

PSP0201

Week 5

Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 16 - [Scripting] Help! Where is Santa?

Tool used: kali Linux, Firefox

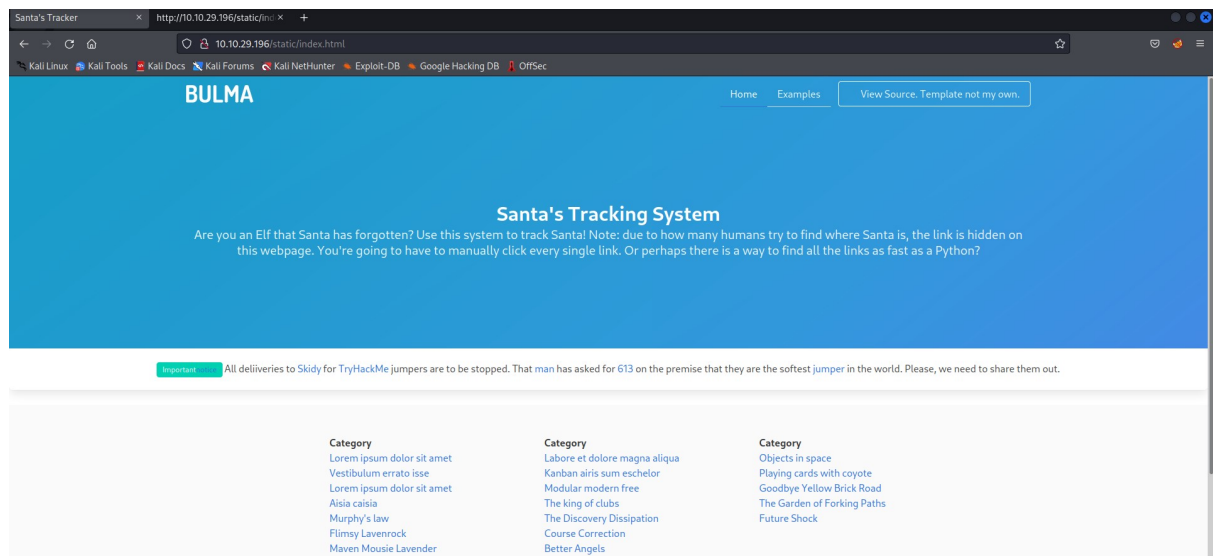
Solution/Walkthrough:

Q1.

```
| ssh-hostkey:
|   2048 31:4e:6f:1b:9b:4d:a6:9f:34:f0:ca:3e:96:31:a6:9e (RSA)
|   256 60:5d:1b:59:24:8b:b8:7a:5f:1c:75:55:5f:bf:e0:83 (ECDSA)
|_  256 05:08:d8:66:d1:04:cf:91:8c:6a:56:55:df:07:a4:d6 (ED25519)
80/tcp open  http      uvicorn
|_ http-title: Santa's Tracker
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     date: Tue, 12 Jul 2022 03:25:06 GMT
|     server: uvicorn
|     content-length: 22
|     content-type: application/json
|     {"detail": "Not Found"}
|   GetRequest:
|     HTTP/1.1 200 OK
|     date: Tue, 12 Jul 2022 03:24:58 GMT
|     server: uvicorn
|     content-type: text/html; charset=utf-8
|     content-length: 7014
|     last-modified: Tue, 29 Dec 2020 00:35:06 GMT
|     etag: fad18236c6876faf561b8ae1bf30c41e
```

By using nmap, the port number can be found.

Q2.



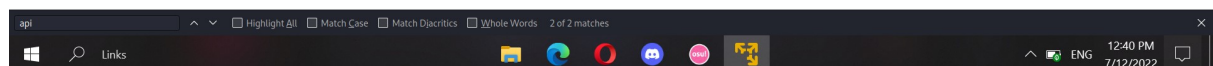
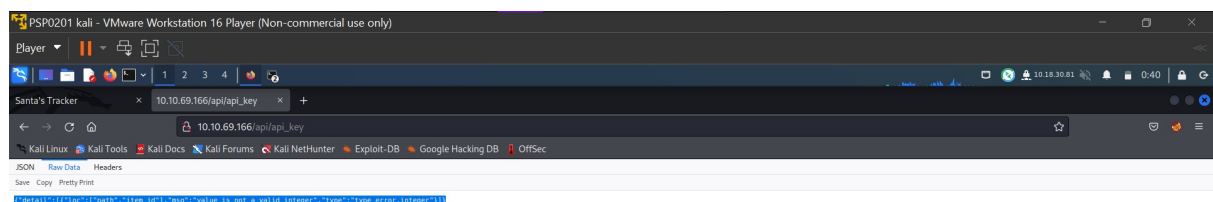
Top left of the site is the name of the template of the site.

Q3.

```
>  
<li><a href="#">Labore et dolore magna aliqua</a></li>  
<li><a href="#">Kanban airis sum eschelor</a></li>  
<li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>  
<li><a href="#">The king of clubs</a></li>  
<li><a href="#">The Discovery Dissipation</a></li>  
<li><a href="#">Course Correction</a></li>  
<li><a href="#">Better Angels</a></li>  
.
```

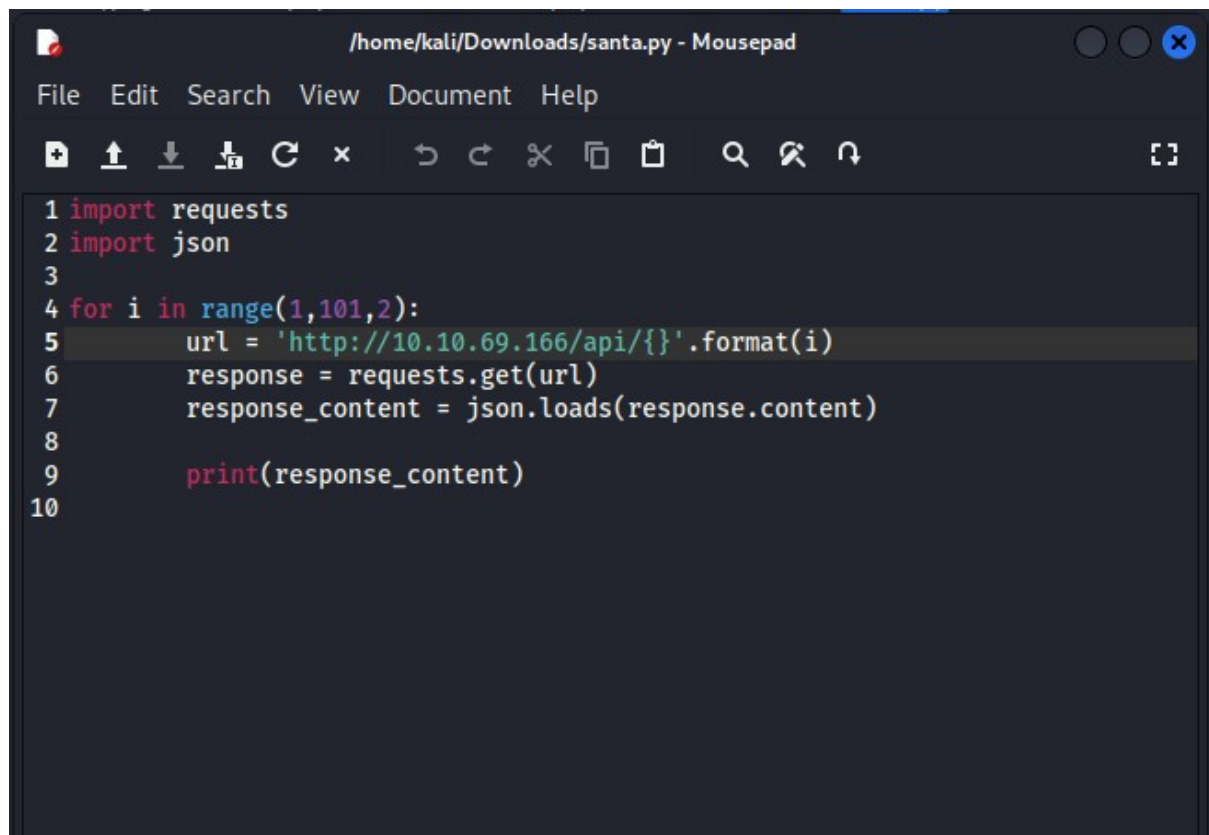
Open the page source of the site. Search api using the find tool and directory can be shown.

Q4.



By using the directory found from Q3, put in our own ip and the raw data can be found.

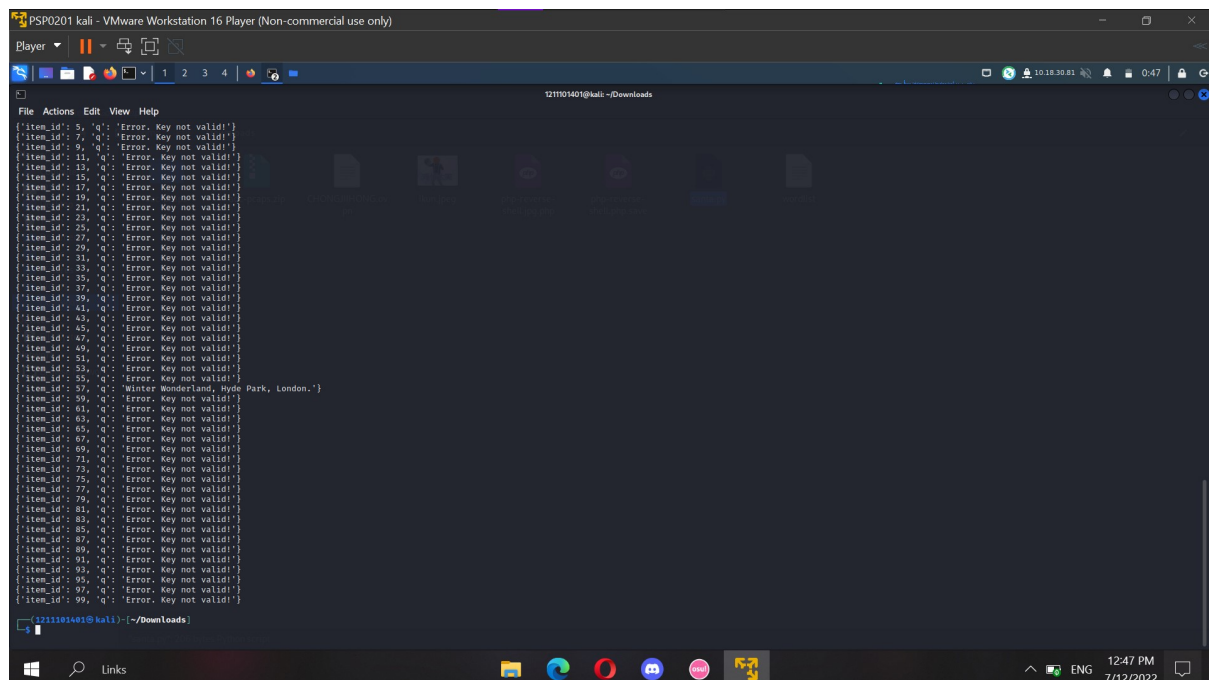
Q5.



The screenshot shows a text editor window titled "/home/kali/Downloads/santa.py - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for file operations and editing. The code is as follows:

```
1 import requests
2 import json
3
4 for i in range(1,101,2):
5     url = 'http://10.10.69.166/api/{}'.format(i)
6     response = requests.get(url)
7     response_content = json.loads(response.content)
8
9     print(response_content)
10
```

Create a python script that can find out the place Santa went. Run the script in terminal and the results will be shown.



The screenshot shows a terminal window titled "PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)". The terminal output displays a list of JSON objects, each representing a location. The output is as follows:

```
{
  "item_id": 5,
  "q": "Error. Key not valid!"
}
{
  "item_id": 7,
  "q": "Error. Key not valid!"
}
{
  "item_id": 9,
  "q": "Error. Key not valid!"
}
{
  "item_id": 11,
  "q": "Error. Key not valid!"
}
{
  "item_id": 13,
  "q": "Error. Key not valid!"
}
{
  "item_id": 15,
  "q": "Error. Key not valid!"
}
{
  "item_id": 17,
  "q": "Error. Key not valid!"
}
{
  "item_id": 19,
  "q": "Error. Key not valid!"
}
{
  "item_id": 21,
  "q": "Error. Key not valid!"
}
{
  "item_id": 23,
  "q": "Error. Key not valid!"
}
{
  "item_id": 25,
  "q": "Error. Key not valid!"
}
{
  "item_id": 27,
  "q": "Error. Key not valid!"
}
{
  "item_id": 29,
  "q": "Error. Key not valid!"
}
{
  "item_id": 31,
  "q": "Error. Key not valid!"
}
{
  "item_id": 33,
  "q": "Error. Key not valid!"
}
{
  "item_id": 35,
  "q": "Error. Key not valid!"
}
{
  "item_id": 37,
  "q": "Error. Key not valid!"
}
{
  "item_id": 39,
  "q": "Error. Key not valid!"
}
{
  "item_id": 41,
  "q": "Error. Key not valid!"
}
{
  "item_id": 43,
  "q": "Error. Key not valid!"
}
{
  "item_id": 45,
  "q": "Error. Key not valid!"
}
{
  "item_id": 47,
  "q": "Error. Key not valid!"
}
{
  "item_id": 49,
  "q": "Error. Key not valid!"
}
{
  "item_id": 51,
  "q": "Error. Key not valid!"
}
{
  "item_id": 53,
  "q": "Error. Key not valid!"
}
{
  "item_id": 55,
  "q": "Error. Key not valid!"
}
{
  "item_id": 57,
  "q": "Winter Wonderland - Hyde Park, London."
}
{
  "item_id": 59,
  "q": "Error. Key not valid!"
}
{
  "item_id": 61,
  "q": "Error. Key not valid!"
}
{
  "item_id": 63,
  "q": "Error. Key not valid!"
}
{
  "item_id": 65,
  "q": "Error. Key not valid!"
}
{
  "item_id": 67,
  "q": "Error. Key not valid!"
}
{
  "item_id": 69,
  "q": "Error. Key not valid!"
}
{
  "item_id": 71,
  "q": "Error. Key not valid!"
}
{
  "item_id": 73,
  "q": "Error. Key not valid!"
}
{
  "item_id": 75,
  "q": "Error. Key not valid!"
}
{
  "item_id": 77,
  "q": "Error. Key not valid!"
}
{
  "item_id": 79,
  "q": "Error. Key not valid!"
}
{
  "item_id": 81,
  "q": "Error. Key not valid!"
}
{
  "item_id": 83,
  "q": "Error. Key not valid!"
}
{
  "item_id": 85,
  "q": "Error. Key not valid!"
}
{
  "item_id": 87,
  "q": "Error. Key not valid!"
}
{
  "item_id": 89,
  "q": "Error. Key not valid!"
}
{
  "item_id": 91,
  "q": "Error. Key not valid!"
}
{
  "item_id": 93,
  "q": "Error. Key not valid!"
}
{
  "item_id": 95,
  "q": "Error. Key not valid!"
}
{
  "item_id": 97,
  "q": "Error. Key not valid!"
}
{
  "item_id": 99,
  "q": "Error. Key not valid!"
}
```

Q6.

From the results at Q5, we can also find out the correct API key.