AppTrana API Protection

OWASP API Security Top 10 2019 – AppTrana API Protection

OWASP API Security Top 10 – 2019	CWE	Coverage	Coverage Comments	Description
A1:2019 – 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 User-Controlled Key			
A2:2019 – 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.
A3:2019 – 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.
A4:2019 – 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		

A5:2019 – 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.
A6:2019 – Mass Assignment	CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes	No	Dynamic functions/real-time execution cannot be detected by WAF.	Permission-related properties: user.is_admin, user.is_vip should only be set by admins, Process-dependent properties: user.cash should only be set internally after payment verification, Internal properties: article.created_time should only be set internally by the application.
A7:2019 – Security Misconfiguration	CWE-2: Environmental Security Flaws	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.
	CWE-16: Configuration			
	CWE-388: Error Handling			
A8:2019 – Injection	CWE-77: Command Injection	Yes	-	Client-supplied data is not validated, filtered, or sanitized by the API, Client-supplied data is directly used or concatenated to SQL/NoSQL/LDAP queries, OS commands, XML parsers, and Object Relational Mapping (ORM)/Object Document Mapper (ODM), Data coming from external systems (e.g., integrated systems) is not validated, filtered, or sanitized by the API.
	CWE-89: SQL Injection			
A9:2019 – Improper Assets Management	CWE-1059: Incomplete Documentation	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 third-party, is missing or outdated, Old or previous API versions are running unpatched.
A10:2019 – Insufficient Logging & Monitoring	CWE-223: Omission of Security-relevant Information	Yes	WAF is providing monitoring and logging.	It does not produce any logs, the logging level is not set correctly, or log messages do not include enough detail, Log integrity is not guaranteed (e.g., Log Injection), Logs are not continuously monitored, API infrastructure is not continuously monitored.
	CWE-778: Insufficient Logging			