


SOC165 - Possible SQL Injection Payload Detected

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

Click on >> and create case and click Continue.

Incident Details	
Incident Name:	EventID: 115 - [SOC165 - Possible SQL Injection Payload Detected]
Description:	EventID: 115
Incident Type:	Web Attack
Created Date:	Jan, 06, 2024, 03:05 PM
<div>Start Playbook!</div>	

×

Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Next

So, the SOC Rule talks about, “Possible SQL Injection Payload” which gives a direction towards the kind of attack we are about to investigate.

We can see that the requested URL is <https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20-%20-%20> which when we pass through URL Decoder comes up as [https://172.16.17.18/search/?q=" OR 1 = 1 - - -](https://172.16.17.18/search/?q=)

With a query such as “ OR 1 = 1”, it is a possible attempt to claim userIDs & passwords from WebServer1001 (mentioned as hostname) with IP address 172.16.17.18

Upon checking the reputation of the source IP address in VirusTotal

The screenshot shows the VirusTotal interface for the IP address 167.99.169.17. At the top, a red circle indicates a 'Community Score' of 5/91. A message states '5 security vendors flagged this URL as malicious'. Below this, a table titled 'Security vendors' analysis' lists several vendors and their detection results:

Vendor	Detection
BitDefender	Phishing
Fortinet	Malware
MalwareURL	Malware
CyRadar	Malicious
G-Data	Phishing
AlphaSOC	Suspicious

By taking a look at the Log management, it can be determined that the WebServer1001 has been receiving hits from source_address=167.99.169.17 since Feb, 25, 2022, 11:30 AM

The screenshot shows a 'New Search' interface with the query 'Raw Log contains "172.16.17.18"'. It displays 10 events. The first event is expanded, showing the following details:

- Event
- Time: [Feb, 25, 2022, 11:34 AM]
- source_address: 167.99.169.17
- source_port: 48575
- destination_address: 172.16.17.18
- destination_port: 443
- raw_log: {"Request URL": "https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20-%20-%20", "User-Agent": "Mozilla/5.0 (Windows ..."

After decoding the URLs, the results are:

<https://172.16.17.18/search/?q=1' ORDER BY 3-->

<https://172.16.17.18/search/?q=' OR 'x'='x>

<https://172.16.17.18/search/?q=' OR '1>

<https://172.16.17.18/search/?q='>

<https://172.16.17.18/>

[https://172.16.17.18/search/?q=" OR 1 = 1 -- -](https://172.16.17.18/search/?q=)

All of the above URLs point to a possible SQL Injection attack on the Webserver. This could be a specific attack on the server. Interestingly, the previous day Feb, 24, 2022, 10:30 AM... there are have been hits on the server at the same time from 4 different IP addresses.

✓	[Feb, 24, 2022, 10:30 PM] source_address=176.33.208.185 source_port=45675 destination_address=172.16.17.18 destination_port=443 raw_log: {Request URL: 'https://172.16.17.18/', 'User-Agent': 'Mozilla/5.0 (Window...
✓	[Feb, 24, 2022, 10:30 PM] source_address=176.33.208.184 source_port=45675 destination_address=172.16.17.18 destination_port=443 raw_log: {Request URL: 'https://172.16.17.18/', 'User-Agent': 'Mozilla/5.0 (Window...
✓	[Feb, 24, 2022, 10:30 PM] source_address=176.33.208.183 source_port=45675 destination_address=172.16.17.18 destination_port=443 raw_log: {Request URL: 'https://172.16.17.18/', 'User-Agent': 'Mozilla/5.0 (Window...
✓	[Feb, 24, 2022, 10:30 PM] source_address=176.33.208.182 source_port=45675 destination_address=172.16.17.18 destination_port=443 raw_log: {Request URL: 'https://172.16.17.18/', 'User-Agent': 'Mozilla/5.0 (Window...

Upon checking one of the addresses on Talos, it has a poor reputation with critical spam level

Lookup data results for IP Address

176.33.208.185

Search by IP, domain, or network owner for real-time threat data.

IP & Domain Reputation Overview | File Reputation Lookup | Email & Spam Data

LOCATION DATA

Kadıköy, Turkey

OWNER DETAILS

IP ADDRESS	176.33.208.185
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	superonline iletişim hizmetleri a.ş.

REPUTATION DETAILS

SENDER IP REPUTATION

Poor

Submit Sender IP Reputation Ticket

WEB REPUTATION

Unknown

Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Critical	

But since there were no follow-ups, this could well be a fire-and-forget scan. Proceeding with the Playbook,

Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
- Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
- Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
- Hostname of the device
- Who owns the device (username)
- Last user login time

Next

Ownership of the IP addresses and devices.: Digital Ocean

If the traffic is coming from outside (Internet); Yes

Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?): Digital Ocean

Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos): Malicious

If the traffic is coming from company network; No

Hostname of the device: WebServer1001

Who owns the device (username): webadmin

Last user logon time: Feb, 10, 2022, 11:12 PM

Examine HTTP Traffic

Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- [Web Attacks 101](#)

Next

Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- [Web Attacks 101](#)

Malicious

Non-malicious

As per our analysis, the traffic has been determined as Malicious with an intention to gain user info.

×

What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

Command Injection

IDOR

LFI & RFI

Other

SQL Injection

XML Injection

XSS

Selecting SQL Injection based on our finding.

×

Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

Not Planned

Planned

Post searching the mail Security tab for any relevant mails, nothing was found. Hence, selecting Not Planned.



What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

Company Network → Company Network

Company Network → Internet

Internet → Company Network

The source address was 167.99.169.17 and was attempting an SQL injection on the Webserver's address... so it's an INTERNET → Company Network.



Check Whether the Attack Was Successful

Investigate whether the attack was successful. Detection mechanisms vary according to the attack type. Some tips that can help with your investigation;

- In Command Injection attacks, you can understand whether the attack was successful by looking at the "Command History" of the relevant device via Endpoint Security. In SQL Injection attacks, attackers can run commands on the device with the help of functions such as "xp_cmdshell". For this reason, you may need to look at the "Command History" in SQL Injection attacks.
- You can guess by looking at the HTTP Response size in SQL Injection and IDOR attacks.

You can access the Web Attacks 101 training below, in which we explain how you can understand whether the attack is successful or not according to the attack type.

- [Web Attacks 101](#)

Next

The attack was not successful because at every attempt, as found in the logs, there was a Response Code of 500 which means it threw a server error. So, the attacker was unable to obtain the required info.

×

Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

Basis above explanation, selecting NO here.

×

Add Artifacts

+

Value	Comment	Type	Remove
167.99.169.17	Malicious URL	IP Address ▾	

Next

Added the recorded artifact which is the attacker's IP address. You may/may not want to add the other IP address who was trying to get a hit on Feb 24, 2022.

×

Do You Need Tier 2 Escalation?

Tier 2 escalation should be performed in the following situations.

- In cases where the attack succeeds,
- When the attacker compromises a device in the internal network (in cases where the direction of harmful traffic is from inside → inside),

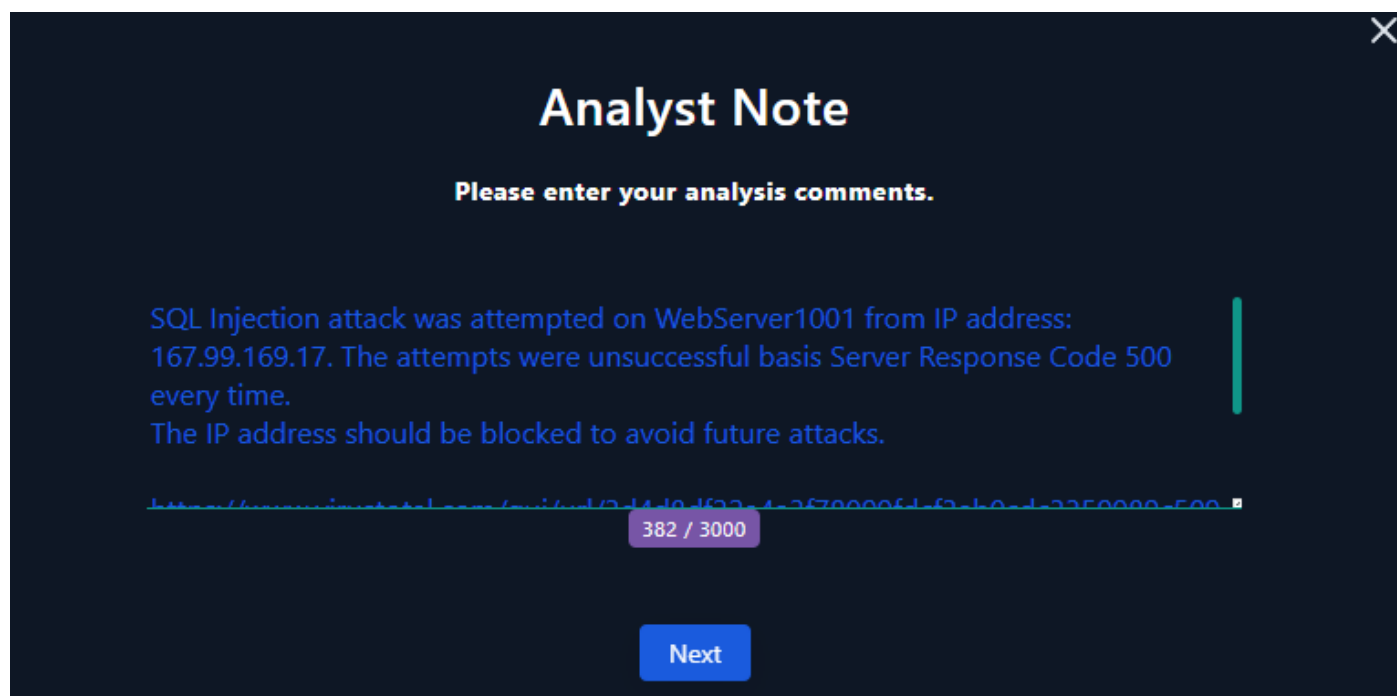
Tier 2 escalation is not required in the following cases.

- In cases where attacks from the Internet do not succeed

**** Institutions may have their own escalation procedure. Don't forget to learn about the escalation procedure in your institution.**

Perform Tier 2 escalation?

Since the attack was not successful, it does not require further Tier 2 escalation. Selecting NO here.

A dark-themed modal window titled "Analyst Note" with a close button (X) in the top right corner. The text inside says "Please enter your analysis comments." followed by a text area containing the following text: "SQL Injection attack was attempted on WebServer1001 from IP address: 167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time. The IP address should be blocked to avoid future attacks." Below the text area is a URL input field containing "https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection" and a character count "382 / 3000". At the bottom is a blue "Next" button.

Analyst Note

Please enter your analysis comments.

SQL Injection attack was attempted on WebServer1001 from IP address: 167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time.
The IP address should be blocked to avoid future attacks.

<https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection>

382 / 3000

Next

Add your finding as comments

“SQL Injection attack was attempted on WebServer1001 from IP address:

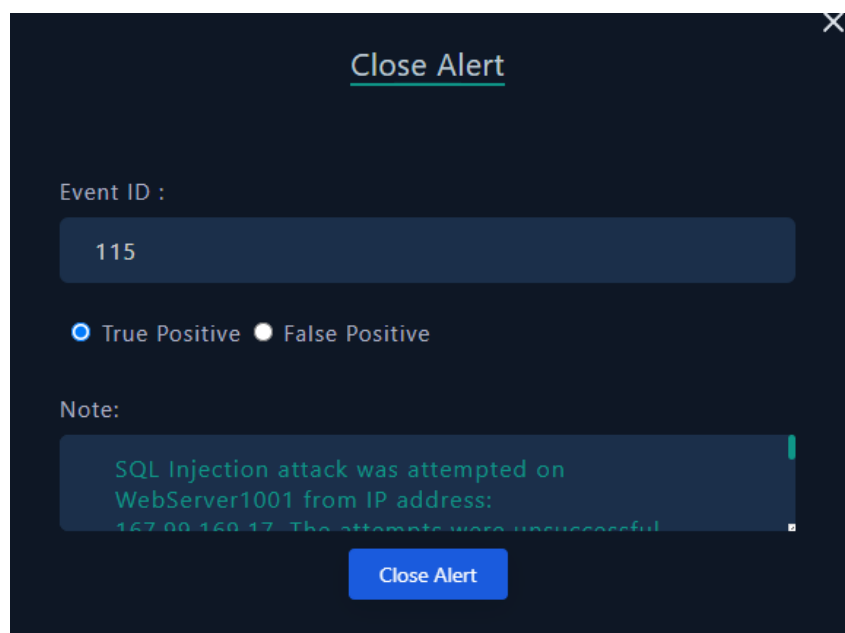
167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time.

The IP address should be blocked to avoid future attacks.

<https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection>

<https://otx.alienvault.com/indicator/ip/167.99.169.17>”

.. And click and confirm on FINISH PLAYBOOK and close the Alert.

A dark-themed modal window titled "Close Alert" with a close button (X) in the top right corner. It contains a form with the following fields: "Event ID :" with a value of "115", radio buttons for "True Positive" (selected) and "False Positive", and a "Note:" field with the text "SQL Injection attack was attempted on WebServer1001 from IP address: 167.99.169.17. The attempts were unsuccessful". At the bottom is a blue "Close Alert" button.

Close Alert

Event ID :

115

☒ True Positive ☐ False Positive

Note:

SQL Injection attack was attempted on WebServer1001 from IP address: 167.99.169.17. The attempts were unsuccessful

Close Alert

This would be a True Positive as a “Possible SQL Injection Payload” was detected.

Let’s check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan. 07, 2024, 12:54 AM	SOC165 - Possible SQL Injection Payload Detected	115	Web Attack	✓	↺
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)				
		Was the Attack Successful? (+5 Point)				
		What Is the Direction of Traffic? (+5 Point)				
		Check If It Is a Planned Test (+5 Point)				
		What Is The Attack Type? (+5 Point)				
Analyst Note :		Is Traffic Malicious? (+5 Point)				
		SQL Injection attack was attempted on WebServer1001 from IP address: 167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time. The IP address should be blocked to avoid future attacks.				
		https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection https://otx.alienvault.com/indicator/ip/167.99.169.17				
Community Walkthrough :		Show				

Hopefully this helped.