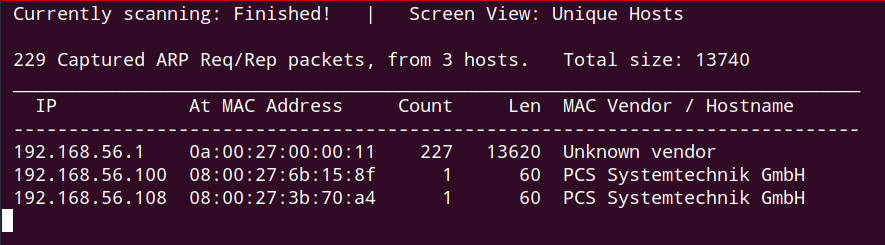
Phineas 1

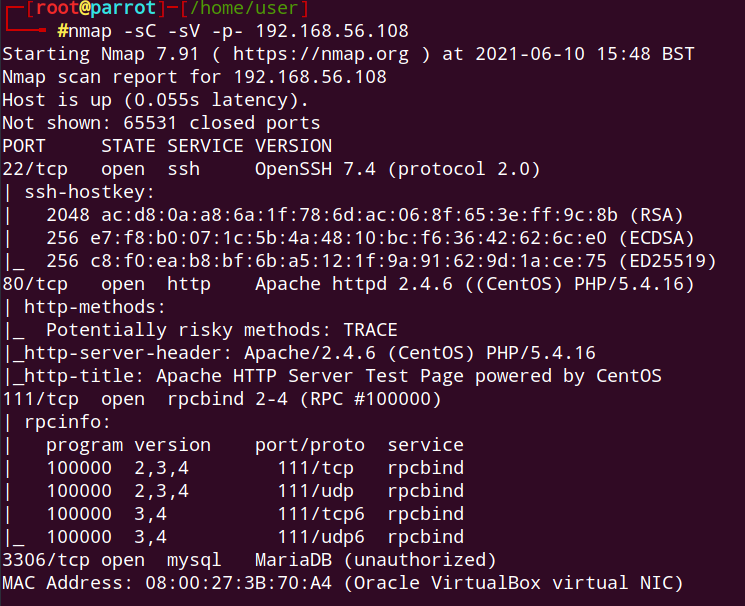
netdiscover scan

Target IP is 192.168.56.108



nmap scan

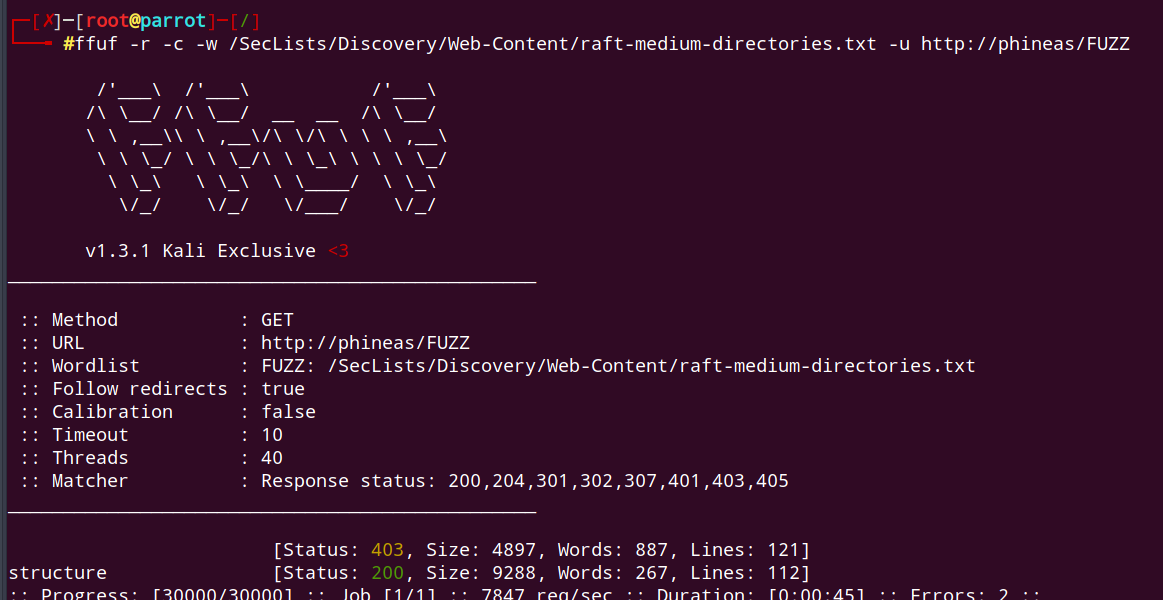
Tcp port: 22, 80, 111, 3306



Main directory:

[http://phineas](http://phineas/)

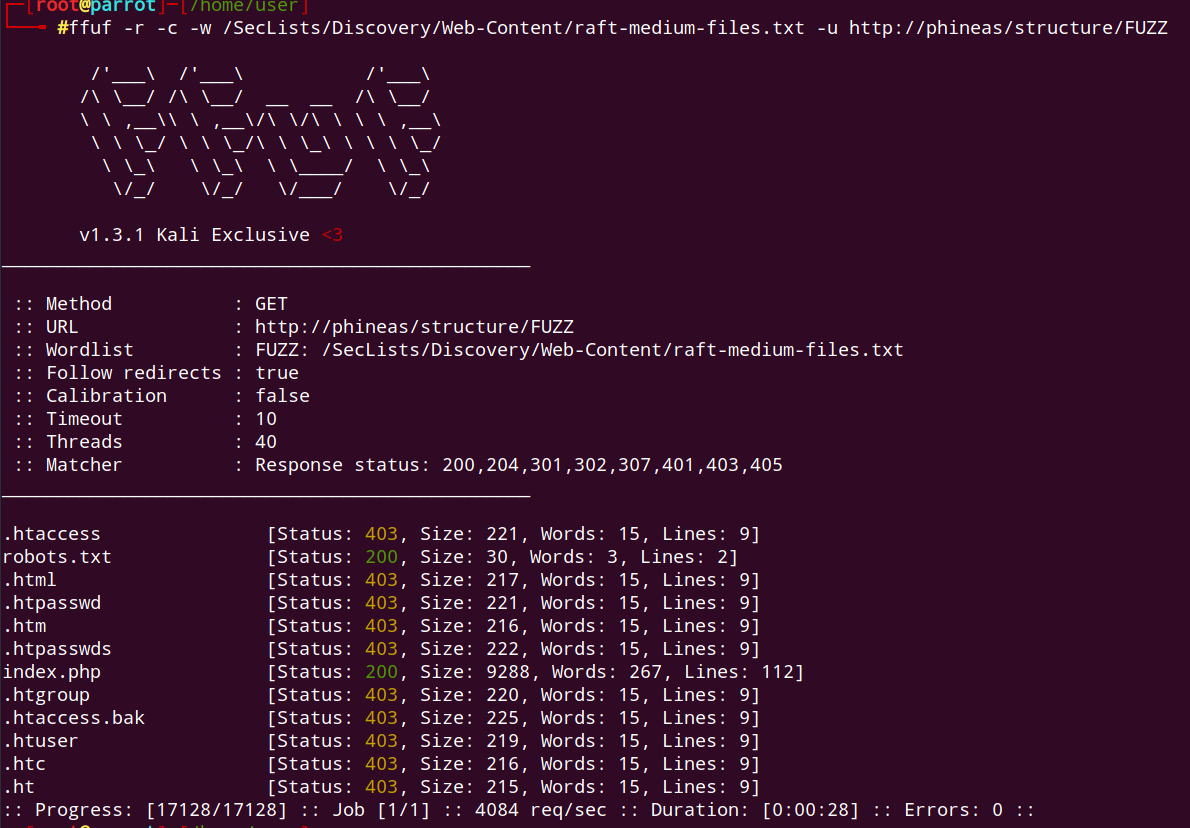
Main objective is to know subdirectories hidden on the main site.



Web Directory:

<http://phinease/structure>

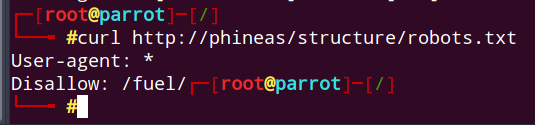
Main objective is to know subdirectories hidden under the structure directory.



hidden web directory:

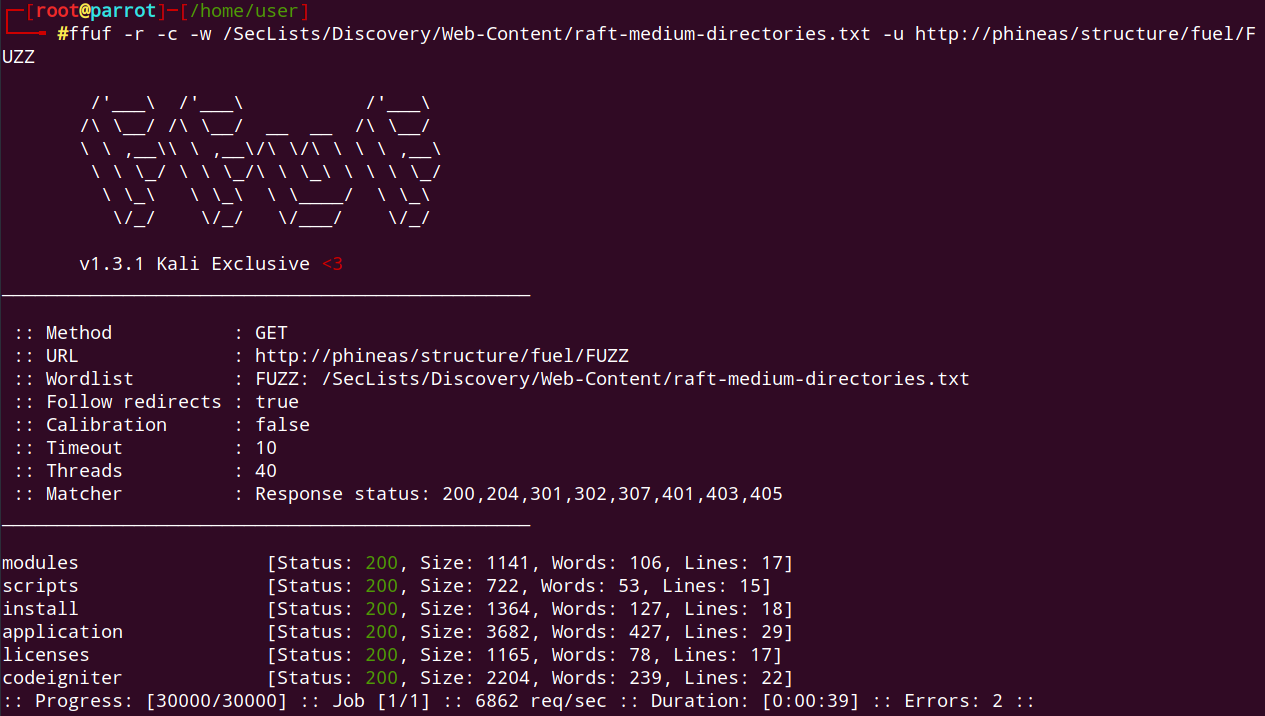
<http://phineas/structure/fuel>

There’s a hidden subdirectory named fuel which turns out to be a vulnerable CMS.



Further fuzzing:

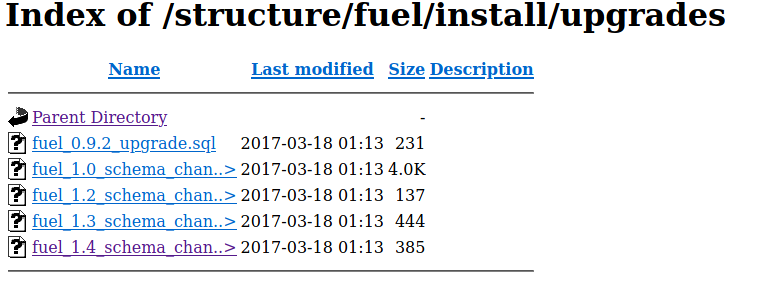
This is to further discover subdirectories hidden under fuel directory.



fuel version

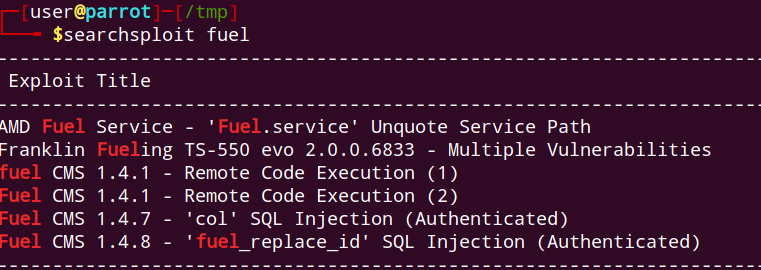
Vulnerable to exploit on searchsploit

On the site itself, there is a high probability that the fuel CMS version that was used is version 1.4



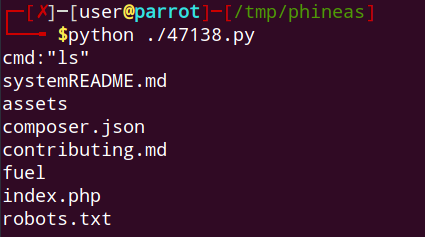
searchsploit fuel

Using exploit – fuel cms 1.4.1 – Remote Code Execution (1)



Confirmed RCE successful:

Able to list current directory



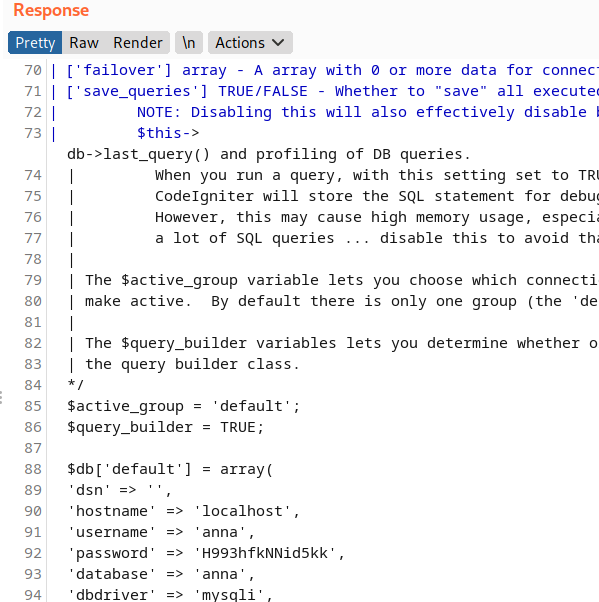
LFI:

cat /var/www/html/structure/fuel/application/config/database.php

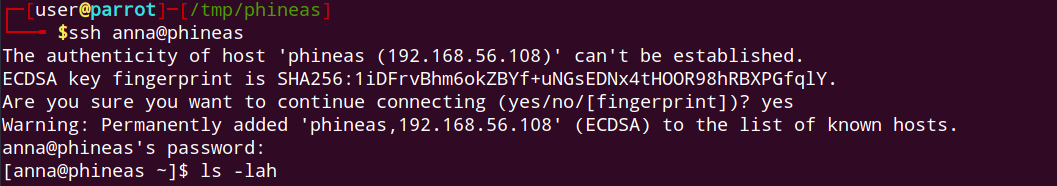
From this alone, anna’s credentials are disclosed.

'username' => 'anna',

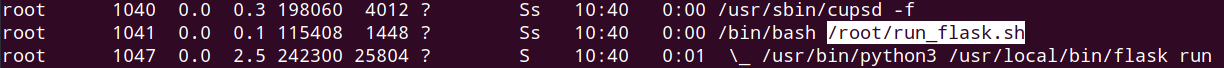
'password' => 'H993hfkNNid5kk'



Login as anna successful.

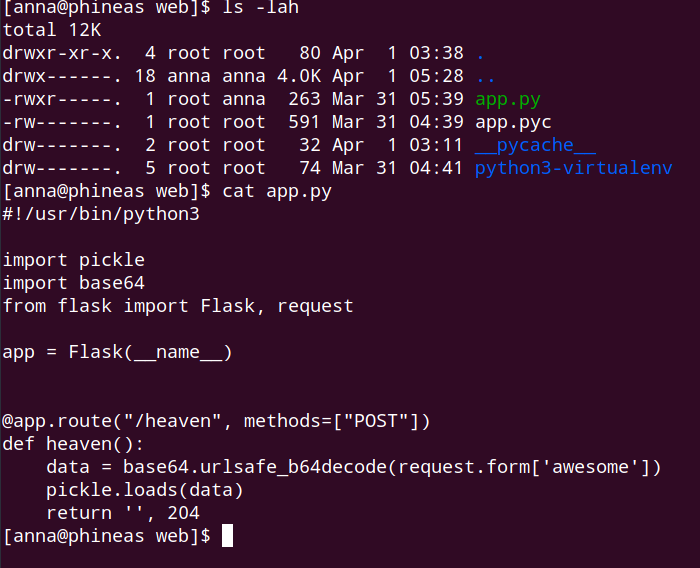


Discovered some python web server running



Source code of the python program running on the python webserver:

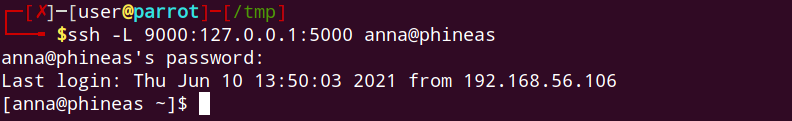
Pickle has a known vulnerability on deserialization.



Port forwarding

Create a connection to the target phineas.

The -L option means to forward to destination port 5000, attacker must connect to port 9000 on the localhost. This whole thing requires authentication, and anna’s credential will be used.



To exploit this deserialization, consult:

<https://davidhamann.de/2020/04/05/exploiting-python-pickle/>

On the website, there is this exploit code, attacking machine IP and PORT needs to be modified. Additional code are added to exploit this deserialization in one go instead of having to input curl commands externally.

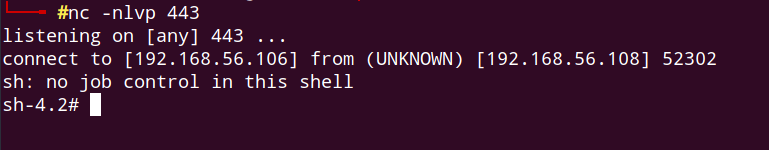
To trigger the exploit code:

1. Launch listener on attacking machine.

2. Do a curl to localhost on port 9000. Remember that by connecting to localhost 9000, connection is forwarded to target machine port 5000.



root shell



root flag

