Threat Vectors Datasheet

TRACEABLE

Introduction

Since 2003, the OWASP Top 10 project has been the authoritative source of information on web application vulnerabilities and the ways to mitigate them. However, rapid API adoption changed the security landscape so much that a new approach was needed. As a result, in 2019, OWASP started an effort to create a version of their Top 10 dedicated specifically to API security. The first OWASP API Security Top 10 list was released on 31 December 2019.

OWASP API Top 10 Details

The OWASP API Top 10 enumerates the unique vulnerabilities and exposure that APIs create in modern applications. This research helps guide engineering, security, and IT teams in prioritizing risks and mitigating business disruptions from API abuse and attack. The current API top 10 are Broken Object Level Authorization, Broken User Authentication, Excessive Data Exposure, Lack of Resources & Rate Limiting, Broken Function Level Authorization, Mass Assignment, Security Misconfiguration, Injection, Improper Assets Management, and Insufficient Logging & Monitoring.

Protecting modern applications against these API vulnerabilities is challenging. New application types are increasingly complex, often built in the cloud from dozens of microservices and connecting to users via the web and to mobile devices. Each level of complexity is a new threat vector.

Traceable's Approach to cover the OWASP API Top 10

Traceable AI is a new API Security application platform, built from the ground up to protect the fast-moving, API-driven applications that power today's increasingly digital economy. Traceable AI's foundation is application observability, enabling Traceable AI to deliver API Security that moves in tandem with API-driven applications through their lifecycle.

Powered by sophisticated data collection agents, the Traceable AI security platform analyzes the aggregated data from APIs across all transactions as they flow through the applications. After the data is collected, correlated and sequenced, powerful machine learning (ML) pieces together the application's business logic, data use patterns and other attributes into a historical baseline model. As the applications and uses change over time, the ML model adapts along with it, learning new changes in normal application and user behavior.

Because the machine learning model comprehensively analyzes complete API user sessions, Traceable AI's platform rapidly and accurately distinguishes legitimate (normal) patterns from malicious users and bot actions. As users and other APIs interact with your APIs and applications, Traceable AI learns the sequences of calls, the flow of data and the normal interactions, determining the developer- and user-intent of the application in context

As more users access the application, Traceable AI continues to build an accurate, ongoing, data-driven, algorithmic model of all the distributed applications, APIs and user profiles. The result is actionable intelligence that accurately discerns any malicious or unintended use across all the targeted applications. For malicious users that perform actions out of step with the normal sequences of actions for an application, Traceable AI immediately surfaces these deviations,]determines their intent as malicious, and initiates the appropriate responses

Traceable AI provides visibility, protection, and deep analytics for your mission-critical applications. Built on a distributed tracing platform, it collects data from all touchpoints across an application's uses, storing it all for deep analysis through powerful ML algorithms that provide comprehensive security insights on how your application intrinsically works and adapts over time. This ensures that your response to expanding API attack surfaces keeps pace with whatever vulnerabilities arise.

www.traceable.ai

Traceable provides full runtime protection for all OWASP Top 10 and API Top 10

A1:2017 - Injection	API8:2019 - Injection	SQL Injection
		NoSQL Injection
		Command Injection
		LDAP Injection
		SQL Comment Injection
		Null Byte Injection
		Shell Injection
		Custom Special Character Injection

A10:2017 Insufficient Logging and Monitoring	API10:2019 Insufficient Logging and Monitoring	Logging
		Monitoring
		Unusual Signups
		Unusual Password Resets
		SearchBot Imposter
		Tor Traffic
	API4: 2019: Lack of Resources and Rate Limiting	App Level DOS - Unbound Filter Queries
		Credential Stuffing

A2:2017 - Broken Authentication	API2:2019 - Broken Authentication	Unauthenticated Access
		Session Fixation
A3:2017 - Sensitive Data Exposure	API3:2019 - Excessive Data Exposure	Sensitive Data Exposure
		Scanning of Sensitive Endpoints
A5:2017 - Broken Access Control	API1:2019 - Broken Object Level Authorization	Authorization Attacks on Objects
	API7:2019 - Security Misconfiguration	Mass Assignment
A6:2017 - Security Misconfiguration	API7:2019 - Security Misconfiguration	Verbose Error Traces
A7:2017 - Cross-site Scripting (XSS)	No API equivalent	Cross-Site Scripting (XSS)
A8:2017 - Insecure Deserialization	No API equivalent	Java Deserialization

Other Attacks	SSRF
	Path Manipulation
	Local File Inclusion (LFI)
	Remote Code Execution
	HTTP Request Smuggling
	HTTP Response Splitting
	Remote File Inclusion (RFI)
	LDAP/JNDI Manipulation
	Scanner Detection
	Credential Stuffing
	Brute forcing
	API Overuse

Anomaly Detection	Missing Consistent Parameter
	Unseen Parameter Types
	Double Parameter /
	Parameter Confusion
	Unexpected Wildcard
	Unexpected Length
	Unexpected Enum Value
	Unknown HTTP Header
	Unknown Device
	Unexpected Content Type
	Unexpected Content Length
	Browser Accessed Non-Browser Endpoint
	Request Size Mismatch
	Unexpected HTTP Method
	Unexpected Response Code

Key CVEs	CVE-2021-44228 - Log4j
	CVE-2022-22965 Spring4Shell
	CVE-2021-31207 - MS Exchange Shell
	CVE-2020--17530 - OGNL/Struts 2
	CVE-2018-7600 - Drupal
	CVE-2014-6271 - RCE
	CVE-2015-4852- Java deserialize

Traceable AI is a leader in API Security for Cloud-Native Apps

Discover and catalog your APIs. Find sensitive data at risk. Stop known and unknown attacks. Go deep for threat analytics, forensics, and troubleshooting.

TRACEABLE

www.traceable.ai

Doc Ver: 2022-04-04