General

```
PORT    STATE SERVICE    REASON         VERSION

22/tcp  open  ssh        syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 41:4d:aa:18:86:94:8e:88:a7:4c:6b:42:60:76:f1:4f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCq9GoYsvJTOUcsgHSES9+20Ix4Q8wjm5slMheJ2ME+COokAqxBzXSr458
KBmHv3bsTLWAH9FxoXJ6zrzDPmPApcqVifB4aI9l/
VYxoeJCj54kKIQlCKkWTZjsAeLBI2Lk2+yJLLFWPTAZ2htwRAwCl9z8YV3xgtqhTa+5BqIm/
GInW4PYV0zi9zOMn2g4jNSWvy91FBUboGLwVgNYslGBydNW8Fhz8X/
LXHZ1x6ulA76W026VEGOiQfoiIi84IFi9CbP8GIKfQ7BHuDlMqgiN9+w7K0z0oFdtiFhAS/
48w89MYn6UOzw7Aaa9eLQi0+zxpW5SpCpw0mC2euzPxow2Z
|   256 4d:a3:d0:7a:8f:64:ef:82:45:2d:01:13:18:b7:e0:13 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMz4UG2gfu7L/
Lxcqek1pZf46d8SocbES1A2a/XUYQgTmIqJuCEpLf3ERgVXS+7Lwdi6+F3xkI/lYFCA5MkRUQA=
|   256 1a:01:7a:4f:cf:95:85:bf:31:a1:4f:15:87:ab:94:e2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDL5ZwzA5dpqtWx4ZzjVQ6NMzVUia8/We8txfiAn+mv4

80/tcp  open  http       syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Photographer by v1n1v131r4

139/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp  open  netbios-ssn syn-ack ttl 61 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

8000/tcp open  http       syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Koken 0.22.24
|_http-title: daisa ahomi
Service Info: Host: PHOTOGRAPHER; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| 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: 2025-01-26T13:45:15-05:00
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s
| nbstat: NetBIOS name: PHOTOGRAPHER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   PHOTOGRAPHER<00>    Flags: <unique><active>
|   PHOTOGRAPHER<03>    Flags: <unique><active>
|   PHOTOGRAPHER<20>    Flags: <unique><active>
```

```
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-time:
|   date: 2025-01-26T18:45:14
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 17210/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 17946/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 50806/udp): CLEAN (Failed to receive data)
|   Check 4 (port 51871/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocke
```

flags

privesc

simple SUID priv esc using php

Port 22 (ssh)

22/tcp open ssh syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 41:4d:aa:18:86:94:8e:88:a7:4c:6b:42:60:76:f1:4f (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCq9GoYsvJTOUcsgHSES9+20Ix4Q8wjm5slMheJ2ME+COokAqxBzXSr458
KBmHv3bsTLWAH9FxoXJ6zrzDPmPApcqVifB4aI9l/
VYxoeJCj54kKIQlCKkWTZjsAeLBI2Lk2+yJLLFWPTAZ2htwRAwCl9z8YV3xgtqhTa+5BqIm/
GInW4PYV0zi9zOMn2g4jNSWvy91FBUboGLwVgNYslGBydNW8Fhz8X/
LXHZ1x6ulA76W026VEGOiQfoiIi84IFi9CbP8GIKfQ7BHuDlMqgiN9+w7K0z0oFdtiFhAS/
48w89MYn6UOzw7Aaa9eLQi0+zxpW5SpCpw0mC2euzPxow2Z
| 256 4d:a3:d0:7a:8f:64:ef:82:45:2d:01:13:18:b7:e0:13 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMz4UG2gfu7L/
Lxcqek1pZf46d8SocbES1A2a/XUYQgTmIqJuCEpLf3ERgVXS+7Lwdi6+F3xkI/lYFCA5MkRUQA=
| 256 1a:01:7a:4f:cf:95:85:bf:31:a1:4f:15:87:ab:94:e2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDL5ZwzA5dpqtWx4ZzjVQ6NMzVUia8/We8txfiAn+mv4

to do;
find creds []

Port 80 (http)

80/tcp open http   syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Photographer by v1n1v131r4

to do ;
Dirbust [✔]
subdomain fuzz
test functionality

```
gobuster dir -u http://192.168.117.76/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt -x php,.txt,html,.,py,js
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.117.76/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ,py,js,php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 279]
/index.html          (Status: 200) [Size: 5711]
/.                   (Status: 200) [Size: 5711]
/.html               (Status: 403) [Size: 279]
/images              (Status: 301) [Size: 317] [--> http://192.168.117.76/images/]
/assets              (Status: 301) [Size: 317] [--> http://192.168.117.76/assets/]
/generic.html        (Status: 200) [Size: 4243]
/elements.html       (Status: 200) [Size: 19831]
/.                   (Status: 200) [Size: 5711]
/.html               (Status: 403) [Size: 279]
/.php                (Status: 403) [Size: 279]
/server-status       (Status: 403) [Size: 279]
Progress: 720766 / 1543927 (46.68%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 720902 / 1543927 (46.69%)
===============================================================
Finished
===============================================================
```

Ports 445/139 (SMB)

139/tcp open netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn syn-ack ttl 61 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

Host script results:
| 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: 2025-01-26T13:45:15-05:00
|_clock-skew: mean: 1h40m00s, deviation: 2h53m13s, median: 0s
| nbstat: NetBIOS name: PHOTOGRAPHER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| PHOTOGRAPHER<00>   Flags: <unique><active>
| PHOTOGRAPHER<03>   Flags: <unique><active>
| PHOTOGRAPHER<20>   Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00>   Flags: <group><active>
| WORKGROUP<1d>   Flags: <unique><active>
| WORKGROUP<1e>   Flags: <group><active>
| Statistics:
| 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_ 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-time:
| date: 2025-01-26T18:45:14
|_ start_date: N/A
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 17210/tcp): CLEAN (Couldn't connect)
| Check 2 (port 17946/tcp): CLEAN (Couldn't connect)
| Check 3 (port 50806/udp): CLEAN (Failed to receive data)
| Check 4 (port 51871/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked

to do ;
test connection[]
download files[1✔]

from the smb samabashare share I downloaded 1 file and 1 folder
The file “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 <>
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 ;)
```

usernames found?
daisa@photographer.com
daisa:

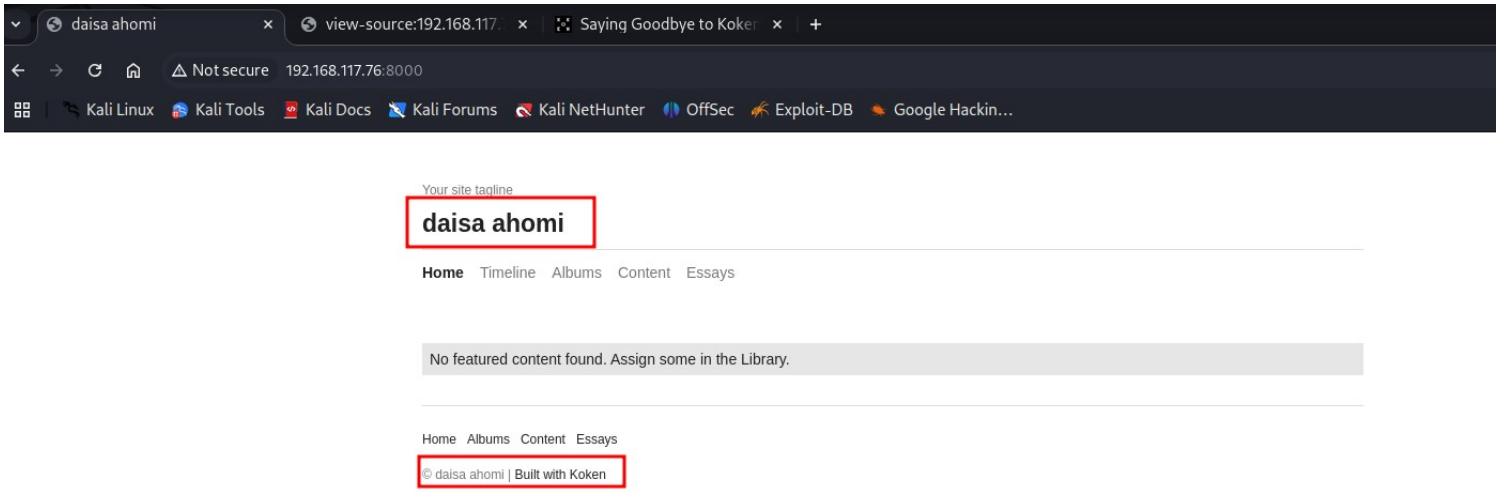
secret? mybabygirl

The folder I downloaded was a WP site backup but no wp-config.php file

Port 8000 (http)

8000/tcp open http   syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Koken 0.22.24
|_http-title: daisa ahomi
Service Info: Host: PHOTOGRAPHER; OS: Linux; CPE: cpe:/o:linux:linux_kernel

To do;
Dirbust
subdomain fuzz
test functionality

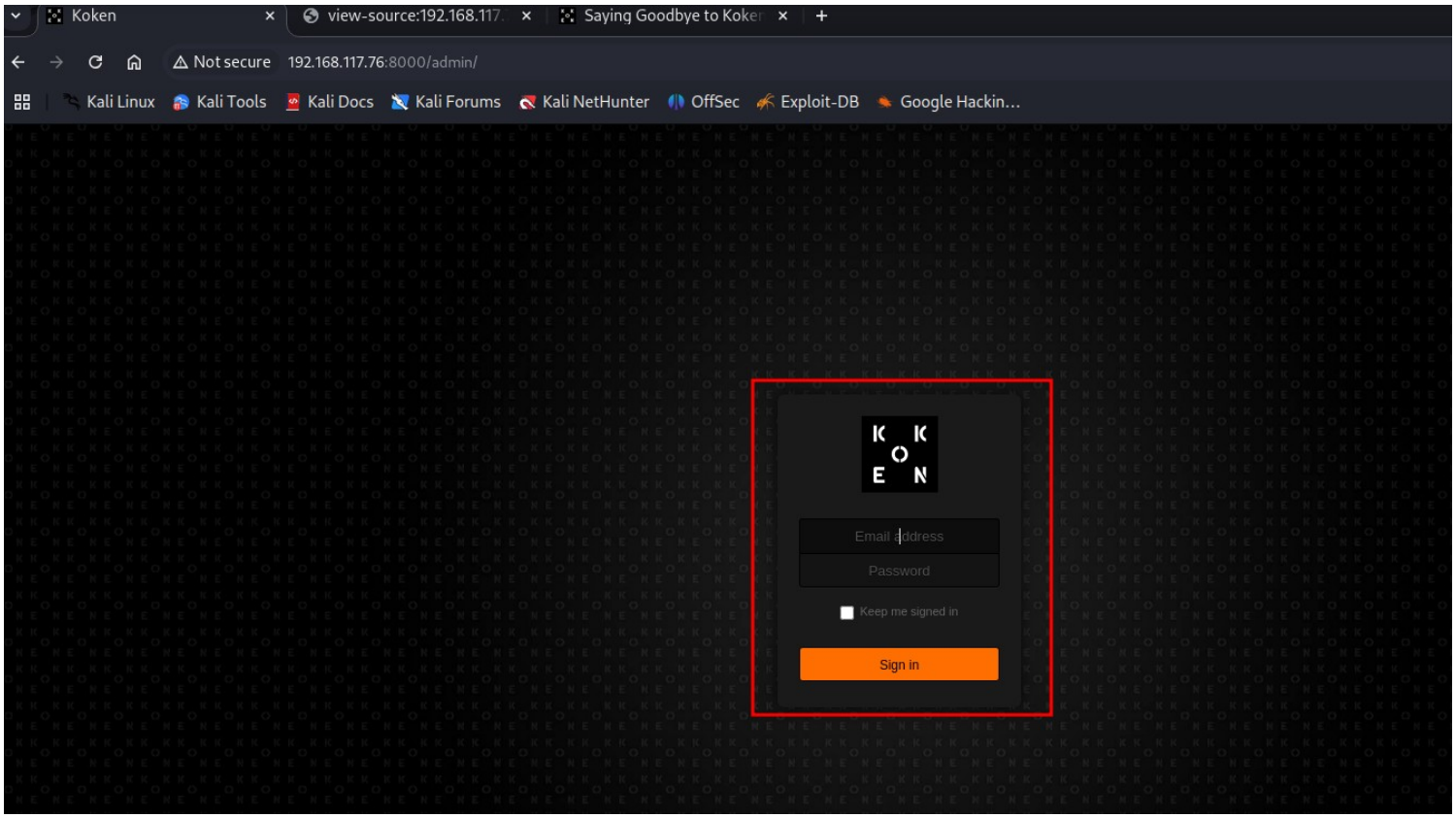


the name daisa poped up again
admins name?

```
gobuster dir -u http://192.168.117.76:8000/ -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -x php,.txt,html,.,py,js  --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.117.76:8000/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                            /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
[+] Negative Status codes:   404
[+] Exclude Length:          0
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,,py,js,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 281]
/.                    (Status: 200) [Size: 4603]
/.html                (Status: 403) [Size: 281]
/index.php            (Status: 200) [Size: 4603]
/admin                (Status: 301) [Size: 323] [--> http://192.168.117.76:8000/admin/]
/storage              (Status: 301) [Size: 325] [--> http://192.168.117.76:8000/storage/]
/app                  (Status: 301) [Size: 321] [--> http://192.168.117.76:8000/app/]
/api.php              (Status: 500) [Size: 600]
/.php                 (Status: 403) [Size: 281]
/.                    (Status: 200) [Size: 4603]
/.html                (Status: 403) [Size: 281]
Progress: 466547 / 1543927 (30.22%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 466632 / 1543927 (30.22%)
===============================================================
Finished
===============================================================
```

Admin Login Page

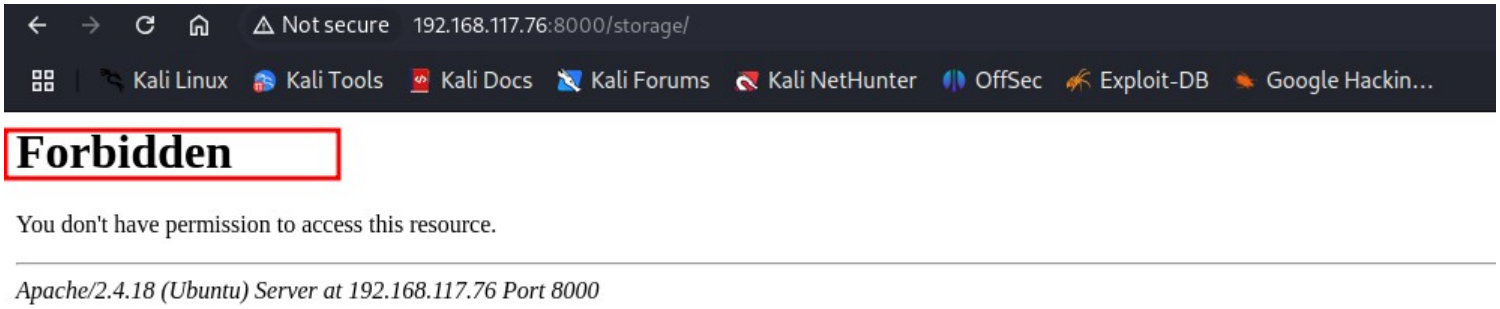


Looks like a normal login page

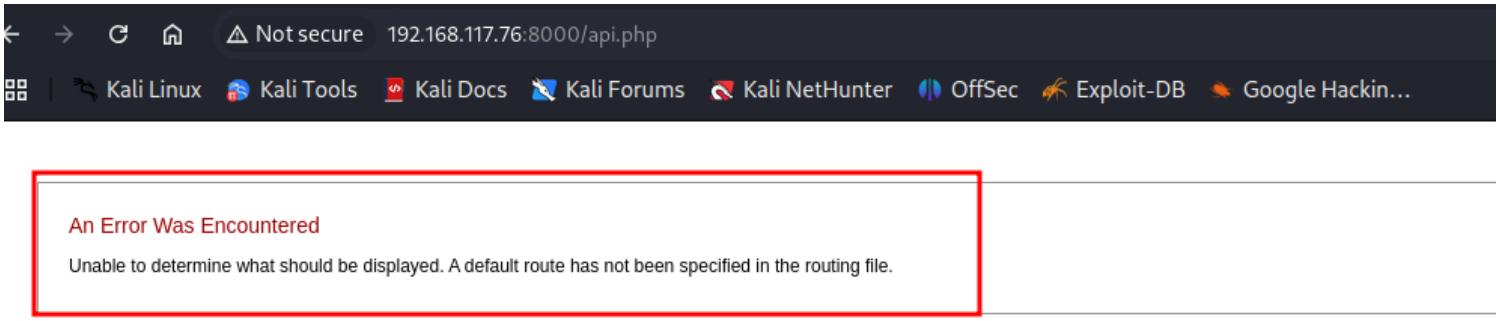
found creds
daisa@photographer.com:b

using Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated)
php/webapps/48706.txt
I uploaded a shell and got a revshell

Storage page



API page



Looks like the API was not impliented right