VAPORTRACE PENETRATION TEST REPORT

CONFIDENTIAL - INTERNAL USE ONLY

META	VALUE
DATE	2026-02-01
MISSION START	2026-02-01 09:23:08
CLASSIFICATION	PROPRIETARY / ADVERSARY EMULATION
ENGINE VERSION	VaporTrace v3.1 (Tactical Suite)

---

1. EXECUTIVE SUMMARY

1.1 Risk Overview

🔴 OVERALL BUSINESS RISK RATING: CRITICAL

The **VaporTrace Tactical Suite** has concluded a penetration test of the core API infrastructure. While the environment maintains basic security controls, we have identified **structural flaws** that pose an immediate threat to the organization's data integrity and operational continuity.

==

⚠️ KEY BUSINESS IMPACT VECTORS

1. UNAUTHORIZED DATA EXFILTRATION (BOLA)

- **The Risk:** A fundamental flaw in the authorization logic allows any authenticated user to access, modify, or delete data belonging to other customers.
- **Business Impact:** Potential **Mass Data Breach**. This leads to direct violation of data privacy regulations (GDPR/Local Laws), resulting in heavy legal fines, loss of customer trust, and brand devaluation.

2. BACKEND INFRASTRUCTURE COMPROMISE (Credential Leak)

- **The Risk:** Discovered hardcoded administrative credentials for our AWS S3 storage environment.
- **Business Impact: Total Data Loss or Ransomware.** An external actor could gain full control over the company's cloud storage, leading to the deletion of backups or the public leaking of

proprietary intellectual property.

3. SYSTEMIC SERVICE VULNERABILITY (Security Misconfiguration)

- **The Risk:** Inconsistent security protocols across 21 critical service endpoints.
- **Business Impact: Operational Downtime.** These gaps allow for sophisticated interception of executive communications and provide a roadmap for competitors or malicious actors to disrupt service availability.

==

💰 FINANCIAL & COMPLIANCE PROJECTION

- **Regulatory Exposure:** High. Failure to remediate the identified BOLA vulnerability creates a non-compliance status with industry standards (PCI-DSS/ISO 27001).
- **Recovery Cost:** Remediation now is estimated to be **10x cheaper** than responding to a live breach involving the identified AWS leak.

✅ EXECUTIVE RECOMMENDATION

Immediate authorization of the **Phase 2 Remediation Plan**. Priority must be given to the "Authorization Logic Patch" and the "Cloud Credential Rotation" to neutralize the threat of data exfiltration within the next 24-48 hours.

==

OVERALL RISK RATING: CRITICAL

METRIC	VALUE
Total Findings	9
Unique Targets	9
Average CVSS	6.9 / 10.0

1.2 Vulnerability Distribution

Breakdown of findings by severity (CVSS v3.1):

- **CRITICAL (9.0+):** 3 (███░░░░░░░)
- **HIGH (7.0-8.9):** 3 (███░░░░░░░)
- **MEDIUM (4.0-6.9):** 2 (██░░░░░░░░)
- **LOW (0.0-3.9):** 1 (█░░░░░░░░░)

---

2. REMEDIATION PRIORITY TRACKER

The following table prioritizes vulnerabilities requiring immediate attention. **Sorted by Severity (CVSS Descending).**

SEVERITY	CVSS	VULNERABILITY (OWASP)	CVE ID	AFFECTED TARGET	ACTION
🔴	9.8	API3	CVE-2022-23131	`https://api.target.corp/admin/roles`	**PATCH IMMEDIATELY**
🔴	9.2	API7	CVE-2021-26855	`https://api.target.corp/hooks/stripe`	**PATCH IMMEDIATELY**
🔴	9.1	API1	CVE-2024-BOLA-GENERIC	`https://api.target.corp/users/1001`	**PATCH IMMEDIATELY**
🟠	8.2	API5	CVE-2023-30533	`https://api.target.corp/v2/delete_user`	Remediate < 7 Days
🟠	8.1	API10	CVE-2024-PROBE	`https://api.target.corp/integrations/webhook`	Remediate < 7 Days
🟠	7.5	API4	CVE-2023-44487	`https://api.target.corp/reports/all`	Remediate < 7 Days
🟡	5.4	API8	CVE-2024-AUDIT	`https://api.target.corp`	Remediate < 30 Days
🟡	4.5	API2	-	`https://api.target.corp/app.bundle.js`	Remediate < 30 Days

---

3. TECHNICAL FINDINGS (DEEP DIVE)

Detailed evidence logs for engineering teams. **Sorted Chronologically (Execution Order).**

[EXPLOITED] API1:2023 Broken Object Level Auth on https://api.target.corp/users/1001

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `bola`
- **Target URL:** `https://api.target.corp/users/1001`
- **Details:** BOLA: Accessed administrative user profile via ID manipulation.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1594`	Collection
NIST CSF v2.0	`PR.AC-03`	Control Mapping
CVE / CVSS	`CVE-2024-BOLA-GENERIC`	**9.1** (Severity Score)

[CRITICAL] API7:2023 Server Side Request Forgery on https://api.target.corp/hooks/stripe

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `ssrf`
- **Target URL:** `https://api.target.corp/hooks/stripe`
- **Details:** SSRF: Cloud Metadata (169.254.169.254) keys exfiltrated.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1071.001`	Command & Control
NIST CSF v2.0	`PR.DS-01`	Control Mapping
CVE / CVSS	`CVE-2021-26855`	**9.2** (Severity Score)

[VULNERABLE] API3:2023 Broken Object Property Level Auth on https://api.target.corp/admin/roles

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `bopla`
- **Target URL:** `https://api.target.corp/admin/roles`
- **Details:** BOPLA: Mass Assignment allowed injection of 'role: admin'.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1592.001`	Privilege Escalation
NIST CSF v2.0	`PR.DS-01`	Control Mapping

Framework	ID / Control	Description / Tactic
CVE / CVSS	`CVE-2022-23131`	**9.8** (Severity Score)

[VULNERABLE] API5:2023 Broken Function Level Auth on https://api.target.corp/v2/delete_user

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `bfla`
- **Target URL:** `https://api.target.corp/v2/delete_user`
- **Details:** BFLA: DELETE method accepted from unprivileged account.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1548.003`	Privilege Escalation
NIST CSF v2.0	`PR.AC-05`	Control Mapping
CVE / CVSS	`CVE-2023-30533`	**8.2** (Severity Score)

[VULNERABLE] API10:2023 Unsafe Consumption of APIs on https://api.target.corp/integrations/webhook

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `probe`
- **Target URL:** `https://api.target.corp/integrations/webhook`
- **Details:** Unsafe Consumption: No signature verification on 3rd party webhook.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1190`	Initial Access
NIST CSF v2.0	`PR.DS-02`	Control Mapping
CVE / CVSS	`CVE-2024-PROBE`	**8.1** (Severity Score)

[VULNERABLE] API4:2023 Unrestricted Resource Consumption on https://api.target.corp/reports/all

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `exhaust`
- **Target URL:** `https://api.target.corp/reports/all`
- **Details:** DoS: Pagination limit fuzzing caused 5s latency spike.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1499.004`	Impact (DoS)
NIST CSF v2.0	`DE.AE-02`	Control Mapping
CVE / CVSS	`CVE-2023-44487`	**7.5** (Severity Score)

[INFO] API9:2023 Improper Inventory Management on https://api.target.corp/v1/swagger.json

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `map`
- **Target URL:** `https://api.target.corp/v1/swagger.json`
- **Details:** Information Disclosure: Full OpenAPI spec exposed publicly.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1595.002`	Reconnaissance
NIST CSF v2.0	`ID.AM-07`	Control Mapping
CVE / CVSS	`N/A`	**0.0** (Severity Score)

[INFO] API2:2023 Broken Auth on https://api.target.corp/app.bundle.js

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `scrape`
- **Target URL:** `https://api.target.corp/app.bundle.js`
- **Details:** Hardcoded Secrets: AWS S3 Bucket URL found in JS.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1552`	Credential Access
NIST CSF v2.0	`PR.AC-01`	Control Mapping
CVE / CVSS	`-`	**4.5** (Severity Score)

[WEAK CONFIG] API8:2023 Security Misconfiguration on https://api.target.corp

- **Timestamp:** 2026-02-01T12:23:11Z
- **Vector/Command:** `audit`
- **Target URL:** `https://api.target.corp`
- **Details:** Misconfiguration: Missing Strict-Transport-Security header.

Compliance Mapping:

Framework	ID / Control	Description / Tactic
MITRE ATT&CK	`T1562.001`	Defense Evasion
NIST CSF v2.0	`PR.PS-01`	Control Mapping
CVE / CVSS	`CVE-2024-AUDIT`	**5.4** (Severity Score)

---

4. METHODOLOGY & FRAMEWORK ALIGNMENT

This assessment was conducted using the **VaporTrace Tactical Engine**, adhering to standard Adversary Emulation protocols.

4.1 Framework Reference

- **MITRE ATT&CK:** Used to classify adversary tactics and techniques (T-Codes).
- **OWASP API Security Top 10 (2023):** Primary standard for API vulnerability classification.
- **NIST CSF v2.0:** Used for mapping findings to defensive controls (Identify, Protect, Detect, Respond, Recover).
- **CVSS v3.1:** Common Vulnerability Scoring System for severity quantification.

End of Report