

## What is SQL injection ?


- SQL injection is a type of attack in which a malicious user is able to execute arbitrary SQL statements on a database by manipulating input data to a web application.
- This can allow the attacker to gain access to sensitive data, such as passwords and personal information and potentially allow them to take over the entire database.

## How to detect SQL injection ?

- To detect SQL injection attacks using a URL, you can look for certain patterns or indicators in the URL itself.
- The presence of unusual characters or symbols, such as a single quote (') , Exclamation mark (!), Ampersand (&) , or Bracket ( ).
- The words like UNION, SELECT, AND , OR.

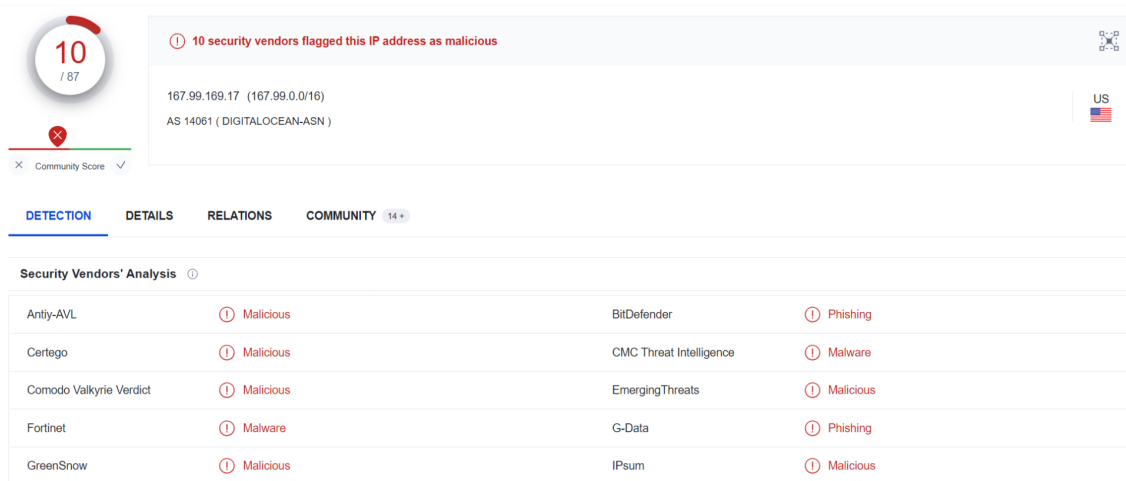
## SOC165 - Possible SQL Injection Payload Detected

Now lets see, what are the detail we have from generated alert ,

|   |   |
|---|---|
| EventID :   | 115   |
| Event Time :  | Feb, 25, 2022, 11:34 AM   |
| Rule :  | SOC165 - Possible SQL Injection Payload Detected                            |
| Level :   | Security Analyst  |
| Hostname :  | WebServer1001   |
| Destination IP Address :  | 172.16.17.18  |
| Source IP Address :   | 167.99.169.17   |
| HTTP Request Method :   | GET   |
| Requested URL :   | https://172.16.17.18/search/?<br>q=%22%20OR%201%20%3D%201%20--%20-          |
| User-Agent :  | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)<br>Gecko/20100101 Firefox/40.1 |
| Alert Trigger Reason :  | Requested URL Contains OR 1 = 1   |
| Device Action :   | Allowed   |
| Show Hint  |   |

- Here we are able to see all the information about SQL injection Attempt on Web Server 1001.
- Source IP Address - 167.99.169.17
- Decoded Requested URL : https://172.16.17.18/search/?q=" OR 1 = 1 -- -

## Investigation on 167.99.169.17:



10 / 87

10 security vendors flagged this IP address as malicious

167.99.169.17 (167.99.0.0/16)  
AS 14061 (DIGITALOCEAN-ASN)

US

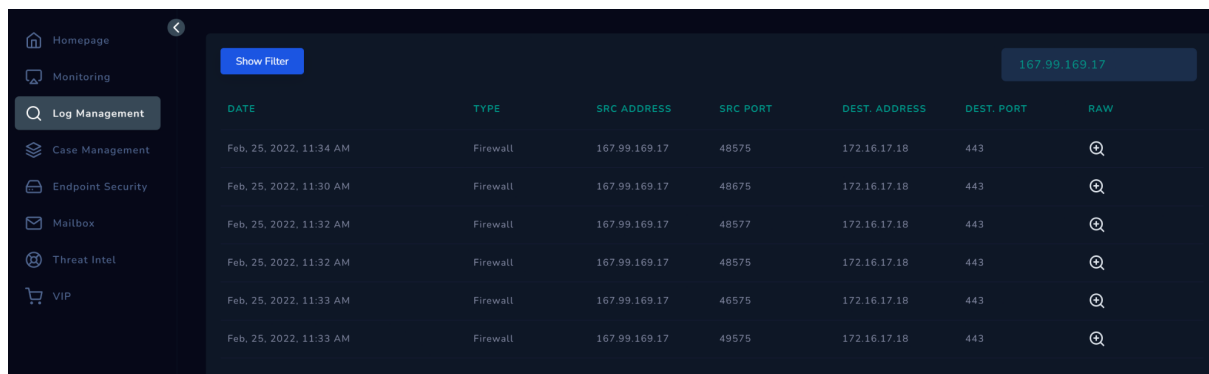
Community Score

DETECTION DETAILS RELATIONS COMMUNITY 14

Security Vendors' Analysis

|                         |           |                         |           |
|-------------------------|-----------|-------------------------|-----------|
| Antiy-AVL               | Malicious | BitDefender             | Phishing  |
| Certego                 | Malicious | CMC Threat Intelligence | Malware   |
| Comodo Valkyrie Verdict | Malicious | EmergingThreats         | Malicious |
| Fortinet                | Malware   | G-Data                  | Phishing  |
| GreenSnow               | Malicious | IPsum                   | Malicious |

- I tried with VirusTotal and Found a “RED FLAG”
- This IP address delivered malicious code, Malware and used to Phishing attacks



| DATE                    | TYPE     | SRC ADDRESS   | SRC PORT | DEST. ADDRESS | DEST. PORT | RAW |
|-------------------------|----------|---------------|----------|---------------|------------|-----|
| Feb. 25, 2022, 11:34 AM | Firewall | 167.99.169.17 | 48575    | 172.16.17.18  | 443        |     |
| Feb. 25, 2022, 11:30 AM | Firewall | 167.99.169.17 | 48675    | 172.16.17.18  | 443        |     |
| Feb. 25, 2022, 11:32 AM | Firewall | 167.99.169.17 | 48577    | 172.16.17.18  | 443        |     |
| Feb. 25, 2022, 11:32 AM | Firewall | 167.99.169.17 | 48575    | 172.16.17.18  | 443        |     |
| Feb. 25, 2022, 11:33 AM | Firewall | 167.99.169.17 | 46575    | 172.16.17.18  | 443        |     |
| Feb. 25, 2022, 11:33 AM | Firewall | 167.99.169.17 | 49575    | 172.16.17.18  | 443        |     |

- Now we are looking into the log, to find what requests are made by 167.99.169.17 .
- We are able to see the sequence of HTTPs requests to the Web server 1001.
- Attackers don't use any SQL injection Tools to initiate the attack. We can say that By viewing time delay between the requests.

Request URL: `https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B`

User-Agent: `Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1`

Request Method: `GET`

Device Action: `Permitted`

HTTP Response Size:: `948`

HTTP Response Status: `500`

- All the time, web server 1001 responded with 500 Internal Server Error
- Same Response size : 948.
- From this same response size we can say that “Attack was Unsuccessful!!”

## PlayBook Answers:

|                    |   |                         |  |
|--------------------|---|-------------------------|--|
| ^                  | High  | Feb, 25, 2022, 11:34 AM | SOC165 - Possible SQL Injection Payload Detected |
| EventID :          | 115   |                         |  |
| Event Time :       | Feb, 25, 2022, 11:34 AM   |                         |  |
| Rule :             | SOC165 - Possible SQL Injection Payload Detected  |                         |  |
| Answer :           | True Positive (+5 Point)  |                         |  |
| Playbook Answers : | Do You Need Tier 2 Escalation? (+5 Point)<br>Was the Attack Successful? (+5 Point)<br>What Is the Direction of Traffic? (+5 Point)<br>Check If It Is a Planned Test (+5 Point)<br>What Is The Attack Type? (+5 Point)<br>Is Traffic Malicious? (+5 Point) |                         |  |

- No need to Tier 2 Escalation
- NO, the attack was unsuccessful
- The Direction of Traffic : Internet To company network
- There is no Mail about the Testing (Attack). So this is Unplanned
- This is SQL based attack
- Yes, the Traffic was Malicious