Write-up DBS401: Group 3

👋 Welcome to my write-up!

🔧 Tools: Burp Suite

🗃️ Flags' Completion Table

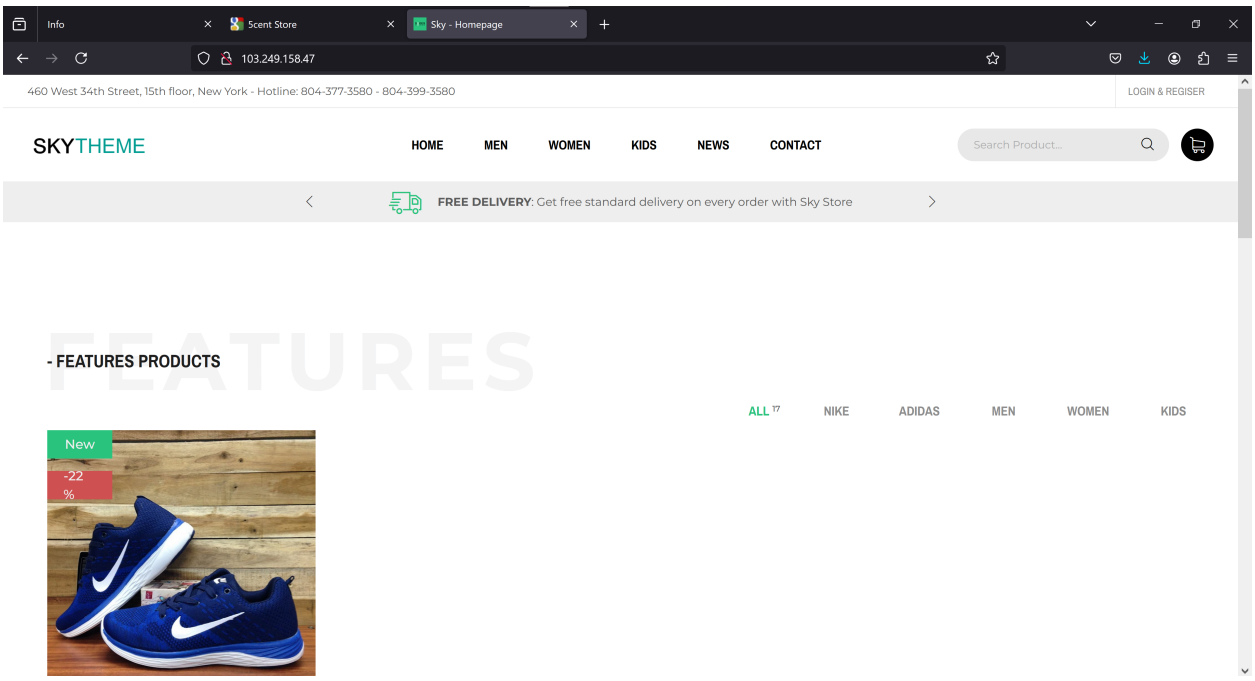
Flag Number	**Vulnerability's Name**	**Done**	**Flag**
1	IDOR	yes	Flag{Team3_flag_1}
2	IDOR	yes	Flag={Team3_Flag_2!!!}
3	?	yes	Nhom3_Flag3{Dayla_Nhom3dbs301_Flag3_ThayTuanAnh}

🚨 Extra vulnerabilities

No.	**Vulnerability's Name**
1	SQL Injection

📝 Description

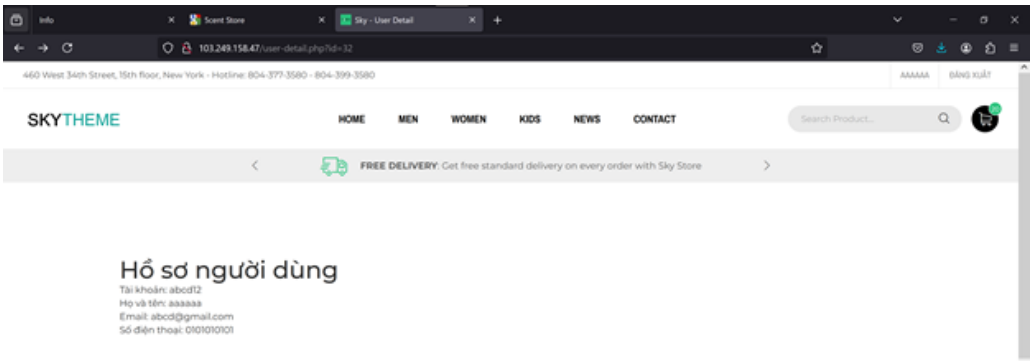
- A website that selling shoes



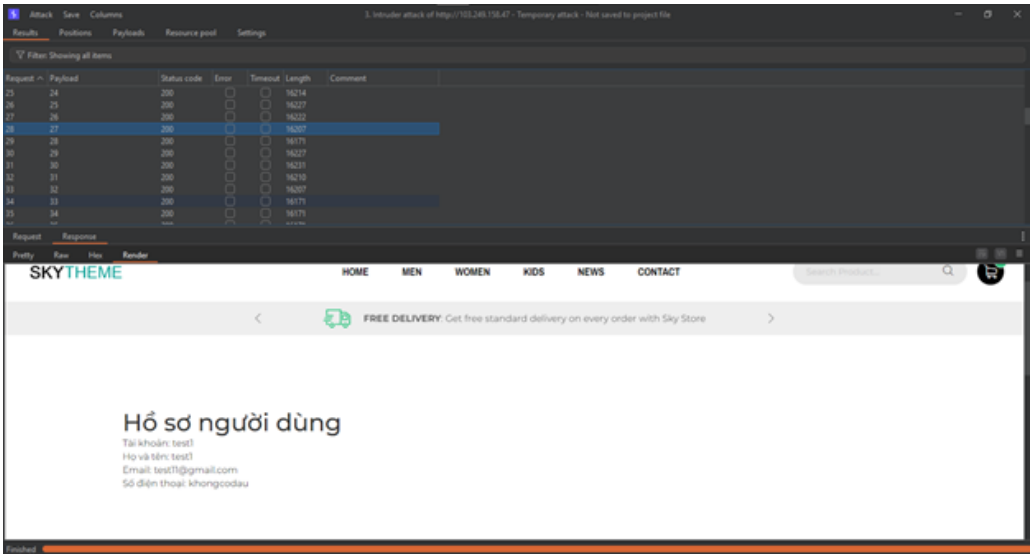
✅ Detailed Analysis

Vulnerability 1: Insecure Direct Object Reference (IDOR)

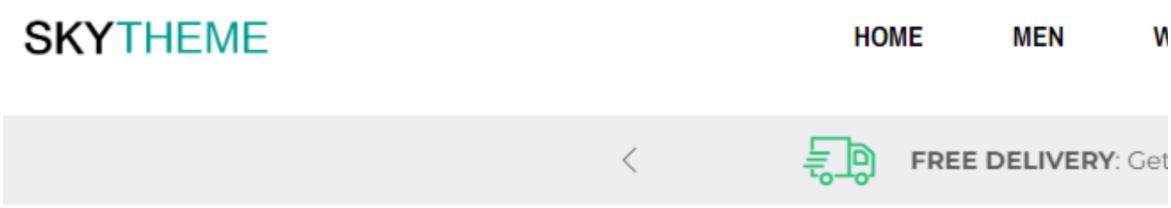
During the registration and login process, we examined the user information function. It was observed that the web application manages user IDs in a predictable manner. For instance, accessing a user's details can be done via a URL like `http://103.249.158.47/user-detail.php?id=32`, which suggests the presence of an IDOR vulnerability.



To confirm this, we utilized the intruder feature of the Burp Suite tool to test a range of user IDs from 0 to 100. Our tests revealed that the application indeed suffers from an IDOR vulnerability, as it allowed us to view the information of other users.

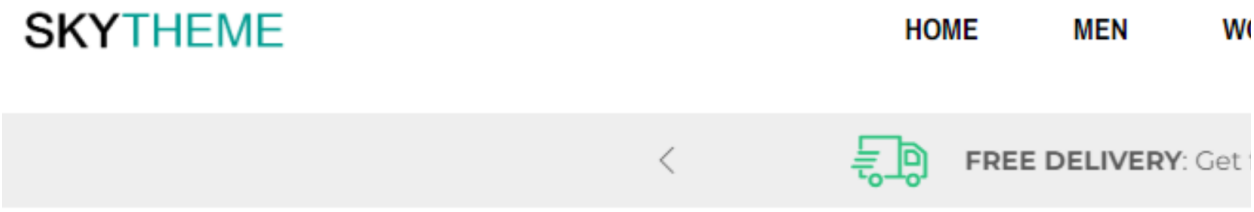


Through our investigation, we discovered two flags from user IDs 15 and 20.



Hồ sơ người dùng

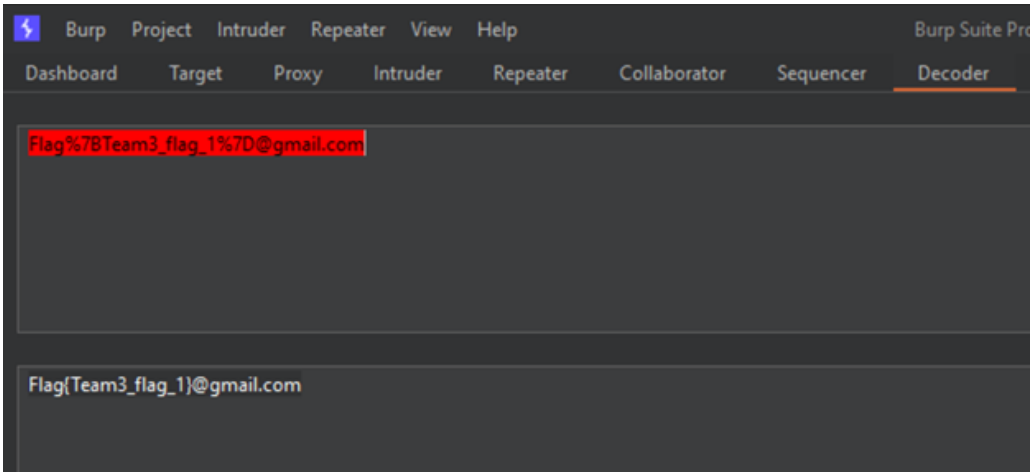
Tài khoản: truong
Họ và tên: Nguyễn Gia Trường
Email: Flag%7BTeam3_flag_1%7D@gmail.com
Số điện thoại: 0345382199



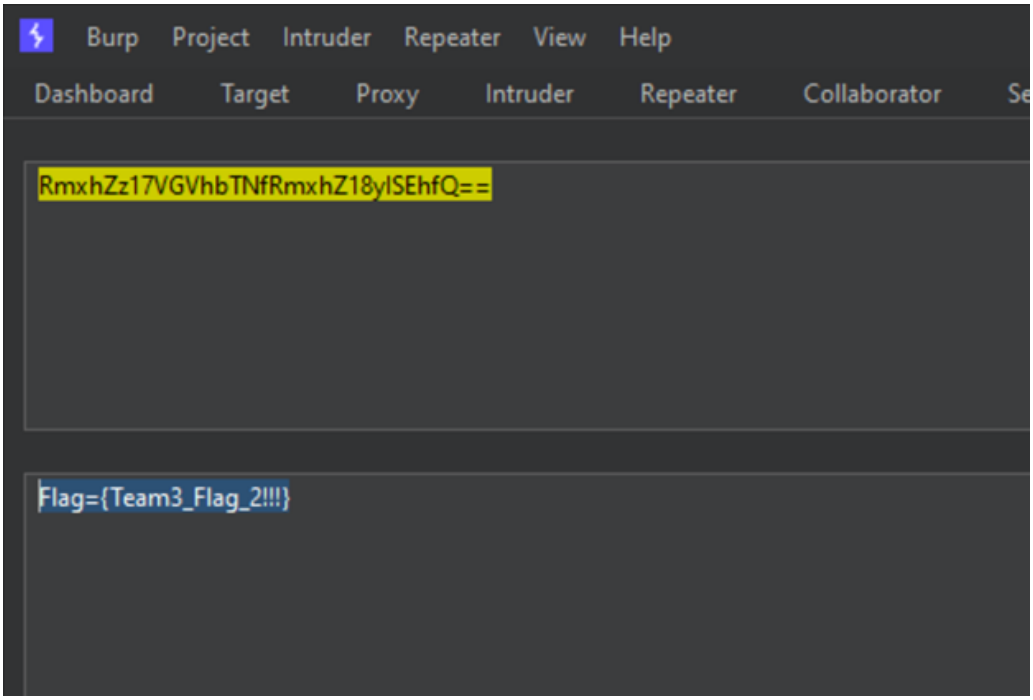
Hồ sơ người dùng

Tài khoản: test2
Họ và tên: test hai
Email: RmxhZz17VGVhbTNfRmxhZ18yISEhfQ==@gmail.com
Số điện thoại: 1233333333

We decoded these flags to retrieve the following:



Flag 1: `Flag{Team3_flag_1}`



- By decoding the Base64 encoded string from user ID 20, we obtained flag 2

Flag 2: `Flag={Team3_Flag_2!!!}`.

Vulnerability 2: SQL Injection

We identified a significant SQL injection vulnerability that can be exploited with knowledge of a valid username. For example, using the username "khanh" and the payload `khanh'OR'1`, we were able to successfully log in without needing a password.

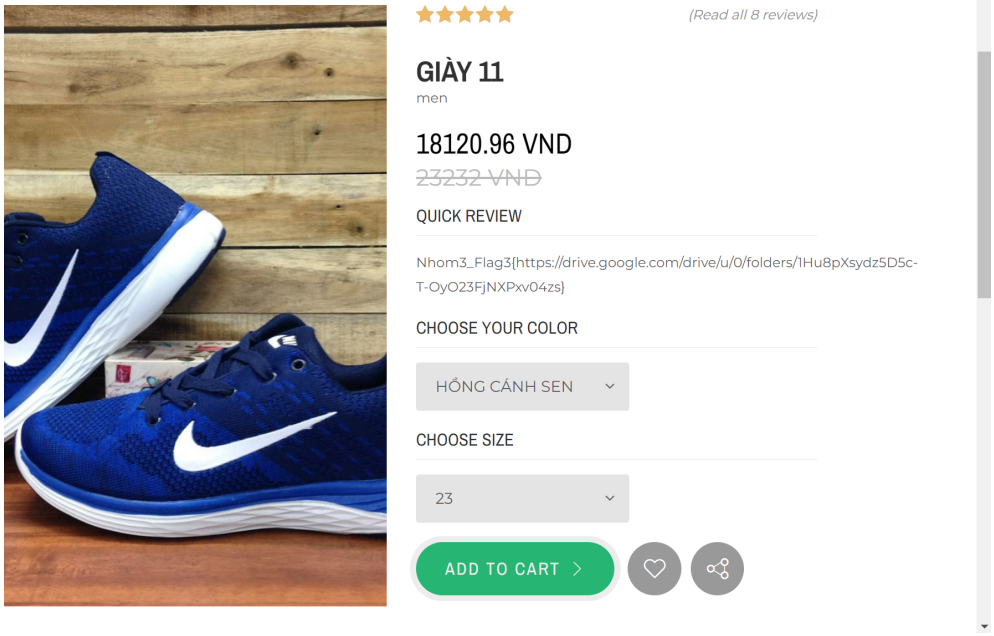
By combining this SQL injection vulnerability with the previously identified IDOR vulnerability, we could enumerate accounts, including the admin account, and gain unauthorized access to the admin

dashboard.

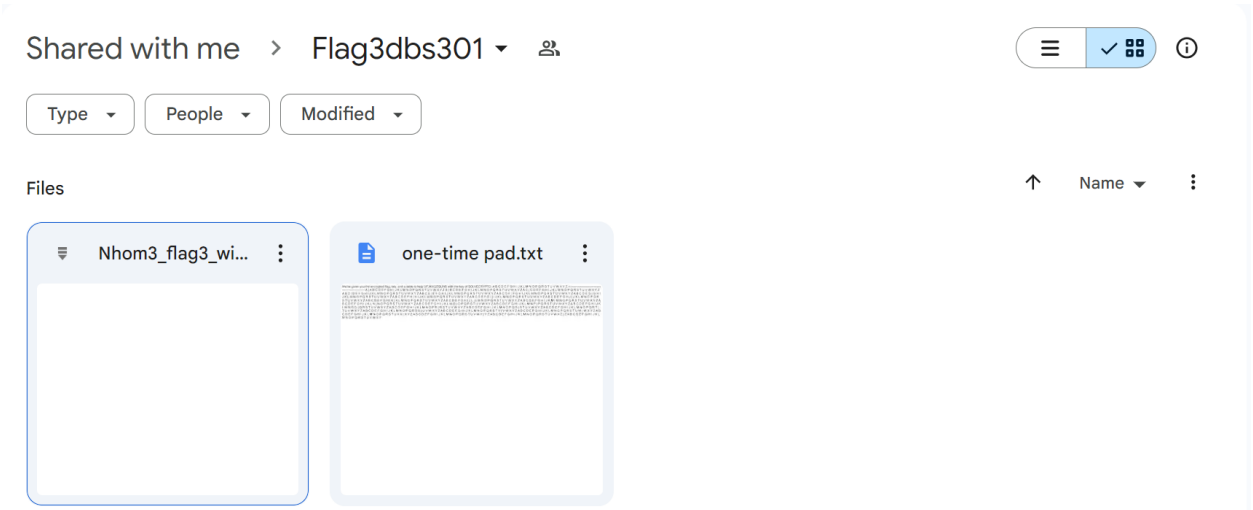
> https://prod-files-secure.s3.us-west-2.amazonaws.com/4c5285c3-faf9-4af8-b7f1-5b223ec82879/901e87c3-4bb5-4187-9b23-6fb68b84dd6f/2024-06-26_19-12-30_(online-video-cutter.com).mp4

Vulnerability 3: ?

When clicking on “GIÀY 11”, in the quick review section we can see a google drive link:



Click on the link, we have 1 zip file with password protected and 1 text file name `one-time pad`. We can guess that the text file will contain the password.

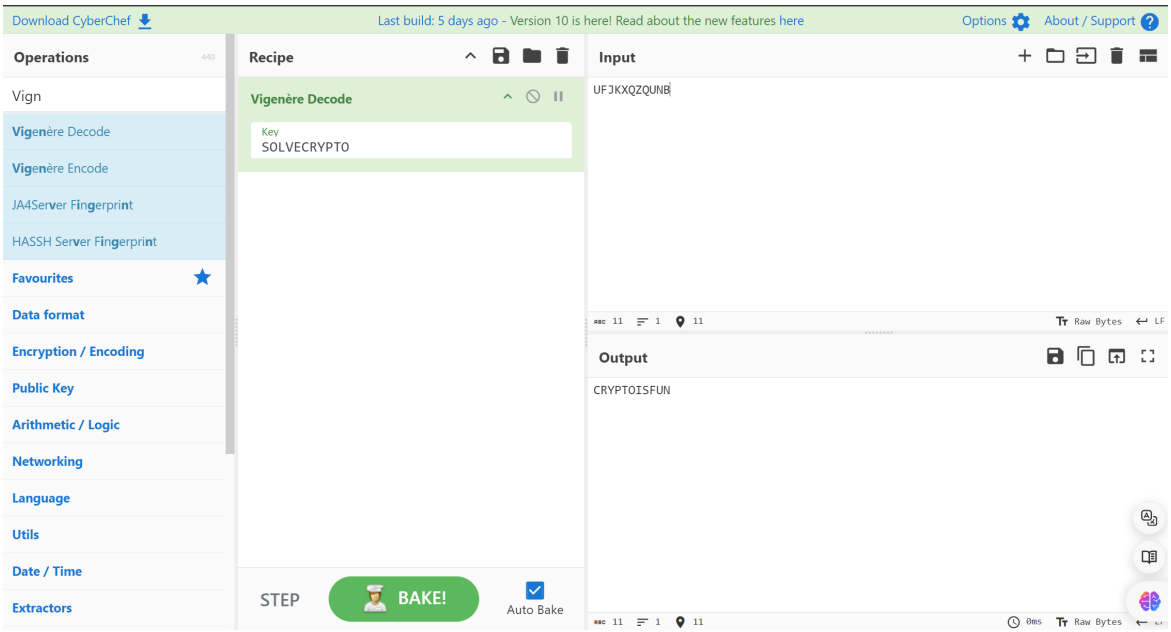


In the text file, we have a Vigenere table, with ciphertext is `UFJKXQZQUNB` and key is `SOLVECRYPTO`.

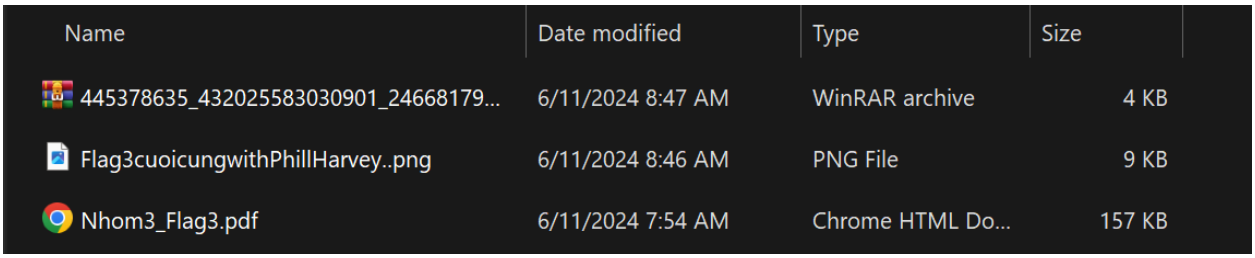
```
We've given you the encrypted flag, key, and a table to help UFJKXQZQUNB with the key of SOLVECRYPTO.


   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  +---------------------------------------------------
A | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B | B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C | C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D | D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E | E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F | F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G | G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H | H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I | I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J | J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K | K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L | L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M | M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N | N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O | O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P | P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q | Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R | R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S | S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T | T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U | U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V | V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W | W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X | X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y | Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z | Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

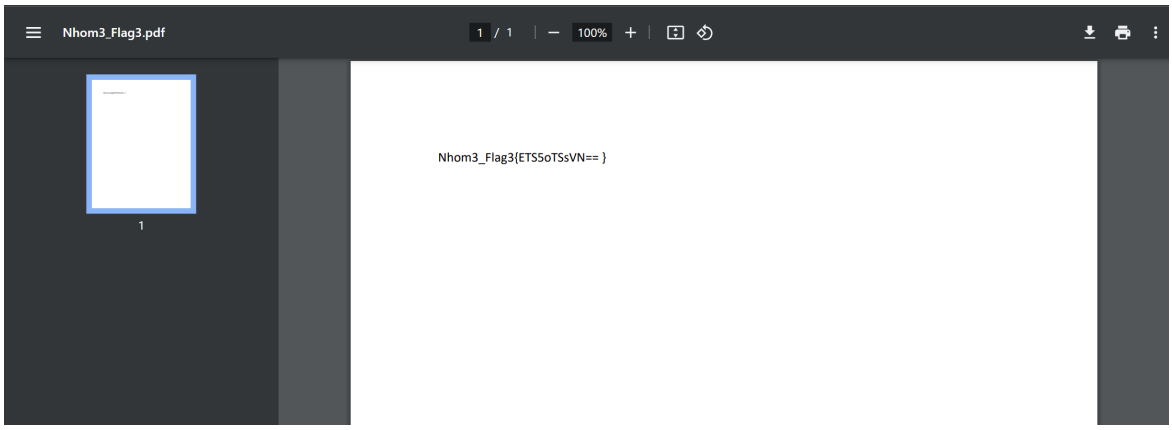
So we just need to decrypt it using Cyberchef and get the zip password



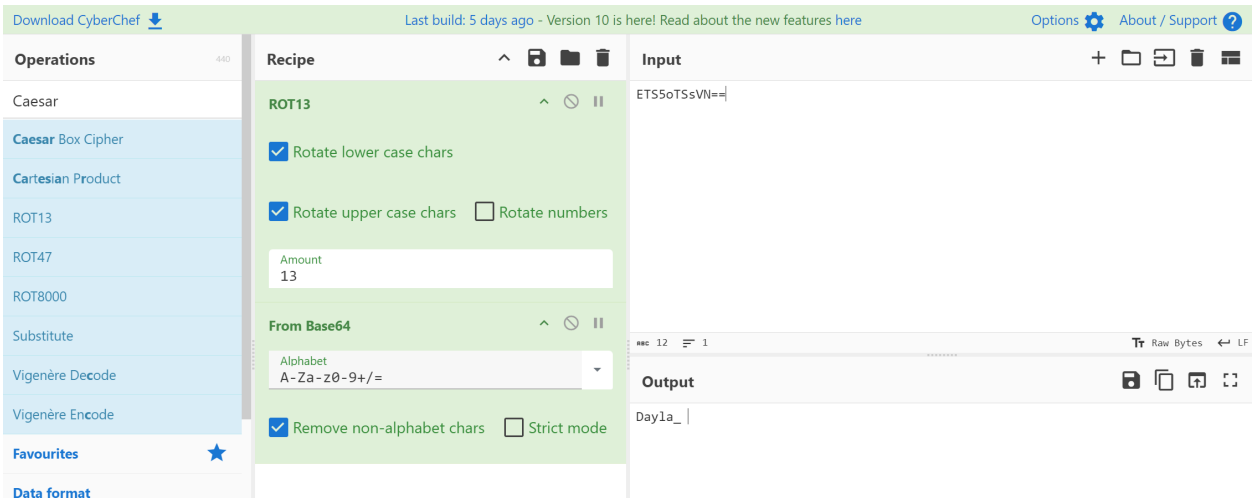
Using `CRYPTOISFUN` to extract the zip file, we have 3 more files:



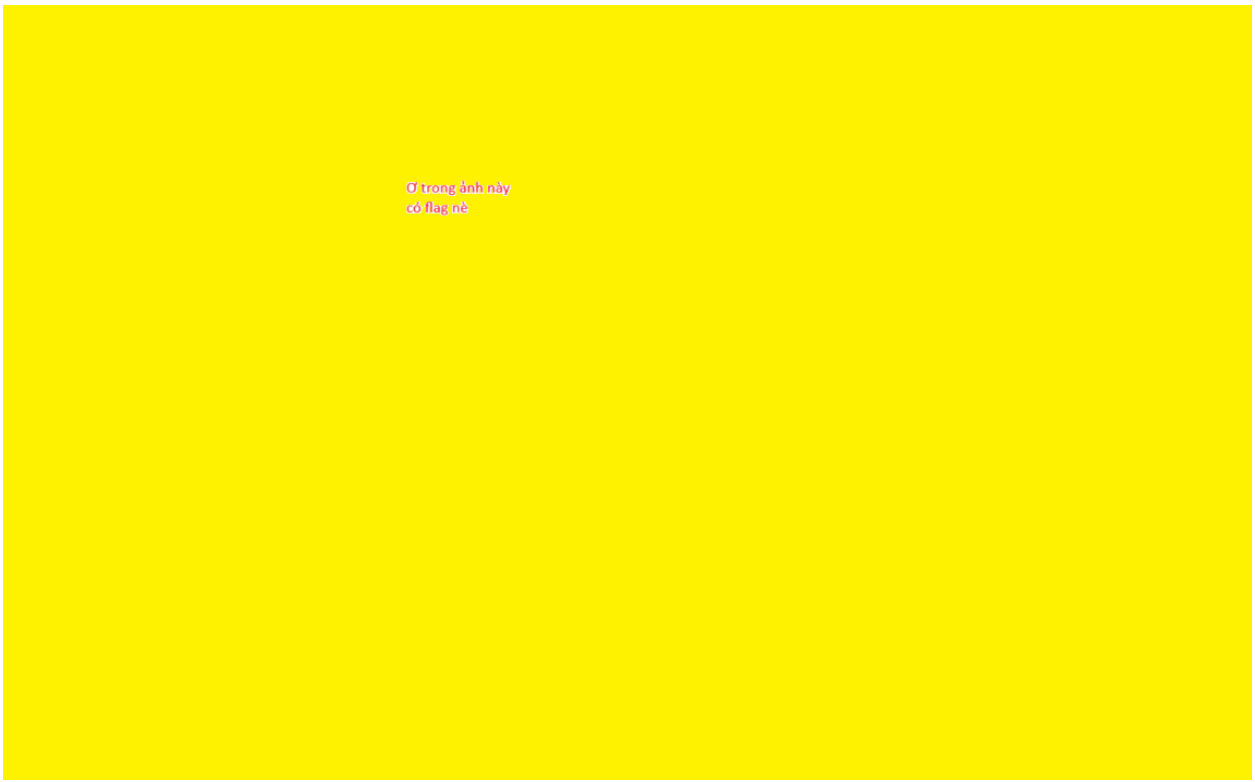
The zip file is password-protected, so let take a look at the remain 2 files. First is the pdf file:



We have a flag with some kind of encode. Based on the first zip file name is `Nhom3_flag3_with_casercipher_and_Base`, we can decode and got the first part of the flag:



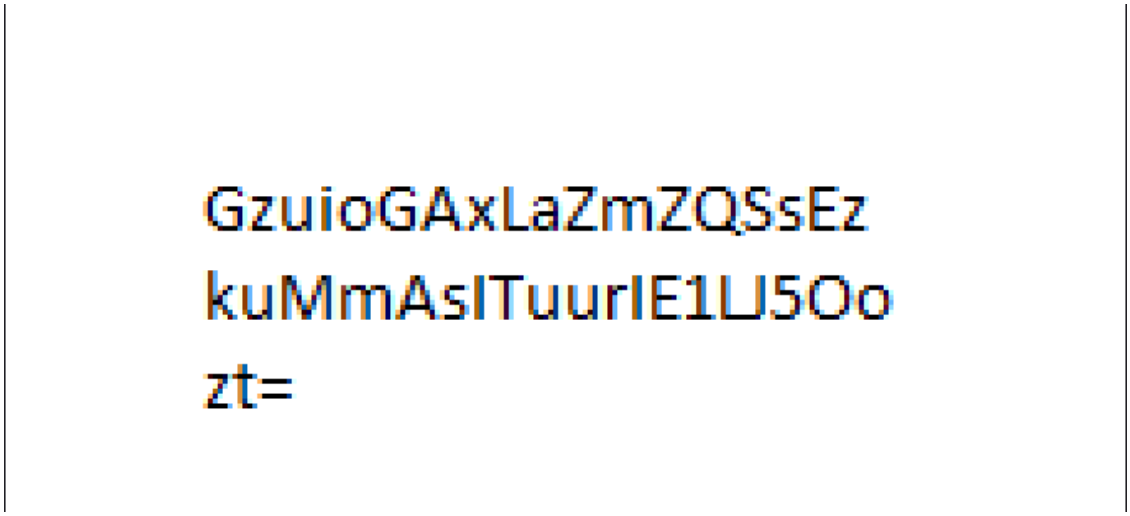
Now in the `.png` file, we have an image like that:



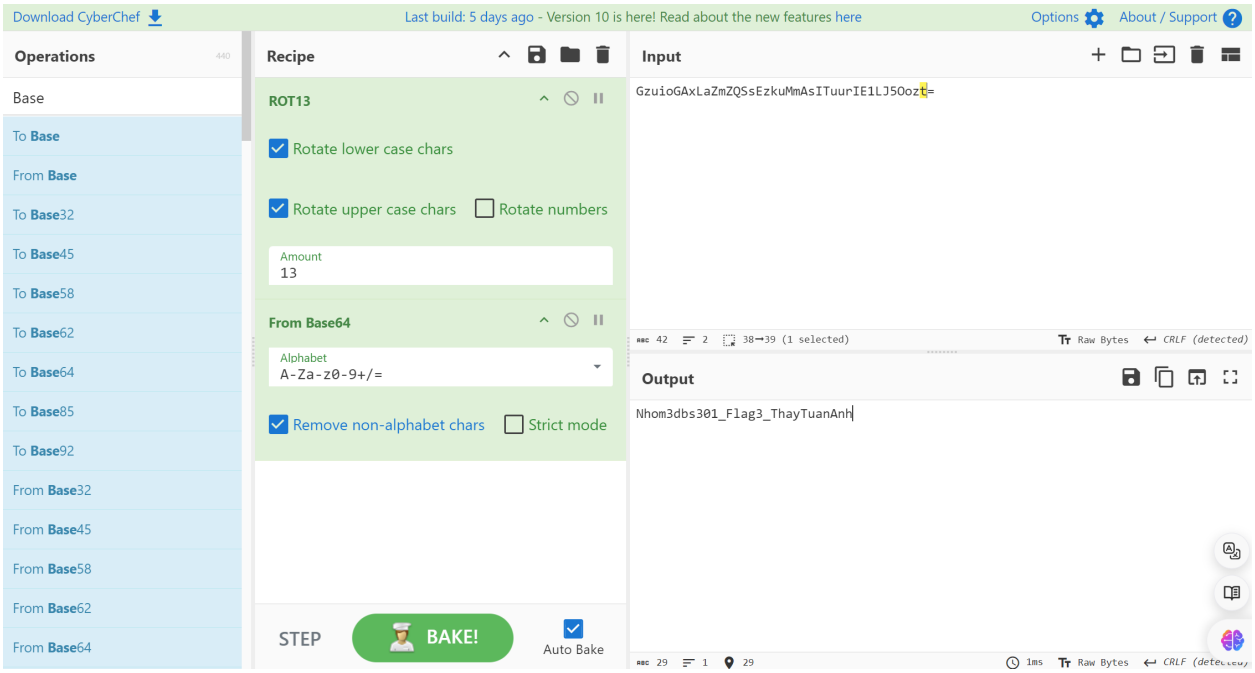
Nothing fancy. The only information I can get in the image is when I look at it metadata, I got the comment `flagcuoicungcuaFlag3`.

I'd thought for a long time just to find out what the password for the zip file was. After all, it was the comment above. What a guessing challenge!

The zip file contain an image:



Just like the `pdf` file, decode and got the last part of flag



Flag 3: `Nhom3_Flag3{Dayla_Nhom3dbs301_Flag3_ThayTuanAnh}`