SECURITY INCIDENT REPORT - SENTINEL EDGE AI

STRICTLY CONFIDENTIAL – INTERNAL USE ONLY.

INCIDENT OVERVIEW

- **Date of Report:** January 5, 2026
- **Incident ID:** SENTINEL-2026-003
- **Detection Agent:** Sentinel Edge AI (Qwen 2.5 Nano)
- **Current Status:** CRITICAL

1. EXECUTIVE SUMMARY.

Threat Level	CRITICAL
Attack Vector	SQL Injection (SQLi)
Confidence Score	98%

The Sentinel Edge AI autonomous agent has detected a high-confidence security anomaly targeting the web application's commerce module. The attack is identified as a **Union-Based SQL Injection**, indicating a serious attempt to bypass authentication mechanisms and exfiltrate sensitive administrative credentials from the backend database. **Immediate containment actions are strongly recommended** to prevent a full breach.

2. TECHNICAL INTELLIGENCEAttack Analysis

The attacker employed a specific SQL injection payload to manipulate a backend database query.

- **Payload Injected:** 'UNION SELECT 1,user,password...'
- **Target Vulnerability:** The 'id' parameter within the /shop/item.php endpoint.
- **Attacker Objective:** To append data from the admin_users table to the legitimate product search results, thereby revealing usernames and passwords.
- **Success Indicator:** The server returned an **HTTP 200 OK** status code, confirming that the application processed the malicious input without rejection. This is a definitive indicator of a successful vulnerability exploitation attempt.
- **Risk Assessment:** A successful exploitation could result in a full database breach, a complete administrative account takeover, and massive data leakage.

3. FORENSIC EVIDENCE (RAW LOG)

The following log entry captures the moment of the attack:

```
192.168.1.105 - - [05/Jan/2026] "GET /shop/item.php?id=999 UNION SELECT
1,user,password FROM admin_users" 200
```

- **Attacker IP Address:** 192.168.1.105
- **Target Endpoint:** /shop/item.php
- **Payload Signature:** UNION SELECT
-

4. REMEDIATION & ACTION PLAN Immediate Actions (0-1 Hour)

1. **Block IP:** Implement a firewall rule immediately to block traffic from the attacker's IP address: **192.168.1.105**.
2. **Session Termination:** Revoke and terminate all active administrator sessions immediately to preempt any unauthorized access following a potential credentials compromise.

Technical Remediation (24 Hours)

1. **Code Patch:** Refactor the vulnerable code in item.php to use **Prepared Statements (Parameterized Queries)** instead of vulnerable string concatenation. This is the only definitive long-term fix for SQL Injection.
2. **Input Validation:** Implement strict whitelist validation for the 'id' parameter to ensure it only accepts expected data, specifically integers.

DISCLAIMER

This report was automatically generated by Sentinel Edge AI. The threat classification is based on probabilistic models and must be verified by a human Security Operations Center (SOC) analyst before any permanent blocking actions are taken.