radware

Guide

CISO's Guide to API Protection in the Age of Business Logic Attacks

Table of Contents

Introduction

The modern threat landscape is a complex reflection of evolving technologies and motivations, putting CISOs on constant alert for outside forces seeking vulnerabilities to attack. With threats to API-based applications now putting the focus on business logic, CISOs and cybercriminals alike are looking inward to gain an advantage in a new cyberattack battleground. These savvy hackers hope to take the reins by using AI-assistance to quickly discover an organization's legitimate business logic and manipulating it for their own malicious purposes. This puts pressure on organizations and their CISOs to find a new level of business logic visibility and protection. The mission for CISOs is clear: business logic attacks (BLA) have arrived. It's up to you to find them and stop them.

Part I. The New API Landscape

The Rise of APIs

The way organizations build and interact with applications has drastically changed in recent years. Application programming interfaces (APIs) have become the backbone of modern applications, enabling seamless communication between systems and delivering fast, connected experiences to users via mobile apps, B2B and B2C platforms and C2C services. But as APIs grow in prominence, they also become prime targets for cybercriminals. To truly protect applications these days, CISOs must understand the evolution of today's threat landscape, the sophisticated techniques hackers now employ and the measures needed to stay ahead.

Evolving Threats to APIs

The focus on API protection traditionally centers around detecting and mitigating embedded attacks. These attacks involve direct exploitation techniques, such as injecting malicious payloads (e.g., SQL injection, cross-site scripting) or exploiting insecure authentication mechanisms. The goal: block malicious requests, stop data exfiltration and minimize disruption to the application.

However, the world of APIs has changed. Modern applications are more intricate, with APIs powering microservices architectures, third-party integrations and dynamic user experiences. This complexity introduces a new set of risks, and attackers have evolved their tactics to exploit them. Hackers now leverage tools powered by AI and generative AI to map out the inner workings of an application, uncover business logic vulnerabilities, and execute API business logic attacks.

Embedded Attacks vs. Business Logic Attacks

It's worth examining the shift in the API threat landscape by zeroing in on the definitions and differences between embedded attacks and business logic attacks.

Embedded Attacks

Embedded attacks focus on exploiting technical vulnerabilities in the API or its underlying infrastructure.

Examples include:

- SQL injection to access sensitive data
- Authentication bypass via weak token validation
- Exploiting outdated libraries or insecure endpoints

These attacks typically target specific API endpoints and are straightforward in nature, usually relying on known patterns or automated scripts. They're often detected and mitigated by traditional web application firewalls (WAFs), API gateways, and runtime application self-protection (RASP) solutions.

To effectively protect against API embedded attacks, make sure your WAF supports the following:

- **API auto-discovery** of all API endpoints and their parameters
- **Auto-generation of a detailed schema file** that is automatically converted into accurate and up-to-date positive security policies
- **Real-time auto-protection** with complete schema enforcement, which is crucial for detecting threats hidden within API calls

Business Logic Attacks

Business logic attacks take a different approach. Rather than exploiting technical flaws, these attacks target logical flaws in the way an API handles requests. Hackers aim to manipulate the intended functionality of the API to achieve malicious outcomes.

Examples include:

- Manipulating API calls to alter pricing in e-commerce applications
- Bypassing rate limits to scrape sensitive data
- Exploiting order workflows to initiate fraudulent transactions

Unlike embedded attacks, BLAs often exploit API flows, involving multiple endpoints, or sequences of API calls, to manipulate business logic and achieve their goals. With the help of AI tools, attackers are now automating the process of analyzing an API's behavior, reverse-engineering its business logic and discovering hidden flaws. This makes BLAs more scalable, harder to detect, and more dangerous than ever before.

Part II. Understanding Business Logic Attacks

The Risks of Business Logic Attacks

Business logic attacks can have devastating consequences for organizations:

- **Data Theft:** Exposing sensitive customer data or intellectual property
- **Revenue Loss:** Exploiting pricing models or payment flows
- **Fraud:** Abusing systems for unauthorized access or transactions
- **Brand Damage:** Losing customer trust after high-profile breaches

The challenge lies in the fact that these attacks don't rely on malicious looking payloads. They appear as legitimate API requests, making them difficult to distinguish from normal traffic. Traditional security solutions often fall short when it comes to detecting these nuanced threats.

Four Challenges of Protecting Against Business Logic Attacks

Due to the ubiquity and behind-the-scenes nature of APIs, keeping them safe from business logic attacks is no small feat. Some of the key challenges include:

1. **Understanding API Behavior:** APIs are often poorly documented, leaving gaps in knowledge about how they're supposed to behave.
2. **Dynamic Workflows:** APIs enable complex, multi-step transactions, making it harder to pinpoint misuse.
3. **Legitimate Appearance:** Since BLA requests mimic normal API traffic, they often evade detection by traditional rule-based systems.
4. **Sophisticated Attackers:** With AI-powered tools, attackers can test and refine their methods much faster than before.

Part III. Seven Must-Haves for Business Logic Attack Protections

Proper API security requires a combination of tools and solutions to ensure comprehensive protection against today's evolving threat landscape. DevOps pre-production tools play a key role in testing and maintaining secure API configurations, while CI/CD pipeline tools support automation and consistent deployments. However, although posture management and CI/CD tools are essential for building and maintaining healthy APIs, they do not provide runtime protection in production environments. This is where API gateways and Web Application and API Protection (WAAP) solutions become critical. In particular, when it comes to business logic attacks, specialized solutions like Radware's API Protection are essential, as they detect and mitigate a wide range of API threats in real time—ensuring the ongoing security of live applications.

To ensure comprehensive API security, organizations should prioritize solutions that provide:

1. Granular API Visibility

- Discover, map and inventory all APIs—including third-party APIs and shadow APIs—which can pose serious security risks by increasing an organization's attack surface.
- Monitor API access patterns and dependencies to identify potential vulnerabilities.

2. Behavioral Analysis and Anomaly Detection

- Leverage advanced AI-powered engines to analyze API behavior and establish baselines.
- Detect and respond to deviations, such as bypassing rate limits or exploiting workflows.

3. Continuous Mapping of Business Logic

- Map API business logic based on actual transactions in real time.

4. AI-driven Auto Security Policy Generation

- Automatically identify and adapt security policies against logical flaws as they emerge.

5. Policy Enforcement

- Provide support for custom business logic rules and automated enforcement to prevent misuse.

6. Real-Time Threat Mitigation

- Provide runtime capabilities to instantly identify business logic attacks and block malicious activities without disrupting legitimate traffic.

7. Cross-Correlation with Other Security Engines

- Seamlessly integrate API security with WAF, bot management, client-side protection, and Layer 7 DDoS protection.
- Use insights from all layers to detect complex, multi-step attack patterns and ensure robust defense.

Part IV. How Radware Stops Business Logic Attacks

Radware is the only vendor to offer runtime/realtime automatic detection and mitigation of business logic vulnerability attacks, providing auto-discovery of APIs and auto-learning of business logic. Unlike most competitors, who don't actually block business logic attacks and only provide vulnerability detection based on past logs, Radware provides immediate auto-policy generation with continuous accuracy optimization.

Multi-layered Detection and Mitigation of Business Logic Attacks

Continuous Real-time Learning of the API's Business Logic

Learns directly from real-time transactions, unlike others that rely on historical logs, allowing for immediate and accurate detection of malicious API calls.

Immediate Mitigation

Automatically generates and applies security policies in real time to block business logic attacks as they occur.

Accurate Bad Actor Identification

Goes beyond simple IP blocking to surgically identify and block the specific malicious user or client responsible for the attack. This prevents false blocking of legitimate users sharing the same IP.

Unmatched Detection and Mitigation Accuracy

Uses real-time AI driven context analysis of security policies to ensure only the most reliable policies are applied and significantly enhances the protection accuracy.

Summary

Navigating Business Logic Attacks and the New API Threat Landscape

APIs are the backbone of modern applications, but their growing complexity has created new opportunities for attackers. Business logic attacks underscore the need to rethink our approach to API security. While preventative measures are important, real-time protection and a multi-layered HTTP security strategy—including WAF, API protection, bot mitigation, client-side protection, and DDoS defense—are essential to stopping sophisticated attacks as they unfold. By leveraging advanced AI technologies that combine behavioral analysis, layered defenses, and continuous monitoring, organizations can stay ahead of evolving threats while keeping their APIs a secure foundation for innovation.

Learn more about API protection against embedded and business logic attacks.

Contact Radware

RWI 502 I 04.28.2025