

**Incident report for SOC**

Writer: Sina Mohebi

How to Write a Comprehensive Incident Report for Security operations



**Sample Incident report**

**In order to Download Docx version please visit:**

**https://blog.sinamohebi.com**

[**https://www.linkedin.com/in/sinamohebi**](https://www.linkedin.com/in/sinamohebi/)

**Please note that all the information provided in this document is fictional and has been created solely for the purpose of serving as a sample incident report for the Security Operations Center.**



Date  
2023-09-02

Incident report

### Copyright

This document has been prepared and compiled only to be presented to the SOC unit, and all its intellectual and material rights belong to Nooranet Institute. Publishing and copying it without written permission from this company is prohibited.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID Code** | **Classification** | **Number of pages** | **Date of issue** | **Version** |
| SOC Incident-report 2023-09-02 | Confidential | 6 | 2023-09-02 | 1.0 |

|  |  |
| --- | --- |
| **Report writer** | **Shift time** |
| Sina Mohebi  Mohebi@nooranet.com | Morning |

**Basic information of the incident**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Description of the incident | Date & Time | The origin of the attack | The target of the attack | The impact of the incident | Target system |
| SQL Injection attack detection | 1402-06-10  ‏ From  16:55 to 17:09 | 40.80.148.42 | 192.168.250.70 | Accessing and obtaining data from the database without authentication | Web Server Microsoft IIS 8.5 |

**Description of the incident**

According to the investigations carried out by the Security Operations Center team and using the security dashboards available in SIEM, it was found that an SQL Injection attack took place from the source 40.80.148.42 to the destination 192.168.250.70 at 16:55 to 17:09. According to further investigations, it was found that the attacker was able to run his malicious codes on the organization's web server by using security weaknesses and bypassing defense mechanisms such as WAF. It was also found that the origin of these attacks was among the ‏malicious addresses on the Internet.

**Technical description of the incident**

In the investigations carried out on the web attack detection dashboard, it was found that many malicious requests for SQL injection attacks of Retrieval hidden information and Time base SQL injection types have been made on the organization's servers from the source 40.80.148.42, which are part of these payloads in the image below.

A screenshot of a computer

Description automatically generated

*Image 1 is an Example of malicious XSS requests.*

As you can see in the image above, the attacker has been trying to execute this attack by sending the malicious values ​​mentioned below.

Malicious values ​​in the Uri\_query field:

;select%20pg\_sleep(10)

(select(0)from(select(sleep(6))

These values ​​are used for the mentioned attacks. Also, to ensure the accuracy of this information from sources such as:

<https://github.com/payloadbox/sql-injection-payload-list>

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection>

It has been used to ensure the accuracy of the diagnosis of this dashboard.

‏It was also found that 178 malicious requests were received from this source, which unfortunately, none of the defense mechanisms such as WAF were able to identify them, and these requests directly reached the organization's web server.

**The impact of the incident**

**Considering that this attack was successful, its effect is as follows:**

Bypass defense mechanisms such as WAF-

Communicating with the database without authentication and gaining access-

Finding out about sensitive and classified values ​​and data in the database-

Access to user identity information-

**Responding to the incident**

‏Due to the sensitivity of the data and the malicious detection of these activities, the source address of these requests was blocked by the firewall for 24 hours.

‏Also, by checking the origin of these requests by the [abuseipdb.com](http://abuseipdb.com/) website, it was determined that the origin of these requests was in the list of malicious Internet addresses, which you can see in the image below.

A screenshot of a computer

Description automatically generated