程式規格說明書

壹、 程式環境需求

OS	Ubuntu 20.04.2 LTS
nginx	nginx/1.18.0
php-fpm	php7.4-fpm
php	PHP 7.4.3
MySQL	MySQL Ver 8.0.26
Metasploit Framework	metasploit-4.20.0
Nmap	Nmap version 7.80
python3	Python 3.8.10

Python 套件	功能	版本
censys	使用 censys 引擎	2.0.0
shodan	使用 shodan 引擎	1.25.0
PyMySQL	python 連接 mysql	1.0.2
pymetasploit3	python 連接 metasploit	1.0.3

貳、 環境建置方法

一、 設定 HTTP 網頁

使用 : Nginx + php7.4-fpm
參考連結 : https://reurl.cc/lodezW

- Nginx

> sudo vim /etc/nginx/nginx.conf

```
user www-data;
worker_processes 4;
worker_cpu_affinity 0001 0010 0100 1000;
worker_rlimit_nofile 1024;
pid /run/nginx.pid;

events {
    use epoll;
    worker_connections 2048;
}

http {
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    keepalive_timeout 65;
    types_hash_max_size 2048;
    server_names_hash_bucket_size 128;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    client_header_buffer_size 2k;
    large_client_header_buffers 4 4k;
    open_file_cache max=102400 inactive=20s;

    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    gzip on;
    gzip_disable "msie6";

    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;
}
```

- Php-fpm

編輯內容如下：

```
[www]
user = www-data
group = www-data

listen = 127.0.0.1:9000
listen.backlog = 65535
listen.owner = www-data
listen.group = www-data

request_terminate_timeout = 600s

pm = dynamic
pm.max_children = 5
pm.start_servers = 2
pm.min_spare_servers = 1
pm.max_spare_servers = 3
```

二、 設定 Https 網頁

- SSL 憑證

使用 Let’s encrtpy！

參考連結 ： https://caloskao.org/ubuntu-use-certbot-to-automatically-update-lets-encrypt-certificate-authority/

```
                    # 安裝軟體管理套件
[Calos@ubuntu-16.04] $ sudo apt-get install -y software-properties-common

                    # 加入 certbot ppa repository，並透過 apt-get update 取得套件資訊
[Calos@ubuntu-16.04] $ sudo add-apt-repository ppa:certbot/certbot
[Calos@ubuntu-16.04] $ sudo apt-get update

                    # 安裝 certbot for apache
[Calos@ubuntu-16.04] $ sudo apt-get install -y python-certbot-apache

                    # 開始進行 Apache 的憑證安裝
[Calos@ubuntu-16.04] $ sudo certbot --apache
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache

Which names would you like to activate HTTPS for?
-------------------------------------------------------------------------------
1: caloskao.org
2: blog.caloskao.org
3: www.caloskao.org
4: example.caloskao.org
-------------------------------------------------------------------------------
Select the appropriate numbers separated by commas and/or spaces, or leave input

blank to select all options shown (Enter 'c' to cancel):
```

```
Obtaining a new certificate
Performing the following challenges:
tls-sni-01 challenge caloskao.org
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-available/caloskao.org-le-ssl.conf
Deploying Certificate for caloskao.org to VirtualHost /etc/apache2/sites-available/caloskao.org-le-ssl.conf
Enabling available site: /etc/apache2/sites-available/caloskao.org-le-ssl.conf
```

```
Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
-------------------------------------------------------------------------------
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```

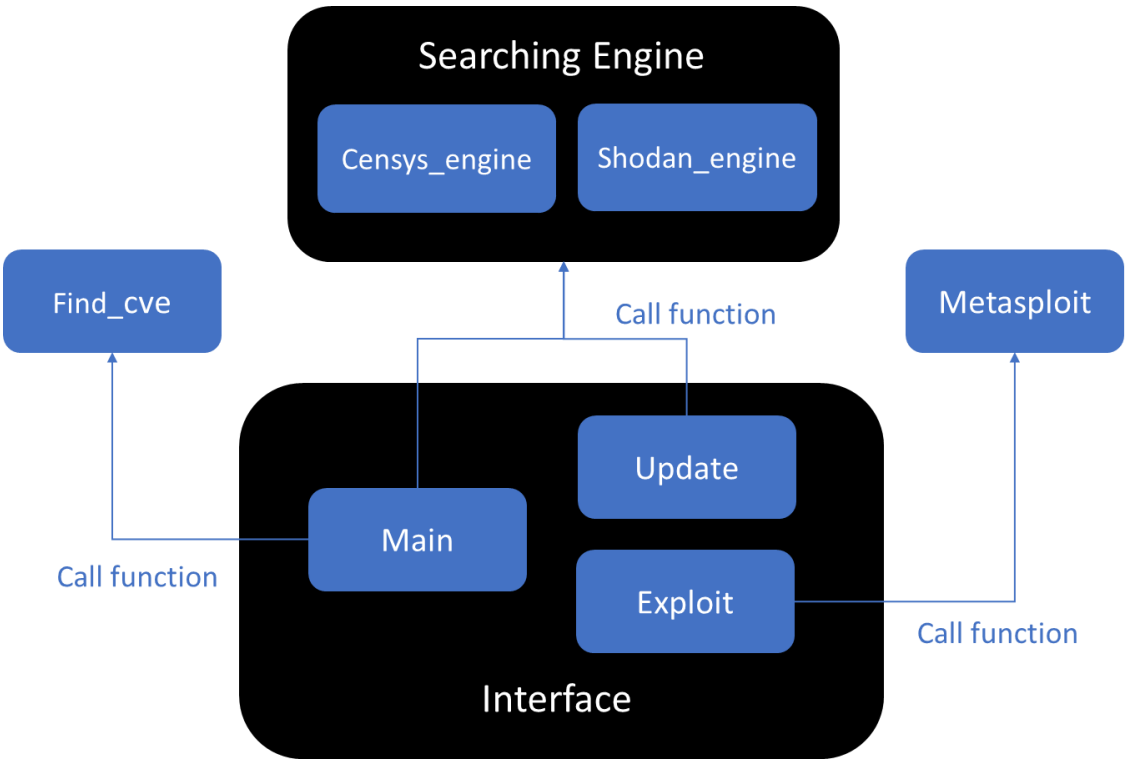
```
---------------------------------------------------------------------------
Congratulations! You have successfully enabled https://caloskao.org

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=caloskao.org
---------------------------------------------------------------------------

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/caloskao.org/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/caloskao.org/privkey.pem
   Your cert will expire on 2018-03-22. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

參、 程式架構

資料夾名稱	功能
ccu_proj_manyPorts	主要程式資料夾
ccu_proj_manyPorts/api/	api 資料夾
ccu_proj_manyPorts/www/	網頁資料夾

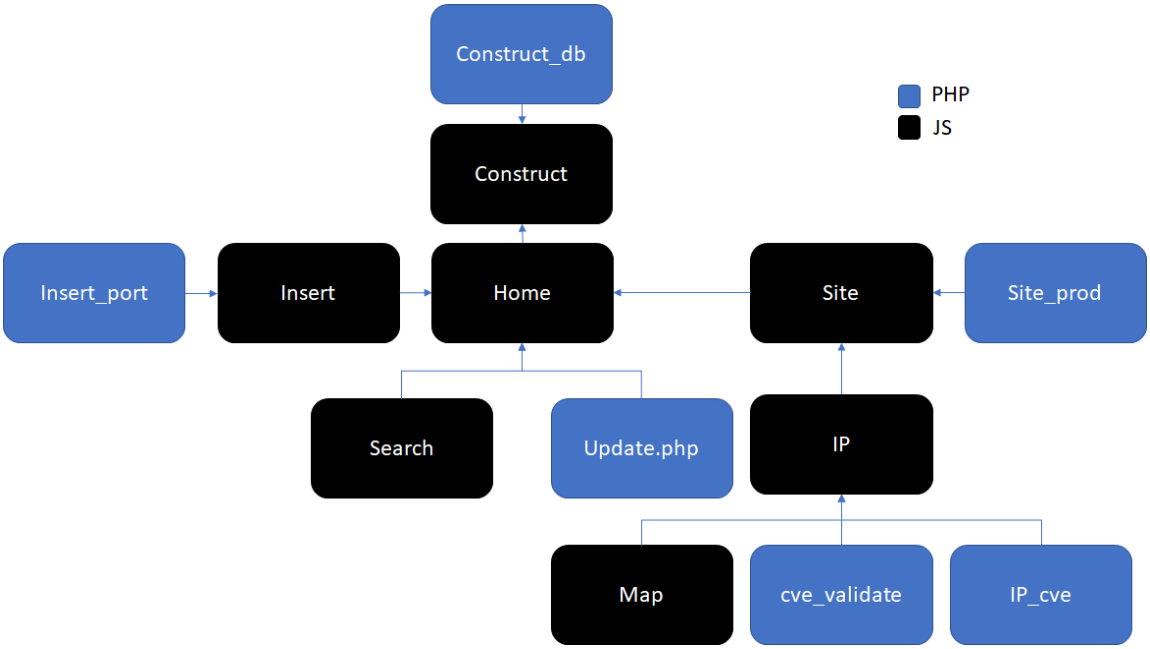
肆、 程式內容說明

一、 api 資料夾



檔案名稱	功能
main.py	建立資料庫的接口
cens.py	執行 censys api 搜尋指定網域
shod.py	執行 shodan api 搜尋指定網域
find_cve.py	尋找潛藏 cve 與所有資訊存入資料庫
exploit.py	驗證弱點
update.py	更新資料庫的資訊，比如 cve 資訊、port、os、型號

二、 網頁資料夾



1. Js

程式名稱	功能
home.js	使用圖表讓使用者快速了解其區域下的物連網設備
site.js	判別有無區域對應表，以不同方式呈現
ip.js	地圖化呈現此 ip 的所在位置，呈現該 ip 的資訊,比如 OS、種類、型號、潛藏 CVE、cve 驗證接口
map.js	畫 ip 位址對應之地圖
insert.js	手動插入物連網設備資訊的接口
search.js	查找符合關鍵字的物連網設備
construct.js	建立給定區域的物聯網設備資料庫

2. php

程式名稱	功能
construct_db.php	呼叫後端，建立資料庫
cve_validate.php	呼叫後端，進行 cve 驗證
insert_post.php	對資料庫新增設備
ip_cve.php	查尋某 ip 的潛藏 cve
site_prod.php	查詢資料庫中某種類 ip

update.php	更新該區域資料庫資訊

伍、 操作方式

一、 後端

1. 資料庫資訊

(1) Database 名稱 : iot

(2) 目前存取 tables,e.g,ip_1、ip_2...

(3) ip_1、cve_1、port_1 : 放中正大學(140.123.0.0/16)資料

(4) table 種類

Ip table

欄位名稱	欄位代號	定義	型態
網域	ip	設備之 ip 位址	char(20)
作業系統	os	設備之作業系統	char(50)
產品型號	product_model	設備之型號	char(50)
產品種類	device_type	設備之種類	char(50)

Port table

欄位名稱	欄位代號	定義	型態
網域	port_ip	設備 ip 位址	char(20)
開放阜	port	代表 ip 有此 open port	int

Cve table

欄位名稱	欄位代號	定義	型態
網域	cve_ip	ip 位址	char(20)
弱點編號	cve_id	cve 編號，代表 cve_ip 有此潛藏 cve	char(50)
弱點嚴重程度	cvss	代表此 cve 的嚴重程度	float
弱點介紹	description	關於此 cve 介紹	text

```
a407410040@IBM1:/var/www/html/ccu_proj_manyPorts/api$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 953
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)
```

```
mysql> use iot
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

```
mysql> show tables
    -> ;
+---------------+
| Tables_in_iot |
+---------------+
| cve_1         |
| cve_2         |
| cve_3         |
| cve_4         |
| ip_1          |
| ip_2          |
| ip_3          |
| ip_4          |
| port_1        |
| port_2        |
| port_3        |
| port_4        |
+---------------+
12 rows in set (0.01 sec)
```

2. 資料庫設定

MySQL環境設定

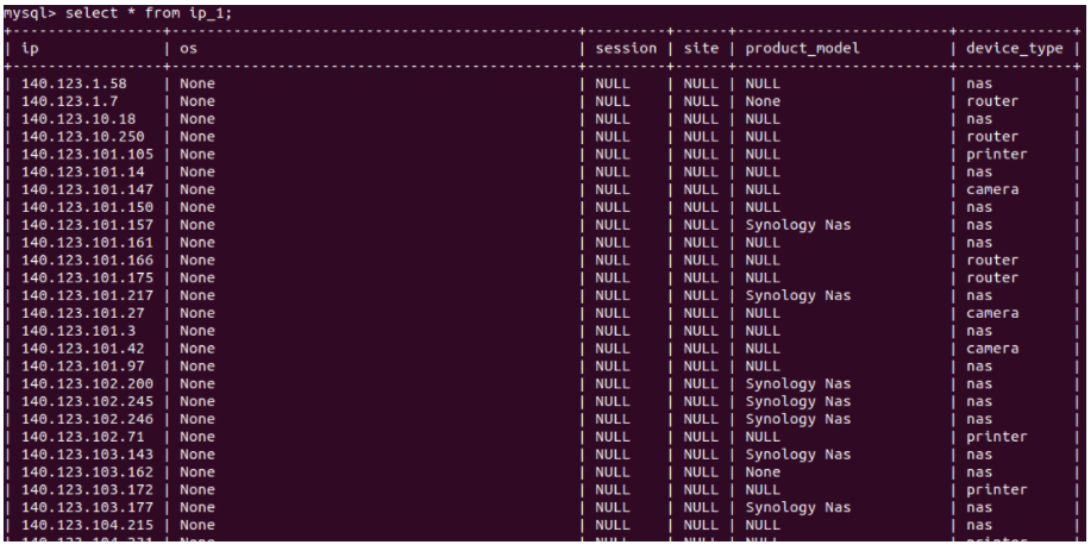
```
> sudo apt-get install mysql-server
> sudo apt install mysql-client
> sudo apt install libmysqlclient-dev
> mysql -u root -p // pwd : a407410040
```

建立Database

```
> use iot

> create table ip(
    ip char(20),
    os char(50),
    site char(20),
    session text,
    product_model char(50),
    device_type char(50),
    primary key (ip)
);

> create table cvee(
    cvee_ip char(20),
    cvee_id char(50),
    description text,
    cvss float,
    primary key (cvee_id),
    foreign key (cvee_ip) references ip(ip) on delete cascade on update cascade
);

> create table port(
    port_ip char(20),
    port int,
    foreign key (port_ip) references ip(ip) on delete cascade on update cascade
);
```

功能說明

```
select * from ip;
```



```
mysql> select * from ip_1;
+----------------+---------------------------------------------+---------+------+----------------------+-------------+
| ip             | os                                          | session | site | product_model        | device_type |
+----------------+---------------------------------------------+---------+------+----------------------+-------------+
| 140.123.1.58   | None                                        | NULL    | NULL | NULL                 | nas         |
| 140.123.1.7    | None                                        | NULL    | NULL | None                 | router      |
| 140.123.10.18  | None                                        | NULL    | NULL | NULL                 | nas         |
| 140.123.10.250 | None                                        | NULL    | NULL | NULL                 | router      |
| 140.123.101.105 | None                                       | NULL    | NULL | NULL                 | printer     |
| 140.123.101.14 | None                                        | NULL    | NULL | NULL                 | nas         |
| 140.123.101.147 | None                                       | NULL    | NULL | NULL                 | camera      |
| 140.123.101.150 | None                                       | NULL    | NULL | NULL                 | nas         |
| 140.123.101.157 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.101.161 | None                                       | NULL    | NULL | NULL                 | nas         |
| 140.123.101.166 | None                                       | NULL    | NULL | NULL                 | router      |
| 140.123.101.175 | None                                       | NULL    | NULL | NULL                 | router      |
| 140.123.101.217 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.101.27 | None                                        | NULL    | NULL | NULL                 | camera      |
| 140.123.101.3  | None                                        | NULL    | NULL | NULL                 | nas         |
| 140.123.101.42 | None                                        | NULL    | NULL | NULL                 | camera      |
| 140.123.101.97 | None                                        | NULL    | NULL | NULL                 | nas         |
| 140.123.102.200 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.102.245 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.102.246 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.102.71 | None                                        | NULL    | NULL | NULL                 | printer     |
| 140.123.103.143 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.103.162 | None                                       | NULL    | NULL | None                 | nas         |
| 140.123.103.172 | None                                       | NULL    | NULL | NULL                 | printer     |
| 140.123.103.177 | None                                       | NULL    | NULL | Synology Nas         | nas         |
| 140.123.104.215 | None                                       | NULL    | NULL | NULL                 | nas         |
```

```
insert into ip (ip,os,site) values ('256.256.256.258','windowXP','中文系');
```

```
mysql> insert into ip_1 (ip , os) values ('111.111.111.111' , 'linux');
Query OK, 1 row affected (0.01 sec)

mysql> select * from ip_1;
+-----------------+-----------------------------------------------+---------+------+-----------------------+-------------+
| ip              | os                                            | session | site | product_model         | device_type |
+-----------------+-----------------------------------------------+---------+------+-----------------------+-------------+
| 111.111.111.111 | linux                                         | NULL    | NULL | NULL                  | NULL        |
| 140.123.1.58    | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.1.7     | None                                          | NULL    | NULL | None                  | router      |
| 140.123.10.18   | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.10.250  | None                                          | NULL    | NULL | NULL                  | router      |
| 140.123.101.105 | None                                          | NULL    | NULL | NULL                  | printer     |
| 140.123.101.14  | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.147 | None                                          | NULL    | NULL | NULL                  | camera      |
| 140.123.101.150 | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.157 | None                                          | NULL    | NULL | Synology Nas          | nas         |
| 140.123.101.161 | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.166 | None                                          | NULL    | NULL | NULL                  | router      |
```

```
delete from ip where ip like '256.256.256.258';
delete from ip_1 where ip like '222.222.222.222';
```

```
mysql> delete from ip_1 where ip like '111.111.111.111';
Query OK, 1 row affected (0.00 sec)

mysql> select * from ip_1;
+-----------------+-----------------------------------------------+---------+------+-----------------------+-------------+
| ip              | os                                            | session | site | product_model         | device_type |
+-----------------+-----------------------------------------------+---------+------+-----------------------+-------------+
| 140.123.1.58    | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.1.7     | None                                          | NULL    | NULL | None                  | router      |
| 140.123.10.18   | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.10.250  | None                                          | NULL    | NULL | NULL                  | router      |
| 140.123.101.105 | None                                          | NULL    | NULL | NULL                  | printer     |
| 140.123.101.14  | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.147 | None                                          | NULL    | NULL | NULL                  | camera      |
| 140.123.101.150 | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.157 | None                                          | NULL    | NULL | Synology Nas          | nas         |
| 140.123.101.161 | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.166 | None                                          | NULL    | NULL | NULL                  | router      |
| 140.123.101.175 | None                                          | NULL    | NULL | NULL                  | router      |
| 140.123.101.217 | None                                          | NULL    | NULL | Synology Nas          | nas         |
| 140.123.101.27  | None                                          | NULL    | NULL | NULL                  | camera      |
| 140.123.101.3   | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.101.42  | None                                          | NULL    | NULL | NULL                  | camera      |
| 140.123.101.97  | None                                          | NULL    | NULL | NULL                  | nas         |
| 140.123.102.200 | None                                          | NULL    | NULL | Synology Nas          | nas         |
| 140.123.102.245 | None                                          | NULL    | NULL | Synology Nas          | nas         |
```

3. 資料庫建立

步驟:

(1) <cat table.txt>，確認即將建立之資料庫 id, e.g, table.txt 存 3, 建立資料庫後, 資料放在 ip_3、port_3、cve_3

(2) 執行 python3 main.py --ip xxxxx

(3) 進入 mysql 確認是否建立成功

e.g, 建立學校網段(140.123.230.32)資料庫

```
a407410040@IBM1:/var/www/html/ccu_proj_manyPorts/api$ cat table.txt
5a407410040@IBM1:/var/www/html/ccu_proj_manyPorts/api$
```

```
root@IBM1:/var/www/html/iotScanner2021/api# python3 main.py --ip 140.123.40.5/24
```

```
mysql> select * from ip_3;
+-----------------+------+---------+------+---------------+-------------+
| ip              | os   | session | site | product_model | device_type |
+-----------------+------+---------+------+---------------+-------------+
| 140.123.40.116 | None | NULL    | NULL | None          | router      |
| 140.123.40.138 | None | NULL    | NULL | None          | printer     |
| 140.123.40.204 | None | NULL    | NULL | None          | printer     |
| 140.123.40.206 | None | NULL    | NULL | None          | nas         |
| 140.123.40.207 | None | NULL    | NULL | None          | nas         |
| 140.123.40.246 | None | NULL    | NULL | None          | router      |
| 140.123.40.249 | None | NULL    | NULL | None          | router      |
+-----------------+------+---------+------+---------------+-------------+
7 rows in set (0.00 sec)

mysql>
```

4. 資料庫更新

步驟

(1) 選定欲更新的資料庫，與此資料庫之 ip 區段
(2) 執行 python3 update.py --ip xxxx --table_id xxxxx

```
root@IBM1:/var/www/html/iotScanner2021/api# python3 update.py --ip 140.123.40.0/24 --table_id 3
```

```
[{'ip': '140.123.40.116', 'os': 'None', 'session': None, 'site': None, 'product_model': 'None', 'device_type': 'router'}, {'ip': '140.123.40.138', 'os': 'None
del': 'None', 'device_type': 'printer'}, {'ip': '140.123.40.204', 'os': 'None', 'session': None, 'site': None, 'product_model': 'None', 'device_type': 'printe
session': None, 'site': None, 'product_model': 'None', 'device_type': 'nas'}, {'ip': '140.123.40.207', 'os': 'None', 'session': None, 'site': None, 'product_
'140.123.40.246', 'os': 'None', 'session': None, 'site': None, 'product_model': 'None', 'device_type': 'router'}, {'ip': '140.123.40.249', 'os': 'None', 'sess
one', 'device_type': 'router'}]
ip:140.123.40.116
port:['80', '139', '443', '445', '3261', '5000', '5001', '5357', '5566']
device_type:
os:
product:linux_kernel
vendor:linux
cve:['CVE-2017-7494', 'CVE-2020-10745', 'CVE-2017-14746', 'CVE-2017-11103', 'CVE-2018-10858', 'CVE-2018-10858', 'CVE-2019-14870', 'CVE-2019-14870', 'CVE-2017
CVE-2021-20277', 'CVE-2021-20277', 'CVE-2020-27840', 'CVE-2020-10704', 'CVE-2017-15275', 'CVE-2021-20254', 'CVE-2019-14833', 'CVE-2017-12163', 'CVE-2018-1685
018-16851', 'CVE-2020-14383', 'CVE-2020-14318', 'CVE-2020-10760', 'CVE-2020-10730', 'CVE-2019-14847', 'CVE-2018-16851', 'CVE-2018-16841', 'CVE-2018-14629', '
4861', 'CVE-2021-20277', 'CVE-2017-7494', 'CVE-2020-10745', 'CVE-2017-14746', 'CVE-2017-11103', 'CVE-2018-10858', 'CVE-2018-10858', 'CVE-2019-14870', 'CVE-20
 'CVE-2020-10704', 'CVE-2021-20277', 'CVE-2021-20277', 'CVE-2020-27840', 'CVE-2020-10704', 'CVE-2017-15275', 'CVE-2021-20254', 'CVE-2019-14833', 'CVE-2017-12
-2018-14629', 'CVE-2018-16851', 'CVE-2020-14383', 'CVE-2020-14318', 'CVE-2020-10760', 'CVE-2020-10730', 'CVE-2019-14847', 'CVE-2018-16851', 'CVE-2018-16841',
-14861', 'CVE-2019-14861', 'CVE-2021-20277']
ip:140.123.40.138
```

5. 驗證弱點

步驟:

(1) 輸入<msfconsole>，開啟 msfconsole 後台
(2) 設定 msfconsole 帳密
(3) 選擇欲驗證的資料庫執行，<python3 exploit.py --table_id xxx>

Note : 後台需持續開啟

範例:

步驟 1

```
a407410040@IBM1:/var/www/html/ccu_proj_manyPorts/api$ msfconsole
```

步驟 2

```
msf6 >
msf6 > load msgrpc Pass=a407410040
[*] MSGRPC Service:  127.0.0.1:55552
[*] MSGRPC Username: msf
[*] MSGRPC Password: a407410040
[*] Successfully loaded plugin: msgrpc
```

步驟 3

```
a407410040@IBM1:/var/www/html/ccu_proj_manyPorts/api$ python3 exploit.py --table_id 1
```

結果

```
root@IBM1:/var/www/html/ccu_proj_manyPorts/api# python3 exploit.py --table_id 3
140.112.10.118 80 cve_1
no corresponding modules
140.112.10.118 80 cve_2
no corresponding modules
140.112.10.125 443 cve_1
no corresponding modules
```

輸出結果	介紹
No corresponding modules	metasploit 無此 modules
Sesssion not found	有 modules，但測試後無此弱點
Sesssion is found	有 modules，且測試後發現此弱點

6. 自動更新

設定 crontab 排程，每日自動更新。

crontab

```
sudo crontab -e //進入編輯介面
```

加入排程指令

```
# m d dom mon dow command
59 23 * * * php /var/www/html/ccu_proj_manyPorts/www/update.php
```

二、 前端

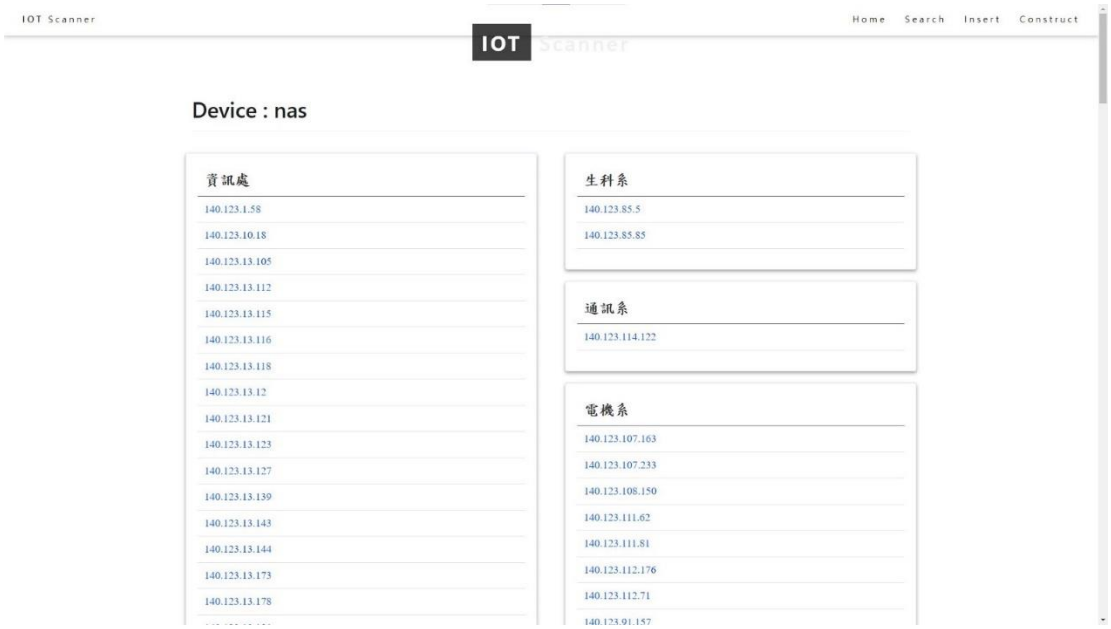
1. 資料庫建立

(1) 使用者點選主頁的 construct 鍵，進入 construct 網頁

(2) 輸入一區域，按下 submit
(3) 系統開始掃描該區域之 IoT 設備
(4) 系統將 IoT 設備資訊加入資料庫中
(5) 使用者可以可以在網頁上看到輸出結果

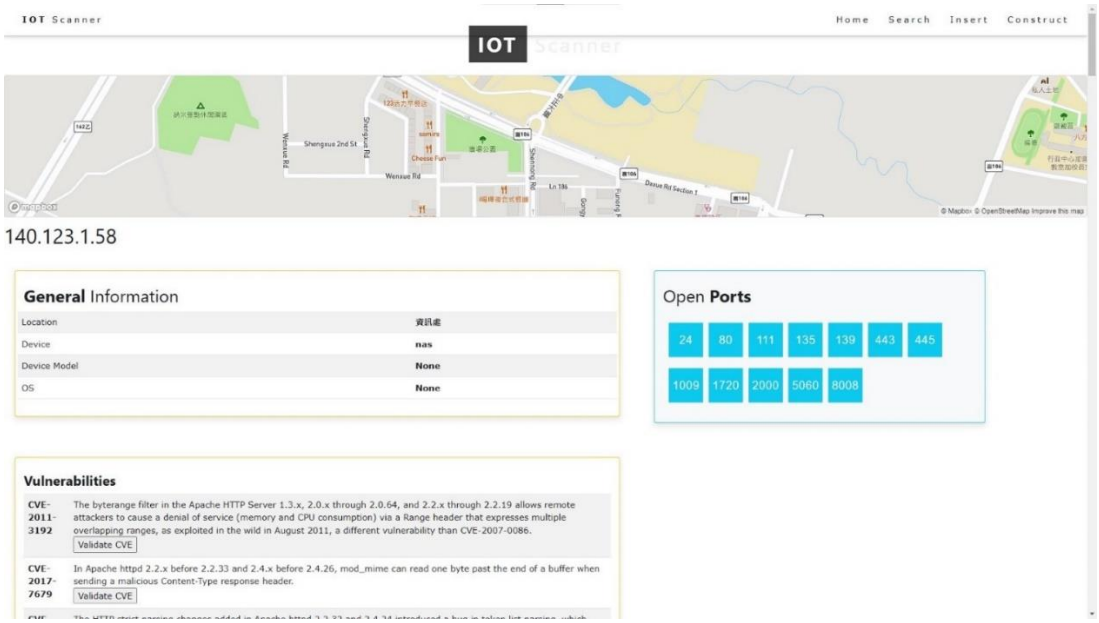
2. 設備對應各單位

(1) 使用者點選主頁的 site 網頁
(2) 系統判別是否有單位對應表
(3) 若有，將各設備對應到不同的單位
(4) 在頁面呈現不同設備之單位



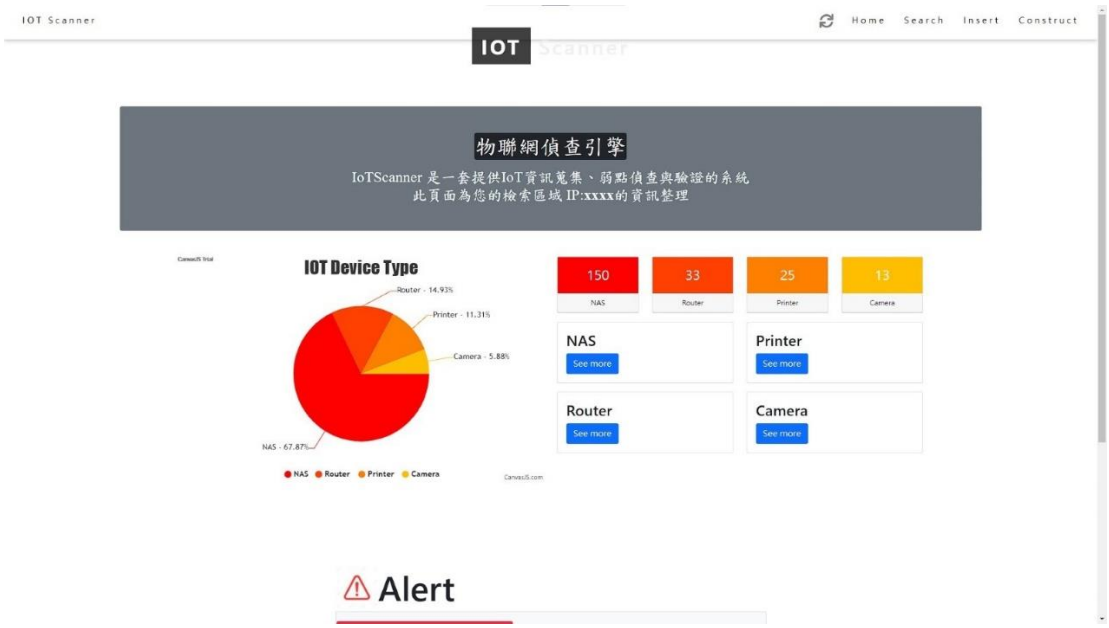
3. IP 資訊呈現

(1) 使用者點選主頁的 site 網頁
(2) 在 site 網頁中選擇 IP，點擊進入單一 IP 資訊頁面
(3) 顯示 IP 資訊，比如 location、os、型號、種類、port、cve



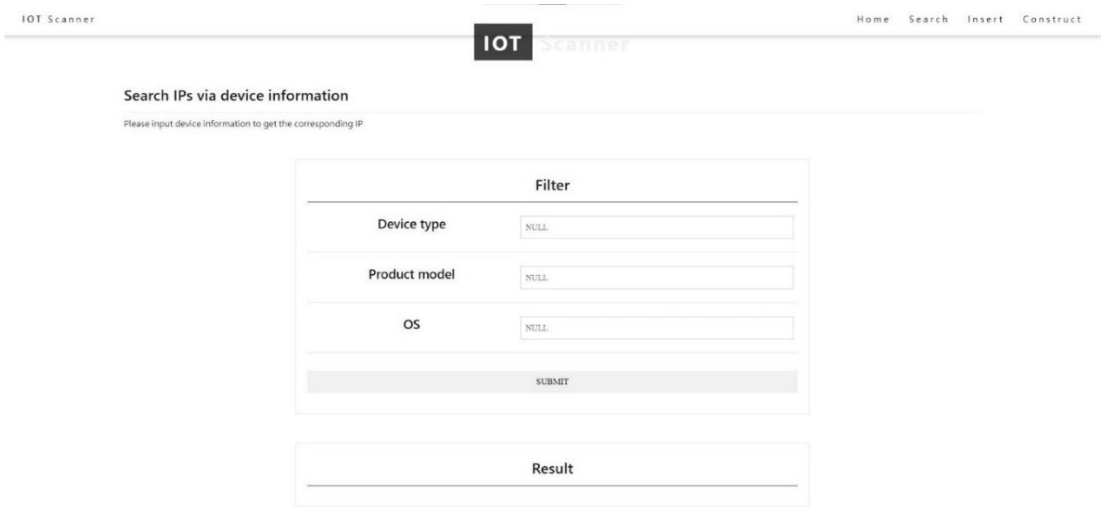
4. 資料庫更新

(1) 使用者點選主頁更新鍵
(2) 開始資料更新且存入資料庫



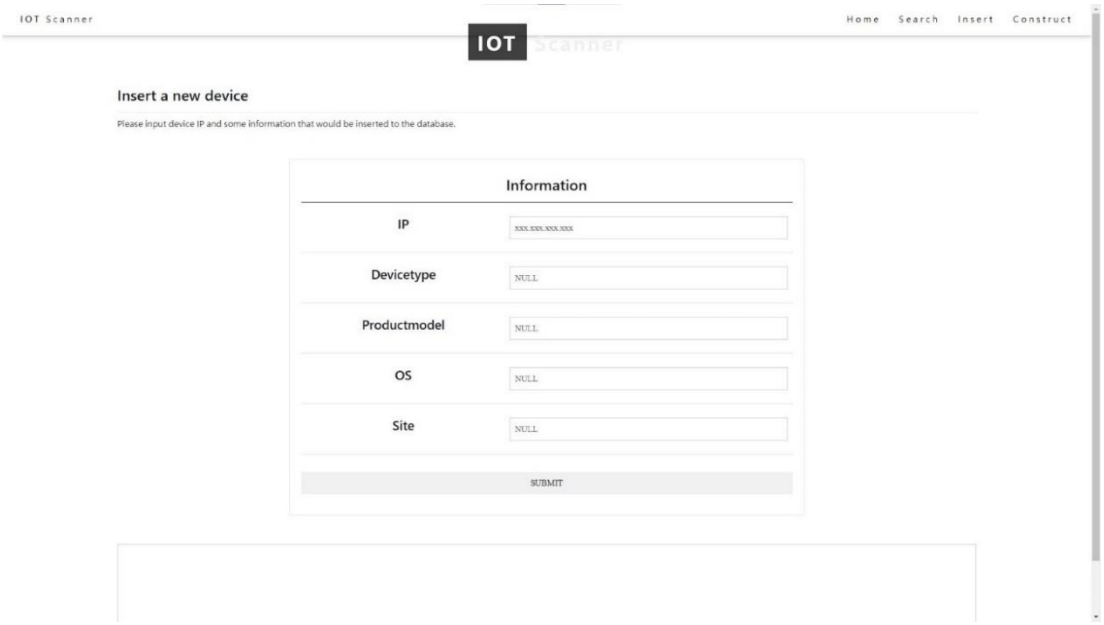
5. 查詢功能

(1) 使用者點選主頁的 search 鍵，進入 search 網頁
(2) 輸入欲查詢之設備關鍵字(種類、型號、os)
(3) 系統判別輸入是否合法
(4) 系統在資料庫中搜尋福符合關鍵字之 IP
(5) 並輸出至 search 網頁上



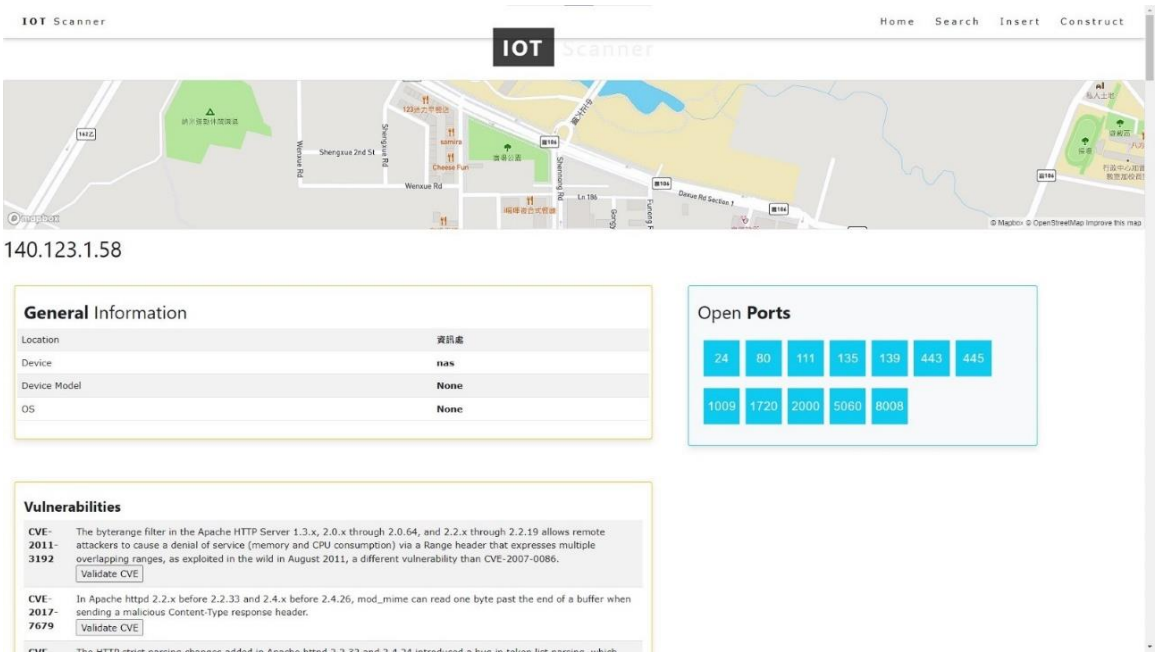
6. 手動匯入設備

(1) 點擊首頁上方 Insert 鍵，進入 Insert 頁面
(2) 輸入 IP 及設備基本資料，點擊 submit 加進資料庫
(3) 新的設備資料儲存到資料庫



7. 漏洞驗證

(1) 後端開啟驗證介面(msfconsole)
(2) 使用者進入欲測試的 IP 頁面按下 Validate CVE，開始驗證
(3) 系統開始驗證，若驗證到，可在驗證介面(msfconsole)輸入指令，若無驗證到，則無輸出
(4) 網頁回傳一文件，若驗證到，則文件輸出 session open，否則，輸出 no session



陸、 Password

Censys	API ID : 558d0b15-07a5-47a4-b68f-b0530181f791 Secret : YwgekK1zvhvmn2rjRmQPFblsKNIMlFwC
	API ID : aabc85e8-b6b9-4692-921a-ed81d1b0a8fc Secret : 66QsgUIAnBviFrFSPt8jMWd99aWbwtiQ
	API ID : 85dd7142-bf92-482a-814c-e5991afbb620 Secret : rPbYeWlMfqkewmOO6RRbqHCsg3x8adFg
Shodan	API ID : 839CrW4f3Omc9wYO9aMWeRq0Go4rEPfN
MySQL	$severname = "localhost"; $username = "root"; $password = "a407410040"; $database = "iot"; $port = 3306;
Metasploit	password : a407410040
SSH key	password : a407410044