclusion	Yes
	Server-Side Request Forgery Detected	Yes
API8: Security Misconfiguration	HTTP DELETE Method Enabled	Yes
	Directory Listing	Yes
	ASP.NET Debug Feature Enabled	Yes
	HTTP PUT Method Enabled	Yes
	Missing Secure Flag from Cookie Header	Yes
	HTTP Basic Authentication Enabled	Yes
	ASP.NET Unencrypted "__VIEWSTATE" Parameter	Yes
	Missing HttpOnly Flag from Cookie	Yes
	Unvalidated Redirects and Forwards/Open Redirection	Yes
	Application Error Message	Yes
	Possible Backup File(s) Detected	Yes
	Possible Sensitive Directories/Files Detected	Yes
	Permissive Cross-domain Policy File Detected	Yes
	Readable .htaccess File Detected	Yes
	ASP.NET ViewState MAC Disabled	Yes
	Insecure Content Security Policy (CSP)/X-Frame-Options	Yes
	Unencoded special characters	Yes

	Cross-Origin Resource Sharing (CORS)	Yes
	HTTP Verb Tampering	Yes
	Old SSL/TLS Version Detected	Yes
	Database Error Message	Yes
	X-XSS-Protection Header Disabled	Yes
	Web Server Default Web Page Detected	Yes
	HTTP OPTIONS Method Enabled	Yes
	ASP.NET Tracing Enabled	Yes
	Microsoft IIS Version Disclosure	Yes
	Missing HSTS Header	Yes
	Cookie Scoped to Parent Domain	Yes
	WordPress XML-RPC Interface Detected	Yes
	Credit Card Number Disclosure	Yes
	Possible Archive File or Compression File (s) Detected	Yes
	Cookie Overly Broad Path Detected	Yes
	Session Cookie Manipulation	Yes
	Web Server Content Sniffing Enabled	Yes
	Core Dump File(s) Detected	Yes
	Uncontrolled Format String	Yes
	Google Chrome Logger Information Disclosure	Yes
	Java Virtual Machine (JVM) Version Disclosure	Yes
	XML External Entity DOS Attack	Yes
	XML External Entity (XXE) Injection Vulnerability	Yes
	Permissive Client Access Policy File Detected	Yes

	Improper Token Handling	Yes
	Unset/Insecure X-Permitted-Cross-Domain-Policies Header	Yes
	Session Resumption Enabled	Yes
	DNSSEC unsigned	Yes
	Content Injection	Yes
	JWT none algorithm	Yes
	Weak Encoding	Yes
	Accessible By IP Address	Yes
API9: Improper Inventory Management	Old Cipher Suites Detected	Yes
	Weak TLS CBC cipher Detected	Yes
API10: Unsafe Consumption of APIs	Cross-Site Scripting (XSS)	Yes
	SQL Injection	Yes
	OS Command Injection	Yes
	XPath Injection	Yes
	Local File Inclusion (LFI)	Yes
	HTML Injection	Yes
	HTTP Host Header Injection	Yes
	User Controllable HTML Attribute	Yes
	Log Injection	Yes
	Remote XSL Inclusion	Yes
	PHP Nginx Remote Command Execution	Yes
	HTTP Request Smuggling	Yes
	Link Injection	Yes
	Iframe Injection	Yes
	Partial user controllable script source	Yes

	Apache Log4j RCE Vulnerability	Yes
	Cross Site Scripting (XSS) OOB	Yes
	Possible Cross-Site Scripting (XSS)	Yes
	Possible HTML Injection	Yes