

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH SỐ 2  
HỌC PHẦN: KỸ THUẬT GIÁM SÁT AN TOÀN MẠNG**

**Tìm hiểu Modsecurity và ELK stack**

Sinh viên thực hiện:

**B21DCAT058      Nguyễn Tuấn Đạt**

Giảng viên hướng dẫn: thS. Ninh Thị Thu Trang

**HÀ NỘI 3-2025**

# Mục lục

1. Mục đích.....Error! Bookmark not defined.
2. Yêu cầu đối với sinh viên .....Error! Bookmark not defined.
3. Nội dung thực hành.....Error! Bookmark not defined.
4. Kết thúc bài lab: .....Error! Bookmark not defined.

# Nội dung và hướng dẫn bài thực hành

## Mục đích

Giúp sinh viên tìm hiểu khái niệm về giám sát an toàn mạng, sử dụng ModSecurity để ngăn chặn tấn công ứng dụng web, sử dụng ELK Stack để thu thập, phân tích log tấn công sql-injection và cấu hình alert phát hiện các hoạt động tấn công trên các ứng dụng web.

## Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ ModSecurity, công cụ ELK Stack, log xác thực và cách thức xây dựng ứng dụng web.

## Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

***startlab nsm-elk-modsecurity***

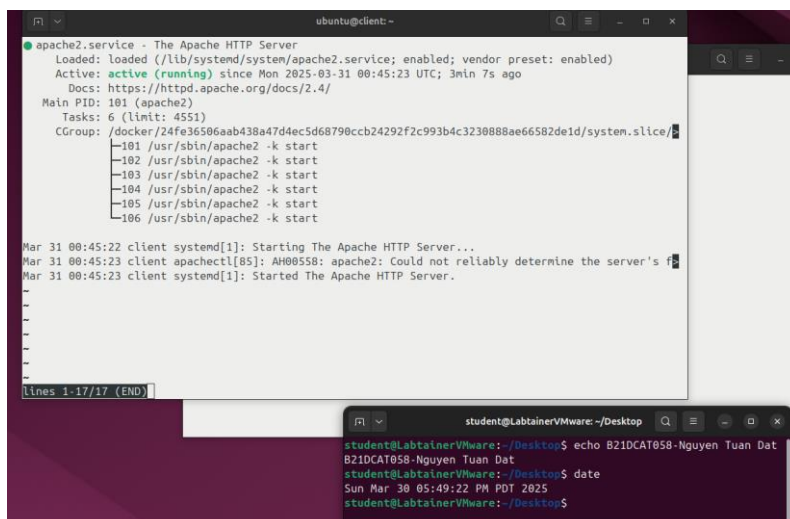
(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong ba terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: **attacker**, một cái là đại diện cho máy nạn nhân: **client**, một cái là đại diện cho máy giám sát: **server**.

Trên terminal **client** thực hiện cấu hình máy chủ web apache để xây dựng ứng dụng web cần theo dõi.

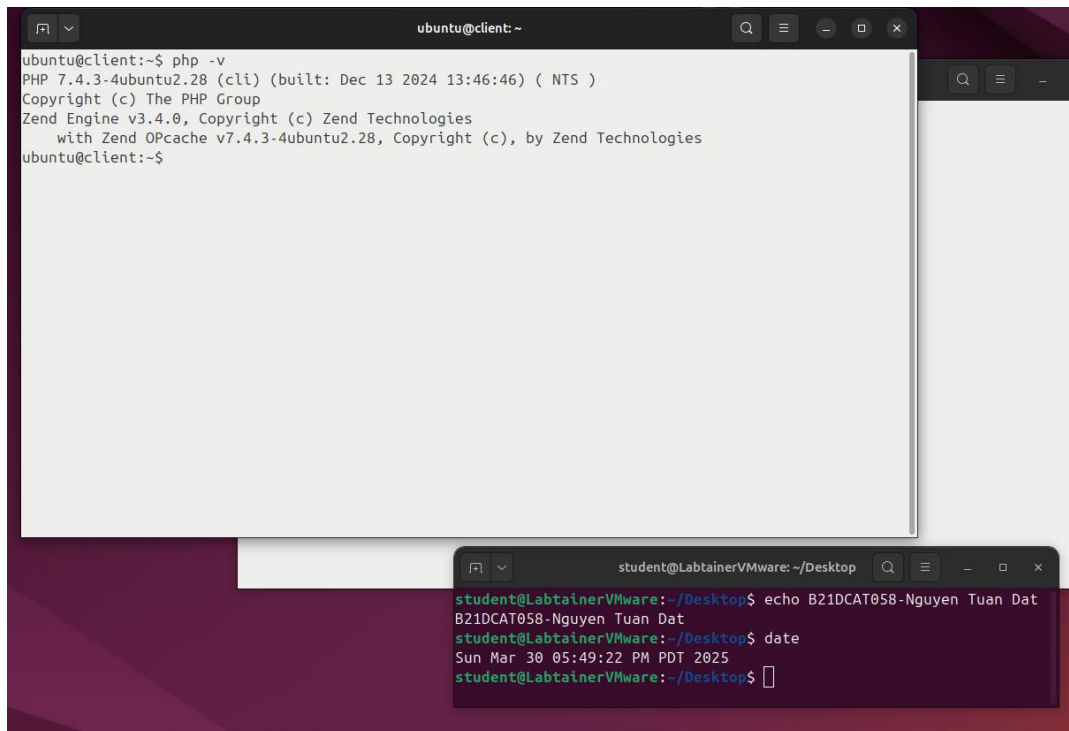
Đầu tiên là kiểm tra các dịch vụ cho quá trình build web bằng các câu lệnh sau:

***sudo systemctl status apache2***



```
ubuntu@client: ~  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)  
   Active: active (running) since Mon 2025-03-31 00:45:23 UTC; 3min 7s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Main PID: 101 (apache2)  
     Tasks: 6 (limit: 4551)  
    CGroup: /docker/24fe36506aab438a47d4ec5d68790ccb24292f2c993b4c3230888ae66582de1d/system.slice/  
            └─101 /usr/sbin/apache2 -k start  
              └─102 /usr/sbin/apache2 -k start  
                └─103 /usr/sbin/apache2 -k start  
                  └─104 /usr/sbin/apache2 -k start  
                    └─105 /usr/sbin/apache2 -k start  
                      └─106 /usr/sbin/apache2 -k start  
  
Mar 31 00:45:22 client systemd[1]: Starting The Apache HTTP Server...  
Mar 31 00:45:23 client apache2[85]: AH00558: apache2: Could not reliably determine the server's f  
Mar 31 00:45:23 client systemd[1]: Started The Apache HTTP Server.  
  
lines 1-17/17 (END)  
  
student@LabtainerVMware: ~/Desktop  
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat  
B21DCAT058-Nguyen Tuan Dat  
student@LabtainerVMware:~/Desktop$ date  
Sun Mar 30 05:49:22 PM PDT 2025  
student@LabtainerVMware:~/Desktop$
```

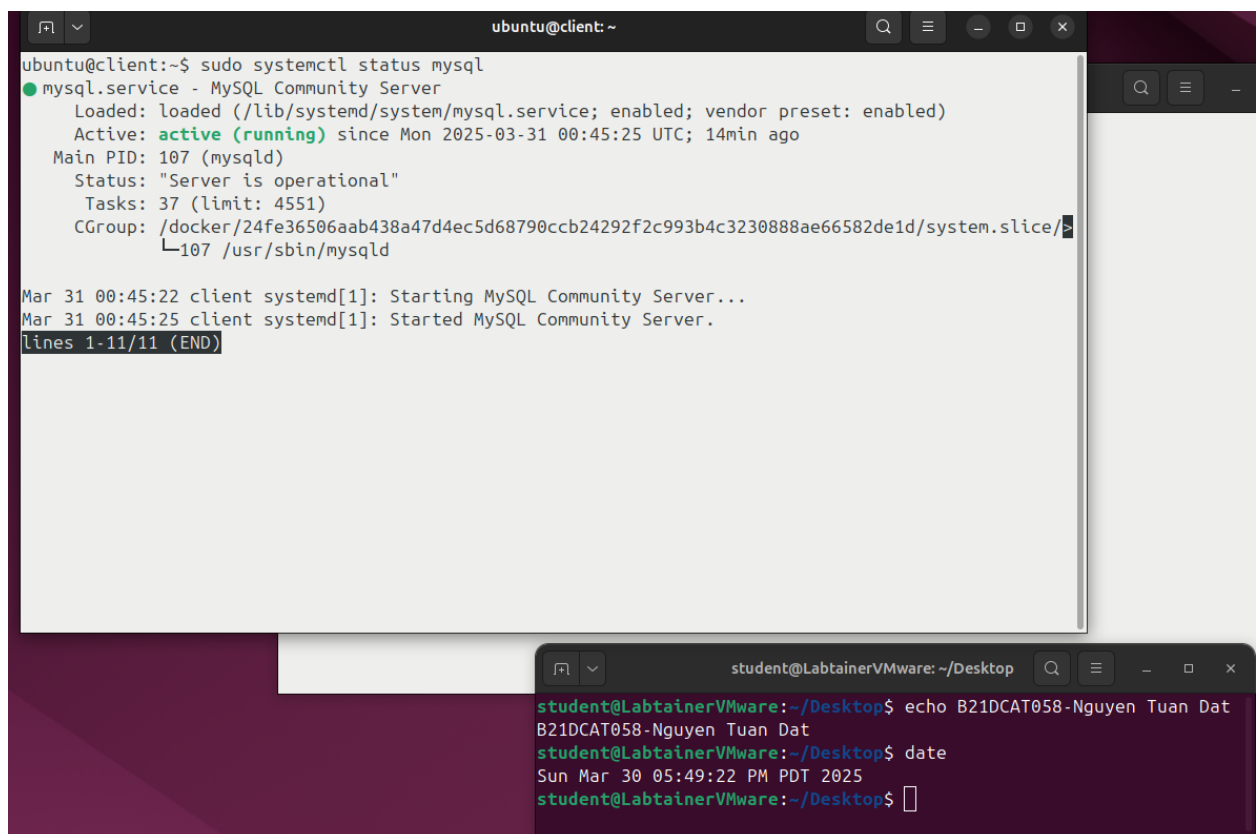
*php -v*



```
ubuntu@client:~$ php -v
PHP 7.4.3-4ubuntu2.28 (cli) (built: Dec 13 2024 13:46:46) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.3-4ubuntu2.28, Copyright (c), by Zend Technologies
ubuntu@client:~$
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

*sudo systemctl status mysql*



```
ubuntu@client:~$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-03-31 00:45:25 UTC; 14min ago
     Main PID: 107 (mysqld)
       Status: "Server is operational"
         Tasks: 37 (limit: 4551)
        CGroup: /docker/24fe36506aab438a47d4ec5d68790ccb24292f2c993b4c3230888ae66582de1d/system.slice/
                └─107 /usr/sbin/mysqld

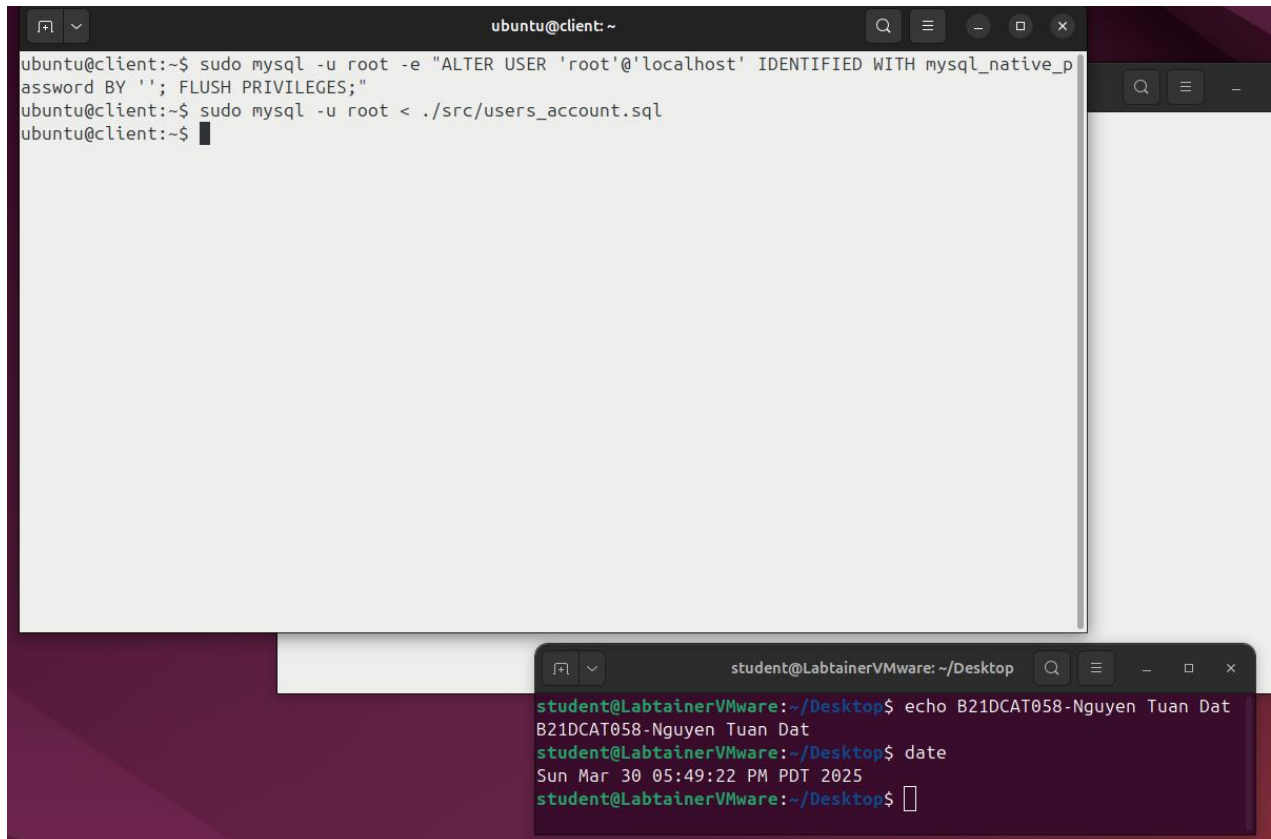
Mar 31 00:45:22 client systemd[1]: Starting MySQL Community Server...
Mar 31 00:45:25 client systemd[1]: Started MySQL Community Server.
lines 1-11/11 (END)
```

```
student@LabtainerVMware:~/Desktop
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

Tiếp theo thực hiện xây dựng cơ sở dữ liệu ứng dụng web:

***sudo mysql -u root -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql\_native\_password BY ''; FLUSH PRIVILEGES;"***

***sudo mysql -u root < ./src/users\_account.sql***



The screenshot shows two terminal windows. The top window, titled 'ubuntu@client: ~', contains the following commands and output:

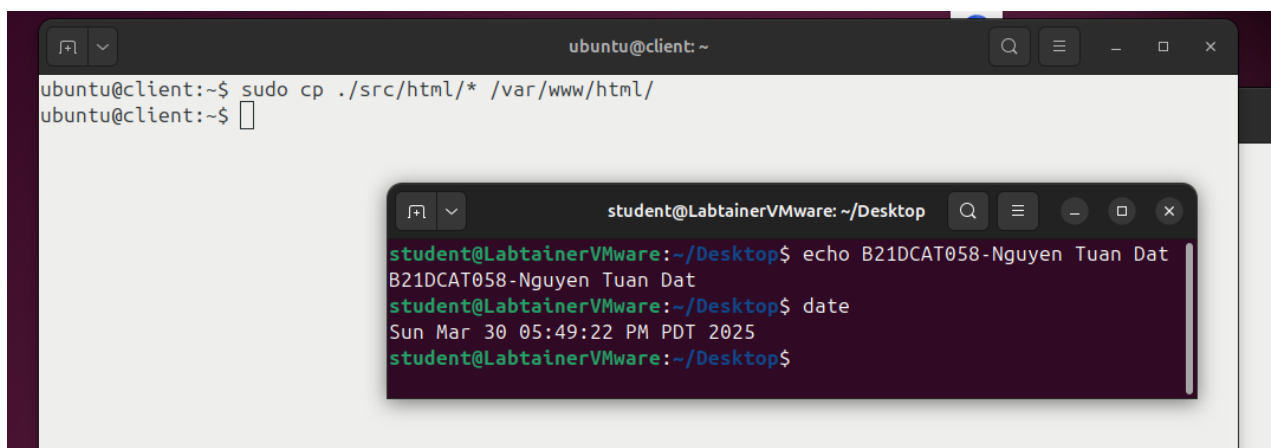
```
ubuntu@client:~$ sudo mysql -u root -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY ''; FLUSH PRIVILEGES;"
ubuntu@client:~$ sudo mysql -u root < ./src/users_account.sql
ubuntu@client:~$
```

The bottom window, titled 'student@LabtainerVMware: ~/Desktop', contains the following commands and output:

```
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

Cuối cùng là tiến hành build source code ứng dụng web.

***sudo cp ./src/html/\* /var/www/html/***



The screenshot shows two terminal windows. The top window, titled 'ubuntu@client: ~', contains the following commands and output:

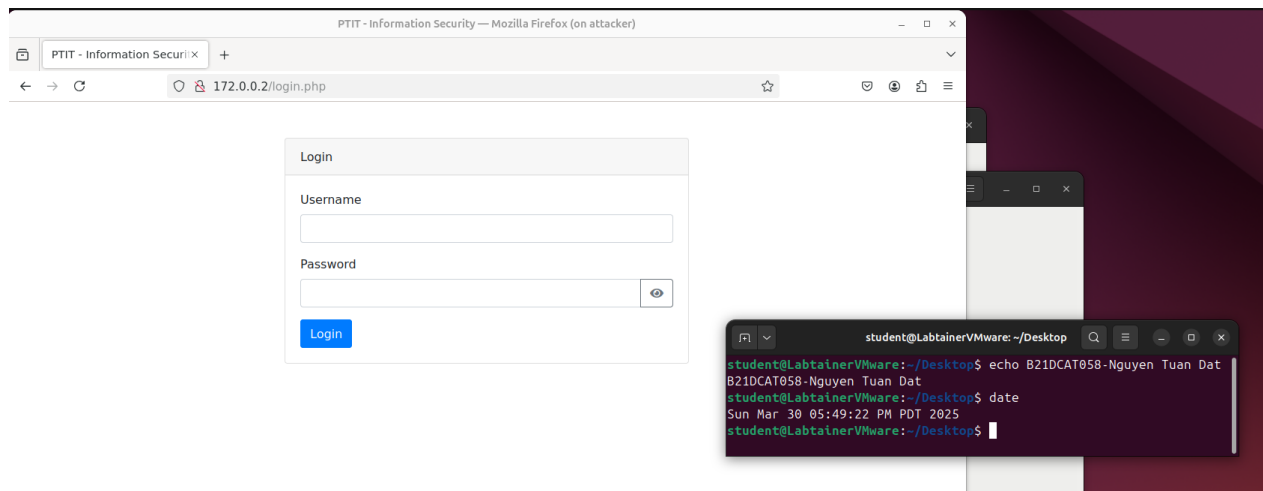
```
ubuntu@client:~$ sudo cp ./src/html/* /var/www/html/
ubuntu@client:~$
```

The bottom window, titled 'student@LabtainerVMware: ~/Desktop', contains the following commands and output:

```
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

Trên terminal **attack** thực hiện mở trình duyệt firefox

(chạy câu lệnh “**firefox &**”) và truy cập ứng dụng web theo đường dẫn **http://172.0.0.2:80/index.php** để đảm bảo trang web hoạt động bình thường.



Quay lại trên terminal **client** thực hiện cài đặt và cấu hình ModSecurity để thực hiện tự động ngăn chặn tấn công đối với ứng dụng web (Hiện tại vẫn đang ở máy client). Sử dụng các câu lệnh sau:

***sudo apt-get install git libapache2-mod-security2 -y***

***sudo a2enmod security2***

***sudo systemctl restart apache2***

***ls -alps /usr/share/modsecurity-crs/***

***sudo rm -rf /usr/share/modsecurity-crs/***

***sudo git clone https://github.com/coreruleset/coreruleset /usr/share/modsecurity-crs/***

***sudo mv /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modsecurity-crs/crs-setup.conf***

***ls -al /etc/modsecurity/***

***sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf***

```
ubuntu@client:~$ sudo a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
ubuntu@client:~$ sudo systemctl restart apache2
ubuntu@client:~$ ls -alps /usr/share/modsecurity-crs/
total 24
4 drwxr-xr-x  4 root root 4096 Mar 31 01:16 ./
8 drwxr-xr-x  1 root root 4096 Mar 31 01:16 ../
4 -rw-r--r--  1 root root 373 Oct 21 2019 owasp-crs.load
4 drwxr-xr-x  2 root root 4096 Mar 31 01:16 rules/
4 drwxr-xr-x 13 root root 4096 Mar 31 01:16 util/
ubuntu@client:~$ sudo rm -rf /usr/share/modsecurity-crs/
ubuntu@client:~$ sudo git clone https://github.com/coreruleset/coreruleset /usr/share/modse
Cloning into '/usr/share/modsecurity-crs'...
remote: Enumerating objects: 35033, done.
remote: Counting objects: 100% (111/111), done.
remote: Compressing objects: 100% (58/58), done.
remote: Total 35033 (delta 90), reused 56 (delta 53), pack-reused 34922 (from 2)
Receiving objects: 100% (35033/35033), 10.09 MiB | 484.00 KiB/s, done.
Resolving deltas: 100% (27736/27736), done.
ubuntu@client:~$ sudo mv /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modse
curity-crs/crs-setup.conf
ubuntu@client:~$ ls -al /etc/modsecurity/
total 80
drwxr-xr-x 3 root root 4096 Mar 31 01:16 .
drwxrwxr-x 1 root root 4096 Mar 31 01:16 ..
drwxr-xr-x 2 root root 4096 Mar 31 01:16 crs
-rw-r--r-- 1 root root 8452 Sep 13 2023 modsecurity.conf-recommended
-rw-r--r-- 1 root root 53146 Dec 4 2018 unicode.mapping
ubuntu@client:~$ sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/mod
security.conf
ubuntu@client:~$
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

Thêm và chỉnh sửa nội dung các file sau để ModSecurity hoạt động được với các thành phần của ứng dụng web:

*sudo nano /etc/modsecurity/modsecurity.conf*

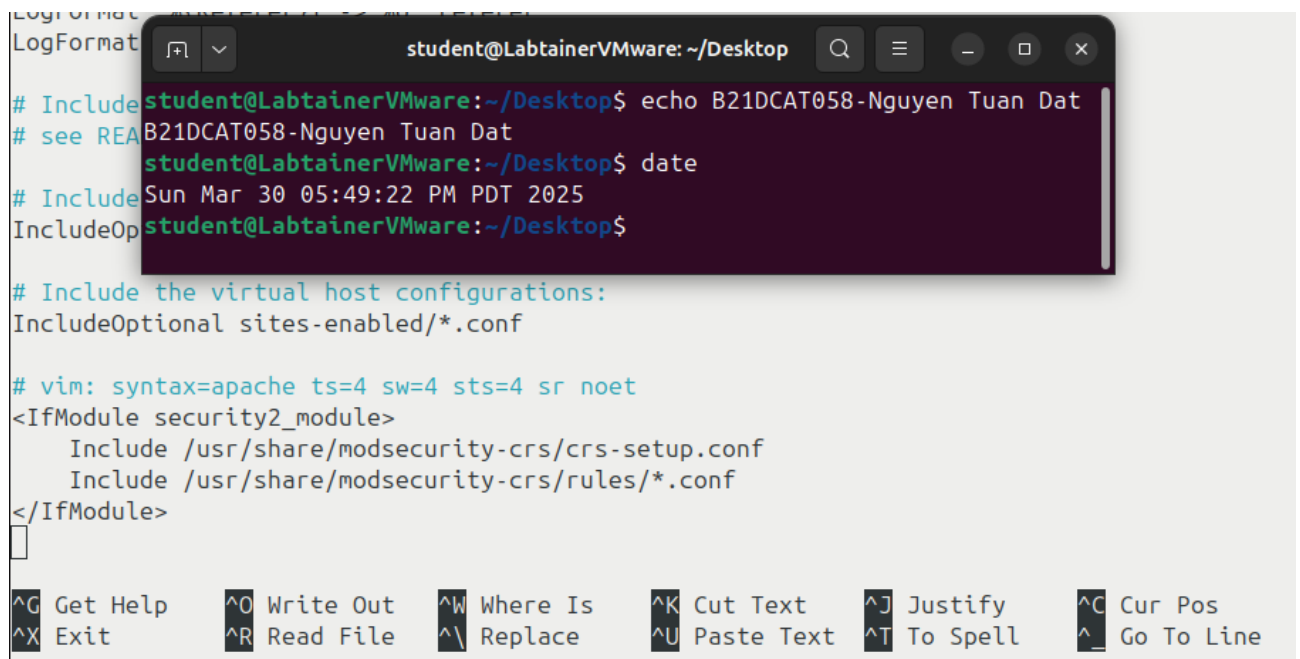
```
SecRuleEngine On
```

```
GNU nano 4.8 /etc/modsecurity/modsecurity.conf Modified
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On
#
#
```

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

*sudo nano /etc/apache2/apache2.conf*

```
<IfModule security2_module>
Include /usr/share/modsecurity-crs/crs-setup.conf
    Include /usr/share/modsecurity-crs/rules/*.conf
</IfModule>
```



```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

```
# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
<IfModule security2_module>
    Include /usr/share/modsecurity-crs/crs-setup.conf
    Include /usr/share/modsecurity-crs/rules/*.conf
</IfModule>
```

^G Get Help    ^O Write Out    ^W Where Is    ^K Cut Text    ^J Justify    ^C Cur Pos  
^X Exit        ^R Read File    ^\ Replace     ^U Paste Text   ^T To Spell    ^\_ Go To Line

*sudo nano /etc/apache2/sites-enabled/000-default.conf*

SecRuleEngine On

```
<IfModule security2_module>
    Include /usr/share/modsecurity-crs/crs-setup.conf
    Include /usr/share/modsecurity-crs/rules/*.conf
</IfModule>
```



```
ubuntu@client: ~
GNU nano 4.8 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

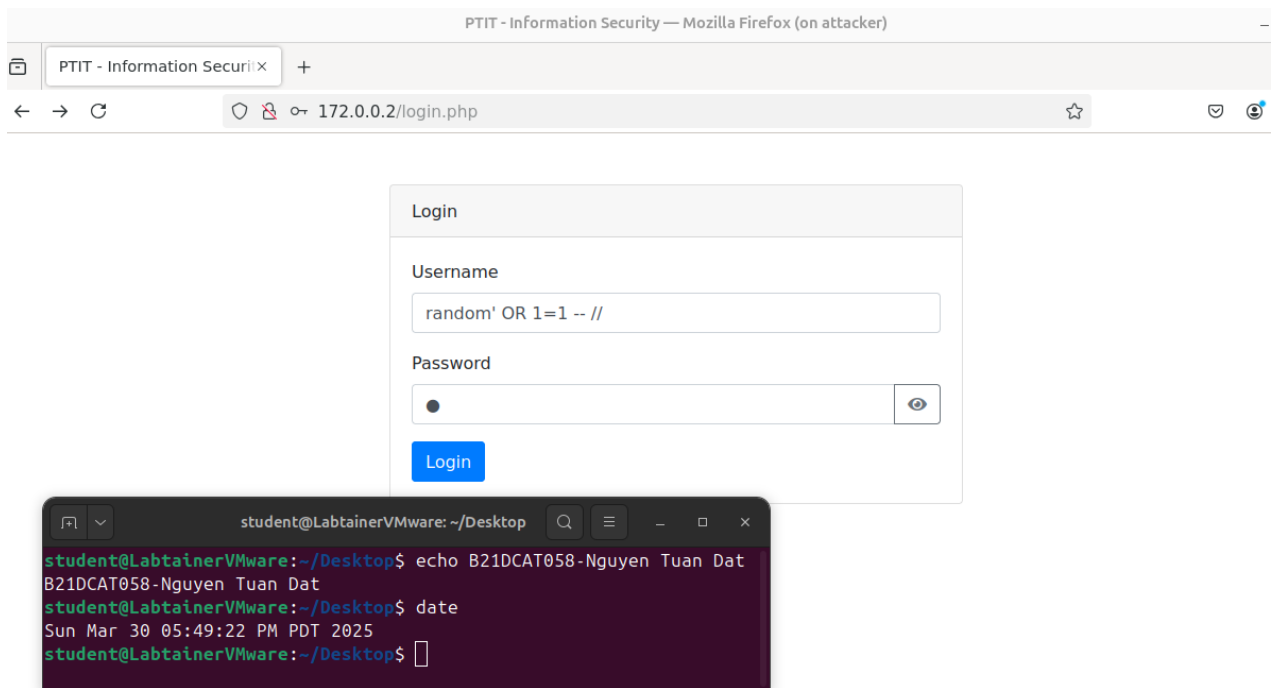
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <IfModule security2_module>
        SecRuleEngine On
        Include /usr/share/modsecurity-crs/crs-setup.conf
        Include /usr/share/modsecurity-crs/rules/*.conf
    </IfModule>

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".

```

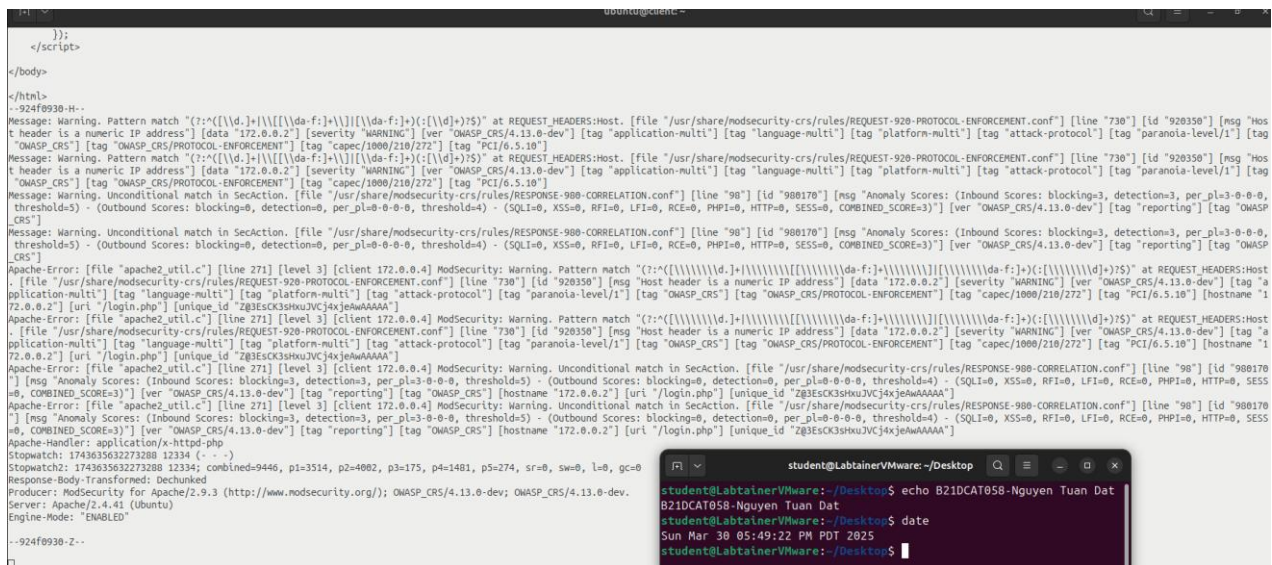
Trên terminal *attack* thực hiện mở trình duyệt firefox (chạy câu lệnh “**firefox &**”) và truy cập ứng dụng web theo đường dẫn **http://172.0.0.2:80/index.php** , tấn công SQL-injection với payload sau:

```
random' OR 1=1 -- //
```



Thực hiện kiểm tra ModSecurity logs đối với hành vi tấn công ứng dụng WEB.

*sudo tail -f /var/log/apache2/modsec\_audit.log*



Quay lại trên terminal **client** thực hiện cấu hình Filebeat để gửi log xác thực đăng nhập tới máy giám sát và khởi động dịch vụ Filebeat.

***sudo nano /etc/filebeat/filebeat.yml***

Thêm vào path của nơi lưu log xác thực: ***/var/log/apache2/modsec\_audit.log*** cùng với ip, port Logstash của máy giám sát nhận log sau đó khởi động dịch vụ Filebeat.

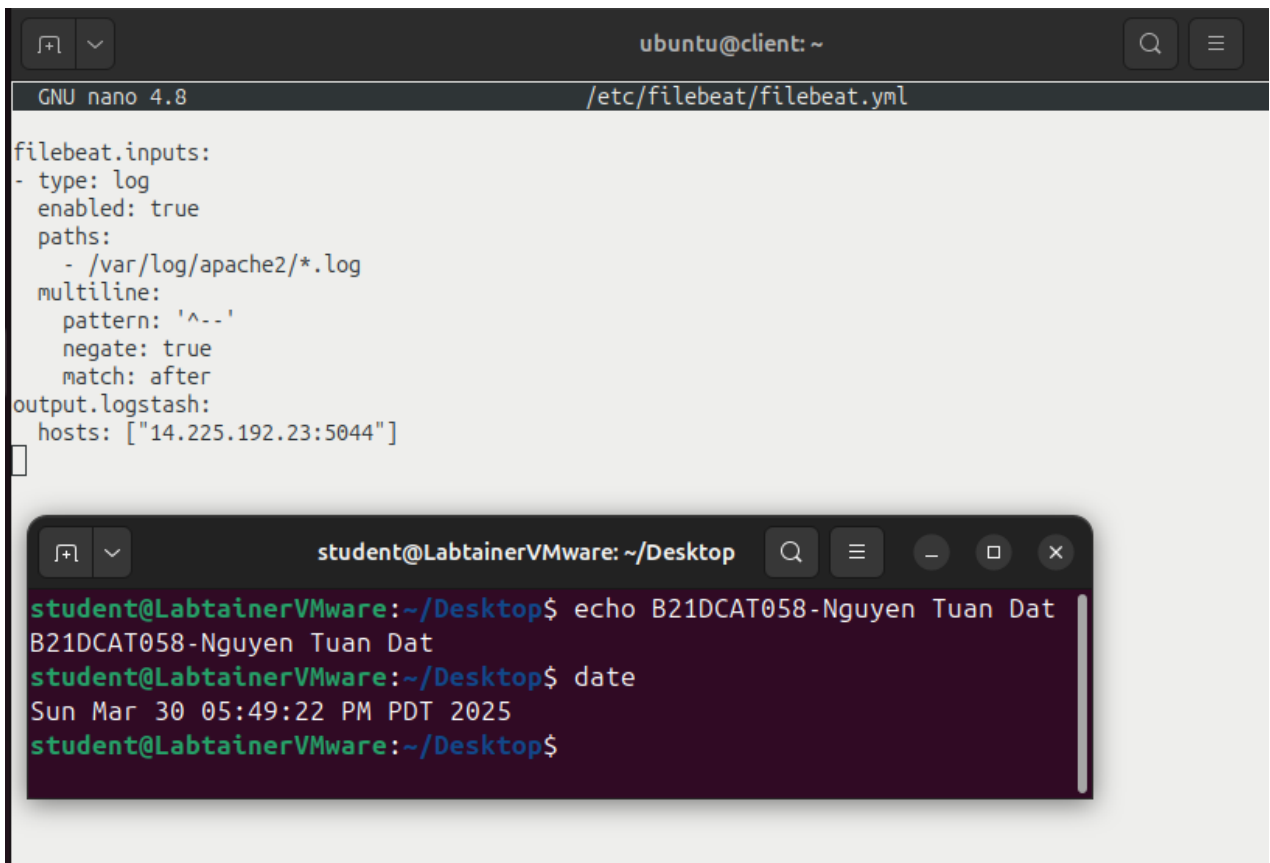
***sudo nano /etc/filebeat/filebeat.yml***

***sudo cat /etc/filebeat/filebeat.yml***

***sudo systemctl start filebeat***

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/apache2/modsec_audit.log
  multiline:
    pattern: '^-'
    negate: true
    match: after

output.logstash:
  hosts: ["172.0.0.3:5044"]
```

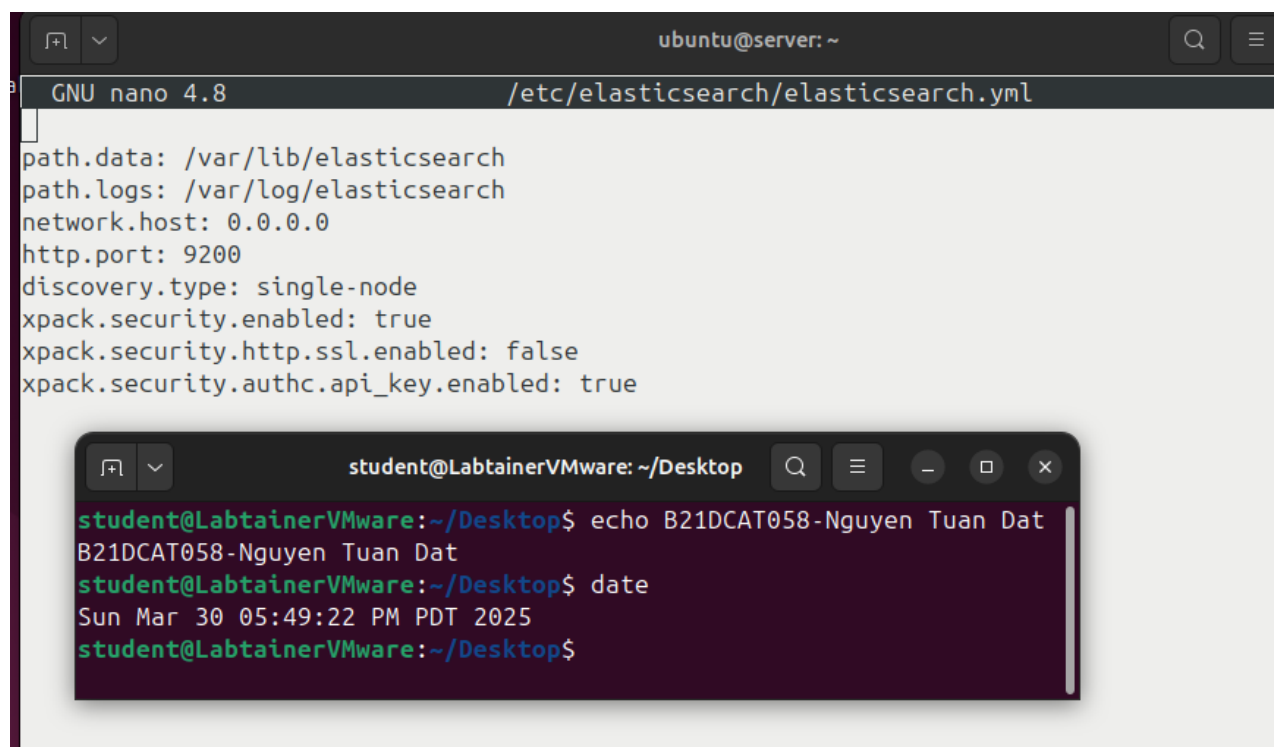


Trên máy server thực hiện cấu hình lại các file hệ thống của Elasticsearch, Kibana và Filebeat.

```
ubuntu@server:~$ sudo cat /etc/elasticsearch/elasticsearch.yml

path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 0.0.0.0
http.port: 9200
discovery.type: single-node
xpack.security.enabled: true
xpack.security.http.ssl.enabled: false
xpack.security.authc.api_key.enabled: true

ubuntu@server:~$
```



The image shows a terminal window titled 'ubuntu@server: ~' running the 'nano 4.8' editor on the file '/etc/elasticsearch/elasticsearch.yml'. The file contains the following configuration:

```
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 0.0.0.0
http.port: 9200
discovery.type: single-node
xpack.security.enabled: true
xpack.security.http.ssl.enabled: false
xpack.security.authc.api_key.enabled: true
```

Overlaid on this is a smaller terminal window titled 'student@LabtainerVMware: ~/Desktop'. It shows the following commands and output:

```
student@LabtainerVMware:~/Desktop$ echo B21DCAT058-Nguyen Tuan Dat
B21DCAT058-Nguyen Tuan Dat
student@LabtainerVMware:~/Desktop$ date
Sun Mar 30 05:49:22 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

Trên máy *server* thực hiện khởi chạy dịch vụ Elasticsearch và mật khẩu ngẫu nhiên cho các thành phần của ELK

*sudo systemctl start elasticsearch*

*sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto*

Lưu mật khẩu được sinh ra (Để điền vào file /etc/kibana/kibana.yml và /etc/logstash/conf.d/apache.conf).

```
ubuntu@server:~$ sudo cat /etc/kibana/kibana.yml
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.hosts: ["http://localhost:9200"]
elasticsearch.ssl.verificationMode: 'none'
elasticsearch.username: "elastic"
elasticsearch.password: "password_elastic"
xpack.security.enabled: true
xpack.encryptedSavedObjects.encryptionKey:
"abcdefgh12345678abcdefgh12345678"
ubuntu@server:~$
```

Thực hiện tạo file “ /etc/logstash/conf.d/modsecurity.conf ”:

*sudo mv /etc/logstash/conf.d/apache.conf /etc/logstash/*

*sudo nano /etc/logstash/conf.d/modsecurity.conf*

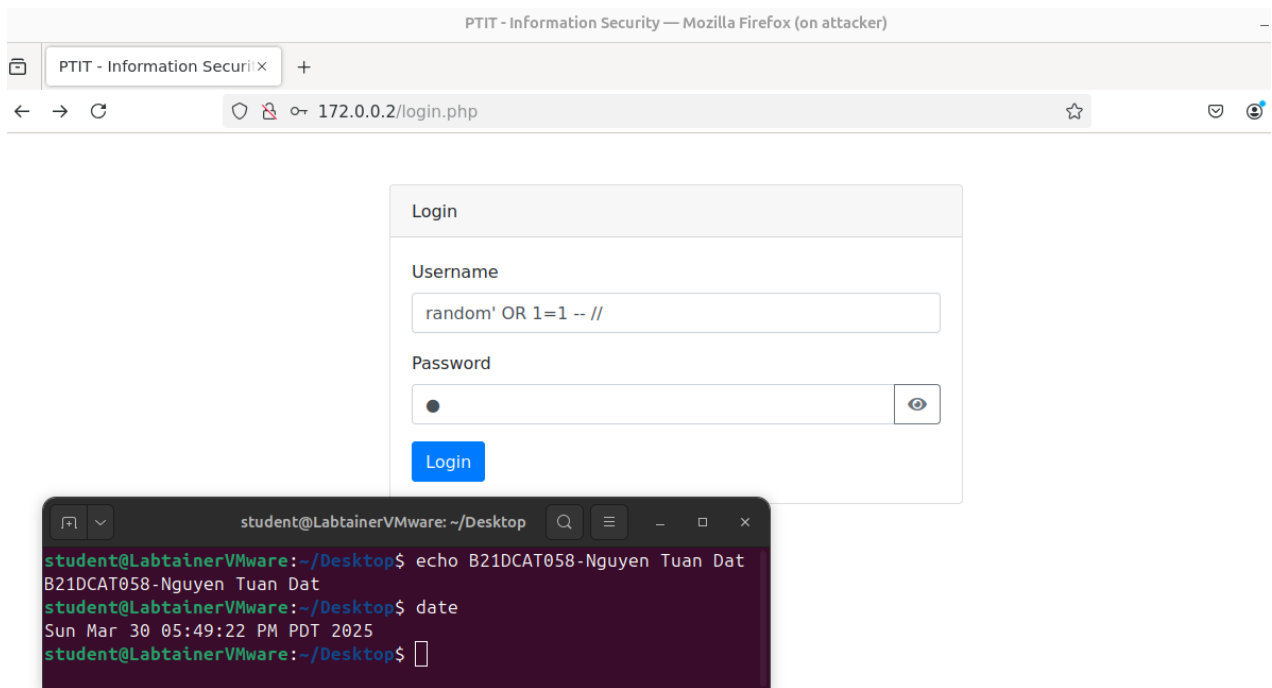
```
ubuntu@server: ~
GNU nano 4.8 /etc/logstash/conf.d/modsecurity.conf
beats {
  port => 5044
}
}
filter {
  if "H--" in [message] {
    grok {
      match => { "message" => "%{GREEDYDATA:modsec_message}" }
    }
    grok {
      match => { "message" => "id\s\"%{NUMBER:rule_id}\"\\s\[msg\s\"%{GREEDYDATA:rule_mes>
    }
    grok {
      match => { "message" => "severity\s\"%{WORD:severity}\"\\s\[severity\s\"%{GREEDYDATA:rule_mes>
    }
    mutate {
      remove_field => ["message"]
    }
  }
}
output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    user => "elastic"
    password => "E24zduXltXIMDtdRtLpx"
    index => "modsecurity-logs"
  }
  stdout { codec => rubydebug }
}
}

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell     ^_ Go To Line
```

Trên máy **attacker** thực hiện tấn công sql injection ứng dụng web bằng payload sau: (Địa chỉ ứng dụng web: <http://172.0.0.2:80/index.php>).

*firefox &*

**random' OR 1=1 -- //**



Thực hiện đăng nhập bằng tài khoản xác thực username “ptit” và password “attt” để so sánh giữa logs tấn công và logs truy cập ứng dụng web bình thường.

Tiếp theo từ trình duyệt của máy client sinh viên xem được nội dung logs từ ModSecurity từ máy *client* (Trên firefox máy CLIENT truy cập ELK qua địa chỉ <http://172.0.0.3:5601/app/home/#/> để theo dõi log qua giao diện Kibana).

*firefox &*

Tạo giao diện phân tích logs trên Elk và tiến hành tìm các logs có field “*severity : \*WARNING\**”. Tạo event theo dõi tên “modsecurity-logs”.

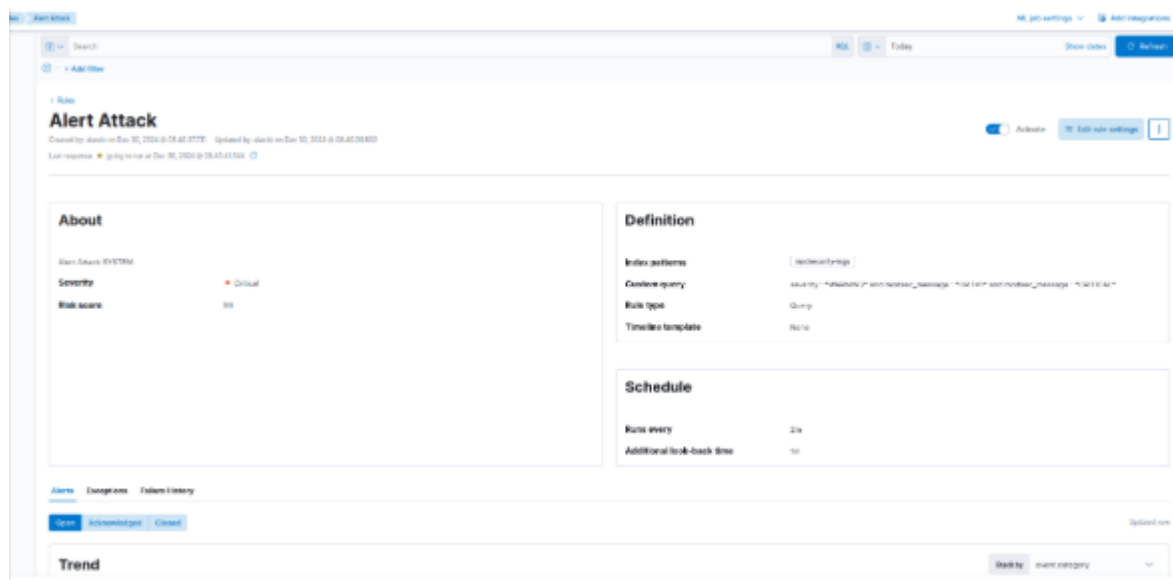
Trên máy Server: Thực hiện truy vấn logs theo câu lệnh để xác định tấn công sqlinjection theo format logs-modsecurity.

```
curl -u "elastic:Dz5Vow9E8DGGgAJ8dW43" -X GET
"http://127.0.0.1:9200/modsecurity-logs/_search?pretty" -H "Content-Type:
application/json" -d '{"query": {"match_all": {}}, "size": 100}' >>
logs_modsecurity.txt
```

```
cat logs_modsecurity.txt | grep "WARNING"
```

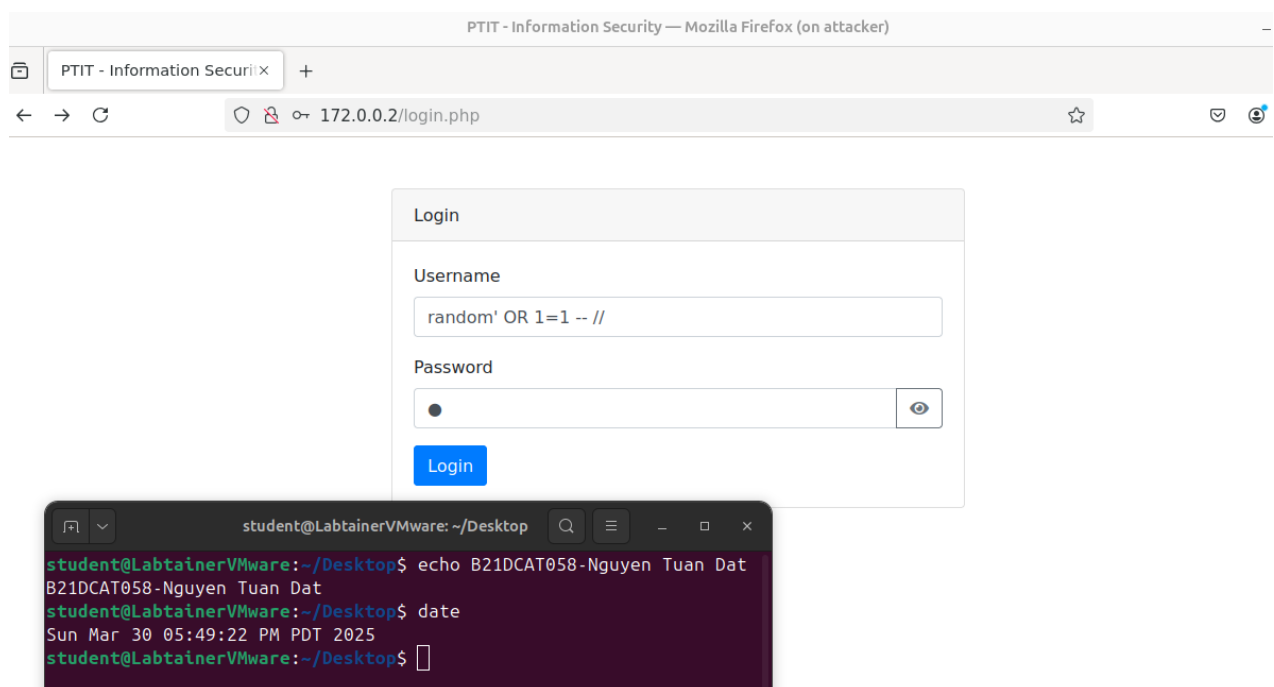
```
cat logs_modsecurity.txt | grep "+OR+1%3DI+"
```

Tiếp theo sinh viên tiến hành cấu hình rule trên elk để hệ thống cảnh báo khi xuất hiện tấn công sql injection. Truy cập Home/Security/Alerts/Rule để cài đặt rule. **Đặt tên rule là Alert Attack để theo dõi và truy vấn:**



Thực hiện tấn công sql injection lại trên đối với ứng dụng web và theo dõi alert tại mục Home/Security/Alerts . Payload tấn công “*random' OR 1=1 -- //*”.

Thực hiện truy vấn alert đối với tấn công sql-injection (máy server):



```
curl -u "elastic:Q8d1fQKXtAmu3wpqyFK7" -X GET
"http://127.0.0.1:9200/.siem-signals-default-000001/_search?pretty" -H
"Content-Type: application/json" -d '{"query": {"match":
{"signal.rule.name": "Alert Attack"}}, {"size": 100}}' >> alert_attack.txt
```



Xem alert vừa truy vấn:

```
cat alert_attack.txt | grep '" OR 1=1 --"
```

```
ubuntu@server:~$ cat alert_attack.txt
{"type": "security_exception",
  "reason": "unable to authenticate user [elastic] for REST request [/siem-signals-default-000001/_search?pretty]",
  "header": {
    "WWW-Authenticate": [
      "Basic realm=\"security\" charset=\"UTF-8\"",
      "ApiKey"
    ]
  }
},
"status": 401
}

ubuntu@server:~$ curl -u "elastic:E24zduXltXIMdtdRtLpx" -X GET "http://127.0.0.1:9200/siem-signals-default-000001/_search?pretty" -H "Content-Type: application/json" -d '{"query": {"match": [{"signal.rule.name": "Alert Attack"}], "size": 100}}' >> alert_attack.txt
ubuntu@server:~$ cat alert_attack.txt | grep '" OR 1=1 --"
{"error": {
  "root_cause": [
    {
      "type": "security_exception",
      "reason": "unable to authenticate user [elastic] for REST request [/siem-signals-default-000001/_search?pretty]",
      "header": {
        "WWW-Authenticate": [
          "Basic realm=\"security\" charset=\"UTF-8\"",
          "ApiKey"
        ]
      }
    }
  ],
  "type": "security_exception",
  "reason": "unable to authenticate user [elastic] for REST request [/siem-signals-default-000001/_search?pretty]"
}
```

## Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

```
stoplab nsm-elk-modsecurity
```

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

```
startlab -r nsm-elk-modsecurity
```

```
student@labtaierVmware:~/labtaier-student$ checkwork
Results stored in directory: /home/student/labtaier_xfer/nsm-elk-modsecurity
Successfully copied 58.0MB to nsm-elk-modsecurity-igrader:/home/instructor/b21dcat058.nsm-elk-modsecurity.lab
Successfully copied 2.56KB to /home/student/labtaier_xfer/nsm-elk-modsecurity
Labname nsm-elk-modsecurity

Student      | web-mysql | web-php | modsec-config | filebeat-path | filebeat-IP | logstash | elasticsearch | kibana | attack-sqli | modsec-logs | modsec-alert |
=====|=====|=====|=====|=====|=====|=====|=====|=====|=====|=====|=====|
b21dcat058  | Y         | Y       | Y             | Y             | Y           | Y        | Y             | Y      | Y           | Y           | Y           |

What is automatically assessed for this lab:
```