SOC165 – Possible SQL Injection Payload Detected

Full Investigation Report (LetsDefend)

Analyst:	Jukuri Nithin Kumar
Platform:	LetsDefend
Date of Analysis:	14-Nov-2025
Case Type:	Web Attack – SQL Injection
Status:	True Positive | Attack Failed

1. Executive Summary

On February 25, 2022, the LetsDefend alert **SOC165 – Possible SQL Injection Payload Detected** was generated. The alert involved suspicious SQL injection test payloads from an external IP (**167.99.169.17**) targeting an internal server (**172.16.17.18**) over HTTPS. Payloads included classical SQL injection tests:

- ' OR 1=1
- ' OR 'x'='x
- ORDER BY 3--
- '
- Encoded payloads (%27, %20, %3D...)

2. Investigation Steps

2.1 Alert Trigger Reason

The alert triggers when SQL Injection signatures appear in the HTTP request, including: **Quotes, OR operator, ORDER BY clause, comment sequences (--), and encoded values.**

3. Data Collection & Enrichment

3.1 Firewall Logs

Time	Source IP	Destination IP	URL	Status
11:30 AM	167.99.169.17	172.16.17.18	/	200
11:32 AM	167.99.169.17	172.16.17.18	/search/?q='	500
11:32 AM	167.99.169.17	172.16.17.18	/search/?q=' OR '1	500
11:33 AM	167.99.169.17	172.16.17.18	/search/?q=' OR 'x'='x	500
11:33 AM	167.99.169.17	172.16.17.18	ORDER BY 3--	500
11:34 AM	167.99.169.17	172.16.17.18	%22 OR 1 = 1	500

Indicators:
• HTTP 500 errors show backend crashes.
• No successful SQL output.
• Clear signs of probing, not exploitation.

3.2 IP Reputation (VirusTotal)

Source IP **167.99.169.17** flagged by 4 vendors. Hosted on DigitalOcean → often used in mass scanning attacks.

3.3 Internal Device Check

No evidence of compromise on internal server (172.16.17.18): - No malicious processes - No SQL shell activity - No suspicious outbound communications - No unusual command execution

4. Attack Analysis

Attack Type: SQL Injection

Direction: Internet → Company Network Pattern resembles automated SQLi scanners like SQLMap.

Was the Attack Successful?

■ No – The attack failed. Repeated HTTP 500s indicate blocked SQL execution.

5. Artifacts Collected

Value	Type	Comment
167.99.169.17	IP	Malicious external IP
172.16.17.18	Internal IP	Web server target
SQLi URLs	URL/Payload	Injection attempts
HTTP 500	Indicator	Shows failed exploitation

6. Final Determination

✔ Alert Accuracy: **True Positive** ■ Attack Success: **Failed** Impact: **None** Escalation: **Not required**

7. Final Analyst Comments

The alert SOC165 accurately detected SQL Injection attempts originating from a malicious external IP. All attempts failed, producing HTTP 500 errors. No compromise occurred. This case is a **True Positive with zero impact**.