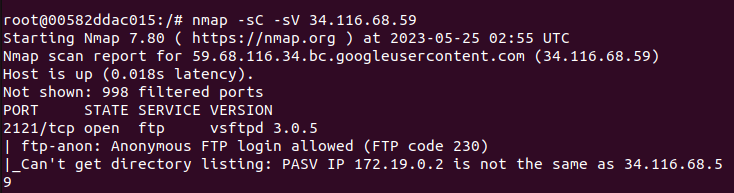
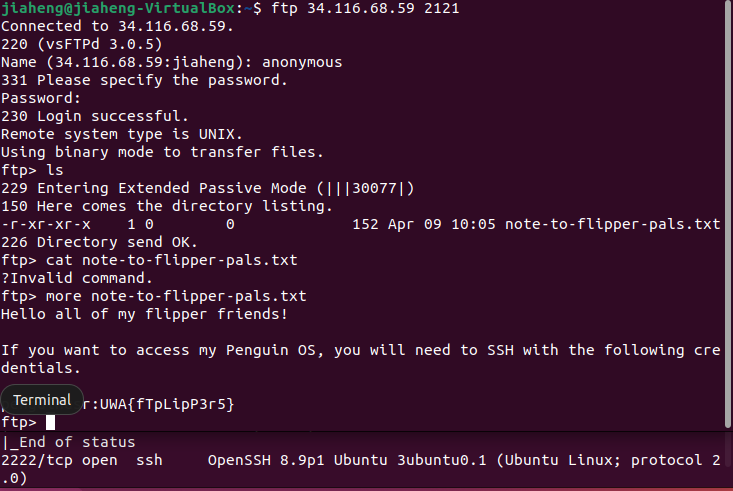
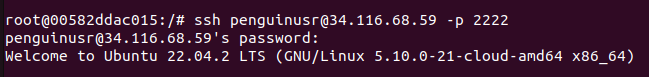
**1.Project: Computer Architecture and Networking**

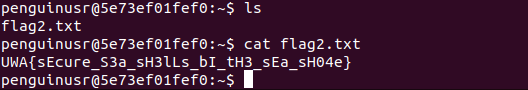
**1.1 Penguin OS Part 1: For the FTP (10)**  
UWA{fTpLipP3r5}

·You can use nmap command available ftp port through the IP provided.  
·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.  
  
 **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,  
use SSH to connect to the port, note that the user is penguinusr, enter password UWA{fTpLipP3r5}.

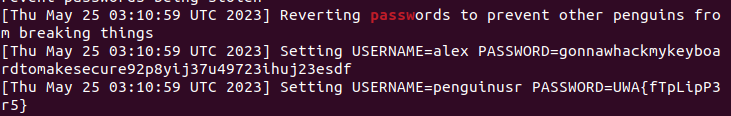
  
·Then use the cat command.

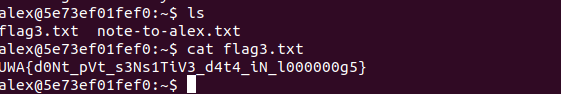
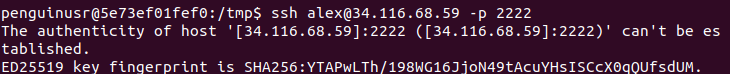
  
**1.3 Penguin OS Part 3: Peas in a Pod (10)**  
UWA{d0Nt\_pVt\_s3Ns1TiV3\_d4t4\_iN\_l000000g5}

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



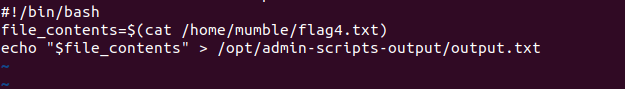


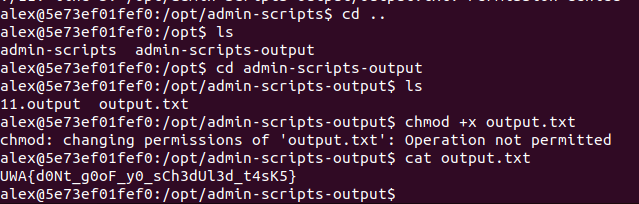
  
·Connect to the alex account via ssh, and then use cat command to flag3.

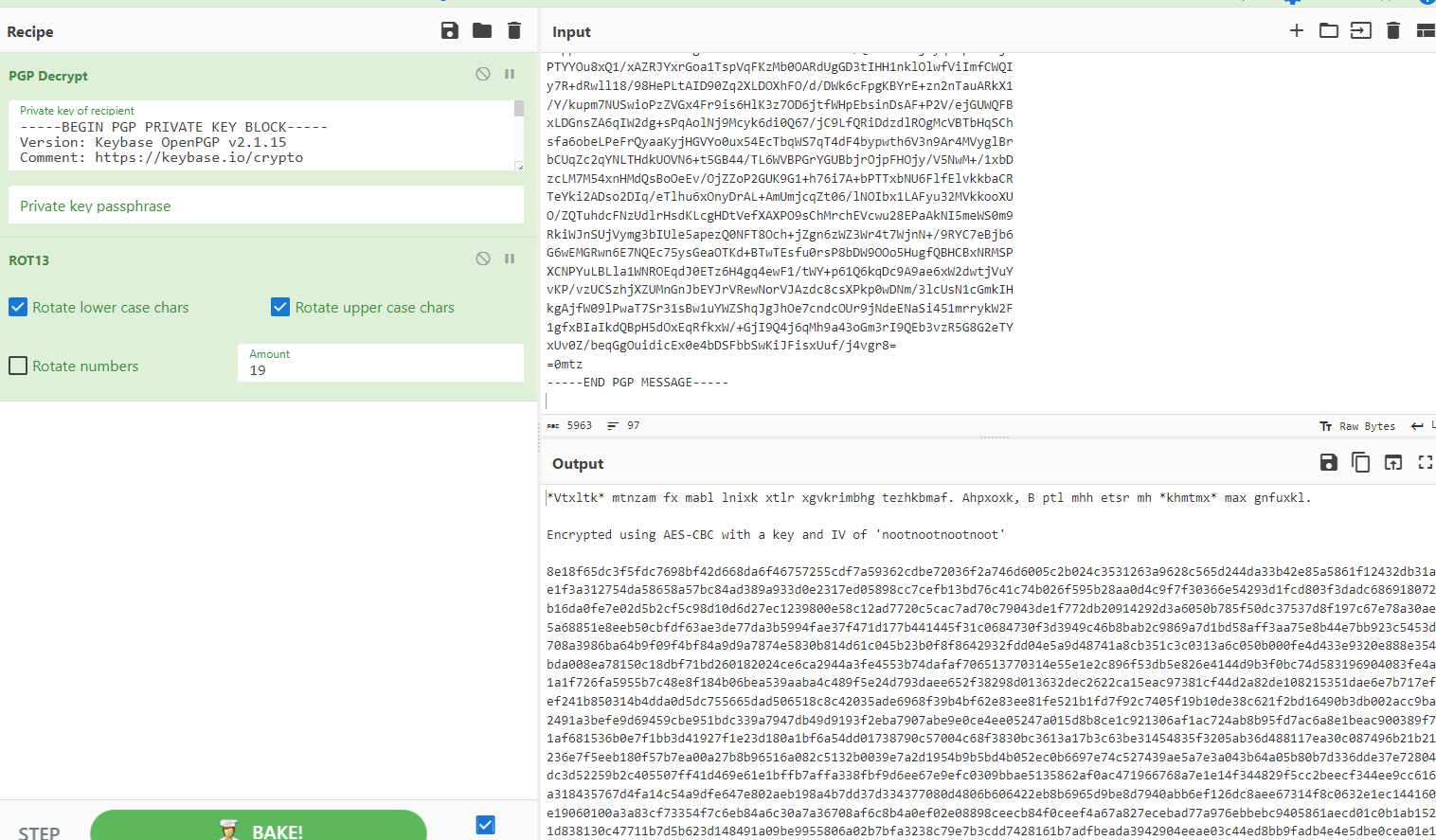
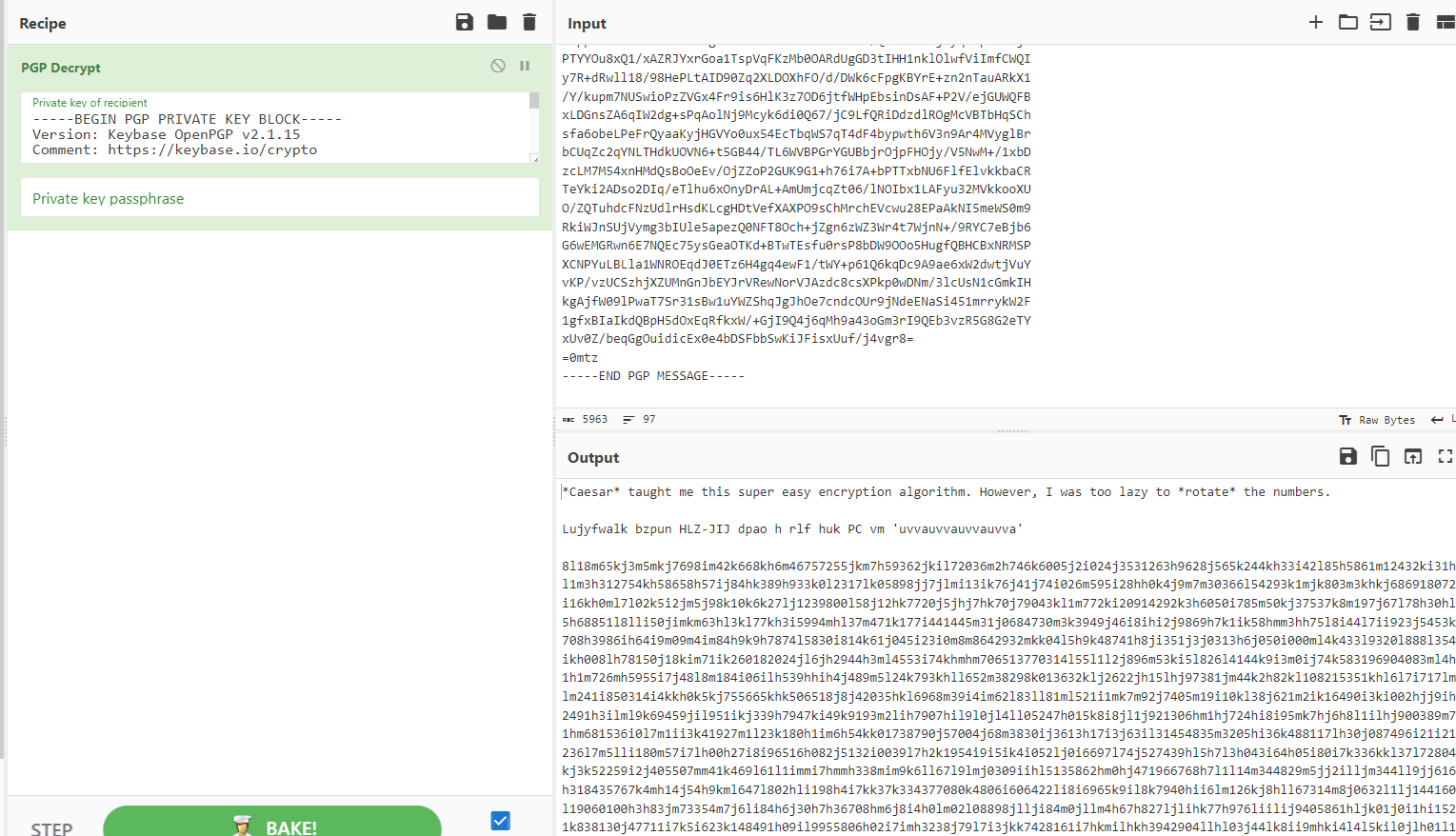
  
**1.4 Penguin OS Part 4: Scheduled Hack(25)**  
UWA{d0Nt\_g0oF\_y0\_sCh3dUl3d\_t4sK5}  
·Go to /opt/admin-scripts to create a shell script, use the cat command to read the contents of /home/mumble/flag4.txt, then print the contents to /opt/admin-scripts-output.

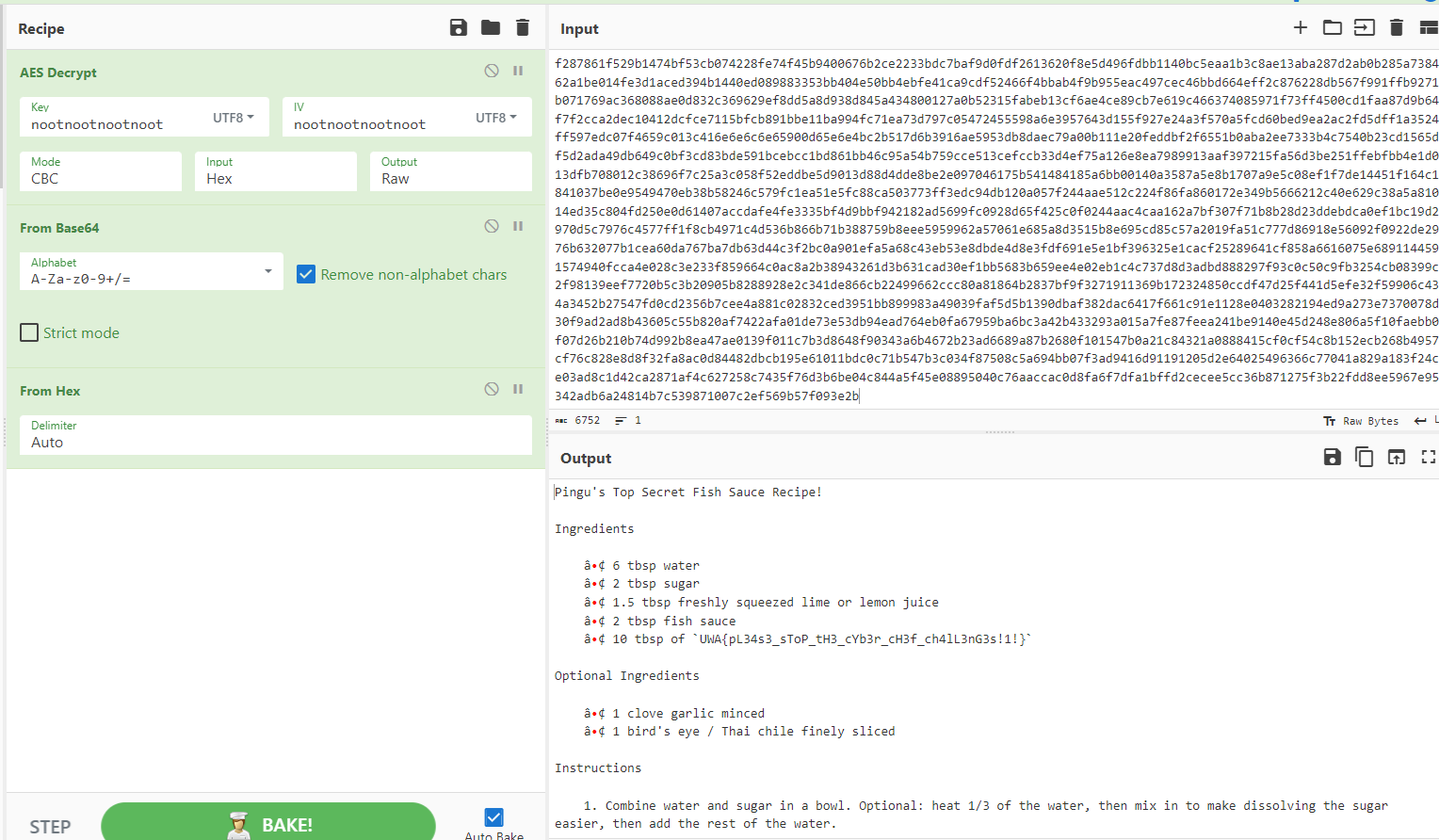
The script is like:

#!/bin/bash  
file\_contents=$(cat /home/mumble/flag4.txt)

echo "$file\_contents" > /opt/admin-scripts-output/output.txt  
  
·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.



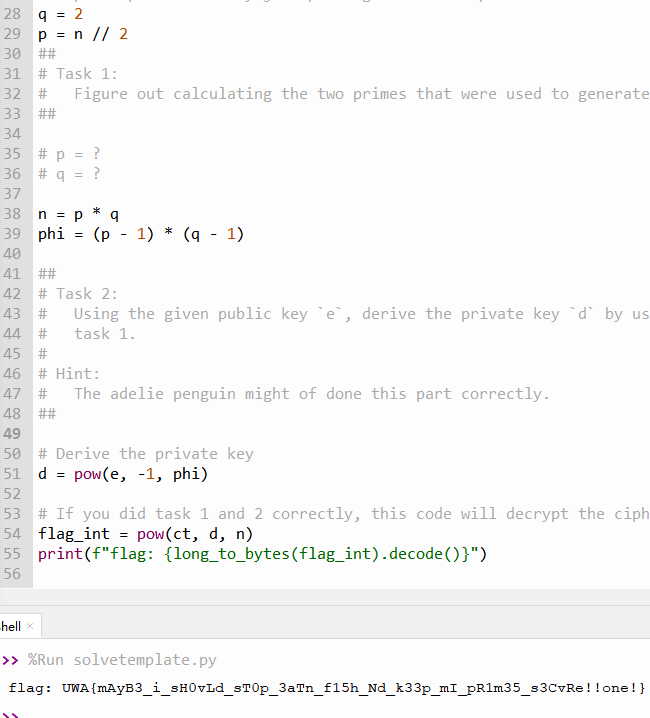
**2.Project: Cryptography**  
**2.1Penguin Translator School(10)**  
UWA{WAA\_WAA\_W00\_MEANS\_I\_H4V3\_L0ST\_MI\_5AN1TI!1ONE}  
·First of all this string consists of wa and woo, so you can use find/replace to convert this string to Morse code by changing wa to . and woo to -  
·Finally use from morse 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.



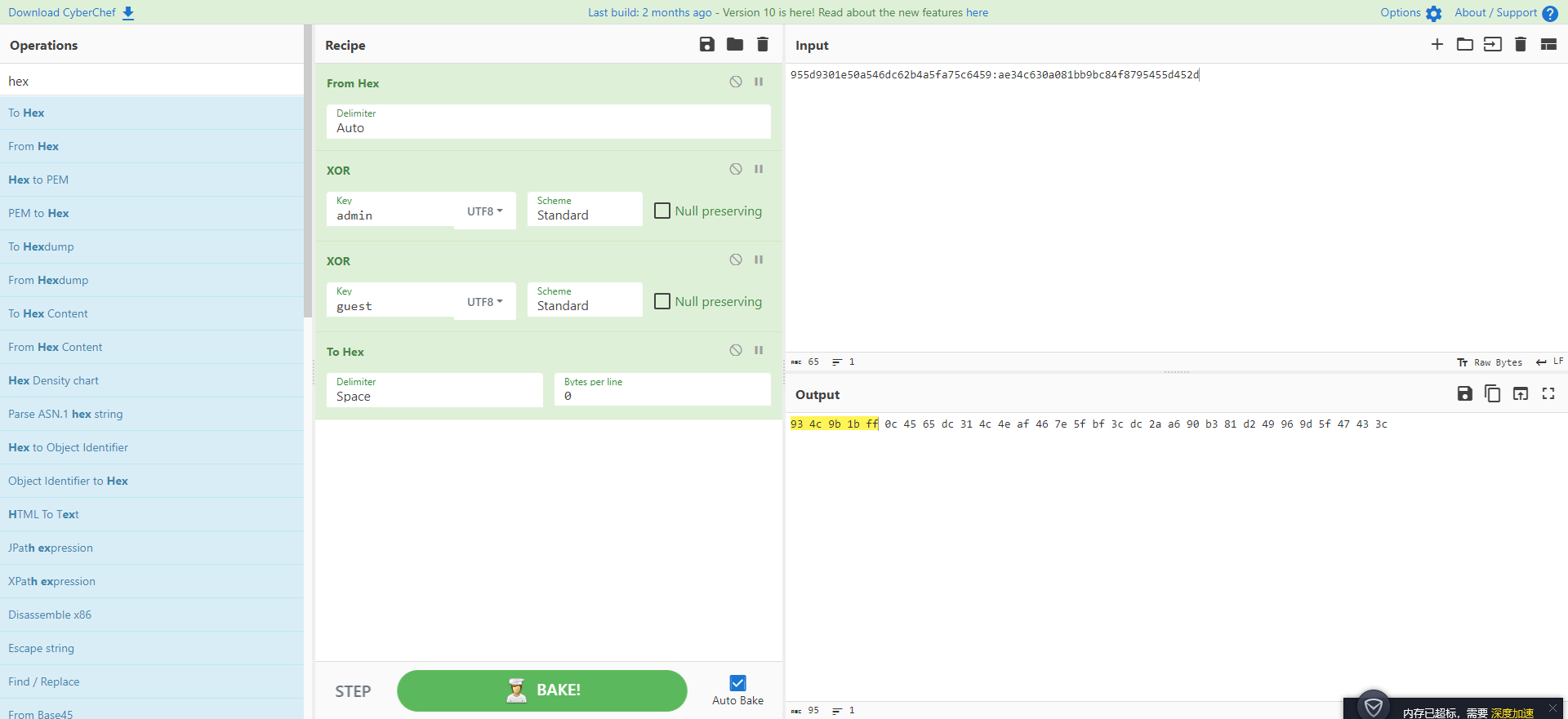
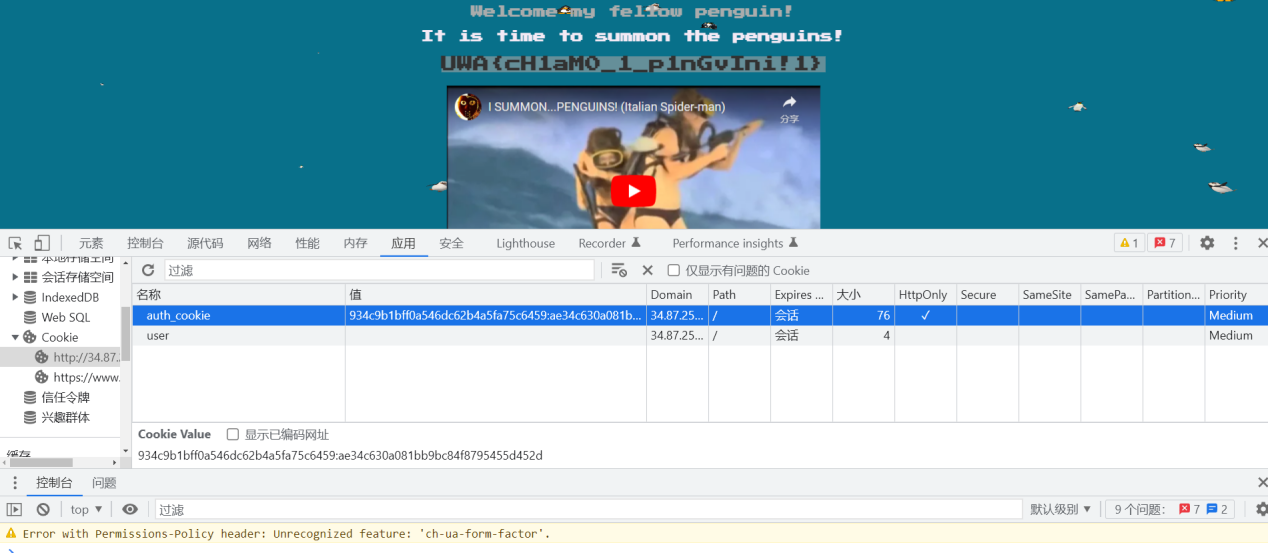
**2.3 Penguin RSA(20)**

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.

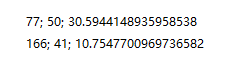


**2.4 Flippin Auth(25)**  
UWA{cH1aM0\_1\_p1nGvIni!1}

·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**

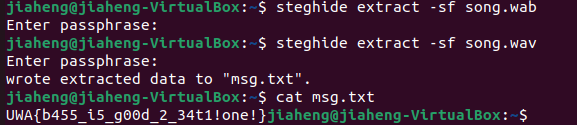
**3.1 Noot Noot(10)**

UWA{Mcmurdo Station}  
·After downloading the image, right click on properties to get to the GPS location of the image, ,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)**

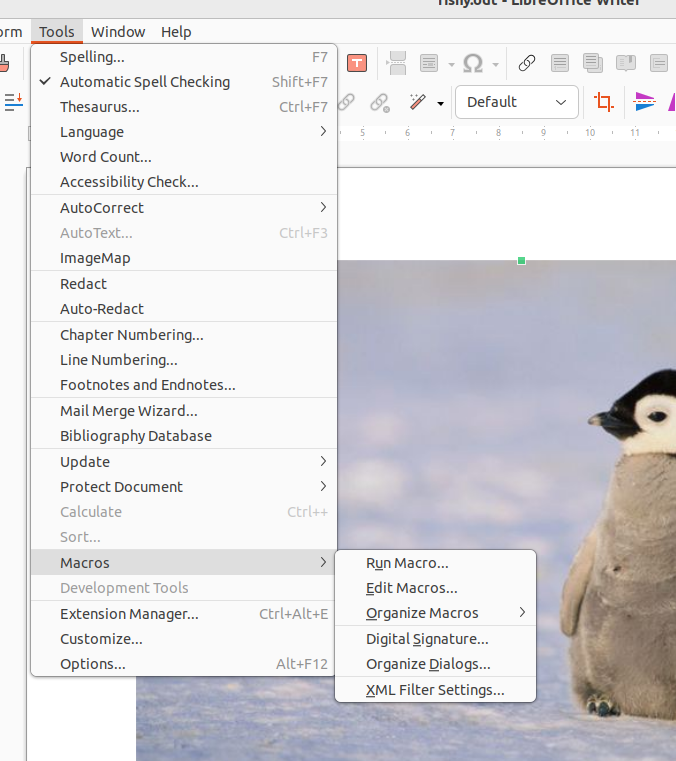
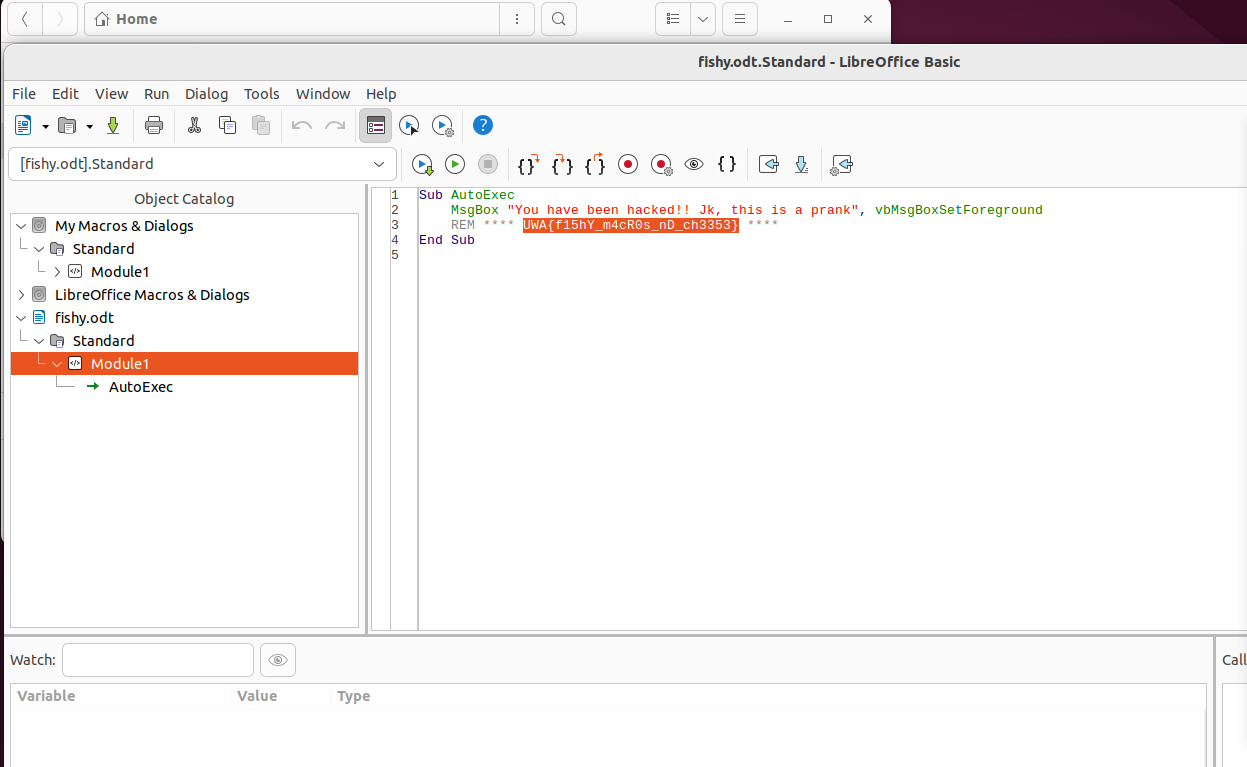
UWA{b455\_i5\_g00d\_2\_34t1!one!}

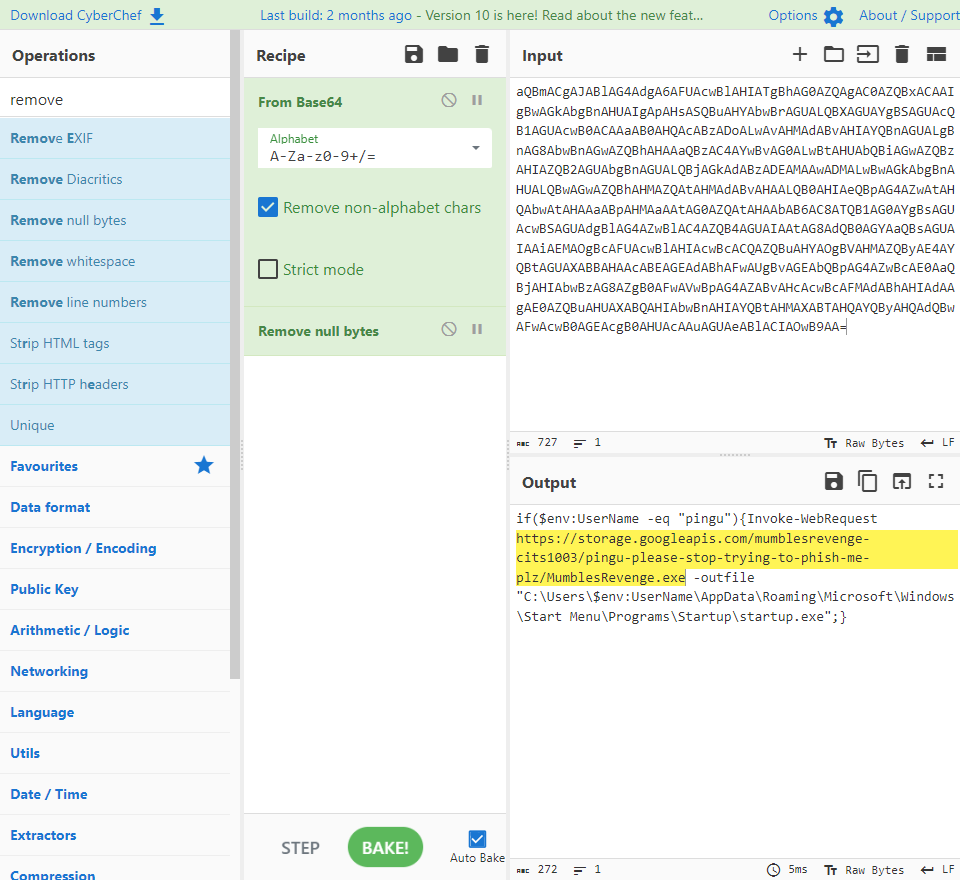
·First, you need to install steghide and the specified music file, after the installation is complete, use cd to enter the path where the file is located, and then use the command steghide extract -sh <filename>to extract data.  
·Then the system will prompt a txt file appears, use the cat command to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


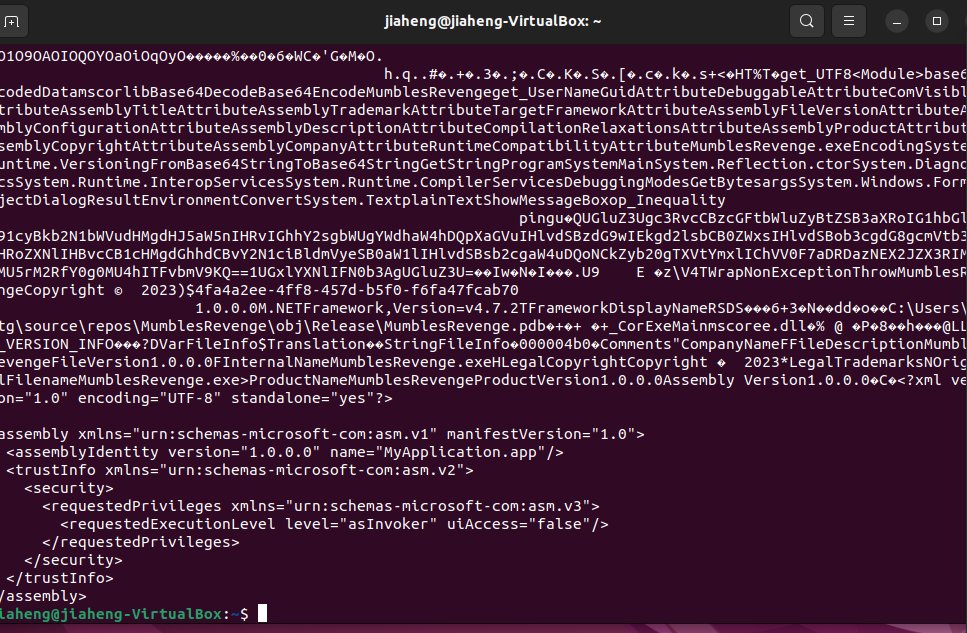
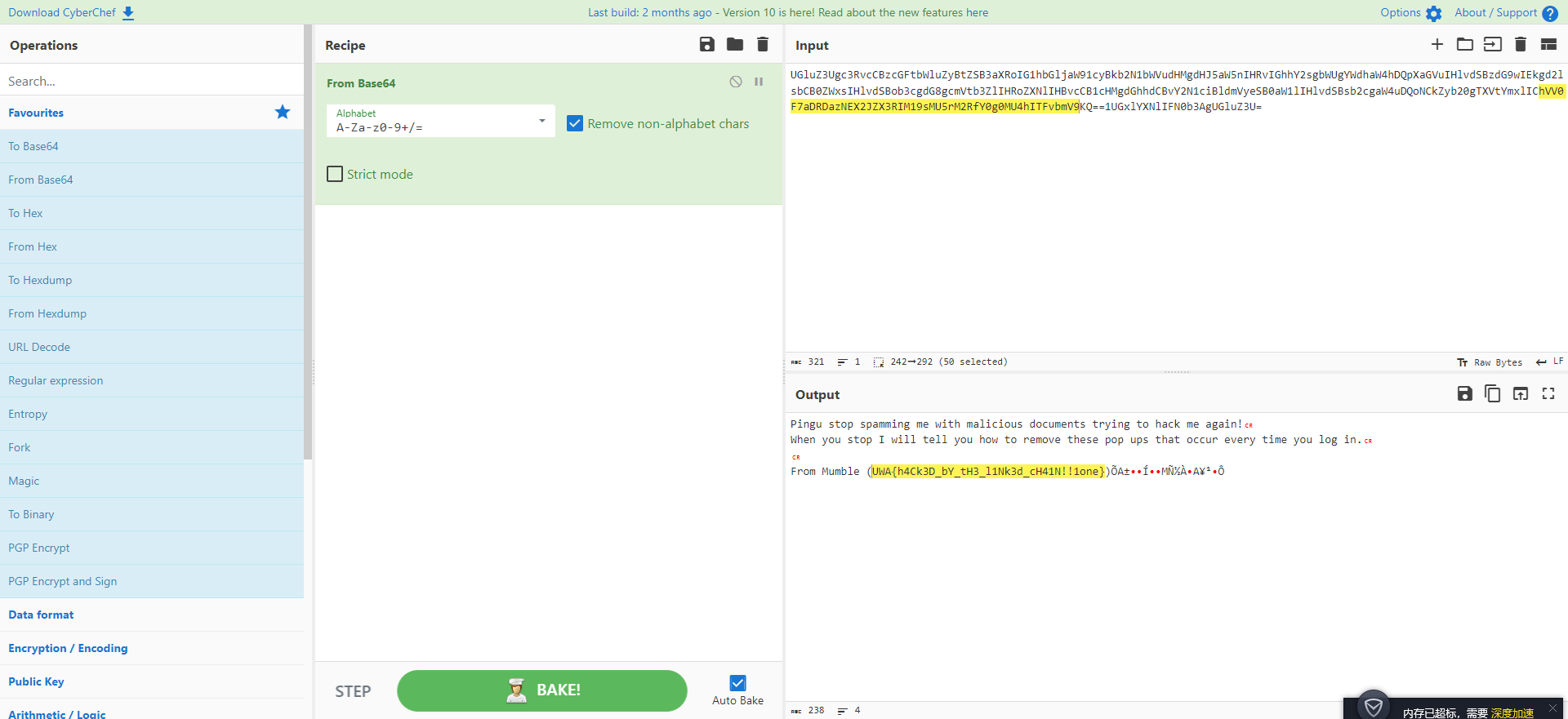
**3.3 Fishy Doc(20)**

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.

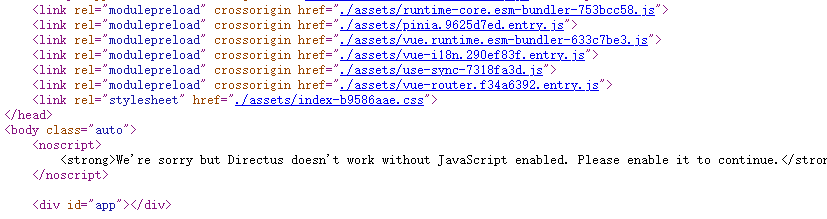
  
·Find the code ending with = in it, and use cyberchef's from base 64 to get the answer.  


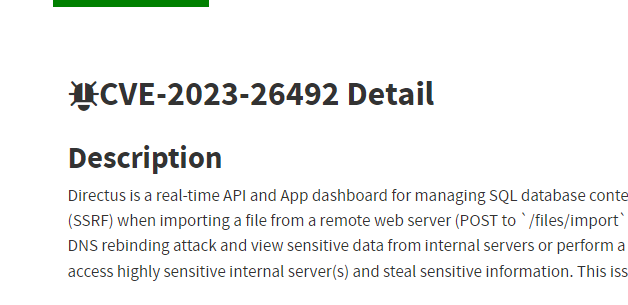
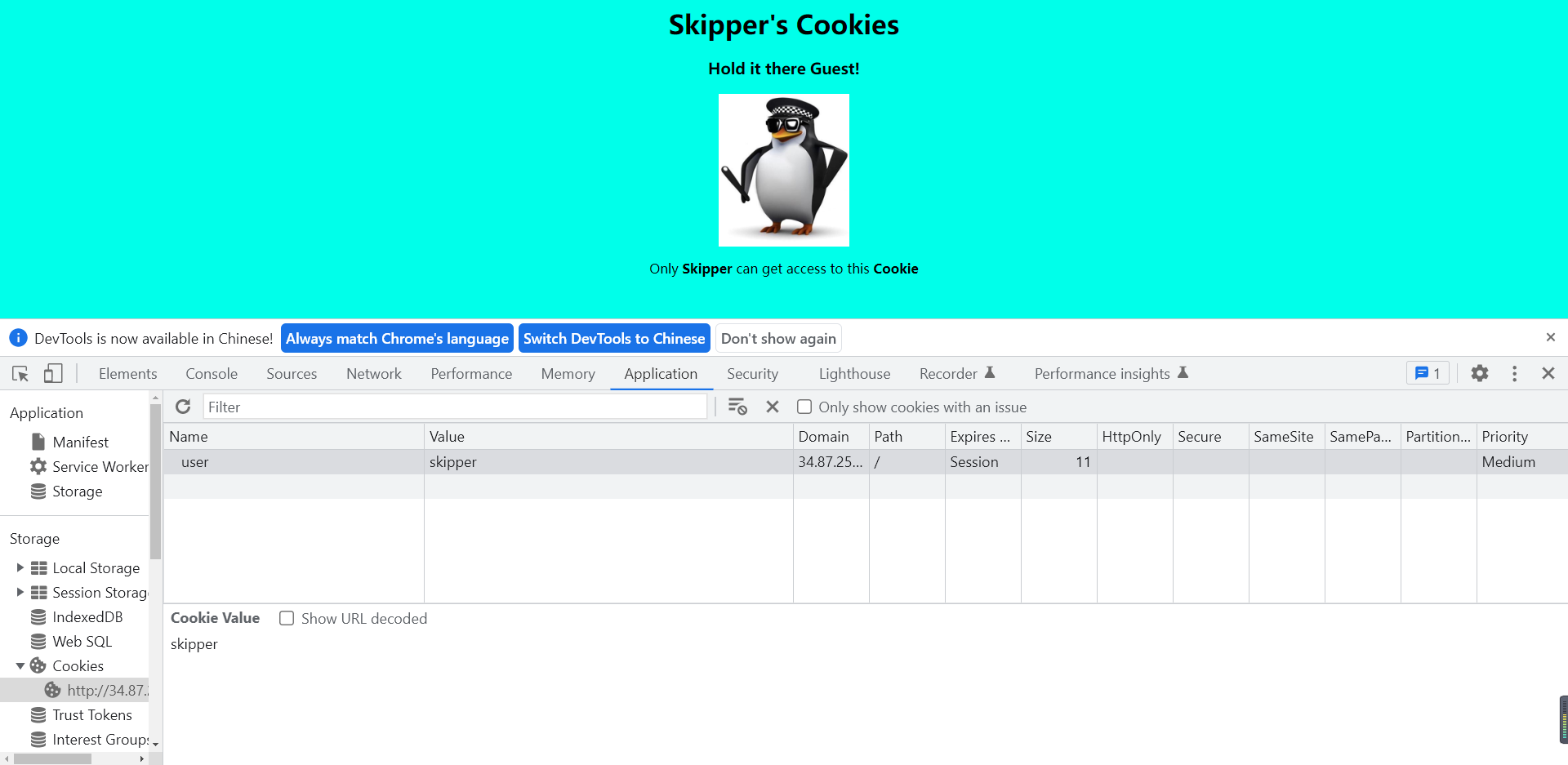
**4.Project: Vulnerabilities**  
**4.1 Arctic File Storage Part 1: Surfing for Vulns(10)**

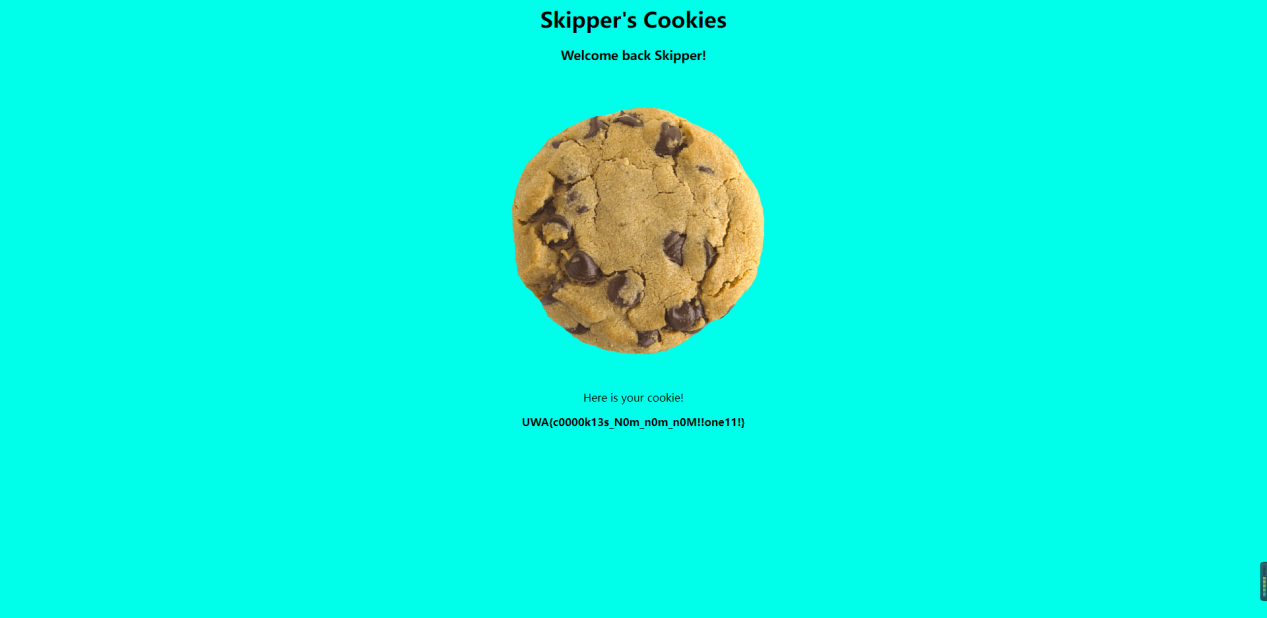
UWA{CVE-2023-26492}

·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.

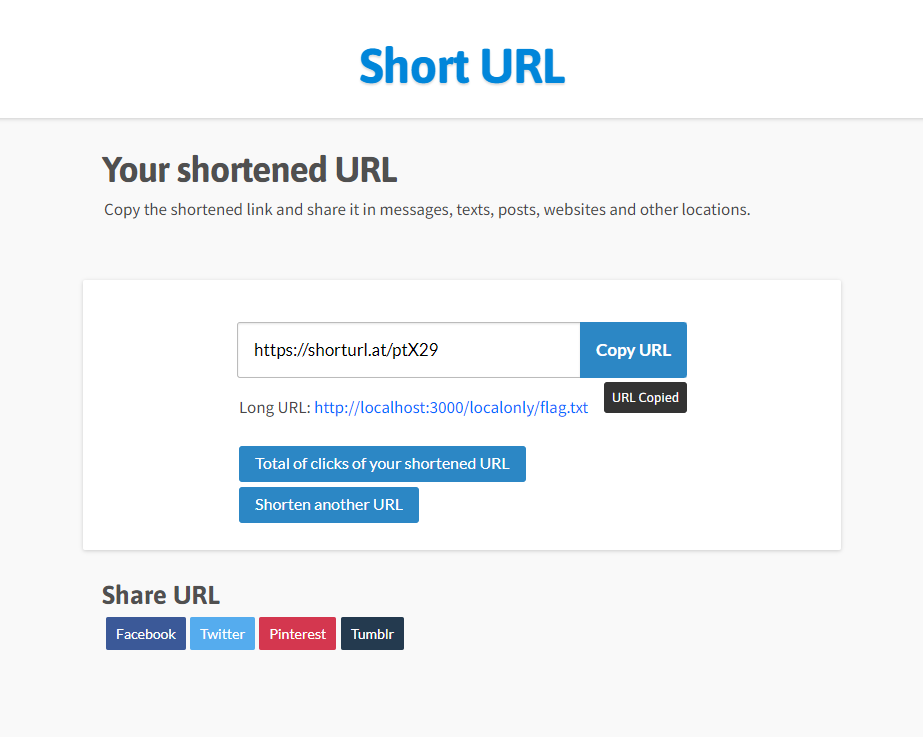
·Then Google the keyword: Directus, CVE ID for the latest Server-Side Request Forgery (SSRF) vulnerability, you will be able to find the CVE ID.

**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.  
