Project Title:

SOC Investigation – Classic SQL Injection Attack Detection

Objective:

Detect, investigate, and document a simulated SQL Injection (SQLi) attack against a web application, following SOC analysis workflows.

Overview of SQLi:

- **Definition:** SQLi occurs when unsanitized user input is embedded directly into SQL queries, allowing attackers to manipulate database queries.
- **In simpler terms:** It's like ordering food at a restaurant and, in the same order, slipping in, *"Oh, and give me the combination to the safe."* If the waiter doesn't double-check and block that part of the request, the attacker walks away with much more than they should.

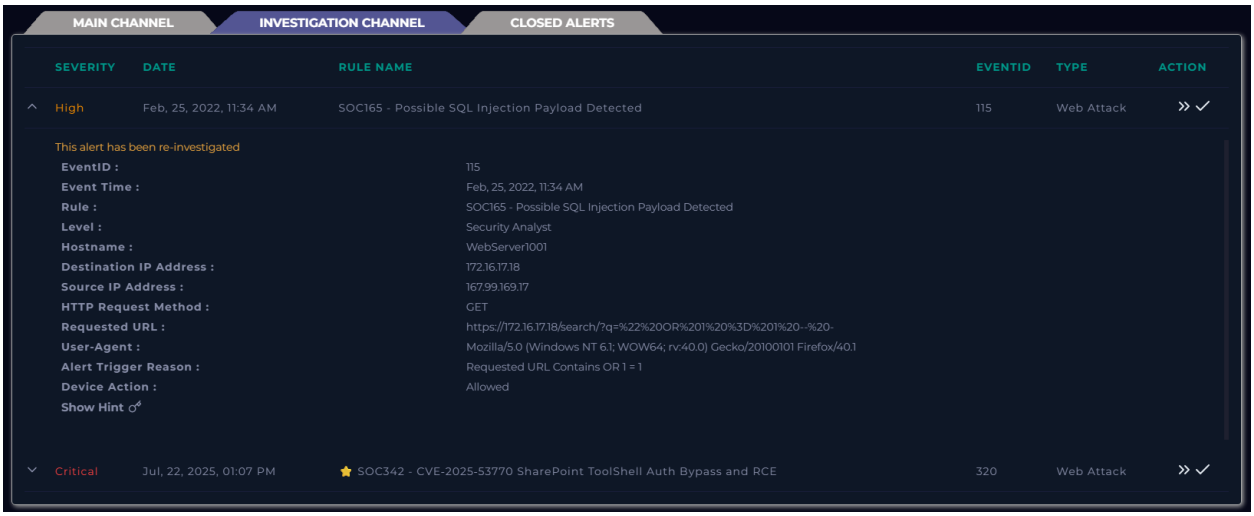
Tools & Techniques Used:

- **Monitoring –** Reviewed alerts in a SOC-style dashboard to identify suspicious activity.
- **Log Management –** Analyzed HTTP traffic and system logs to spot SQL patterns.
- **Case Management –** Claimed alert, opened a case, and documented steps using structured workflows.
- **Endpoint Security –** Checked affected systems for signs of compromise or malware.
- **Email Security –** Investigated potential phishing or coordination attempts.
- **Threat Intelligence –** Queried attacker IPs in AbuseIPDB and VirusTotal for reputation data.

Investigation Workflow:

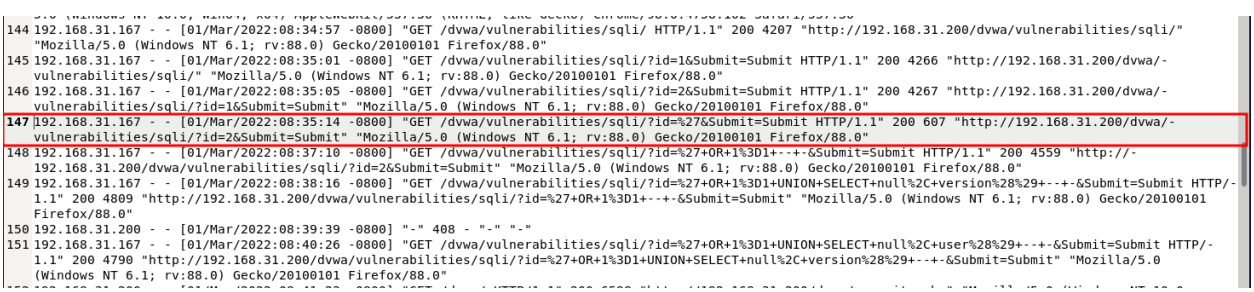
1. **Alert Claim & Case Initiation**

- Claimed the SQLi alert in the SOC system and initiated the playbook to ensure a structured investigation and documentation process.



2. **Log Analysis**

- Found a request containing a suspicious SQLi payload.
- Noted a change in response size compared to other attempts, marking the start of the exploitation phase.
- Determined as malicious activity requiring deeper review.



```
144 192.168.31.167 - - [01/Mar/2022:08:34:57 -0800] "GET /dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4207 "http://192.168.31.200/dvwa/vulnerabilities/sqli/"
    "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
145 192.168.31.167 - - [01/Mar/2022:08:35:01 -0800] "GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 200 4266 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
146 192.168.31.167 - - [01/Mar/2022:08:35:05 -0800] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1" 200 4267 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/?id=1&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
147 192.168.31.167 - - [01/Mar/2022:08:35:14 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit HTTP/1.1" 200 607 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/?id=2&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
148 192.168.31.167 - - [01/Mar/2022:08:37:10 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+--+-&Submit=Submit HTTP/1.1" 200 4559 "http://-
    192.168.31.200/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
149 192.168.31.167 - - [01/Mar/2022:08:38:16 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+version%28%29+--+-&Submit=Submit HTTP/-
    1.1" 200 4809 "http://192.168.31.200/dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+--+-&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101
    Firefox/88.0"
150 192.168.31.200 - - [01/Mar/2022:08:39:39 -0800] "-" 408 - "-" "-"
151 192.168.31.167 - - [01/Mar/2022:08:40:26 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+user%28%29+--+-&Submit=Submit HTTP/-
    1.1" 200 4790 "http://192.168.31.200/dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+version%28%29+--+-&Submit=Submit" "Mozilla/5.0
    (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
```

3. **Source IP Investigation**

   - Checked the attacker's IP using AbuseIPDB and VirusTotal, confirming prior malicious activity reports.

IP Abuse Reports for **167.99.169.17**:

This IP address has been reported a total of **14,926** times from 1,106 distinct sources. 167.99.169.17 was first reported on November 21st 2020, and the most recent report was **2 months ago**.

Old Reports: The most recent abuse report for this IP address is from **2 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC)	Comment	Categories
Anonymous	2025-06-01 14:50:00 (2 months ago)	.	Hacking, SQL Injection, Brute-Force, Exploited Host, Web App Attack, SSH
JA	2023-07-12 14:00:37 (2 years ago)	ssh login attempt	Brute-Force, SSH
Esoutien	2023-01-28 20:34:34 (2 years ago)	2023-01-19T12:05:50.310926server.espacesoutien.com sshd[4530]: Invalid user ftptest from 167.99.169. ... show more	Hacking, Brute-Force, SSH
zwh	2023-01-28 08:21:00 (2 years ago)	SSH Brute-Force	Brute-Force, SSH
ThreatBook.io	2023-01-22 21:25:50 (2 years ago)	ThreatBook Intelligence: Scanner,Zombie more details o n https://threatbook.io/ip/167.99.169.17	SSH
MU-star.net	2023-01-21 09:39:49 (2 years ago)	Invalid user jack from 167.99.169.17 port 41800	Port Scan, Brute-Force, SSH
itbyhf	2023-01-21 09:05:31 (2 years ago)	Jan 21 04:00:56 ns08 sshd[574347]: Failed password fo r invalid user ghostuser from 167.99.169.17 por ... show more	Brute-Force, SSH
Anonymous	2023-01-21 09:05:13	$f2bV_matches	Brute-Force

3 / 94

Community Score -15

3/94 security vendors flagged this IP address as malicious

Reanalyze | Similar | More

167.99.169.17 (167.99.0.0/16)

AS 14061 (DIGITALOCEAN-ASN)

US

Last Analysis Date 1 day ago

DETECTION | DETAILS | RELATIONS | COMMUNITY 176

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

ArcSight Threat Intelligence	Malware	BitDefender	Phishing
G-Data	Phishing	alphaMountain.ai	Suspicious
AlphaSOC	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean

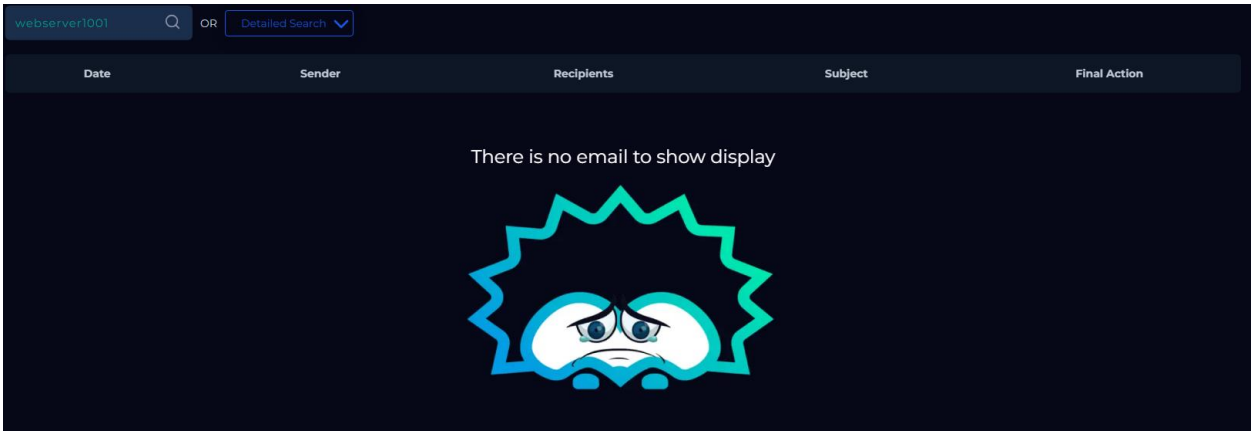
4. **Attack Classification**

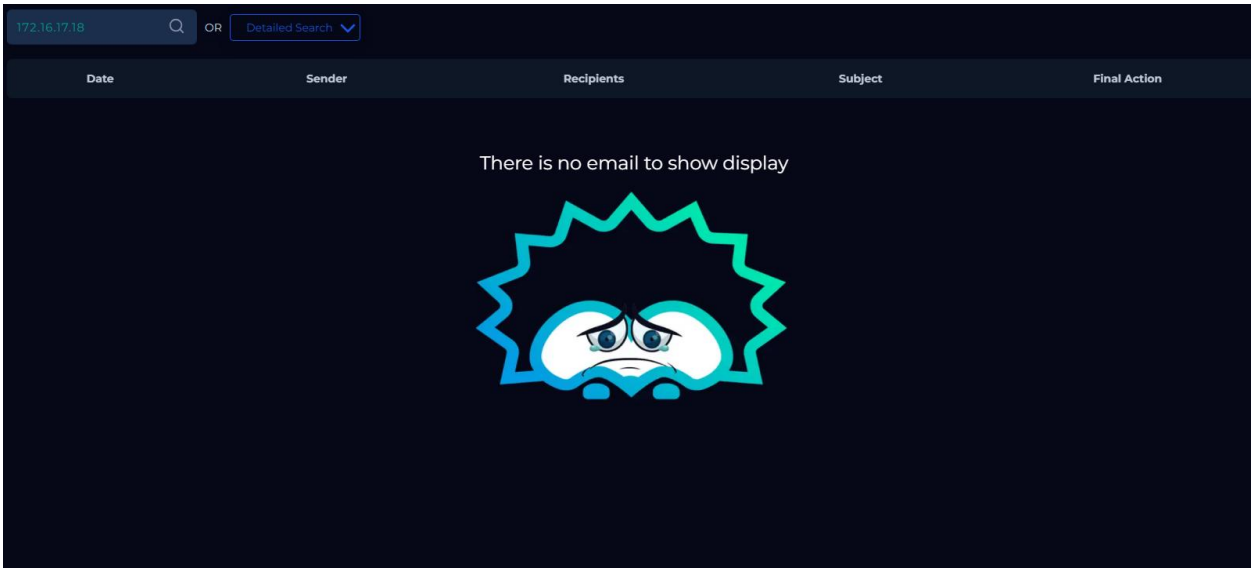
   - Classified as Classic (In-band) SQL Injection: The attacker received an immediate HTTP 200 (OK) response, providing real-time feedback — a hallmark of this SQLi type.

```
144 192.168.31.167 - - [01/Mar/2022:08:34:57 -0800] "GET /dvwa/vulnerabilities/sqli/ HTTP/1.1" 200 4207 "http://192.168.31.200/dvwa/vulnerabilities/sqli/"
    "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
145 192.168.31.167 - - [01/Mar/2022:08:35:01 -0800] "GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1" 200 4266 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
146 192.168.31.167 - - [01/Mar/2022:08:35:05 -0800] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1" 200 4267 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/?id=1&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
147 192.168.31.167 - - [01/Mar/2022:08:35:14 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit HTTP/1.1" 200 607 "http://192.168.31.200/dvwa/-
    vulnerabilities/sqli/?id=2&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
148 192.168.31.167 - - [01/Mar/2022:08:37:10 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+--+-&Submit=Submit HTTP/1.1" 200 4559 "http://-
    192.168.31.200/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
149 192.168.31.167 - - [01/Mar/2022:08:38:16 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+version%28%29+--+-&Submit=Submit HTTP/-
    1.1" 200 4809 "http://192.168.31.200/dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+--+-&Submit=Submit" "Mozilla/5.0 (Windows NT 6.1; rv:88.0) Gecko/20100101
    Firefox/88.0"
150 192.168.31.200 - - [01/Mar/2022:08:39:39 -0800] "-" 408 - "-" "-"
151 192.168.31.167 - - [01/Mar/2022:08:40:26 -0800] "GET /dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+user%28%29+--+-&Submit=Submit HTTP/-
    1.1" 200 4790 "http://192.168.31.200/dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1+UNION+SELECT+null%2C+version%28%29+--+-&Submit=Submit" "Mozilla/5.0
    (Windows NT 6.1; rv:88.0) Gecko/20100101 Firefox/88.0"
```

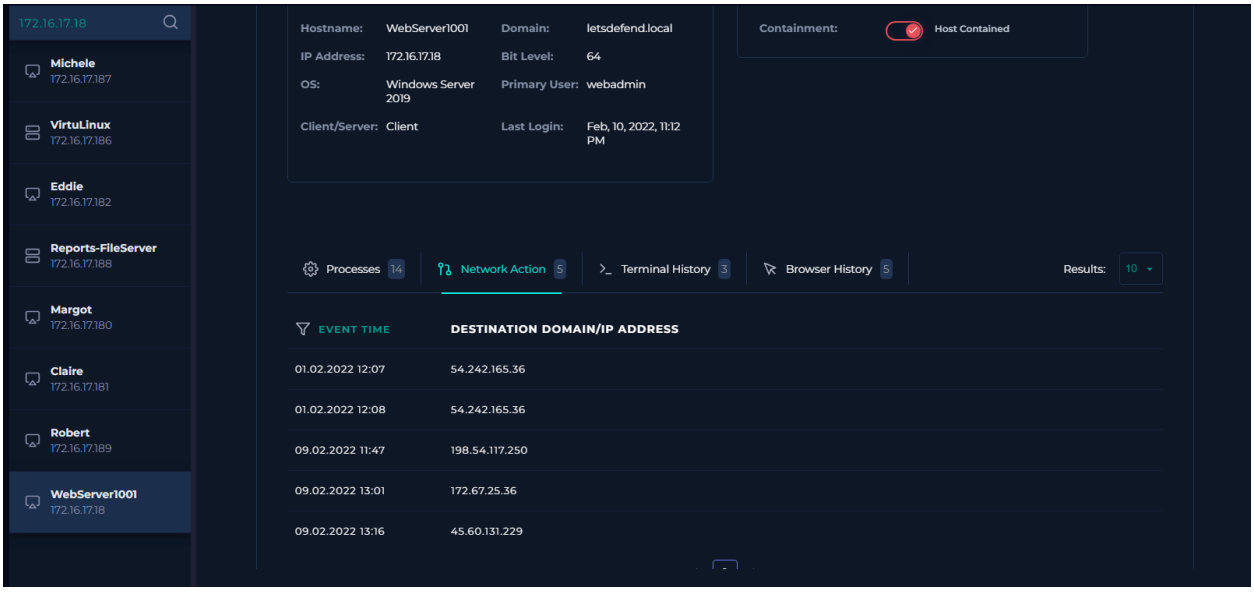
5. **Additional Checks & Success Evaluation**

   - Reviewed related email records — no evidence of pre-attack coordination found.





- Checked the targeted endpoint — no unauthorized services, additional network activity, or executed commands detected.



172.16.17.18

- Michele 172.16.17.187
- VirtuLinux 172.16.17.186
- Eddie 172.16.17.182
- Reports-FileServer 172.16.17.188
- Margot 172.16.17.180
- Claire 172.16.17.181
- Robert 172.16.17.189
- WebServer1001 172.16.17.18

Host Information

Hostname:	WebServer1001	Domain:	letsdefend.local
IP Address:	172.16.17.18	Bit Level:	64
OS:	Windows Server 2019	Primary User:	webadmin
Client/Server:	Client	Last Login:	Feb, 10, 2022, 11:12 PM

Action

Containment: Host Contained

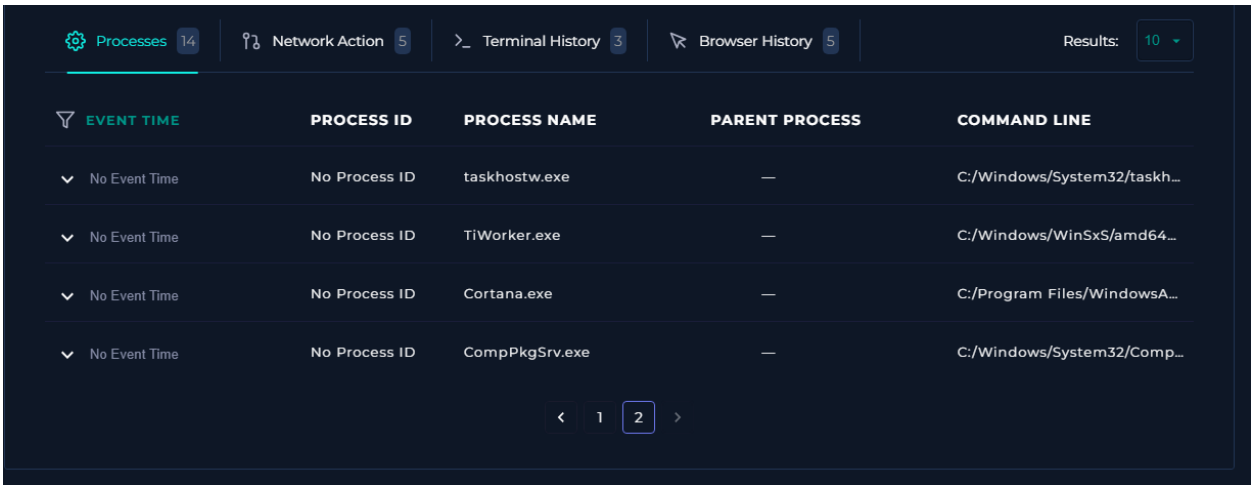
Processes 14 | Network Action 5 | Terminal History 3 | Browser History 5 | Results: 10

EVENT TIME	COMMAND LINE
01.02.2022 16:19	cd web-root
01.02.2022 16:20	docker-compose -f docker-compose-deploy.yml build
01.02.2022 16:24	docker-compose -f docker-compose-deploy.yml up

Processes 14 | Network Action 5 | Terminal History 3 | Browser History 5 | Results: 10

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	wininit.exe	—	C:/Windows/System32/winin...
No Event Time	No Process ID	services.exe	—	C:/Windows/System32/servi...
No Event Time	No Process ID	svchost.exe	—	C:/Windows/System32/svcho...
No Event Time	No Process ID	OfficeClickToRun.exe	—	C:/Program Files/Common F...
No Event Time	No Process ID	winlogon.exe	—	C:/Windows/System32/winlo...
No Event Time	No Process ID	explorer.exe	—	C:/Windows/explorer.exe
No Event Time	No Process ID	chrome.exe	—	C:/Program Files/Google/Ch...
No Event Time	No Process ID	smss.exe	—	C:/Windows/System32/smss....
No Event Time	No Process ID	csrss.exe	—	C:/Windows/System32/csrss....
No Event Time	No Process ID	OUTLOOK.exe	—	C:/Program Files (x86)/Micro...

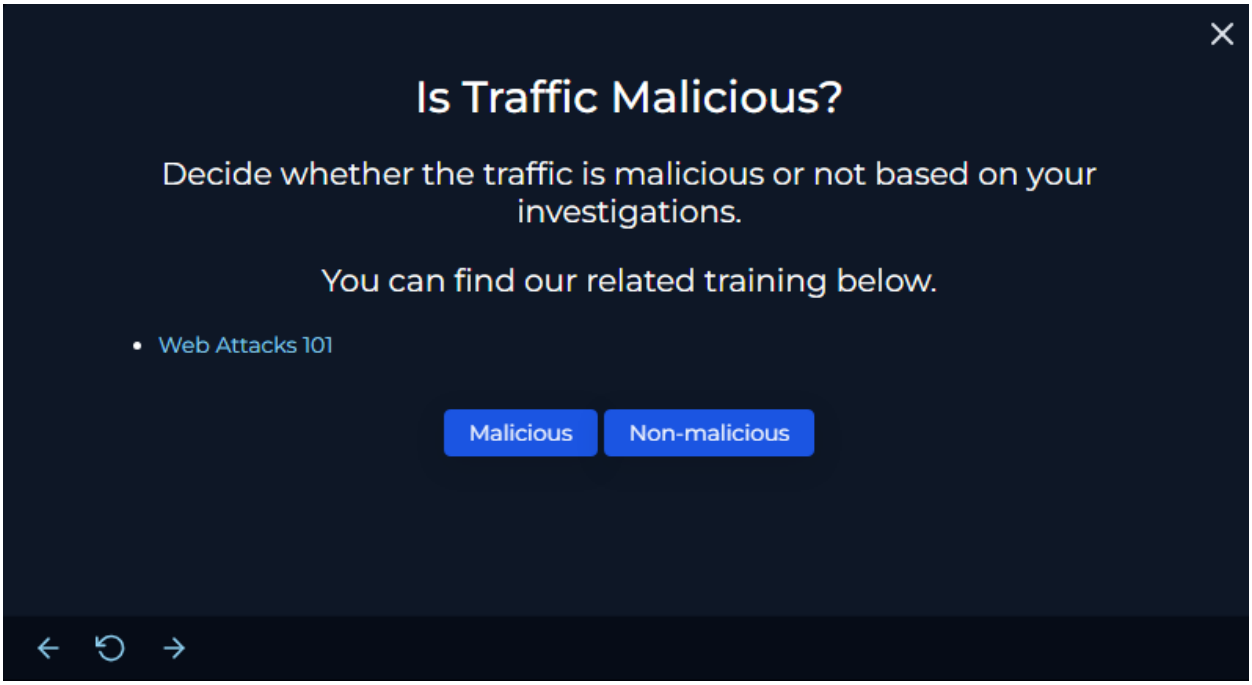
1 2



- Concluded the SQLi attempt was unsuccessful.

6. **Documentation & Closure**

- Added artifacts (payload samples, decoded data, log snippets) to the case.
- Recorded investigation notes and closed with "Attempted SQLi – No Compromise."



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

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

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.

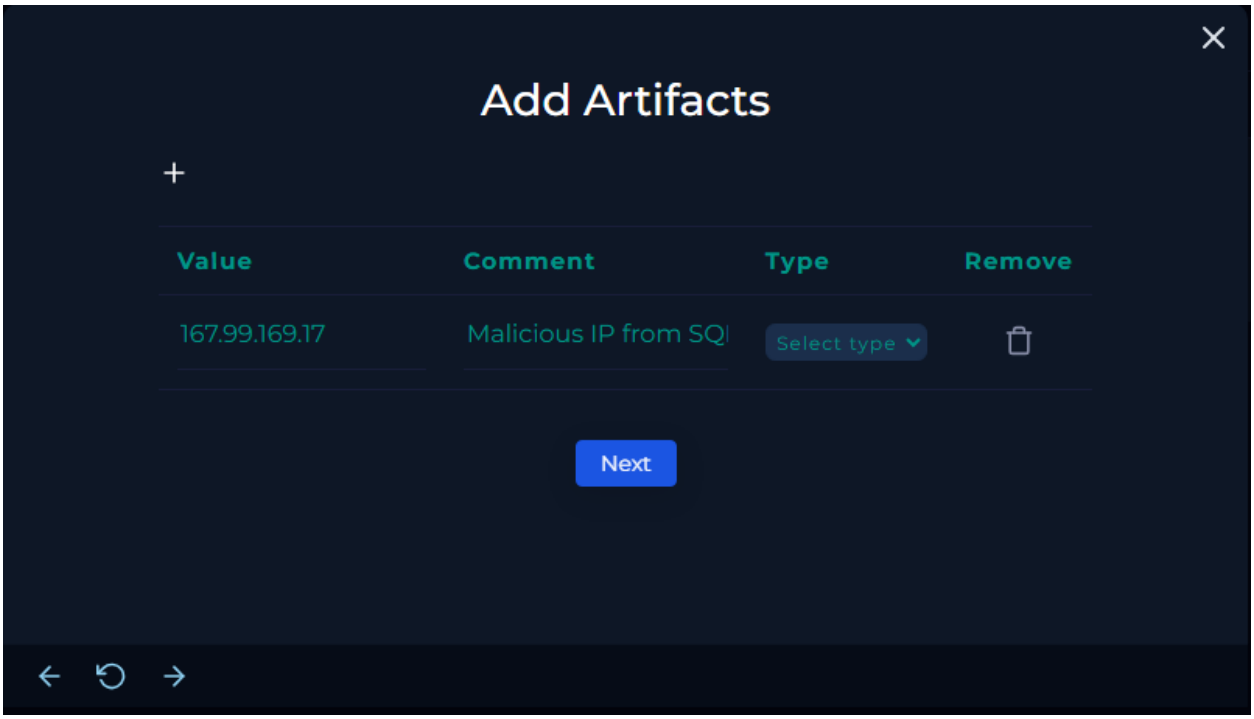
No | Yes

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



Key Skills Demonstrated:

- Threat detection & log analysis
- HTTP traffic analysis
- Threat intelligence gathering
- SOC workflow adherence (alert handling, playbook execution, case documentation)

Outcome:

The SQLi attempt was detected, classified, and investigated thoroughly. No compromise occurred, and findings were documented for potential use in refining detection rules, audits, and future analyst training.