wallarm

PRODUCT DATASHEET

Wallarm Protection for OWASP Top 10 Business Logic Abuse

The OWASP Top 10 for Business Logic Abuse identifies the most critical ways attackers exploit flaws in application logic to bypass rules, manipulate workflows, or trigger unintended behaviors. Unlike traditional vulnerabilities such as injections or remote code execution, business logic abuse targets the design of the application itself. These flaws often lead to fraud, data leakage, and operational disruption. As APIs become central to business processes, protecting against these logic-level threats is essential for maintaining trust, integrity, and service availability.

Wallarm offers robust, AI-driven API security features that directly address the OWASP Top 10 for Business Logic Abuse. This data sheet outlines how Wallarm mitigates each of the ten categories of business logic abuse with its advanced API protection capabilities.

wallarm

Lifecycle & Orphaned Transitions Flaws

These flaws arise when temporary artifacts from multi-step workflows (like tokens or sessions) are not properly invalidated, allowing attackers to invoke orphaned or expired processes.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
API Discovery	Identifies orphaned or shadow APIs that no longer align with valid workflows.
Specification Enforcement	Blocks calls to deprecated or undefined endpoints.
Session Anomaly Detection	Prevents use-after-expiration by tracking session behavior and detecting reuse of expired tokens.

Logic Bomb, Loops, and Halting Issues

These vulnerabilities involve hidden triggers or infinite loops caused by missing termination checks, unbounded recursion, or unchecked input, potentially leading to denial of service.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Payload Inspection	Detects and blocks recursive or looping payloads (e.g., XML entity expansions, zip bombs).
GraphQL Protection	Enforces depth limits and fragment nesting rules.
Threat Replay Testing	Identifies non-terminating routines through safe replay of known exploits.

wallarm

Data Type Smuggling

This category targets failures in data-type enforcement, where attackers exploit type mismatches to bypass logic checks or trigger application errors.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Specification Enforcement	Validates that parameters match declared data types in OpenAPI specifications.
Custom Detectors	Blocks mismatched or unsafe parameter types (e.g., arrays instead of scalars).
Deserialization Monitoring	Flags suspicious or anomalous serialization patterns.

Sequential State Bypass

These issues occur when applications fail to enforce correct ordering of business logic steps, allowing attackers to skip mandatory states.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Session-Aware Anomaly Detection	Uses AI to detect invalid state transitions within the same user session.
Threat Replay Testing	Validates business process integrity by replaying request sequences.

wallarm

Data Oracle Exposure

These flaws allow attackers to infer internal application states (e.g., valid usernames or object existence) through varied responses, messages, or timing.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Infoleak Detection	Identifies and logs sensitive data exposures in API responses.
Response Normalization	Blocks GraphQL introspection/debug endpoints and rewrites sensitive headers.
Sensitive Data Discovery	Automatically flags endpoints that expose PII.

Missing Roles and Permission Checks

This vulnerability occurs when APIs fail to validate that a caller has the proper role or permission before allowing sensitive operations.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
BOLA & Enumeration Protections	Detects and blocks ID tampering, brute force, and forced browsing attempts.
Role-Based Access Control Enforcement	Allows fine-grained validation of user roles using custom logic.
Account Abuse Detection	Identifies account takeover and credential stuffing behavior.

wallarm

Transition Validation Flaws

These flaws result from missing or misapplied checks that ensure business rules are met before progressing to the next step in a process.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Parameter Enforcement	Ensures presence and correctness of all required request parameters.
Behavioral Anomaly Detection	Uses AI to validate logical correctness of parameter values.
Flow Order Enforcement	Detects and alerts on out-of-order requests.

Replays of Idempotent Operations

This category covers failures to enforce one-time execution of operations, enabling attackers to replay requests and trigger repeated actions.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Replay Detection	Blocks repeated identical operations within a session.
One-Time Token Monitoring	Flags and halts reuse of previously consumed tokens.
Abuse Prevention	Stops excessive retries to sensitive endpoints.

wallarm

Race Condition and Concurrency Issues

These issues stem from improper handling of concurrent requests or state transitions, allowing attackers to exploit timing gaps.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Concurrent Request Detection	Identifies high-frequency duplicate calls from the same actor.
Concurrency Throttling	Limits near-simultaneous requests to critical endpoints.
Session Correlation	Detects race conditions using sequence analysis of API sessions.

Resource Quota Violations

These vulnerabilities occur when applications lack adequate rate limiting or quota enforcement, making it possible to exhaust system resources.

Wallarm Capabilities

CAPABILITY	HOW IT HELPS
Rate Limiting	Enforces per-user, per-IP, or geo-based usage limits.
GraphQL Operation Controls	Caps operation size, nesting, and request complexity.
Quota Abuse Detection	Identifies abuse of costly operations (e.g., PDF generation, LLM queries).

wallarm

BOOK A DEMO

Why Wallarm?

Wallarm brings together API discovery, schema enforcement, AI-based anomaly detection, and abuse prevention in one unified platform. Its capabilities are purpose-built to detect and mitigate complex logic-layer threats across modern, microservice-based applications. As business logic abuse increasingly becomes the target of sophisticated attacks that traditional security controls overlook, Wallarm offers a unique combination of runtime visibility, behavioral understanding, and context-aware enforcement. This empowers security teams to stop fraud, prevent misuse, and ensure that application workflows function exactly as intended, even under hostile conditions. With Wallarm, organizations can move beyond generic input validation and gain the precision needed to secure API-driven business processes at the logic layer.

Learn more.....wallarm.com
Follow us.....Blog | X | LinkedIn | YouTube
Explore product.....tour.playground.wallarm.com