

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



**Môn: Thực tập cơ sở**

**BÀI BÁO THỰC TẬP CƠ SỞ**

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

<b>Họ và tên giảng viên:</b>	TS.Đinh Trường Duy
<b>Họ và tên:</b>	Nguyễn Quốc Khánh
<b>Mã sinh viên:</b>	B20DCAT103
<b>Lớp:</b>	D20CQAT03-B
<b>Số điện thoại:</b>	0964137761

**Hà Nội 2023**

## 1.1 Mục đích

Bài thực hành này giúp sinh viên hiểu được mối đe dọa đến từ các công cụ tìm kiếm bao gồm Shodan và Google.

## 1.2 Nội dung thực hành

### 1. Tìm hiểu lý thuyết

Tìm hiểu về shodan và google hack. Tài liệu tham khảo:

- <https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>
- Principles of Computer Security: CompTIA Security+ and Beyond

#### a. Shodan

Shodan là một công cụ tìm kiếm trên internet cho các thiết bị kết nối mạng như máy tính, camera, máy in, router, v.v. Shodan có thể cung cấp nhiều thông tin về các thiết bị này như địa chỉ IP, hệ điều hành, phiên bản phần mềm, vị trí địa lý, v.v. Shodan có thể được sử dụng cho nhiều mục đích khác nhau như nghiên cứu, giáo dục, bảo mật, phát hiện lỗ hổng, v.v. Shodan cũng có thể được sử dụng cho các mục đích xấu như tấn công, đột nhập, đánh cắp dữ liệu, v.v.

Shodan là một công cụ tìm kiếm Internet, hoạt động bằng cách quét các địa chỉ IP trên Internet và lưu trữ thông tin về các thiết bị và hệ thống được kết nối trên đó. Shodan sử dụng một loạt các công cụ và kỹ thuật để tìm kiếm các thiết bị, bao gồm:

- Scanning: Shodan sử dụng kỹ thuật quét để tìm kiếm các thiết bị và hệ thống trên mạng. Nó có thể quét các cổng mạng khác nhau để xác định các dịch vụ đang chạy trên một thiết bị cụ thể.
- Banner grabbing: Shodan sử dụng kỹ thuật banner grabbing để lấy thông tin từ các banner HTTP và các thông điệp trả về từ các dịch vụ trên một thiết bị. Các thông tin này cung cấp cho Shodan thông tin chi tiết về thiết bị và các dịch vụ đang chạy trên đó.
- Các công cụ phân tích: Shodan sử dụng các công cụ phân tích để xác định các lỗ hổng bảo mật và các thông tin khác liên quan đến các thiết bị và hệ thống trên mạng. –

Sau khi Shodan đã tìm thấy các thiết bị và hệ thống trên mạng, nó sẽ lưu trữ thông tin về chúng trong một cơ sở dữ liệu lớn và cung cấp cho người dùng truy cập

thông tin này thông qua giao diện tìm kiếm và API. Người dùng có thể tìm kiếm các thiết bị và hệ thống trên mạng bằng cách sử dụng các tiêu chí như địa chỉ IP, tên miền, dịch vụ và các thông tin khác liên quan đến các thiết bị và hệ thống trên mạng

## **b. Google hacking**

Google Hacking là một kỹ thuật máy tính sử dụng các toán tử hoặc lệnh để lọc thông tin mà chúng ta nhận được từ công cụ tìm kiếm Google, có thể được sử dụng để tìm các lỗ hổng bảo mật trong cấu hình và mã nguồn được sử dụng trên các trang web, cũng có thể được sử dụng để thực hiện các vụ tấn công, bằng cách khai thác thông tin nhạy cảm hoặc ẩn trên mạng.

Google Hacking sử dụng các toán tử nâng cao của Google để tìm kiếm chính xác hơn và giới hạn phạm vi tìm kiếm. Google Hacking yêu cầu kiến thức cơ bản về cách hoạt động của Google và cách sử dụng các cú pháp tìm kiếm đặc biệt. 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 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.

Các kỹ thuật Google hacking thường bao gồm việc sử dụng các từ khóa đặc biệt để tìm kiếm các thông tin như tên đăng nhập và mật khẩu, các tập tin không được bảo mật, thông tin về hệ thống, tên miền và các thông tin khác liên quan đến các trang web và hệ thống trên mạng. Các từ khóa đặc biệt này thường được sử dụng để tìm kiếm các tài liệu nhạy cảm trên các trang web và các hệ thống trên mạng.

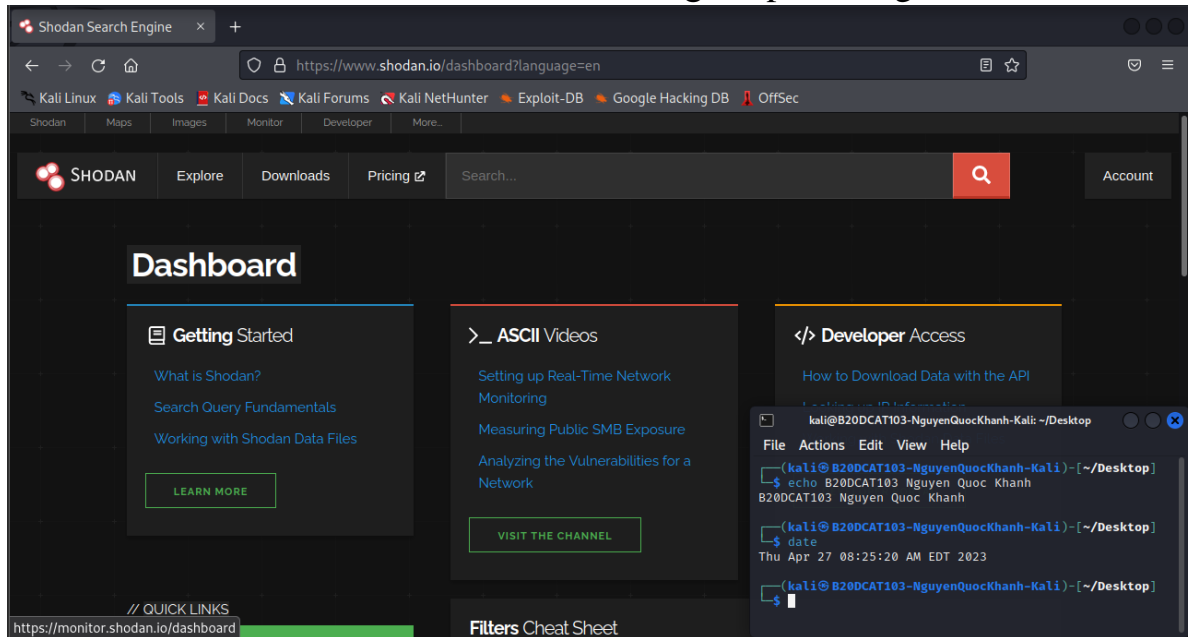
Các từ khóa đặc biệt này được sử dụng để giới hạn kết quả tìm kiếm của Google theo các tiêu chí cụ thể, ví dụ như tìm kiếm các tập tin không được bảo mật trên một trang web cụ thể, tìm kiếm thông tin về tên đăng nhập và mật khẩu, tìm kiếm thông tin về hệ thống và các thông tin khác liên quan đến các trang web và hệ thống trên mạng.

## 2. Thực hành

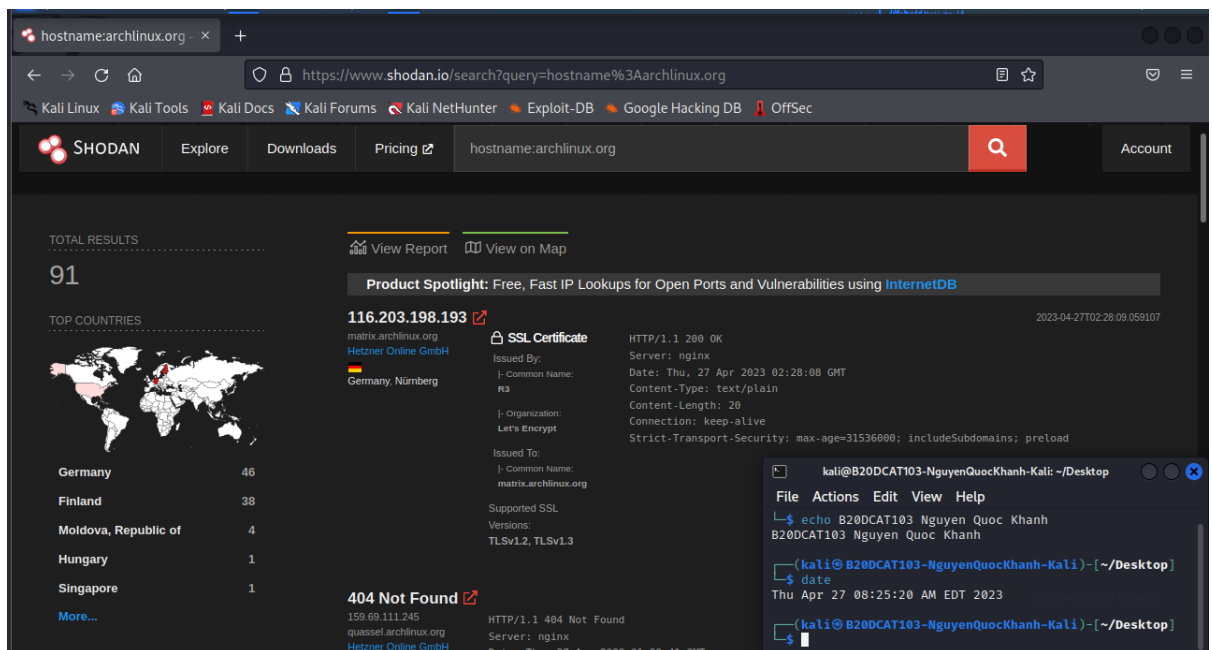
### a. Thử nghiệm với Shodan

Các bước thực hiện:

- 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 results page displays 8 total results. The top ports listed are 21, 80, 137, 443, and 445. The top products listed are nginx, Netatalk, and Samba. The product spotlight for '122.116.83.44' shows it is a Diskstation with a NetBIOS response and an SSL certificate. A terminal window on the right shows the user 'kali@B20DCAT103-NguyenQuocKhanh-Kali' running commands like 'echo B20DCAT103 Nguyen Quoc Khanh' and 'date'.

- 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 results page displays 98,440 total results. The top cities listed are Hanoi, Ho Chi Minh City, Da Nang, Phú Vang, and Biên Hòa. The top ports listed are 22 and 3333. The product spotlight for '103.139.41.23' shows it is a SSH service with a key type of 'ssh-rsa'. A terminal window on the right shows the user 'kali@B20DCAT103-NguyenQuocKhanh-Kali' running commands like 'echo B20DCAT103 Nguyen Quoc Khanh' and 'date'.

- 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 75,956 total results. The top cities listed are Ho Chi Minh City (27,759), Hanoi (26,217), Da Nang (1,174), Bắc Kạn (1,136), and Nam Định (891). The top ports listed are 80 (24,615), 443 (18,285), and 7547 (8,622). The product spotlight is 'Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB'. The main result is for IP 61.28.229.208, which is a VinaData Information Technology Service JSC server in Ho Chi Minh City, running Apache/2.4.18.12 on port 80. The server is configured with 'Server: Apache/2.4.18.12' and 'Server: Apache/2.4.18.12'. The connection is 'Upgrade: h2,h2c'. The last modified date is 'Tue, 14 Jun 2022 06:29:20 GMT'. The ETag is '2c-5e162865b5262'. The accept-ranges are 'bytes'. The content-length is '44'. The vary is 'User-Agent'. The content-type is 'text/html'. The SSL certificate is issued by 'Logjam'. The vulnerabilities are listed as 'Logjam'.

- 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 search results show 239,370 total results. The top cities listed are Ho Chi Minh City (81,974), Hanoi (66,842), Cần Thơ (5,479), Biên Hòa (4,448), and Nha Trang (4,410). The top ports listed are 80 (91,685), 443 (78,407), and 5000 (5,119). The product spotlight is 'Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB'. The main result is for IP 42.116.108.34, which is a FPT Telecom Company server in Ho Chi Minh City, running NGINX/1.2.3 on port 80. The server is configured with 'Server: nginx/1.2.3' and 'Server: nginx/1.2.3'. The connection is 'close'. The last modified date is 'Thu, 27 Apr 2023 12:36:11 GMT'. The content-type is 'text/html'. The transfer-encoding is 'chunked'. The connection is 'close'. The main result is for IP 14.162.104.222, which is a static.vnpt.vn server in Hanoi, running NGINX/1.18.0 (Ubuntu) on port 80. The server is configured with 'Server: nginx/1.18.0 (Ubuntu)' and 'Server: nginx/1.18.0 (Ubuntu)'. The connection is 'keep-alive'. The WWW-Authenticate is 'Basic realm="calibre"'. The vulnerabilities are listed as 'Logjam'.

- 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 1234:

The screenshot shows the Shodan search interface with the query 'admin/1234'. The search results show 2,267 total results. The top countries are listed as Viet Nam (953), Russian Federation (207), Taiwan (161), Poland (146), and Ukraine (115). A world map highlights the top countries. The product spotlight is 'Pure - Login'. The search results for 'Pure - Login' are displayed, showing the IP address 194.66.38.36, the domain pure.coventry.ac.uk, and the organization Coventry University. The search results also show the SSL certificate details for the IP address, including the common name, organization, and supported SSL versions.

- Sử dụng shodan để tìm kiếm thông tin các máy chủ có hệ điều hành Windows 2003:

The screenshot shows the Shodan search interface with the query 'windows 2003'. The search results show 54,253 total results. The top countries are listed as China (18,078), Taiwan (4,924), United States (4,626), France (3,430), and Hong Kong (1,655). A world map highlights the top countries. The product spotlight is 'Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB'. The search results for 'Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB' are displayed, showing the IP address 114.142.110.147, the domain mail.hakuunsha.co.jp, and the organization OTnet, Inc. The search results also show the SSL certificate details for the IP address, including the common name, organization, and supported SSL versions.

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

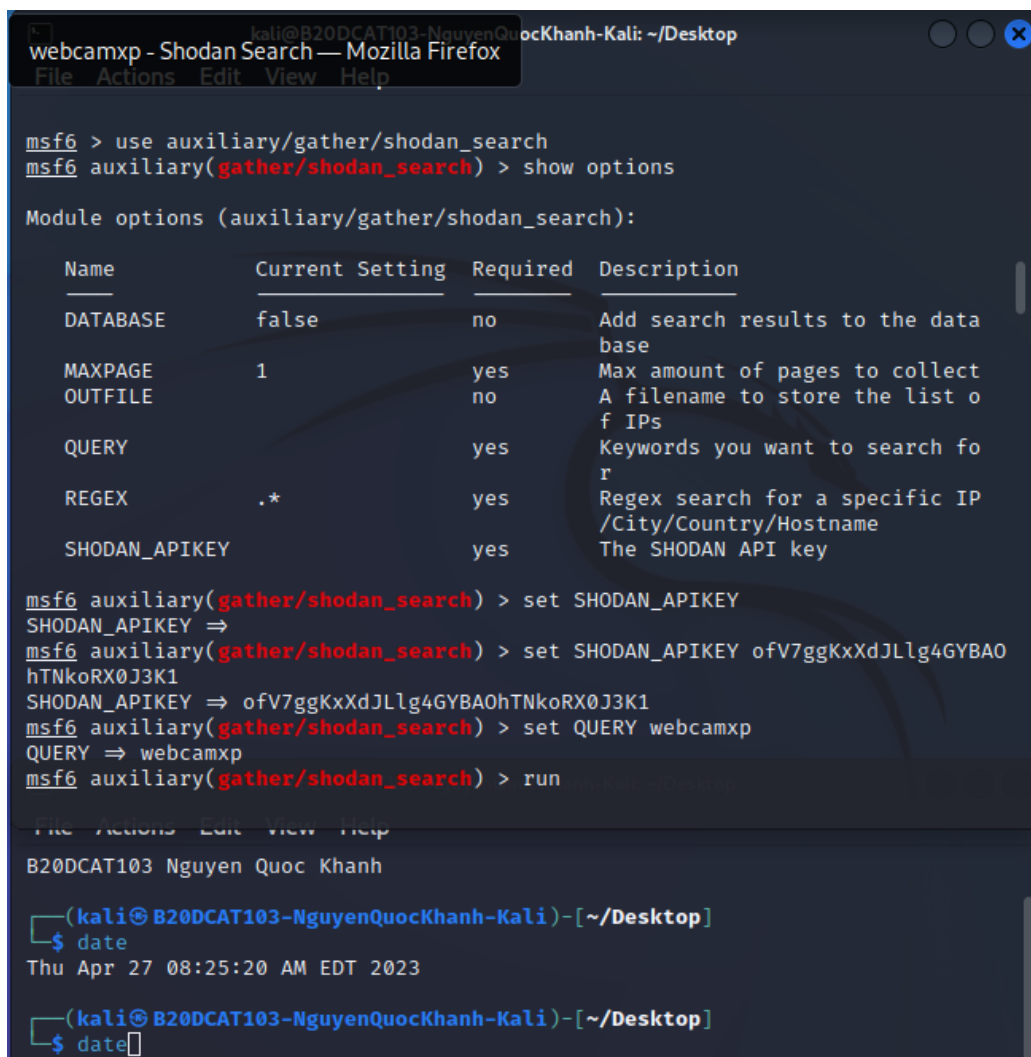
The screenshot shows the Shodan search interface with the query 'anonymous user logged in'. The results page displays 150,463 total results. A world map highlights top countries, with the United States having the most results (80,992). A 'Product Spotlight' for InternetDB is visible. A detailed view of a specific result shows an FTP server (220 RICOH Aficio MP 2851) where an anonymous user successfully logged in. A terminal window in the bottom right corner shows a user running a command to echo the IP and date.

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

The screenshot shows the Shodan search interface with the query 'smartax mt882'. The results page displays 124 total results. A world map highlights top countries, with Venezuela having the most results (123). A 'Protected Object' section shows details for a specific result, including the IP 186.89.33.226 and the router model SmartAX MT882. A terminal window in the bottom right corner shows a user running a command to echo the IP and date.



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



```

kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
webcamxp - Shodan Search — Mozilla Firefox
File Actions Edit View Help

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 data
  base
  MAXPAGE       1                yes       Max amount of pages to collect
  OUTFILE       no               no        A filename to store the list o
  f IPs
  QUERY         .*               yes       Keywords you want to search fo
  r
  REGEX         .*               yes       Regex search for a specific IP
  /City/Country/Hostname
  SHODAN_APIKEY yes              yes       The SHODAN API key

msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY
SHODAN_APIKEY =>
msf6 auxiliary(gather/shodan_search) > set SHODAN_APIKEY ofV7ggKxXdJLlg4GYBA0
hTNkoRX0J3K1
SHODAN_APIKEY => ofV7ggKxXdJLlg4GYBA0hTNkoRX0J3K1
msf6 auxiliary(gather/shodan_search) > set QUERY webcamxp
QUERY => webcamxp
msf6 auxiliary(gather/shodan_search) > run

File Actions Edit View Help
B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date
Thu Apr 27 08:25:20 AM EDT 2023

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date

```

```

kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help
msf6 auxiliary(gather/shodan_search) > exploit

[*] Total: 205 on 3 pages. Showing: 1 page(s)
[*] Collecting data, please wait...

Search Results

IP:Port      City          Country      Hostname
-----
108.48.149.30:8080 Washington    United States mail.fifiscreative
0 kidscenter.com
108.48.26.47:8080 Leesburg     United States pool-108-48-26-47.
washdc.fios.verizo
n.net
109.173.96.35:777 Moscow       Russian Federatio broadband-109-173-
7 n 96-35.ip.moscow.r
t.ru
109.192.213.146:888 Aalen        Germany      ip-109-192-213-146
.um38.pools.vodafo
ne-ip.de
109.233.191.130:8080 Belgrade     Serbia       ip-109-233-191-130
.oriontelekom.rs
114.42.3.144:8080 Taichung     Taiwan       114-42-3-144.dynam
ic-ip.hinet.net
121.141.136.178:8080 Seoul        Korea, Republic o
f

B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date
Thu Apr 27 08:25:20 AM EDT 2023

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date

```

## b. Thử nghiệm với Google Hacking

- Vào website [www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database), sử dụng Filters

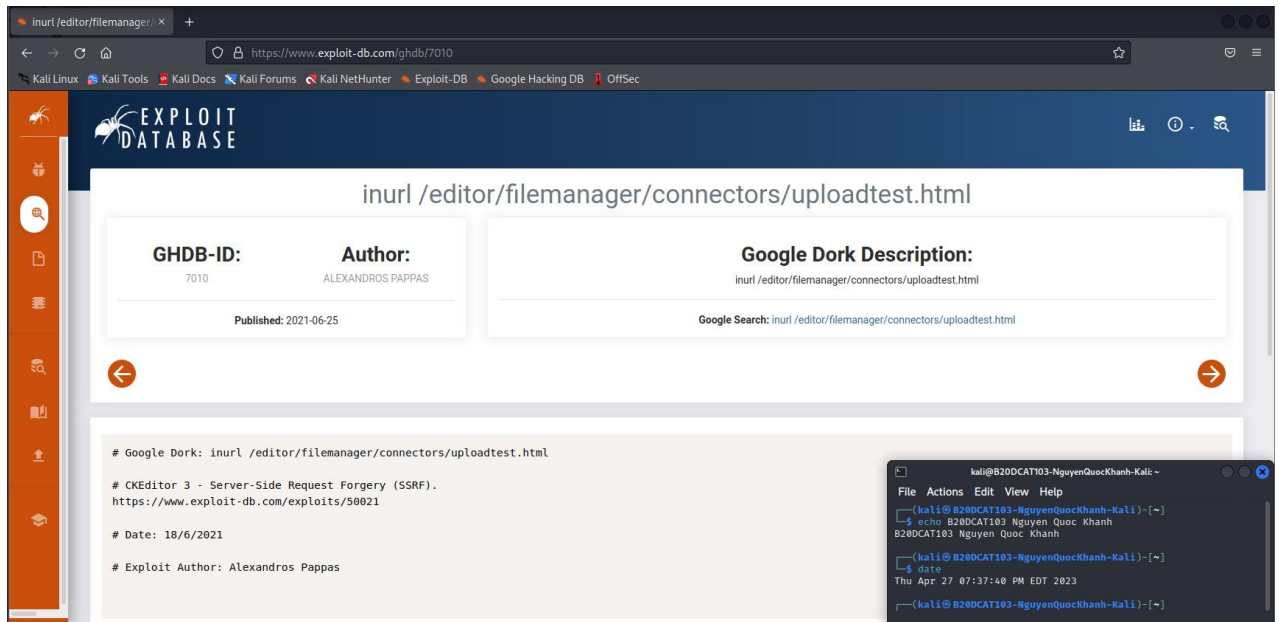
The screenshot shows the Google Hacking Database interface. The search results are filtered by Category 'Vulnerable Servers' and Author 'Alexandros Pappas'. The results table shows several entries with their Date Added, Dork, Category, and Author.

Date Added	Dork	Category	Author
2021-06-25	inurl /editor/filemanager/connectors/uploadtest.html	Vulnerable Servers	Alexandros Pappas
2020-10-01	intitle:"Vulnerability Report" "Critical" ext:pdf	Vulnerable Servers	Alexandros Pappas
2020-07-17	intitle:"Wing FTP Server - Web"	Vulnerable Servers	Alexandros Pappas
2020-06-17	intext:"Powered By Gila CMS"	Vulnerable Servers	Alexandros Pappas
2020-06-04	intext:"(c) GUnet 2003-2007"	Vulnerable Servers	Alexandros Pappas
2020-06-02	"Powered by Jira Service Desk"	Vulnerable Servers	Alexandros Pappas

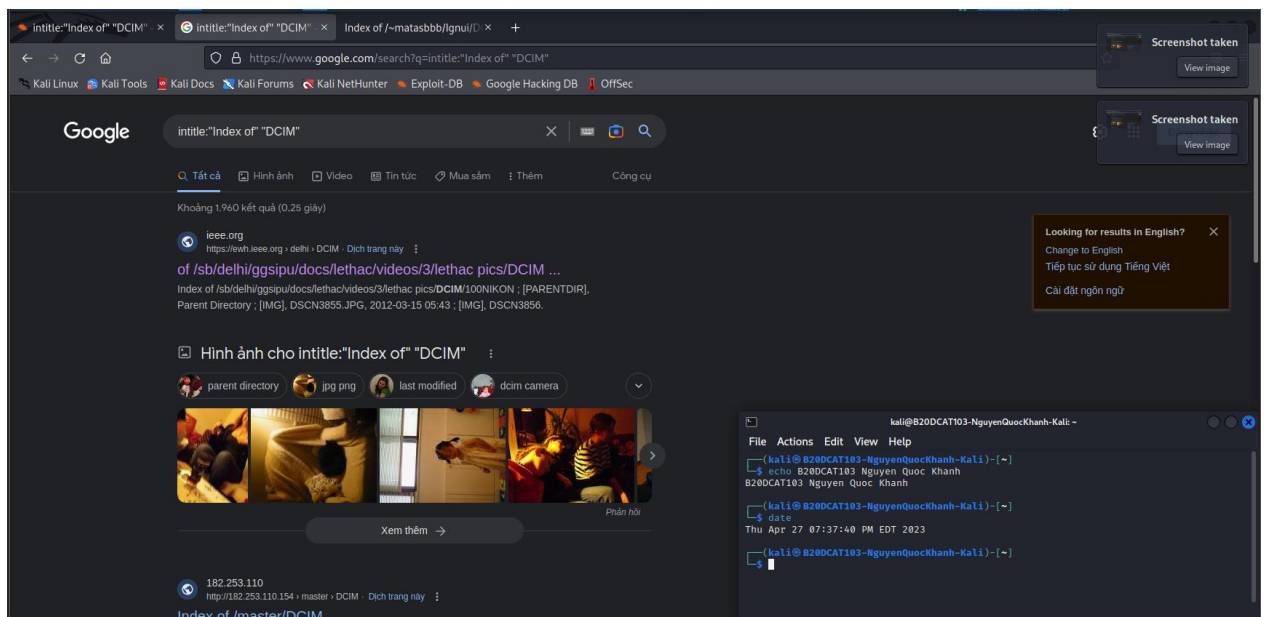
Showing 1 to 6 of 6 entries

At the bottom, there are sections for Downloads (Kali Linux, Kali NetHunter), Certifications (OSCP, OSWP), and Training (Penetration Testing with Kali Linux (PWK) (PEN-200), All new for 2020, Offensive Security Wireless Attacks (WiFi) (PEN-210)).

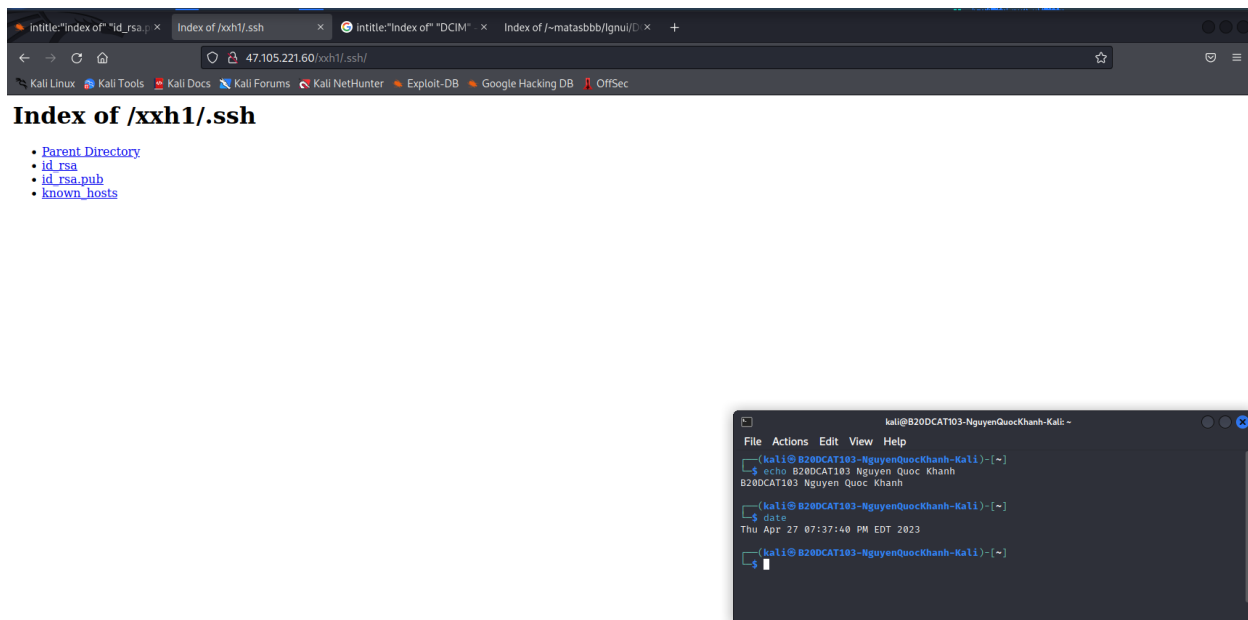
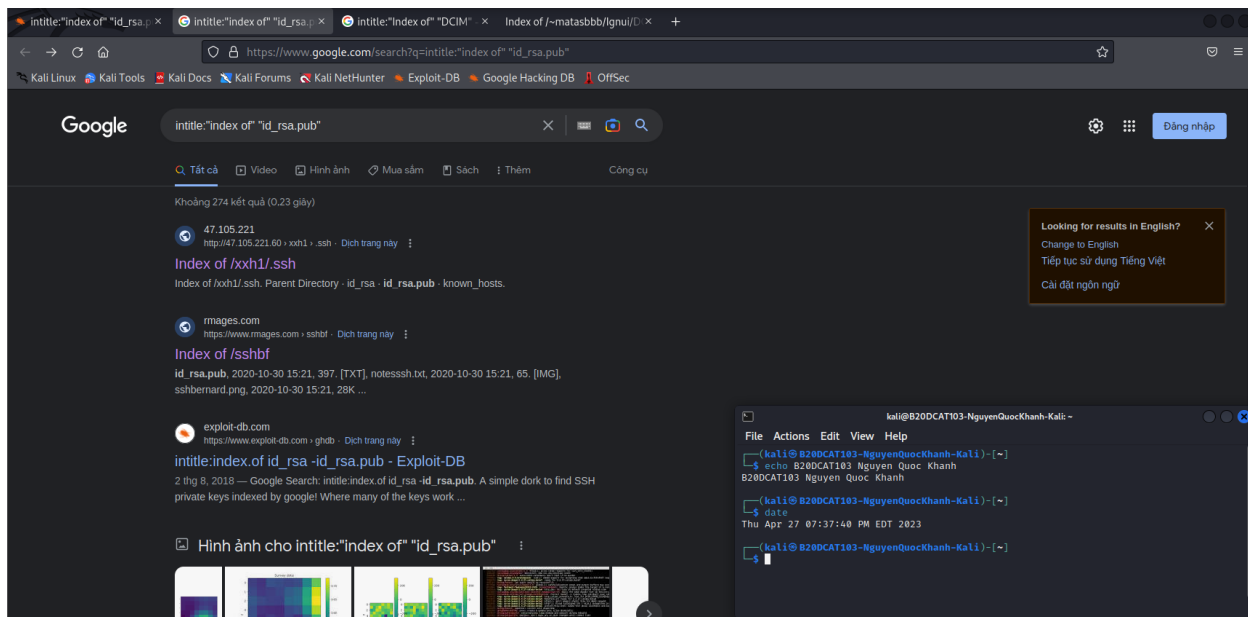
- Chọn một mục để hiển thị ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác:



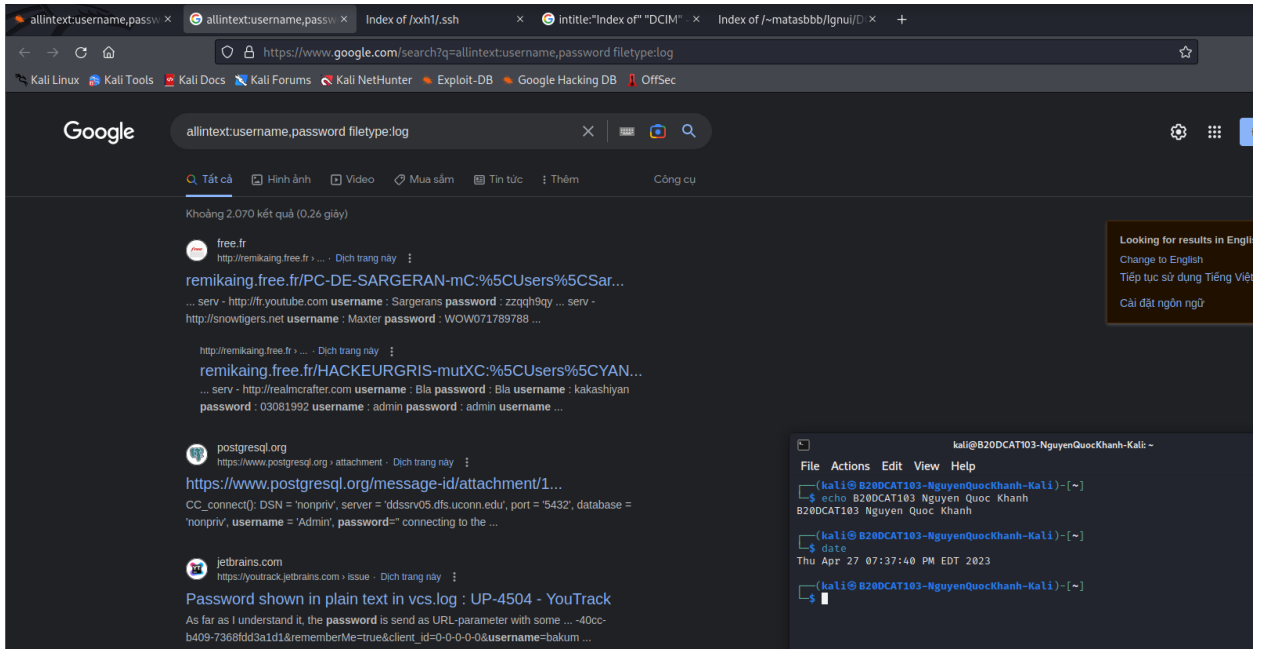
- Thử nghiệm với ví dụ tại <http://www.exploit-db.com/ghdb/4057>, trong đó từ khóa intitle tìm kiếm những từ ở trong tiêu đề của trang web, DCIM là tên thư mục thường sử dụng để lưu ảnh



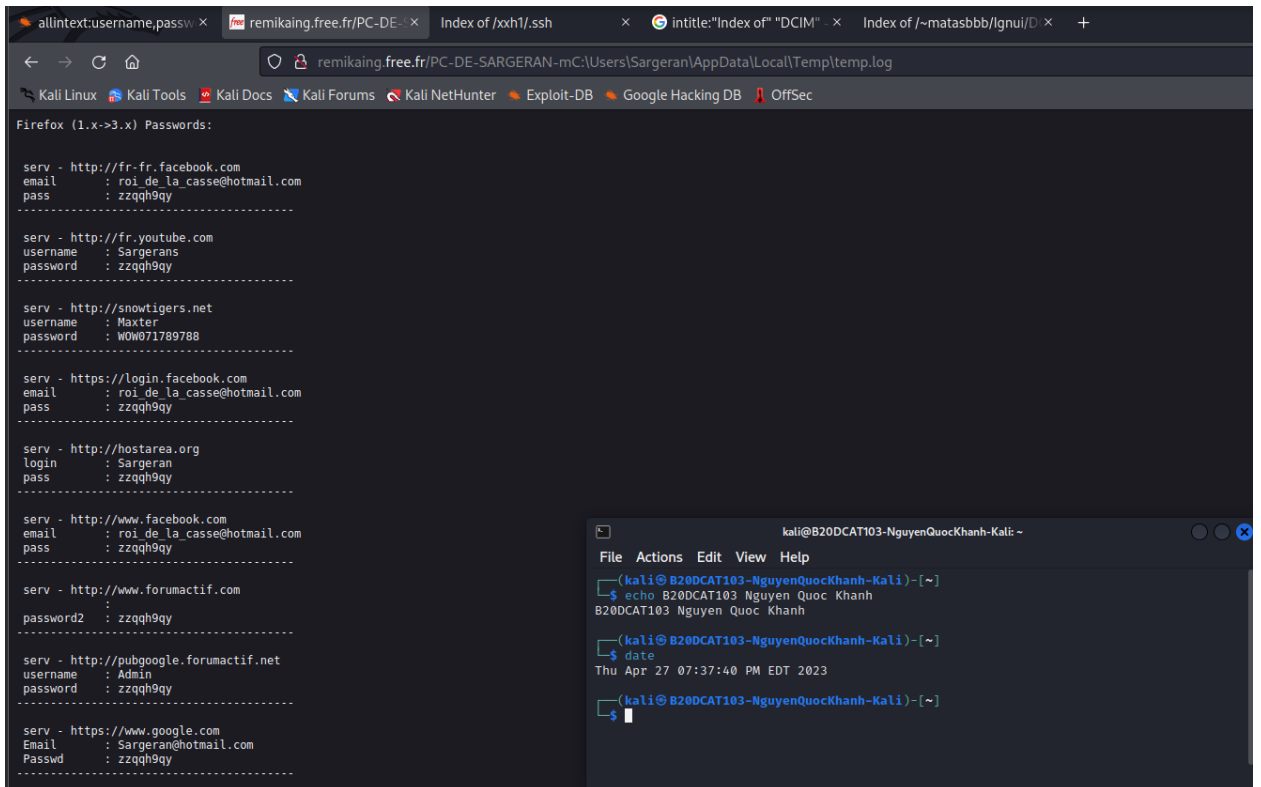
- Thử nghiệm câu lệnh tại <https://www.exploit-db.com/ghdb/6322>, kết quả trả về các thư mục và tập tin nhạy cảm có chứa khóa ssh:



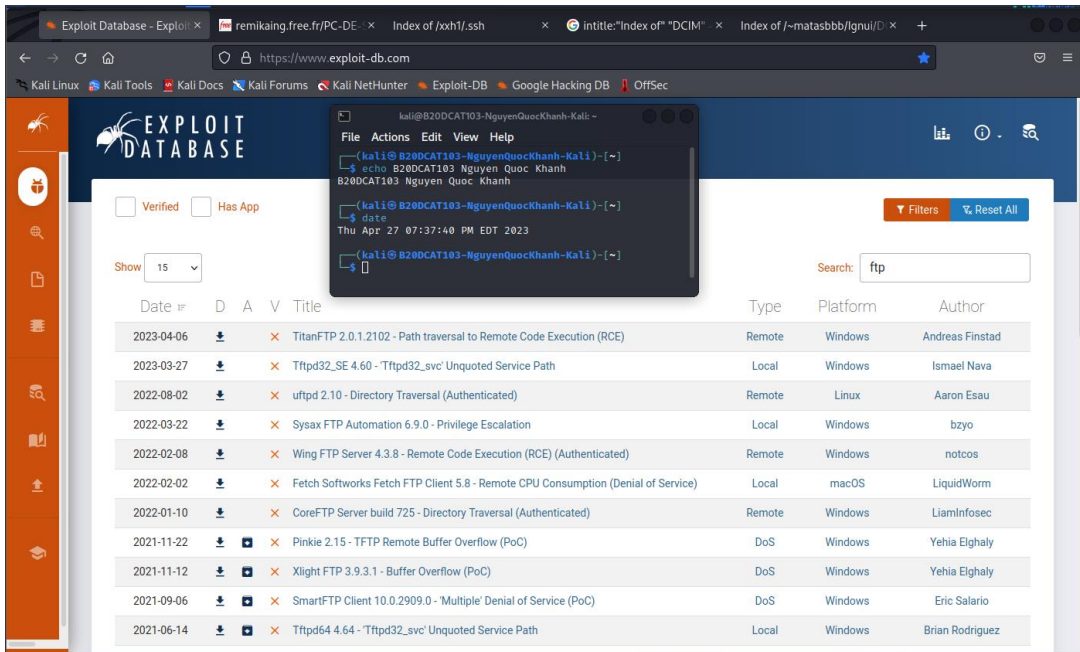
- Thử nghiệm lệnh tại [www.exploit-db.com/ghdb/6412](http://www.exploit-db.com/ghdb/6412):



- Tìm được log có tên người dùng và mật khẩu:

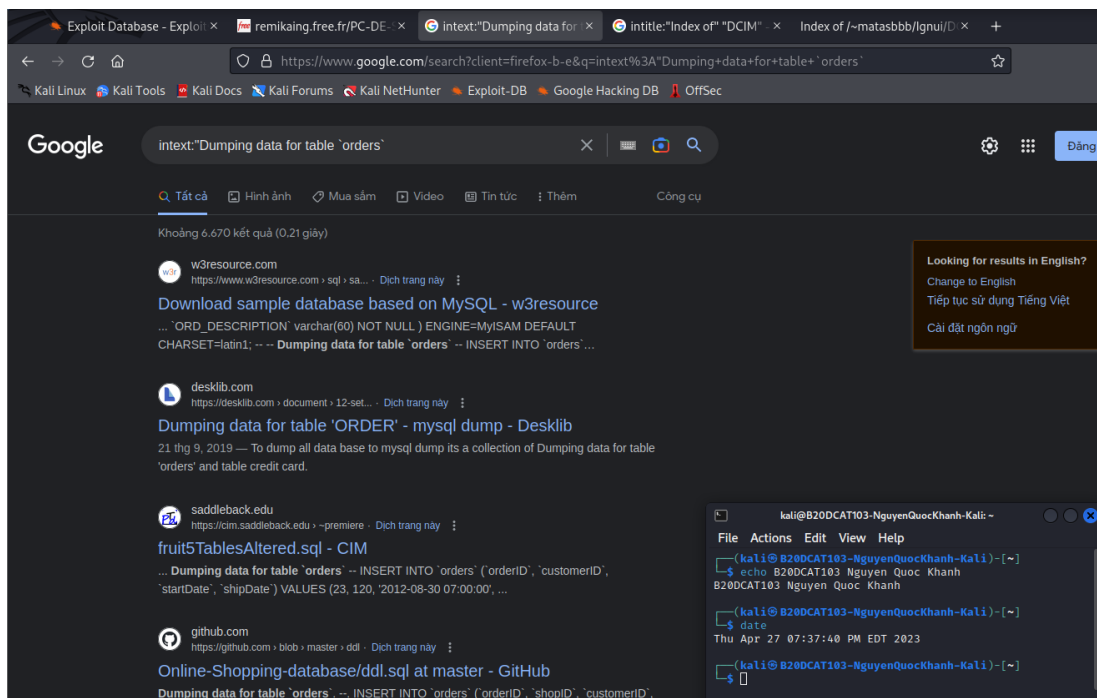


- Quay lại GHDB (www.exploit-db.com/google-hacking-database) và trong hộp văn bản Tìm kiếm nhanh ở bên phải, nhập FTP. Xuất hiện rất nhiều Google dorks liên quan đến Giao thức truyền tệp (FTP):

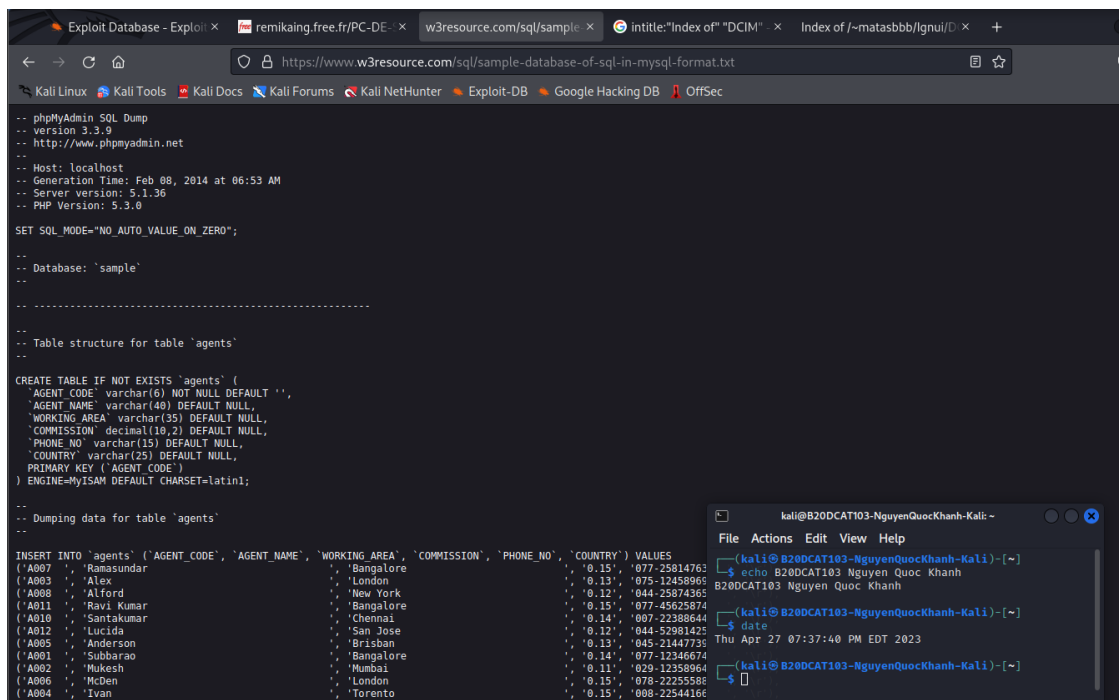


Thực hành tìm hiểu trên năm câu lệnh Google dork:

- 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:



```
-- phpMyAdmin SQL Dump
-- version 3.3.9
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Feb 08, 2014 at 06:53 AM
-- Server version: 5.1.36
-- PHP Version: 5.3.0

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

--
-- Database: 'sample'
--

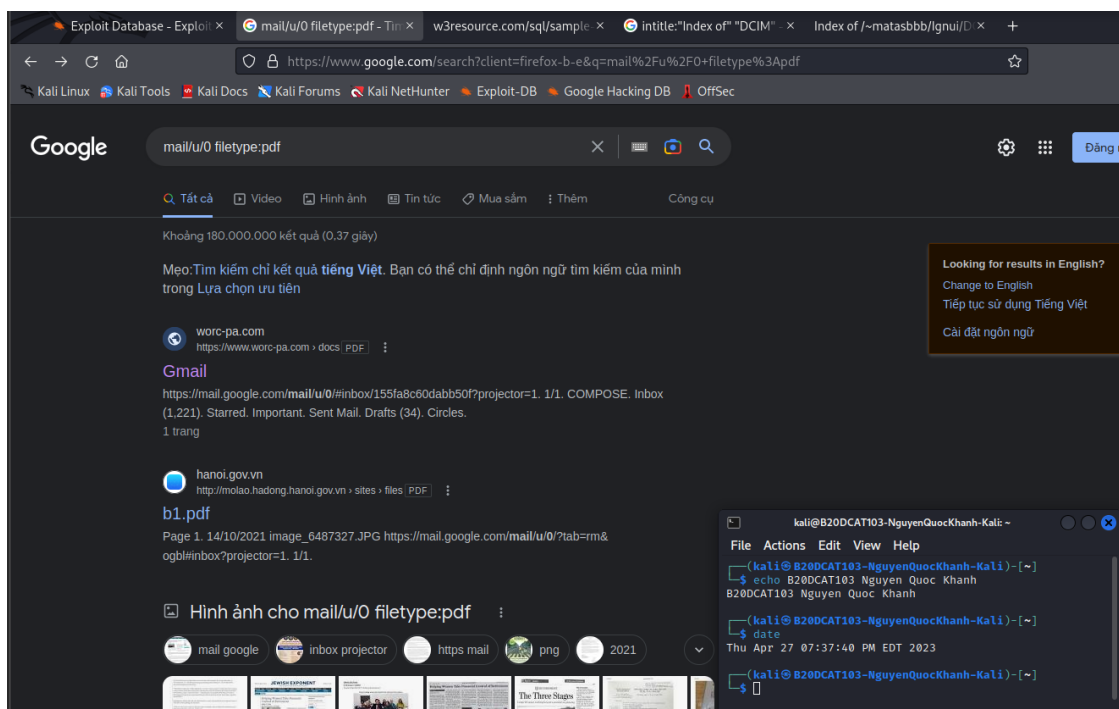
--
-- Table structure for table 'agents'
--

CREATE TABLE IF NOT EXISTS `agents` (
  `AGENT_CODE` varchar(6) NOT NULL DEFAULT '',
  `AGENT_NAME` varchar(40) DEFAULT NULL,
  `WORKING_AREA` varchar(35) DEFAULT NULL,
  `COMMISSION` decimal(10,2) DEFAULT NULL,
  `PHONE_NO` varchar(15) DEFAULT NULL,
  `COUNTRY` varchar(25) DEFAULT NULL,
  PRIMARY KEY (`AGENT_CODE`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;

--
-- Dumping data for table 'agents'
--

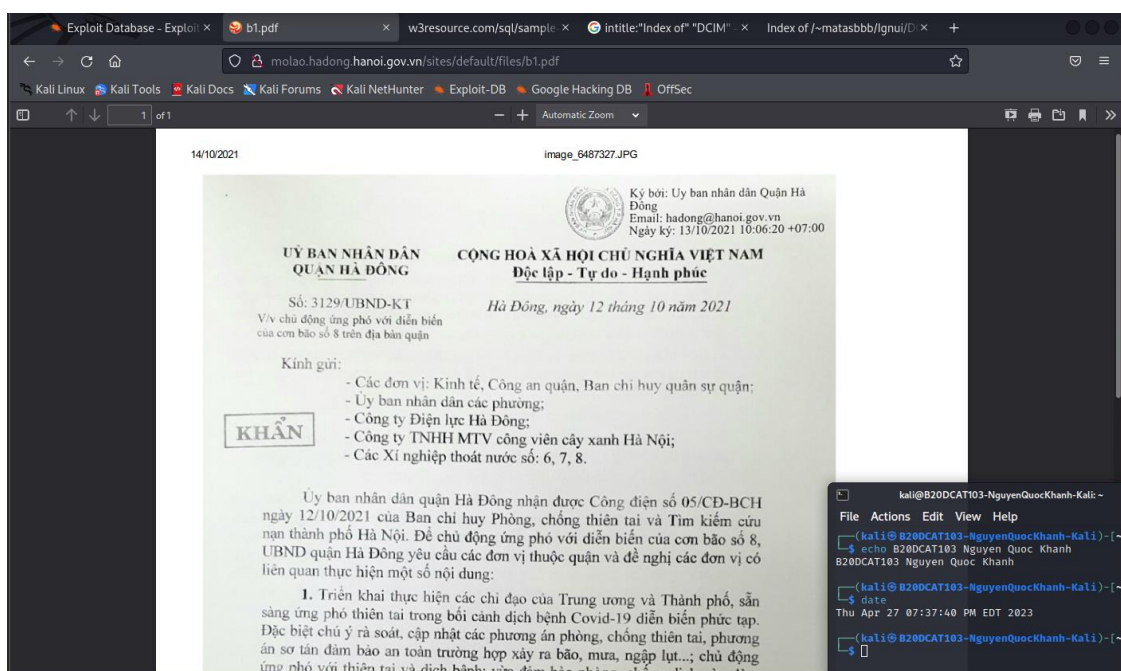
INSERT INTO `agents` (`AGENT_CODE`, `AGENT_NAME`, `WORKING_AREA`, `COMMISSION`, `PHONE_NO`, `COUNTRY`) VALUES
('A007', 'Ramasundar', 'Bangalore', '0.15', '077-25014763', 'India'),
('A003', 'Alex', 'London', '0.13', '075-12458965', 'UK'),
('A008', 'Alford', 'New York', '0.12', '044-25874365', 'USA'),
('A011', 'Ravi Kumar', 'Bangalore', '0.15', '077-45625874', 'India'),
('A010', 'Santakumar', 'Chennai', '0.14', '087-22388644', 'India'),
('A012', 'Lucida', 'San Jose', '0.12', '044-52981423', 'USA'),
('A005', 'Anderson', 'Brisban', '0.13', '045-21447739', 'Australia'),
('A001', 'Subbarao', 'Bangalore', '0.14', '077-12346674', 'India'),
('A002', 'Mukesh', 'Mumbai', '0.11', '029-12358964', 'India'),
('A006', 'McDen', 'London', '0.15', '078-22255588', 'UK'),
('A004', 'Ivan', 'Toronto', '0.15', '068-22544166', 'Canada');
```

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

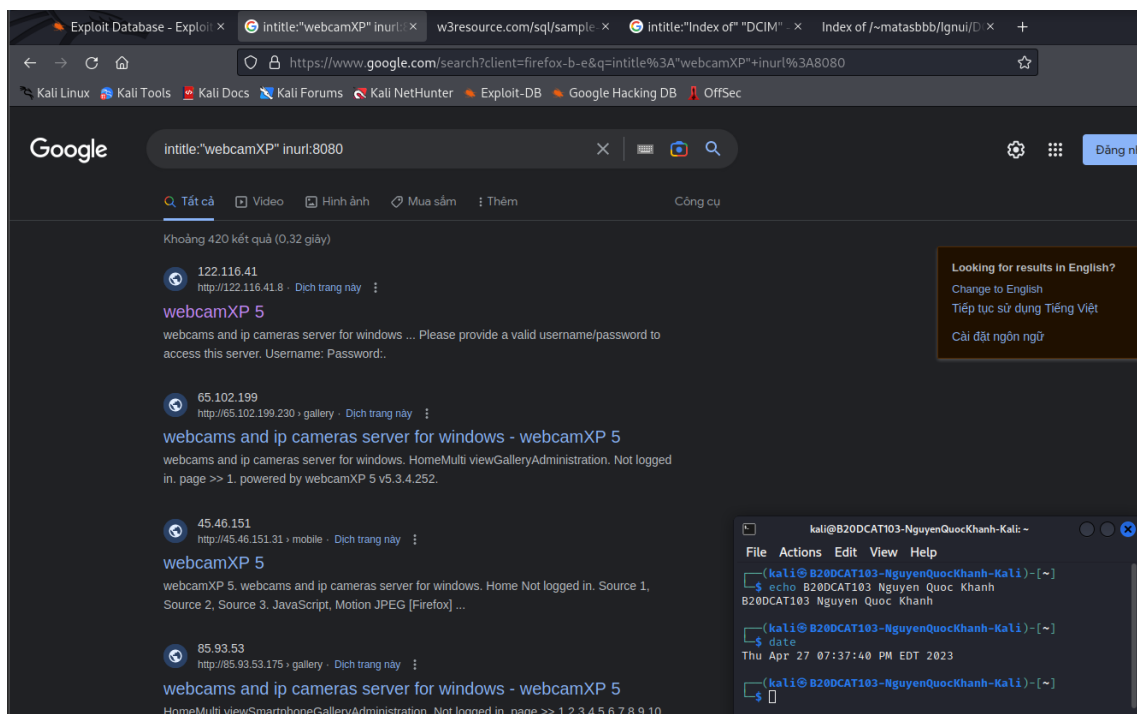




- Nhấp vào một liên kết và nhận được văn bản dưới đây:



- 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 để nhận biết:





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

