SALT

CASE STUDY

Global healthcare leader caught a double-encoded attack, closing the compliance gap.

Executive Summary

A Fortune 500 Healthcare Technology company relying on a leading CDN WAF for perimeter defense discovered a critical blind spot. Attackers utilized **double-encoding evasion techniques** to bypass standard OWASP signatures targeting their catalog APIs. Salt Security identified the attack that caused the WAF to fail, allowing the customer to patch the vulnerability immediately.

The Challenge: The Illusion of Protection

The customer utilizes a top-tier CDN WAF with strict OWASP rulesets enabled. They assumed they were protected against standard injection and traversal attacks.

- **The Incident:** Attackers launched a campaign targeting the customer's product catalog (catalog.[domain].com).
- **The Vector**: Local File Inclusion (LFI) and Path Traversal attempts.
- **The Bypass:** The WAF inspection layer decoded the request once, found nothing malicious, and passed the traffic. However, the application backend decoded the input a second time, which would have rendered the malicious payload executable.

The Salt Solution

Unlike the WAF, which relies on static signatures at the edge, Salt Security analyzes the full context of API traffic.

- **Behavioral Detection:** Salt detected the anomalous payload structure despite the encoding evasion. We didn't just look for a string match; we looked for intent.
- **Campaign Intelligence:** Salt grouped similar attack patterns from multiple IPs, highlighting a coordinated campaign rather than isolated incidents.

- **Defending Against AI Agents:** This behavioral approach is critical for the AI era. While a human might try a few encoding tricks, AI Agents can autonomously cycle through thousands of encoding variations (Triple Encoding, Unicode, etc.) to find the single gap in your WAF ruleset. Salt catches the behavior regardless of the encoding used.
- **Actionable Remediation:** Salt surfaced the specific payload intelligence, enabling the security team to design and deploy a custom WAF rule to permanently mitigate this vector.

"Our CDN's WAF OWASP ruleset did not block the request because the payload was double-encoded... Thanks to the payload intelligence surfaced by Salt, and the similar patterns it grouped, we were able to quickly design and deploy a custom WAF rule to mitigate this vector moving forward."
— Principal Security Architect, Global Healthcare Technology Company

Key Takeaway for Security Teams

Compliance-based security (WAFs) is necessary but insufficient. In an era where attackers, and now AI Agents, can iterate through thousands of encoding variations to find a bypass, you need Salt Security to catch the logic abuse and evasion techniques that slip past the gateway.