

Confidential Internal Memo

Project: Horizon Phoenix

Date:

From: Jonathan Miller – Senior Security Analyst

To: Operations & Development Teams

Subject: Security Vulnerability Report – URGENT

Following the penetration test completed on \_\_\_\_\_, the following high-risk issues were identified in our production systems:

1. Customer Data Leak Risk:

- Database server db-prod-03 contains an unsecured table with names, addresses, and credit card numbers for ~24,500 customers.
- Vulnerability located in PaymentGatewayController.php line 221, related to unescaped SQL queries.
- Impacted accounts include high-profile clients:
  - \_\_\_\_\_ (CEO, J-Tech Solutions)
  - \_\_\_\_\_ (CFO, BrightView Capital)
  - \_\_\_\_\_ (Minister of Infrastructure)

2. Hardcoded Credentials:

- API key for Stripe payments: sk\_live\_51HvX34fL2mN7zQb6T...
- Root admin password for staging server: Adm1n#2025! shared among three developers.

3. Network Exposure:

- Firewall misconfiguration on vpn-hq-secure allowing inbound SSH from any IP.
- Last successful suspicious login: \_\_\_\_\_ from IP 185.23.91.42 (Ukraine).

Required Actions:

- Immediately rotate all credentials listed above.
- Patch SQL injection vulnerability by end of day \_\_\_\_\_.
- Restrict VPN to internal IP ranges only.

Note: This memo and all attachments are classified INTERNAL – EYES ONLY. Any external sharing is prohibited and subject to disciplinary action.