Kong THE CLOUD CONNECTIVITY COMPANY

Kong and OWASP Top 10 API Security

Kalidass Mookkaiah, Senior Field Engineer

August 2022

Agenda

1. OWASP context
2. Kong and OWASP top 10

OWASP Context

- OWASP Top 10 APi Security considerations are critical
- https://owasp.org/www-project-api-security/

API1:2019 Broken Object Level Authorization

- Definition: APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user
- Kong Approach
  - Use Authentication and Authorization plugins
  - Use Protocols and Auth flows
  - Number of Authentication and Authorization plugins
  - Plugin integrates with Third Party Identity Providers
  - Authentication metadata from IDP is passed to upstream service
  - Upstream responsible for ensuring authenticated users has privilege
- Ref
  - https://docs.konghq.com/hub/#authentication

API2:2019 Broken User Authentication

- **Definition:** Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user’s identities temporarily or permanently. Compromising a system’s ability to identify the client/user, compromises API security overall
- Kong Approach
  - Organisation can delegate authentication/configuration/governance to API layer
  - Kong allows central configuration
- Ref
  - https://docs.konghq.com/hub/#authentication

API3:2019 Excessive Data Exposure

- Definition: Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before displaying it to the user
- Kong Approach
  - Backend responsible to provide content
  - Kong can obfuscate or remove data that need filtering
  - Kong can provide different clients different data from the same upstream service
- Ref
  - https://docs.konghq.com/hub/kong-inc/response-transformer-advanced/

API4:2019 Lack of Resources & Rate Limiting

- Definition: Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force
- Kong Approach
  - Many options to prevent client from inadvertently or maliciously use
    - Rate Limiting plugin
      - many options to configure
      - Can be applied at global, service, route or consumer level
      - Can be tracked by consumer, IP, credential, service or header
      - Highly performant with redis support
    - Request Size Limiting Plugin
      - Prevent unexpected large request payload
        - Protect Kong and backend services
        - Specify payload size limit, required content-length header
- Ref
  - https://docs.konghq.com/hub/kong-inc/rate-limiting-advanced/
  - https://docs.konghq.com/hub/kong-inc/request-size-limiting/

API5:2019 Broken Function Level Authorization

- Definition: Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions
- Kong Approach
  - Can enforce endpoint/route level authentication and Authorization
  - Kong can prevent consumer without appropriate role from accessing route
- Ref
  - https://docs.konghq.com/hub/kong-inc/acl/
  - https://konghq.com/blog/token-based-access-control

API6:2019 Mass Assignment

- Definition: Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on an allow list, usually leads to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to
- Kong Approach
  - Can use Request Validator PLugin to prevent inadvertent acceptance of unpublished parameters and fields of backend data model
  - Support JSON request body schema
  - Enforce parameter schema based on OAS
  - Enforce specific allowed content types
- Ref
  - https://docs.konghq.com/hub/kong-inc/request-validator/

API7:2019 Security Misconfiguration

- Definition: Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad-hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information
- Kong Approach
  - Kong Route narrow the scope of API endpoints, methods, protocols etc exposed by backend service
  - CORS plugin from granular CORS access definition
  - Response Transformer and Exit Transformer plugins to modify or obfuscate response bodies and status codes to prevent leak
- Ref
  - https://docs.konghq.com/gateway/2.8.x/reference/proxy/#routes-and-matching-capabilities
  - https://docs.konghq.com/hub/kong-inc/cors/
  - https://docs.konghq.com/hub/kong-inc/response-transformer-advanced/
  - https://docs.konghq.com/hub/kong-inc/exit-transformer/

API8:2019 Injection

- Definition: Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization
- Kong Approach
    - Authentication and Authorization
        - Every request must be authenticated and Authorized.
        - And ACL to enforce endpoint level authorization
    - Input validation
        - Strict input validation (request parameters and request body to schema)
    - Request sanitation: Request transformer plugin to scrub and filter body and parameters
    - Response Cleansing
        - Response Transformer Plugin to control response
        - Response Size Limit Plugin to limit response size
- Ref
    - https://docs.konghq.com/hub/#authentication
    - https://docs.konghq.com/hub/kong-inc/acl/
    - https://konghq.com/blog/token-based-access-control

API8:2019 Injection cont…

- Ref
  - https://docs.konghq.com/hub/kong-inc/request-validator/
  - https://docs.konghq.com/hub/kong-inc/request-transformer-advanced/
  - https://docs.konghq.com/hub/kong-inc/response-transformer-advanced/
  - https://docs.konghq.com/hub/optum/kong-response-size-limiting/

API9:2019 Improper Assets Management

- Definition: `APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints`
- Kong Approach
  - Kong Route abstracts away the details of the upstream service to meet API7:2019 Security Misconfiguration
  - Route abstracts away API versions without impacting API client
  - Developer Portal allows documentation + publication + discovery + registration
  - Developer portal support third party IDP to control Access
- Ref
  - https://docs.konghq.com/gateway/2.8.x/reference/proxy/#routes-and-matching-capabilities
  - https://docs.konghq.com/gateway/2.8.x/developer-portal/

API10:2019 Insufficient Logging & Monitoring

- Definition: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, extract, or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring
- Kong Approach
  - Kong provides observability pillars - Logging + Metrics + Tracing
  - Provides many generic (HTTP, TCP, UDP) and vendor specific (DataDog, Prometheus, StatsD..) logging
  - Metrics plugins for exposing both Aggregated and Request level logs and metrics
  - Support many standard tracing headers like b3, b3-single, w3c, jaeger etc
- Ref
  - https://docs.konghq.com/hub/#analytics-monitoring
  - https://docs.konghq.com/hub/#logging

Thank You