SQL Injection là một hình thức tấn công bảo mật trên ứng dụng web, trong đó kẻ tấn công chèn các câu lệnh SQL độc hại vào đầu vào (input) của ứng dụng để thực hiện các truy vấn không mong muốn tới cơ sở dữ liệu. Mục tiêu của cuộc tấn công này là truy cập, thay đổi hoặc xóa dữ liệu mà không được phép.

Kịch bản: Tấn công vào database. Kẻ tấn công sẽ sử dụng kỹ thuật SQL Injection để tấn công vào database của máy chủ Web:

- Wazuh Server: sẽ chịu trách nhiệm thu thập log phân tích và sau đó hiển thị cảnh báo
- Wazuh Agent: sẽ là máy victim bị tấn công SQL Injection
- Kali linux: là máy attacker

Lưu ý: Tường lửa có thể đang chặn cổng 80. Đảm bảo rằng tường lửa đã mở cổng 80 cho HTTP. Có thể sử dụng lệnh sau để kiểm tra cấu hình tường lửa:

- *Trên Ubuntu với UFW (Uncomplicated Firewall)**:***

  sudo ufw status

- *Nếu cổng 80 không được mở, có thể mở bằng cách:*

  sudo ufw allow 80/tcp

B1: Ở máy Agent Ubuntu cập nhật và cài đặt máy chủ Web Apache

apt install apache2

B2: Kiểm tra trạng thái dịch vụ Apache đã chạy hay chưa

systemctl status apache2.service

```
root@ubuntu-agent:~# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Mon 2024-09-30 00:12:41 +07; 1min 23s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 4543 (apache2)
      Tasks: 55 (limit: 2135)
     Memory: 5.5M
        CPU: 175ms
     CGroup: /system.slice/apache2.service
             ├─4543 /usr/sbin/apache2 -k start
             ├─4544 /usr/sbin/apache2 -k start
             └─4545 /usr/sbin/apache2 -k start

ก.ย. 30 00:12:41 ubuntu-agent systemd[1]: Starting The Apache HTTP Server...
ก.ย. 30 00:12:41 ubuntu-agent apachectl[4542]: AH00558: apache2: Could not reli>
ก.ย. 30 00:12:41 ubuntu-agent systemd[1]: Started The Apache HTTP Server.
```

B3: Cập nhật cấu hình tệp ossec.conf

Điều này cho phép máy Agent Ubuntu giám sát log truy cập của máy chủ Web Apache

Thêm đoạn script sau và lưu lại:

#sql_injection

<ossec_config>

  <localfile>

    <log_format>apache</log_format>

    <location>/var/log/apache2/access.log</location>

  </localfile>

</ossec_config>

```
  GNU nano 6.2                  /var/ossec/etc/ossec.conf *

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>

</ossec_config>

#sql_injection
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

B4: Khởi động lại dịch vụ wazuh agent để áp dụng các thay đổi cấu hình

systemctl restart wazuh-agent.service

B5: Ở máy attacker nhập lệnh tấn công

curl -XGET "http://192.168.198.148/users/?id=SELECT+*+FROM+users";

```
┌──(root㉿kali)-[~/Desktop]
└─# curl -XGET "http://192.168.198.148/users/?id=SELECT+*+FROM+users";
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 192.168.198.148 Port 80</addres
</body></html>
```

Kết quả: Đây là một cảnh báo về cuộc tấn công SQL Injection có:

- Rule ID là 31103 và level là 7

Sep 30, 2024 @ 00:42:23.142	T1190	Initial Access	SQL injection attempt.	7	31103

- Chúng ta có thể thấy được địa chỉ nguồn của cuộc tấn công này là: 192.168.198.129

data.protocol	GET
data.srcip	192.168.198.129
data.url	/users/?id=SELECT+*+FROM+users
decoder.name	web-accesslog

- Đây là cuộc tấn công vào database nhằm lấy thông tin của người dùng

full_log	192.168.198.129 - - [30/Sep/2024:00:42:22 +0700] "GET /users/?id=SELECT+*+FROM+users HTTP/1.1" 404 438 "-" "curl/8.8.0"