DEFEND AGAINST OWASP API SECURITY TOP 10

R&S®Trusted Application Factory shields you with advanced API protection mechanisms

A1 BROKEN OBJECT LEVEL AUTHORIZATION

- APIs expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue.
- Object level authorization checks are lacking in every function that accesses a data source using an input from the user.

R&S®Trusted Application Factory:
Randomizes application identifiers (ids) by session with random tokens to increase difficulty in guessing unauthorized ids.

A2 BROKEN USER AUTHENTICATION

- Authentication mechanisms are implemented incorrectly, allowing attackers to compromise authentication tokens to assume other user's identities.
- This compromises API security overall.

R&S®Trusted Application Factory:
Assigns JSON Web Token (JWT) on user authentication. Applies rate limiting on authentication endpoints.

A3 EXCESSIVE DATA EXPOSURE

- Developers tend to expose all object properties without considering their individual sensitivity.
- They rely on clients to perform the data filtering before displaying it to the user.

R&S®Trusted Application Factory:
Detects sensitive error messages and confidential data with outgoing filtering capabilities with schema validation on all API responses.

A4 LACK OF RESOURCES & RATE LIMITING

- APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user.
- This can affect the API server performance, leading to denial of service (DoS), and authentication flaws such as brute force attacks.

R&S®Trusted Application Factory:
Includes API request rate limiting, API parser and schema validation to stop brute force attacks.

A5 BROKEN FUNCTION LEVEL AUTHORIZATION

- Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, lead to authorization flaws.
- By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

R&S®Trusted Application Factory:
Involves API schema validation like OpenAPI3 to block unauthorized or unknown actions defined at design time.

A6 MASS ASSIGNMENT

- Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on an allowlist, 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.

R&S®Trusted Application Factory:
Includes API schema validation like OpenAPI3 to block unauthorized actions in requests defined at design time.

A7 SECURITY MISCONFIGURATION

- Security misconfiguration is a result of unsecure 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.

R&S®Trusted Application Factory:
Adds security headers to clients. Detects error messages with outgoing filtering. Allows virtual patching capabilities on access control using Workflow-as-Code.

A8 INJECTION

- 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.

R&S®Trusted Application Factory:
Detects injections with blacklist engines (ICX) and blocks unknown resources/data with API schema validation.

A9 IMPROPER ASSETS MANAGEMENT

- 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.

R&S®Trusted Application Factory:
Includes API schema validation like OpenAPI3 to block unauthorized actions defined at design time. Allows to Whitelist or Blacklist known, unknown or deprecated API endpoints.

A10 INSUFFICIENT LOGGING & MONITORING

- Lack or ineffectiveness of the means of surveillance and event logging results in system sensitivity.
- Most intrusion studies show that the average detection time of an attack is more than 200 days.
- An attack is detected by external service providers rather than through internal monitoring and processes.

R&S®Trusted Application Factory:
Delivers detailed monitoring via access logs on traffic and security logs on detected events (with the entire request context). Sends logs to SIEM system for consolidation. Allows only logging and not blocking requests on detection.

ROHDE&SCHWARZ