INDUSFACE™

AppTrana API Protection

OWASP API Security Top 10 2023 – AppTrana API Protection

OWASP API Security Top 10 – 2023	CWE	Coverage	Coverage Comments	Description
A1:2023 – Broken Object Level Authorization	CWE-284: Improper Access Control	Limited through Custom Rules	Custom Rules possible when we can identify user and relevant action through URI.	Authorization checks should validate that the logged-in user does have access to perform the requested action on the requested object.
	CWE-285: Improper Authorization			
	CWE-639: Authorization Bypass Through UserControlled Key			
A2:2023 – Broken Authentication	CWE-798: Use of Hard-coded Credentials	Limited through Custom Rules	Custom rule possible for some scenarios after checking POC details.	Permits credential stuffing whereby the attacker has a list of valid usernames and passwords, Permits attackers to perform a brute force attack on the same user account, without presenting captcha/account lockout mechanism, Permits weak passwords, Sends sensitive authentication details, such as auth tokens and passwords in the URL, Doesn't validate the authenticity of tokens, Accepts unsigned/weakly signed JWT tokens ("alg":"none")/doesn't validate their expiration date, Uses plain text, encrypted, or weakly hashed passwords, Uses weak encryption keys.
A3:2023 – Excessive Data Exposure	CWE-213: Intentional Information Exposure	Yes	We can hide/mask sensitive info if it does not affect working of API.	API returns sensitive data like PII, CC info, etc.
A4:2023 – Lack of Resources & Rate Limiting	CWE-307: Improper Restriction of Excessive Authentication Attempts	Yes	-	Brute-force attacks, Rate limiting: Execution timeouts, Max allocable memory, Number of file descriptors, Number of processes, Request payload size (e.g., uploads), Number of requests per client/resource, Number of records per page to return in a single request response.
	CWE-770: Allocation of Resources Without Limits or Throttling	Yes		

A5:2023 – Broken Function Level Authorization	CWE-285: Improper Authorization	No	Cannot distinguish between legit & malicious traffic. WAF cannot detect which user can use which function.	Forced Browsing.
A6:2023 – Unrestricted Access to Sensitive Business Flows	CWE-306: Missing Authentication for Critical Function	Limited through Custom Rules	WAF can detect and block unauthorized access to sensitive API flows by enforcing rules for roles or user actions. But dynamic functions/real-time execution cannot be detected by WAF.	APIs expose sensitive business operations without proper access control, allowing unauthorized actions. WAF rules can enforce IP whitelisting or block requests from unauthorized users trying to access this endpoint.
A7:2023 – Server-Side Request Forgery (SSRF)	CWE-918: Server-Side Request Forgery (SSRF)	Limited through Custom Rules	WAF can inspect API requests for malicious or unauthorized URLs and block known SSRF patterns.	WAF can block malicious payloads in user inputs. It can detect and block requests targeting internal/private network addresses. WAF can enforce URL whitelisting to restrict the domains or IP ranges that the server is allowed to contact.
A8:2023 – Security Misconfiguration	CWE-2: Environmental Security Flaws CWE-16: Configuration CWE-388: Error Handling	Yes	Custom rule possible for some scenarios after checking POC.	Appropriate security hardening is missing across any part of the application stack, or if it has improperly configured permissions on cloud services, The latest security patches are missing, or the systems are out of date, Unnecessary features are enabled (e.g., HTTP verbs), Transport Layer Security (TLS) is missing, Security directives are not sent to clients (e.g., Security Headers), A Cross-Origin Resource Sharing (CORS) policy is missing or

				improperly set, Error messages include stack traces, or other sensitive information is exposed.
A9:2023 – Improper Inventory Management	CWE-1059: Incomplete Documentation CWE-440: Improper Handling of Insufficiently Documented or Deprecated APIs	Yes	We can apply access restriction based rules to APIs. Ex test APIs could be accessed by certain IPs only etc.	The purpose of an API host is unclear, and there are no explicit answers to the following questions: Which environment is the API running in (e.g., production, staging, test, development)? Who should have network access to the API (e.g., public, internal, partners)? Which API version is running? What data is gathered and processed by the API (e.g., PII)? What's the data flow? There is no documentation, or the existing documentation is not updated, There is no retirement plan for each API version, Hosts inventory is missing or outdated, Integrated services inventory, either first- or thirdparty, is missing or outdated, Old or previous API versions are running unpatched.
A10:2023 – Unsafe Consumption of APIs	CWE-863: Incorrect Authorization CWE-915: Improper Data Validation CWE-20: Improper Input Validation	Yes	WAF rules can monitor payloads for malicious content and custom rules can be added to validate APIs for its format, type, and expected values.	WAF can monitor and validate incoming data to ensure it meets expected patterns (e.g., formats, headers). It can block malicious payloads from external APIs by inspecting headers or content and can enforces strict API security rules, such as CORS and security headers (e.g., Content-Security-Policy).