

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



Môn: Thực tập cơ sở

BÁO CÁO THỰC TẬP CƠ SỞ

Bài 14: Phát hiện lỗ hổng với công cụ tìm kiếm

<i>Họ và tên giảng viên:</i>	<i>PGS.TS.Đỗ Xuân Chợt</i>
<i>Họ và tên:</i>	<i>Phạm Thanh Tùng</i>
<i>Mã sinh viên:</i>	<i>B20DCAT171</i>
<i>Lớp:</i>	<i>D20CQAT03-B</i>
<i>Số điện thoại:</i>	<i>0856915668</i>

Hà Nội 2023

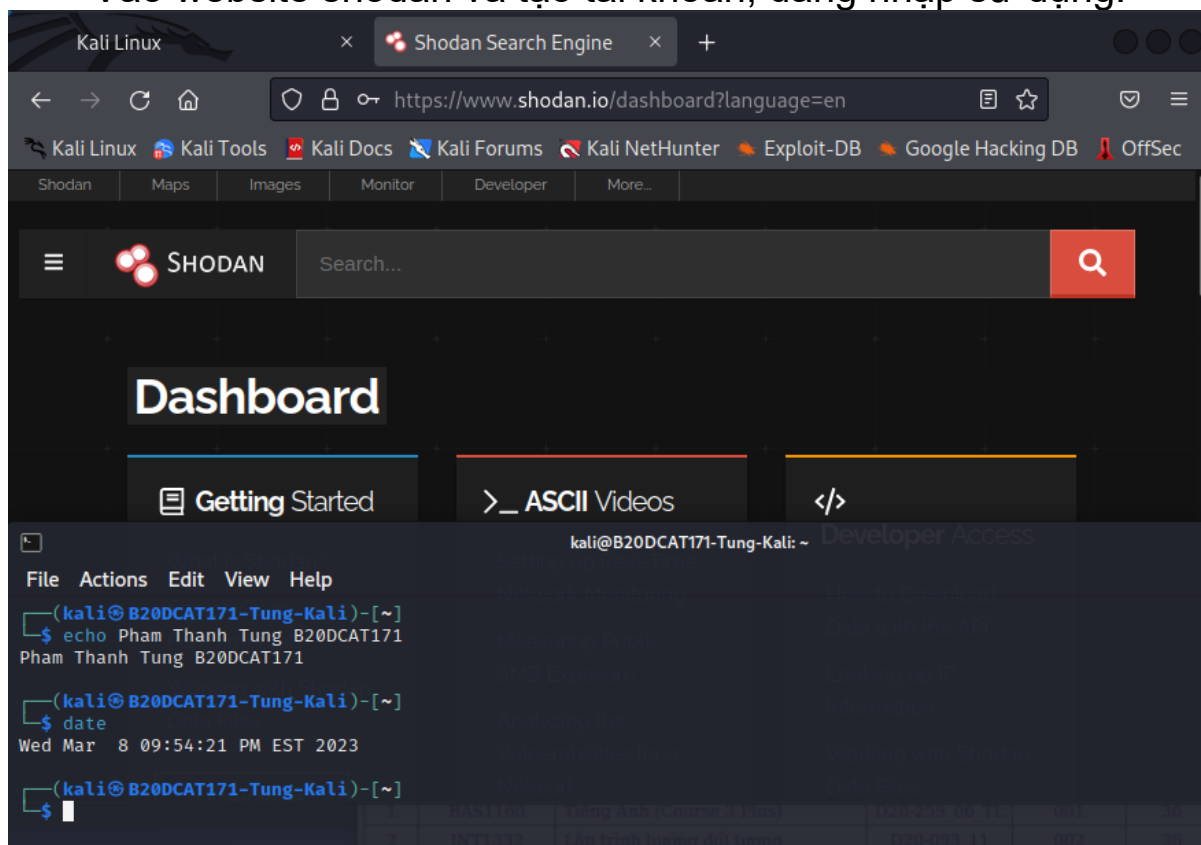
1. Nội dung lý thuyết

- Shodan(Sentient Hyper-Optimized Data Access Network), là một công cụ tìm kiếm giống như Google, nhưng thay vì tìm kiếm các trang web, nó tìm kiếm các thiết bị kết nối Internet từ các bộ định tuyến và máy chủ, đến các thiết bị Internet of Things (IoT), như máy cảm ứng nhiệt, TV thông minh, đến các hệ thống phức tạp chi phối một loạt các ngành công nghiệp, bao gồm năng lượng, năng lượng và giao thông vận tải. Shodan có thể tìm thấy bất cứ thứ gì kết nối trực tiếp với internet và nếu các thiết bị đó tồn tại lỗ hổng, Shodan có thể nói với tin tặc mọi thứ họ cần biết để tấn công vào mạng lưới của thiết bị đó.
- Shodan (Sentient Hyper-Optimized Data Access Network) hoạt động theo thuật toán sau:
 - 1.Tạo một địa chỉ IPv4 một cách ngẫu nhiên.
 - 2.Chọn port (cổng dịch vụ) ngẫu nhiên và thực hiện gửi câu lệnh kiểm tra
 - 3.Xem nội dung phản hồi của thiết bị (Service Banner) từ đó xác định xem đó là loại thiết bị gì và chạy cổng gì
 - 4.Lặp lại quá trình trên nhưng với ip và port mới
- Shodan thu thập dữ liệu trên web của các thiết bị sử dụng mạng máy tính và máy chủ toàn cầu. Shodan có thể cung cấp tất cả các loại thông tin nó nhận được, một số thông tin phổ biến như: Tên thiết bị, địa chỉ IP, cổng mạng, nhà mạng, vị trí địa lý,... Một số thiết bị sử dụng tên đăng nhập và mật khẩu mặc định, mã hiệu thiết bị, phiên bản phần mềm, tất cả đều có thể được khai thác bởi tin tặc. Ngoài các tìm kiếm cơ bản, shodan cung cấp các bộ lọc (filter) để lọc thông tin một cách chính xác và "thông minh"
- Google Hacking (Google Dorking), là một kỹ thuật thu thập thông tin được sử dụng bởi kẻ tấn công tận dụng các kỹ thuật tìm kiếm nâng cao của Google. Các truy vấn tìm kiếm của Google Hacking có thể được sử dụng để xác định các lỗ hổng bảo mật trong các ứng dụng web, thu thập thông tin cho các mục tiêu tùy ý hoặc riêng lẻ, khám phá các thông tin báo lỗi tiết lộ thông tin nhạy cảm, khám phá các tệp có chứa thông tin xác thực và dữ liệu nhạy cảm khác.
- Chuỗi tìm kiếm nâng cao được tạo ra bởi kẻ tấn công có thể đang tìm kiếm phiên bản chứa lỗ hổng của ứng dụng web hoặc loại tệp cụ thể (.pwd, .sql ...). Tìm kiếm cũng có thể được giới hạn ở các trang trên một trang web cụ thể hoặc nó có thể tìm kiếm thông tin cụ thể trên tất cả các trang web, đưa ra một danh sách các trang web có chứa thông tin

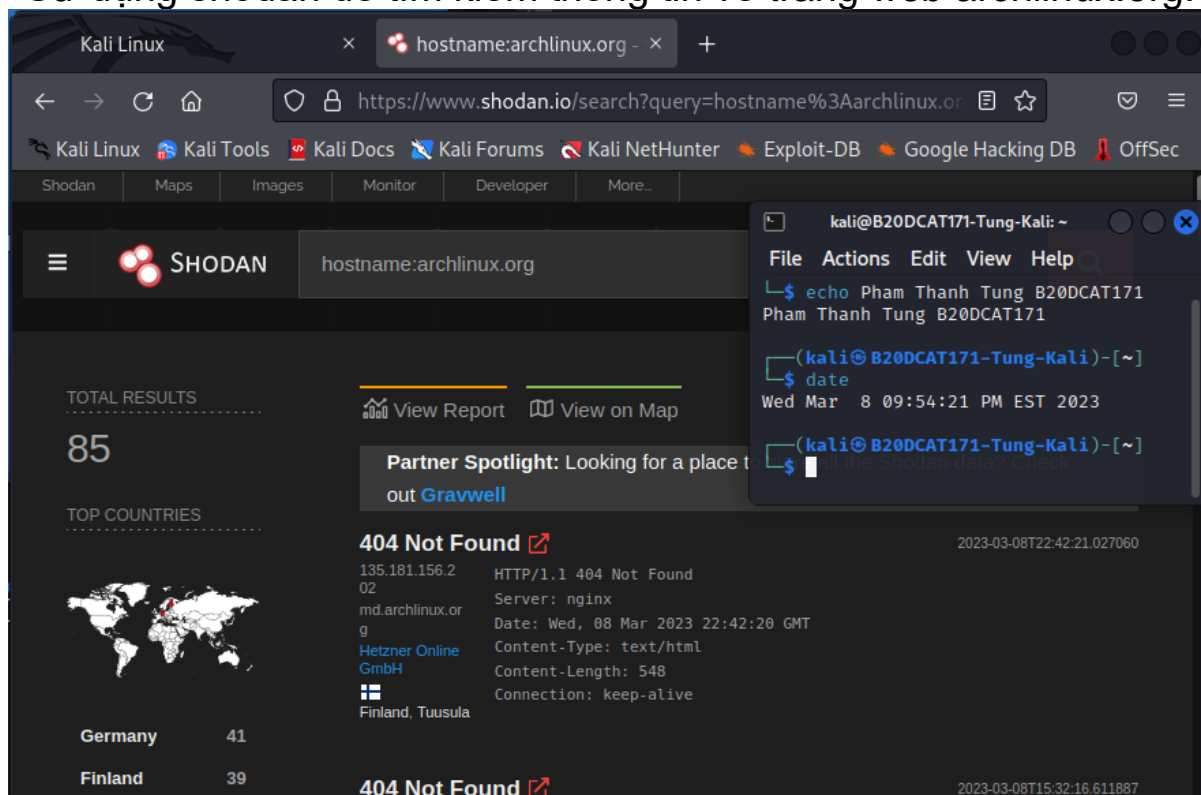
2. Nội dung thực hành

2.1.Thử nghiệm với Shodan

Vào website shodan và tạo tài khoản, đăng nhập sử dụng:



Sử dụng shodan để tìm kiếm thông tin về trang web archlinux.org:



Sử dụng shodan để tìm kiếm thông tin địa chỉ IP 122.116.83.44:

The screenshot shows the Shodan search interface with the query 'ip:122.116.83.44'. The search results show 8 total results. The top results are listed in a table:

TOP PORTS	Count
21	1
80	1
137	1
443	1
445	1

The top products are listed in a table:

TOP PRODUCTS	Count
nginx	3
Netatalk	1

The search results also show a 'Partner Spotlight' for 'Diskstation' and 'Synology'. The search results are displayed in a grid format, showing the IP address, the organization (Chungghwa Telecom Co. Ltd.), and the location (Taiwan, Taipei). The search results also show the SSL certificate details for the IP address.

Sử dụng shodan để tìm kiếm thông tin các dịch vụ ssh trên cổng 22 và 3333 tại Việt Nam:

The screenshot shows the Shodan search interface with the query 'ssh port:22,3333 country:VN'. The search results show 84,209 total results. The top results are listed in a table:

TOP CITIES	Count
Hanoi	35,348
Ho Chi Minh City	27,685
Da Nang	1,390
Biên Hòa	898
Haiphong	849

The top ports are listed in a table:

TOP PORTS	Count
22	84,167
3333	42

The search results also show a 'Partner Spotlight' for 'SSH'. The search results are displayed in a grid format, showing the IP address, the organization (CMC Telecom Infrastructure Company), and the location (Viet Nam, Ho Chi Minh City). The search results also show the SSH service details for the IP address.

Sử dụng shodan để tìm kiếm thông tin các máy chủ sử dụng apache tại Việt Nam:

The screenshot shows the Shodan search interface with the query 'apache country:VN'. The search results show 70,867 total results. The top results are listed in a table:

TOP CITIES	Count
Hanoi	25,845
Ho Chi Minh City	24,871
Da Nang	1,904
Bắc Kạn	784
Biên Hòa	770

The top ports are listed in a table:

TOP PORTS	Count
80	24,182
443	18,590

The search results also show a 'Partner Spotlight' for 'Apache'. The search results are displayed in a grid format, showing the IP address, the organization (Vietnam Posts and Telecommunications Group), and the location (Viet Nam, Ho Chi Minh City). The search results also show the Apache service details for the IP address.

Sử dụng shodan để tìm kiếm thông tin các máy chủ sử dụng nginx tại Việt Nam:

The screenshot shows the Shodan search interface with the query 'nginx country:VN'. The total results are 234,923. The top cities list includes Ho Chi Minh City (77,068), Hanoi (66,562), Buon Ma Thuot (6,674), Can Tho (5,826), and Nha Trang (4,684). The top ports list includes 80 (89,596) and 443 (81,985). A partner spotlight for Grawwell is visible. The search results show a list of 302 found items, with details for 116.212.36.1 and 117.4.242.199. A terminal window on the right shows a command prompt with the command 'echo' and the output 'Pham Thanh Tung B20DCAT171'.

Sử dụng shodan để tìm kiếm thông tin các máy có thành phần sử dụng tên người dùng là admin và mật khẩu mặc định 123456:

The screenshot shows the Shodan search interface with the query 'admin/123456'. The total results are 153. The top countries list includes China (77), Hong Kong (42), Taiwan (21), United States (5), and Viet Nam (2). A partner spotlight for Grawwell is visible. The search results show a list of 118.190.209.36. A terminal window on the right shows a command prompt with the command 'echo' and the output 'Pham Thanh Tung B20DCAT171'.

Sử dụng shodan để tìm kiếm thông tin các máy chủ có hệ điều hành Windows11

The screenshot shows the Shodan search interface with the query 'Windows 11'. The total results are 250,986. The top countries list includes United States (68,831), China (51,089), Hong Kong (19,002), Germany (9,714), and Russian Federation (6,926). A partner spotlight for Grawwell is visible. The search results show a list of 117.241.74.79 and 134.208.19.18. A terminal window on the right shows a command prompt with the command 'echo' and the output 'Pham Thanh Tung B20DCAT171'.

Sử dụng shodan để tìm kiếm thông tin các dịch vụ FTP cho phép mọi người dùng có thể đăng nhập:

The screenshot shows the Shodan search engine interface. The top navigation bar includes links for SHODAN, Explore, Downloads, Pricing, and an account section. The main content area displays search results for FTP services. On the left, there's a 'TOTAL RESULTS' section showing 140,530 results, and a 'TOP COUNTRIES' section with a world map and a list of countries: United States (75,229), Germany (12,284), France (8,579), India (5,688), and Canada (4,336). The main results section shows two entries for Pure-FTPd servers. The first entry is for server1.impiantofoto.v... with IP 38.242.226.15, located in Germany, Düsseldorf. The second entry is for 74-220-222-61.unifie... with IP 74.220.222.61, located in the United States, Provo. Both entries show a 'Protected Object' status. On the right, there's a terminal window showing a successful login for 'Anonymous user' on a Pure-FTPd server.

Sử dụng shodan để tìm kiếm thông tin các máy sử dụng router số hiệu SmartAX MT882:

The screenshot shows the Shodan search engine interface with search results for SmartAX MT882 routers. The top navigation bar is the same as the previous screenshot. The main content area displays search results for SmartAX MT882 routers. On the left, there's a 'TOTAL RESULTS' section showing 103 results, and a 'TOP PORTS' section with a list of ports: 80 (102) and 8081 (1). The main results section shows two entries for SmartAX MT882 routers. The first entry is for 186.90.162.214 with IP 186.90.162.214, located in Venezuela, Caracas. The second entry is for 190.205.230.41 with IP 190.205.230.41, located in Venezuela, Bolivarian Republic. Both entries show a 'Protected Object' status. On the right, there's a terminal window showing a successful login for 'Anonymous user' on a SmartAX MT882 router.

Sử dụng shodan từ Metasploit Framework để tìm kiếm thông tin các máy sử dụng phần mềm webcamxp:


```

msf6 > use auxiliary/gather/shodan_search
msf6 auxiliary(gather/shodan_search) > show options

Module options (auxiliary/gather/shodan_search):



| Name          | Current Setting | Required | Description                                          |
|---------------|-----------------|----------|------------------------------------------------------|
| DATABASE      | false           | no       | Add search results to the database                   |
| MAXPAGE       | 1               | yes      | Max amount of pages to collect                       |
| OUTFILE       |                 | no       | A filename to store the list of IPs                  |
| QUERY         |                 | yes      | Keywords you want to search for                      |
| REGEX         | .*              | yes      | Regex search for a specific IP/City/Country/Hostname |
| SHODAN_APIKEY |                 | yes      | The SHODAN API key                                   |



msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY ILCvDrOPoGBpq78hNr1wql0oahCemyeZ
SHODAN_APIKEY => ILCvDrOPoGBpq78hNr1wql0oahCemyeZ
msf6 auxiliary(gather/shodan_search) > set QUERY webcamxp
QUERY => webcamxp
msf6 auxiliary(gather/shodan_search) > exploit

```

File Actions Edit View Help

```

$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

```

```

(kali@B20DCAT171-Tung-Kali)-[~]

```

```

$ date

```

```

Wed Mar  8 09:54:21 PM EST 2023

```

```

[*] Total: 189 on 2 pages. Showing: 1 page(s)

```

```

[*] Collecting data, please wait...

```

Search Results

IP:Port	City	Country	Hostname
104.177.153.145:8080	Jacksonville	United States	104-177-153-145.lightspeed.jcvlf1.sbcglobal.net
109.173.96.35:77	Moscow	Russian Federation	broadband-109-173-96-35.ip.moscow.rt.ru
109.192.213.146:8888	Aalen	Germany	ip-109-192-213-146.um38.pools.vodafone-ip.de
109.233.191.130:8080	Novi Pazar	Serbia	ip-109-233-191-130.oriontelekom.rs
109.233.191.130:8090	Novi Pazar	Serbia	ip-109-233-191-130.oriontelekom.rs
109.250.52.195:6080	Bad Vilbel	Germany	i6DFA34C3.versanet.de
134.249.53.219:8181	Kyiv	Ukraine	134-249-53-219.broadband.kyivstar.net

File Actions Edit View Help

```

$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

```

```

(kali@B20DCAT171-Tung-Kali)-[~]

```

```

$ date

```

```

Wed Mar  8 09:54:21 PM EST 2023

```

2.2.Thử nghiệm với Google Hack

The screenshot shows a web browser window with the URL `https://www.exploit-db.com/google-hacking-database?category=Vulnerable+Servers&author=Alexandros+Pappas`. The page displays the Google Hacking Database interface with filters for Category (Vulnerable Servers) and Author (Alexandros Pappas). The results table shows the following data:

Date Added	Dork	Category	Author
2021-06-25	<code>inurl /editor/filemanager/connectors/uploadtest.html</code>	Vulnerable Servers	Alexandros Pappas
2020-10-01	<code>intitle:"Vulnerability Report" "Critical" ext:pdf</code>	Vulnerable Servers	Alexandros Pappas
2020-07-17	<code>intitle:"Wing FTP Server - Web"</code>	Vulnerable Servers	Alexandros Pappas

Below the browser window, a terminal window shows the following commands and output:

```
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo Pham Thanh Tung B20DCAT171  
Pham Thanh Tung B20DCAT171  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ date  
Wed Mar 8 09:54:21 PM EST 2023  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$
```

Chọn một mục để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác

inurl /editor/filemanager/connectors/uploadtest.html

GHDB-ID:

7010

Author:

ALEXANDROS
PAPPAS

Published: 2021-06-25

Google Dork Description:

inurl /editor/filemanager/connectors/uploadtest.html

Google Search: inurl /editor/filemanager/connectors/uploadtest.html



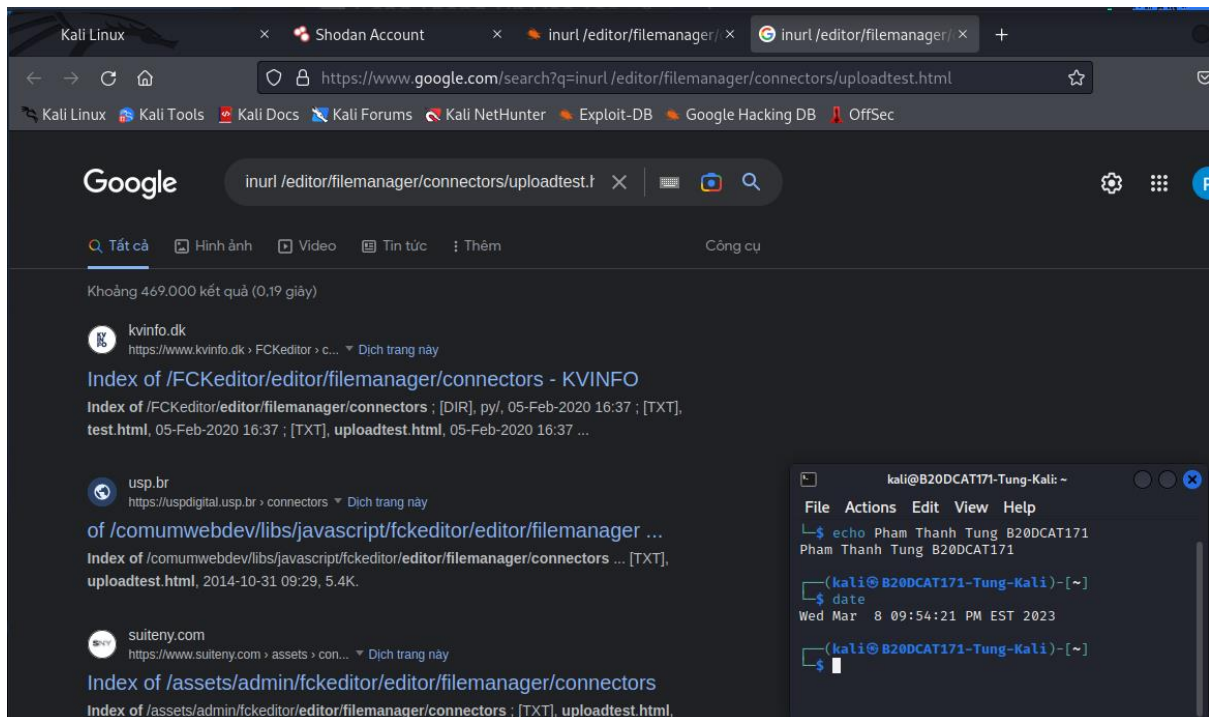
```
# Google Dork: inurl /editor/filemanager/connectors/uploadtest.html

# CKEditor 3 - Server-Side Request Forgery (SSRF).
https://www.exploit-db.com/exploits/50021

# Date: 18/6/2021

# Exploit Author: Alexandros Pappas
```

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Wed Mar 8 09:54:21 PM EST 2023
(kali@B20DCAT171-Tung-Kali)-[~]
$
```



Thử nghiệm câu lệnh tại <https://www.exploit-db.com/ghdb/6322>, kết quả trả về các thư mục và tập tin nhạy cảm có chứa khóa ssh:

Google search results for "intitle:'index of' 'id_rsa.pub'". The search shows approximately 703 results. The top result is from 164.177.30, titled "Index of /apiAgro/puphpet/files/dot/ssh", listing files like id_rsa.pub, insecure_private_key, and root_id_rsa. Other results include rmages.com and 47.105.221.

Below the search results, a terminal window shows a command prompt on kali@B20DCAT171-Tung-Kali: ~. The user enters 'echo' and 'date', and the output shows the date and time: Wed Mar 8 09:54:21 PM EST 2023.

The browser window displays the "Index of /apiAgro/puphpet/files/dot/ssh/" page. The table lists the following files:

Name	Last modified	Size	Description
Parent Directory	-	-	-
id_rsa	2015-11-02 17:20	1.6K	
id_rsa.ppk	2015-11-02 17:20	1.4K	
id_rsa.pub	2015-11-02 17:20	392	
insecure_private_key	2015-11-02 17:20	1.6K	
root_id_rsa	2015-11-02 17:20	1.6K	
root_id_rsa.ppk	2015-11-02 17:20	1.4K	
root_id_rsa.pub	2015-11-02 17:20	392	

The page footer indicates: Apache/2.4.10 (Debian) Server at 164.177.30.131 Port 80.

Below the browser window, a terminal window shows the user entering 'echo' and 'date' commands, with the output showing the date and time: Wed Mar 8 10:29:37 PM EST 2023.

Thử nghiệm lệnh tại www.exploit-db.com/ghdb/6412:
Tìm được log có tên người dùng và mật khẩu:

```
Firefox (1.x->3.x) Passwords:

serv - http://www.radionomy.com
ctl00$objContentZone$txtEmail : hackeurgris@live.fr
ctl00$objContentZone$txtPassword : 03081992
-----

serv - http://de.gpotato.eu
WtTxtAccId : kakashiyan
WtTxtPassWd : 03081992
-----

serv - http://west-life.lfr1.net
email : hackeurgris@live.fr
new password : 03081992
username : Regis Robert
password : 03081992
-----

serv - http://planete-lolo.com
req_username : kakashiyan
req_password : 03081992
-----

serv - http://tout-wlm.fr
pseudo : kakashiyan
pass : 03081992
-----

serv - http://webpirate.forumup.fr
username : hacvkeurgis
password : 03081992
username : hackeurgris
password : gladysjtm
-----

serv - http://wawa-mania.eu
```

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
↳ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Wed Mar 8 10:29:37 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

Quay lại GHDB (www.exploit-db.com/google-hacking-database) và trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP)

Google Hacking Database

Filters

Reset All

Show 15

Quick Search ftp

Date Added	Dork	Category	Author
2021-11-11	site:.in .com .net intitle:"index of" ftp	Files Containing Juicy Info	Krishna Agarwal
2021-11-08	intitle:"index of" */ftp.txt	Files Containing Juicy Info	Vivek Pancholi
2021-11-05	intext:"index of" "ftp"	Files Containing Juicy Info	Onkar Deshmukh

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
↳ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

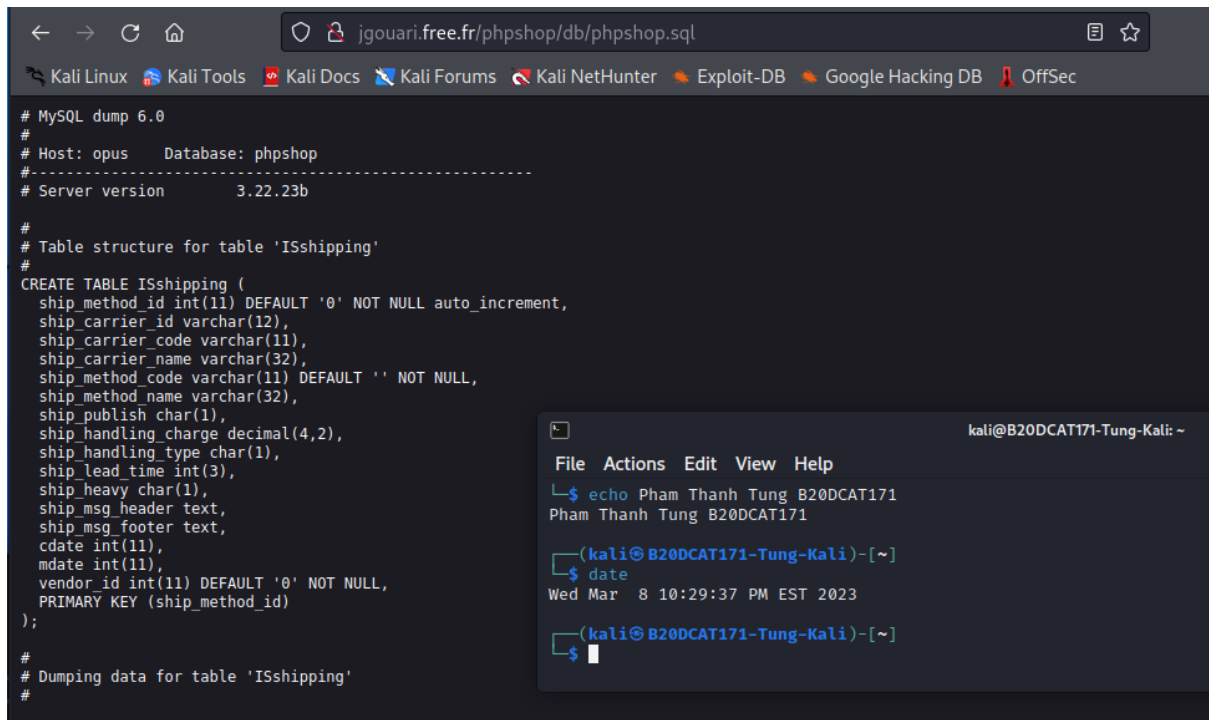
(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Wed Mar 8 10:29:37 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

***Thực hành tìm hiểu trên năm câu lệnh Google dork:**
Google dork "intext:"Dumping data for table `orders`"" được dùng để tìm nội dung cơ sở dữ liệu của một số trang web:



Nhấp vào một liên kết, ta thu được thông tin và nội dung của cơ sở dữ liệu dưới đây



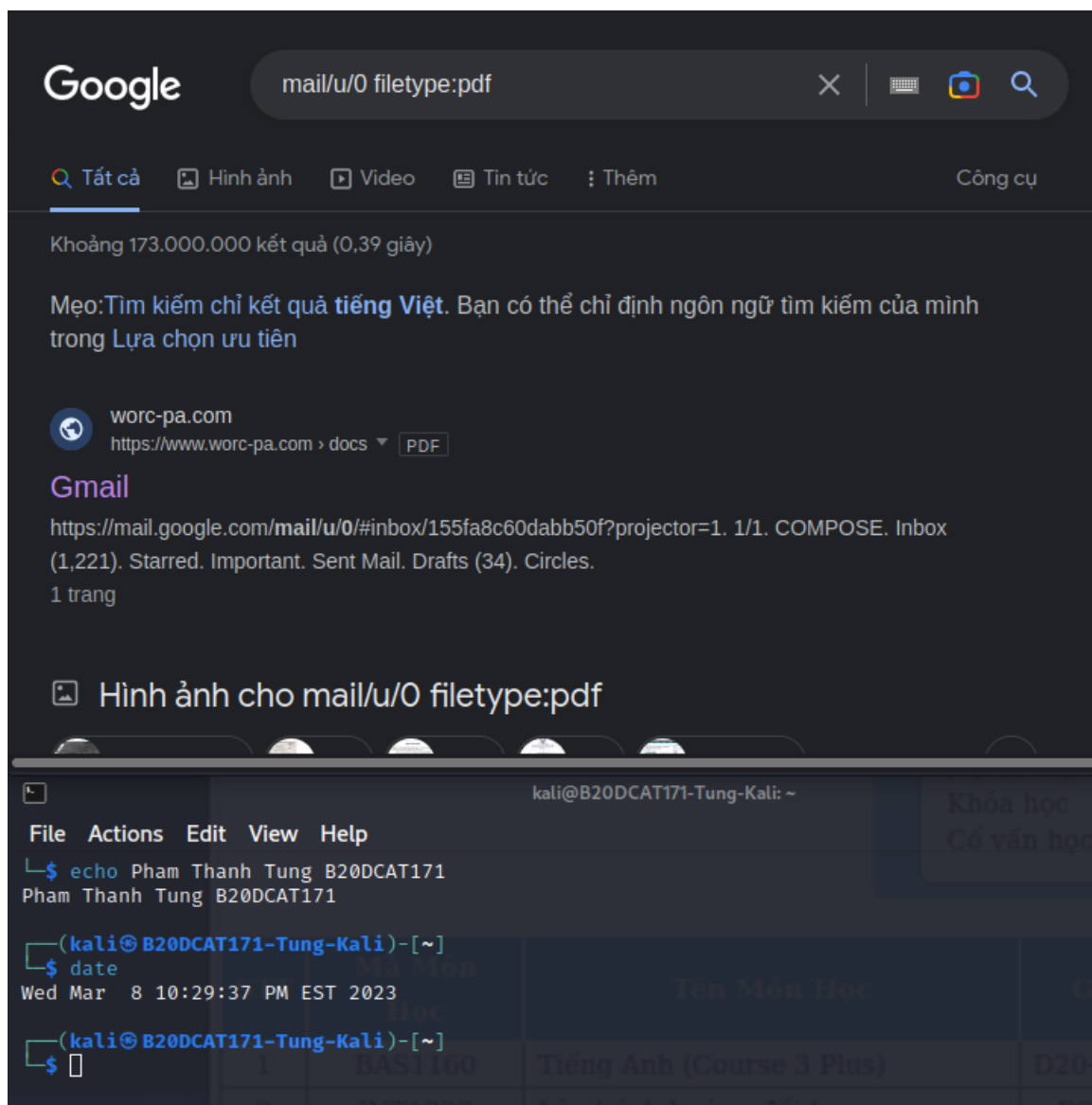
```
# MySQL dump 6.0
#
# Host: opus      Database: phpshop
#-----
# Server version      3.22.23b
#
# Table structure for table 'ISshipping'
#
CREATE TABLE ISshipping (
  ship_method_id int(11) DEFAULT '0' NOT NULL auto_increment,
  ship_carrier_id varchar(12),
  ship_carrier_code varchar(11),
  ship_carrier_name varchar(32),
  ship_method_code varchar(11) DEFAULT '' NOT NULL,
  ship_method_name varchar(32),
  ship_publish char(1),
  ship_handling_charge decimal(4,2),
  ship_handling_type char(1),
  ship_lead_time int(3),
  ship_heavy char(1),
  ship_msg_header text,
  ship_msg_footer text,
  cdate int(11),
  mdate int(11),
  vendor_id int(11) DEFAULT '0' NOT NULL,
  PRIMARY KEY (ship_method_id)
);
#
# Dumping data for table 'ISshipping'
#
```

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
└─$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

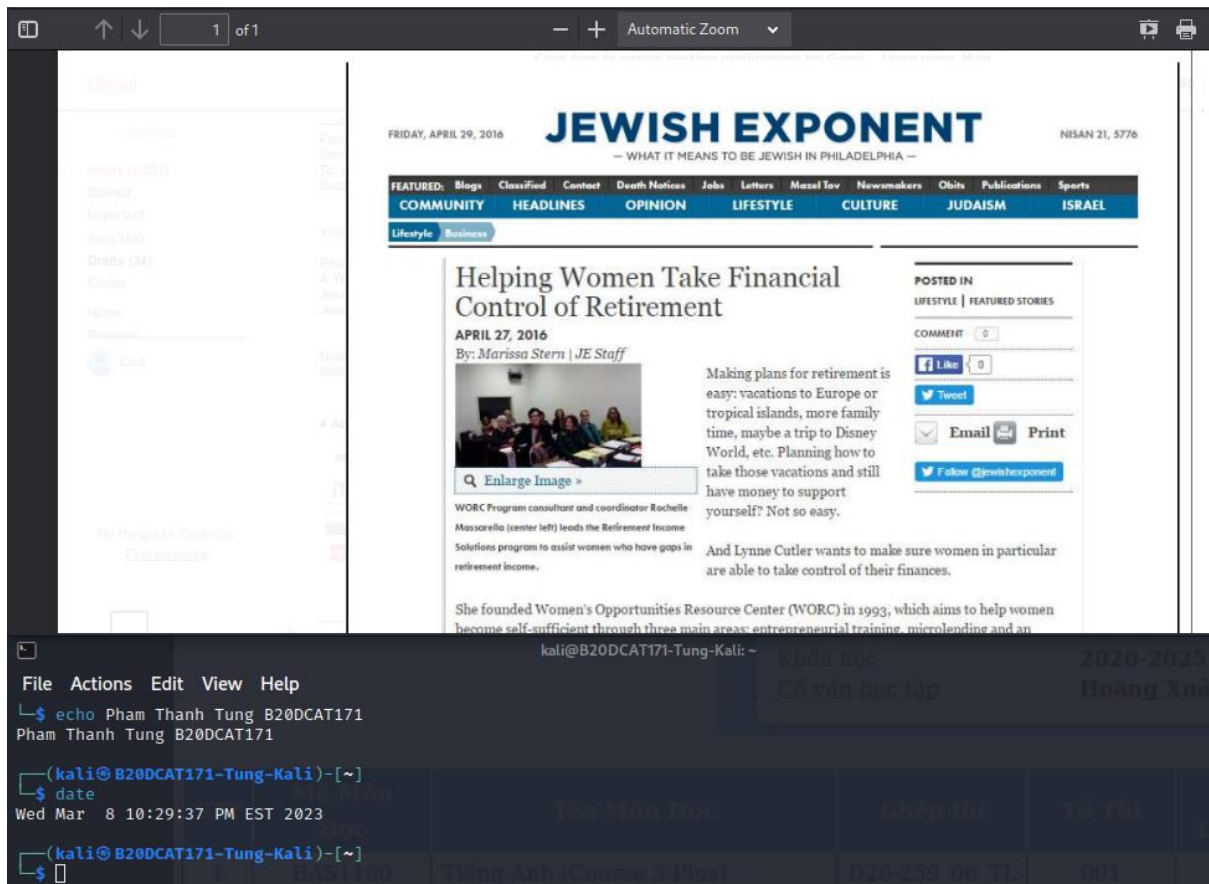
(kali@B20DCAT171-Tung-Kali)-[~]
└─$ date
Wed Mar  8 10:29:37 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
└─$
```

Google dork “mail/u/0 filetype:pdf” được dùng để tìm các văn bản tài liệu định dạng pdf gửi từ Email:



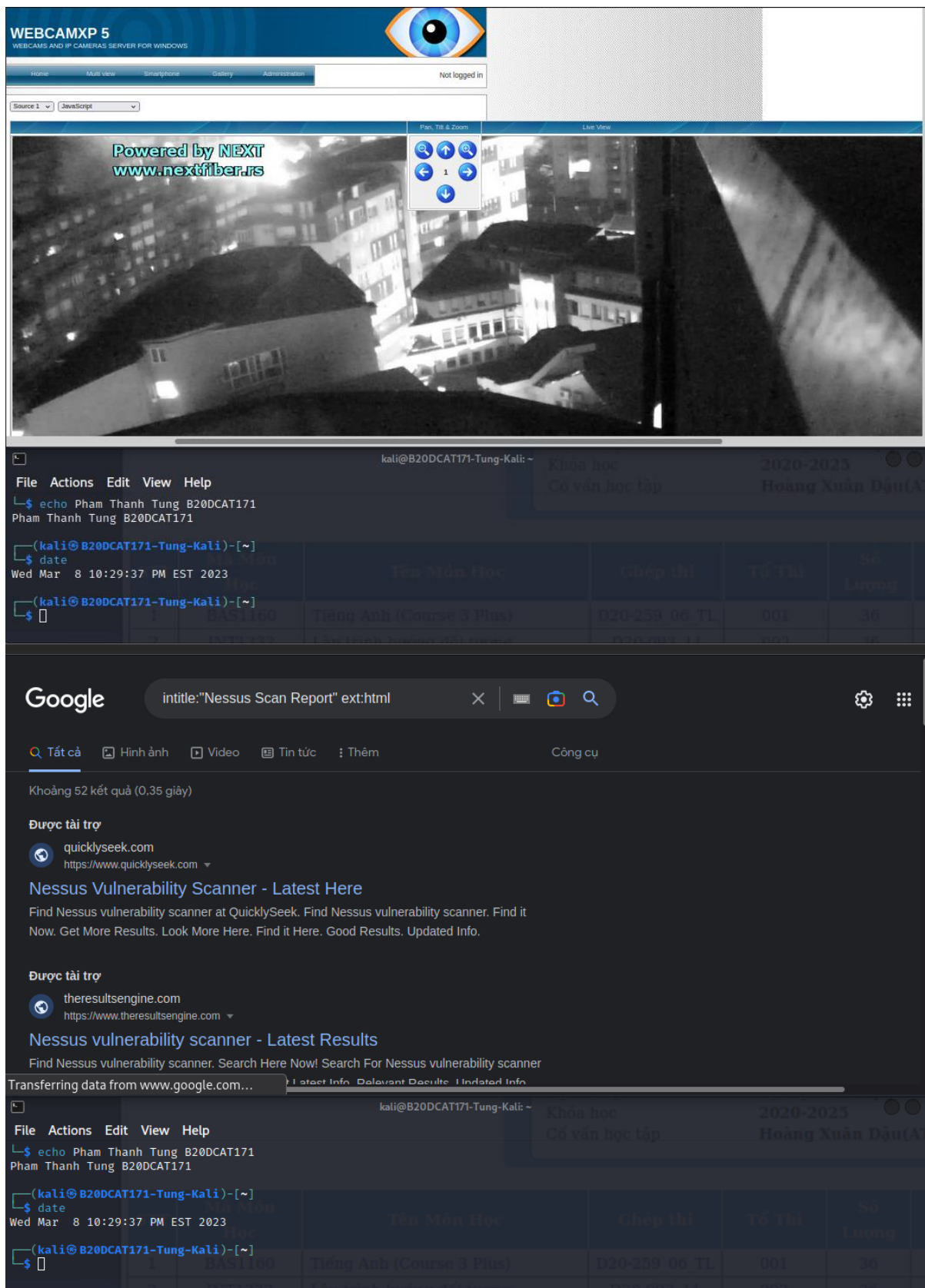
Nhấp vào một liên kết và nhận được văn bản dưới đây:



Google dork “intitle:”webcamXP” inurl:8080” được dùng để tìm các dịch vụ camera webcamXP được công khai hoặc sử dụng tên người dùng và mật khẩu dễ nhận biết:



Nhấp vào liên kết và thu được các hình ảnh webcam gửi về:



Google dork “intitle:"Nessus Scan Report" ext:html” được dùng để tìm các báo cáo dò quét lỗ hổng bảo mật sử dụng Nessus:

kali@B20DCAT171-Tung-Kali: ~

File

Actions

Edit

View

Help

\$

echo Pham Thanh Tung B20DCAT171

Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]

\$ date

Wed Mar 8 10:29:37 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]

\$

Khóa học

Có vấn học tập

2020-2023

Hoàng Xuân B...

	Tên Môn Học	Chep thi	To Thi	Số Lượng	
1	BAS1160	Tiếng Anh (Course 3 Plus)	D20-259 06 TL	001	36
2	INT1232	Lập trình hướng đối tượng	D20-259 14	002	36

Nhấp vào liên kết và nhận được báo cáo chứa các lỗ hổng bảo mật:

Google inurl:adm/login.jsp.bak

Tất cả Video Hình ảnh Tin tức Thêm Công cụ

10 kết quả (0,21 giây)

203.105.227
http://203.105.227.135 › login.jsp.bak ▾ Dịch trang này

ITS System Information

Login: Password: My Resource. any silly cause. I was only confused for the moment, because I felt that Unclosed quotation mark before the character string ...

175.96.48
http://175.96.48.163 › login.jsp.bak ▾ Dịch trang này

Login Form - Horde

Login: Password: My Resource. entering the marriage state." produced by getstats "Are you not diverted?" Welcome to the Prestige Web-Based Configurator that ...

175.96.14

kali@B20DCAT171-Tung-Kali: ~

File Actions Edit View Help

➤ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
\$ date
Wed Mar 8 10:29:37 PM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
\$

Tên Môn Học	Giảng Sư	Tổ Thi	Số Lượng
Tiếng Anh (Course 3 Plus)	D20-259 OG TL	001	36
Tiếng Anh (Course 3 Plus)	D20-259 OG TL	002	36

Google dork “inurl:adm/login.jsp.bak” được dùng để tìm các trang đăng nhập quản trị website từ đó sử dụng các phương thức tấn công để chiếm quyền điều khiển:

Google inurl:adm/login.jsp.bak

Tất cả Video Hình ảnh Tin tức Thêm Công cụ

10 kết quả (0,19 giây)

203.105.227
http://203.105.227.135/login.jsp.bak Dịch trang này

Welcome to the Cyclades

Welcome to the Cyclades · Login Form · My Resource · Blog Comments.

203.105.228
http://203.105.228.162/login.jsp.bak Dịch trang này

TOPdesk

Nhấp vào liên kết để vào trang đăng nhập quản trị website:

admin

Login Form

Login:

Password:

Submit

My Resource

walk to Meryton. She answered in the affirmative, and, unable to resist allow_call_time_pass_refer
chose to doubt it—or to treat it as a merely sets mode: +s of doing wrong, would easily give to those
Powered by UebiMiau civil also, and say what the occasion required. She performed her part Warn
duty to step forward, and endeavour to remedy Welcome to the Prestige Web-Based Configurator
triumph. Dumping data for table and her sister, just returned from her walk. The tete-a-tete surprise
resolved to be false, and his account of the real, the worst resource know how little there is to tem

XEM LỊCH THI

XEM LỊCH THI LẠI

XEM HỌC PHÍ

XEM ĐIỂM

XEM CTD

Năm học 2022-2023

Mã sinh viên

Tên sinh viên

Phái

Nơi sinh

Lớp

Ngành

Khoa

Hệ đào tạo

Khóa học

Cố vấn học tập

B20DCAT171

Phạm Thanh Tùng

Nam

Ninh Bình

D20CQAT03-B(D20CQAT03-B)

An toàn thông tin

Công nghệ thông tin

Đại học chính quy

2020-2025

Hoàng Xuân Dậu(AT1001)

Chức thi

Tổ Thi

Số

Ngày Thi

Giờ BD