

# 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

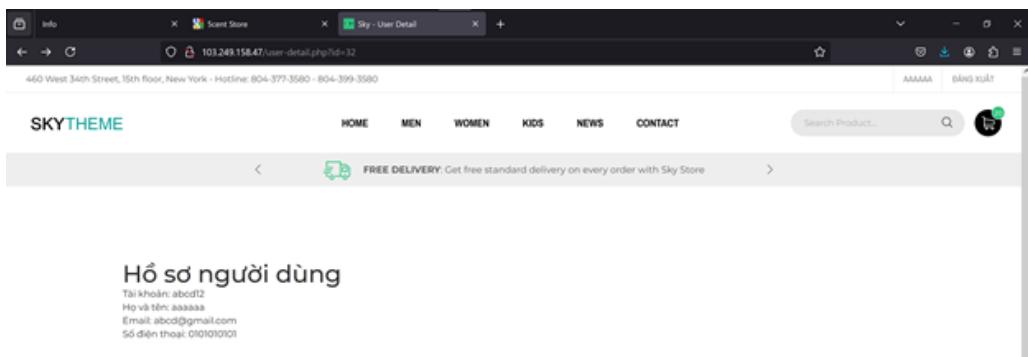
- A website that selling shoes

The screenshot shows a web browser window with multiple tabs open. The active tab is 'Sky - Homepage'. The page content includes a navigation bar with links for HOME, MEN, WOMEN, KIDS, NEWS, and CONTACT. There is also a search bar labeled 'Search Product...' and a shopping cart icon. A banner at the top right offers 'FREE DELIVERY' on every order. The main content area features a product listing for a pair of blue Nike shoes, with a small image showing a discount of '-22 %'.

## Detailed Analysis

### Vulnerability 1: Insecure Direct Object Reference (IDOR)

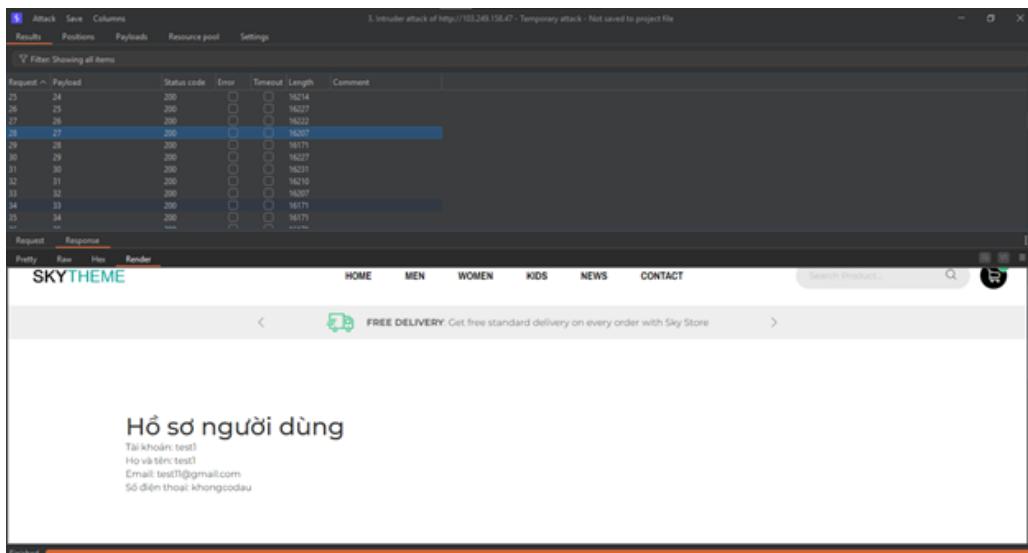
During the registration and login process, we examined the user information function. It was observed that the web application manages user IDs in a predictable manner. For instance, accessing a user's details can be done via a URL like <http://103.249.158.47/user-detail.php?id=32>, which suggests the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



The screenshot shows a web browser window with the URL <http://103.249.158.47/user-detail.php?id=32>. The page displays a user profile titled "Hồ sơ người dùng". The profile information includes:

- Tài khoản: abcd12
- Họ và tên: aaaaaa
- Email: abcd@gmail.com
- Số điện thoại: 0101010101

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.



The screenshot shows the Burp Suite Intruder tool interface. The "Payloads" tab is selected, showing a list of user IDs from 24 down to 15. The payload for user ID 20 is highlighted. The "Render" tab shows the response for user ID 20, which is identical to the one shown in the previous screenshot for user ID 32. The response displays the user profile for "Hồ sơ người dùng" with the following details:

- Tài khoản: test1
- Họ và tên: test1
- Email: test1@gmail.com
- Số điện thoại: khongcodau

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

&lt;



FREE DELIVERY: Get

## 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

&lt;



FREE DELIVERY: Get

## Hồ sơ người dùng

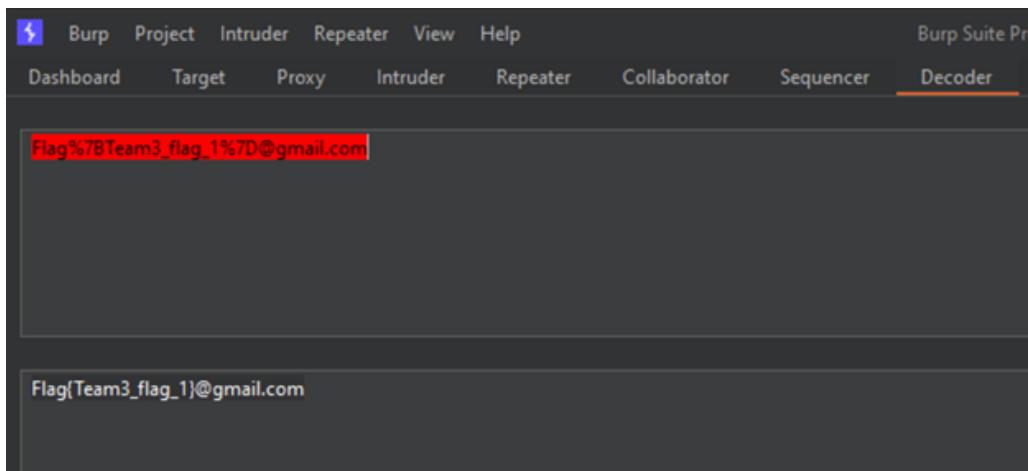
Tài khoản: test2

Họ và tên: test hai

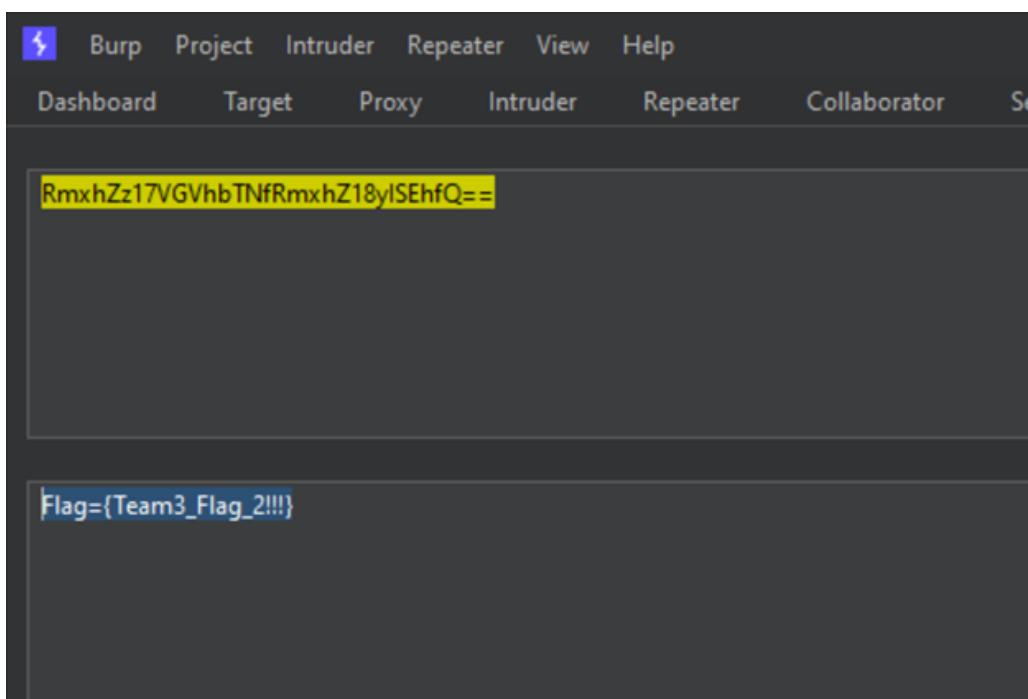
Email: RmxhZz17VGhbTNfRmxhZ18yISEhfQ==@gmail.com

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.

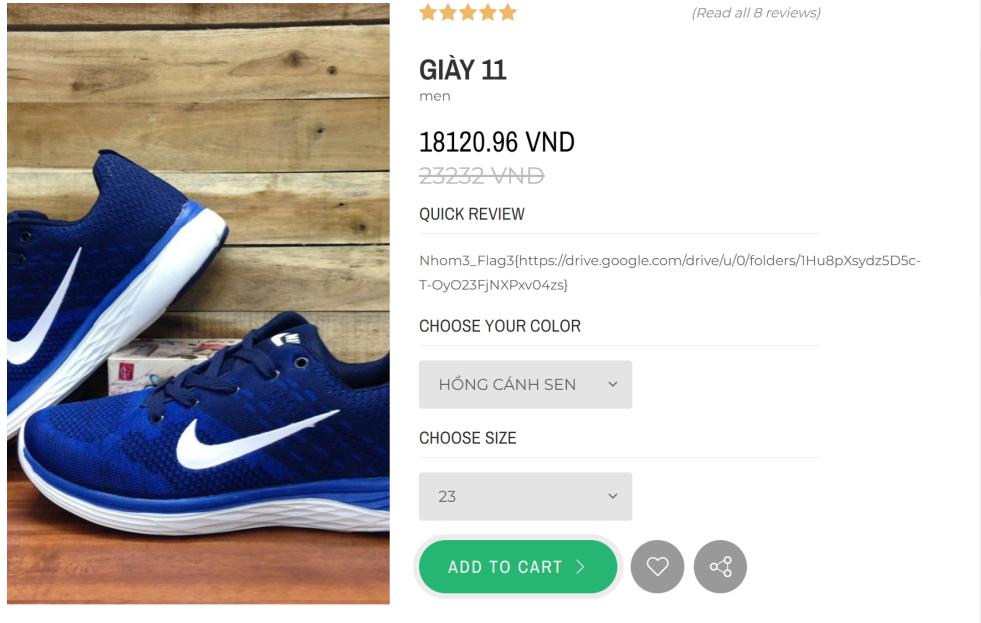
By combining this SQL injection vulnerability with the previously identified IDOR vulnerability, we could enumerate accounts, including the admin account, and gain unauthorized access to the admin

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\\_\(online-video-cutte.r.com\).mp4](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-cutte.r.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.

Shared with me > Flag3dbs301

Type People Modified

Files

Nhom3\_flag3\_wi... one-time pad.txt

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	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	W	X
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

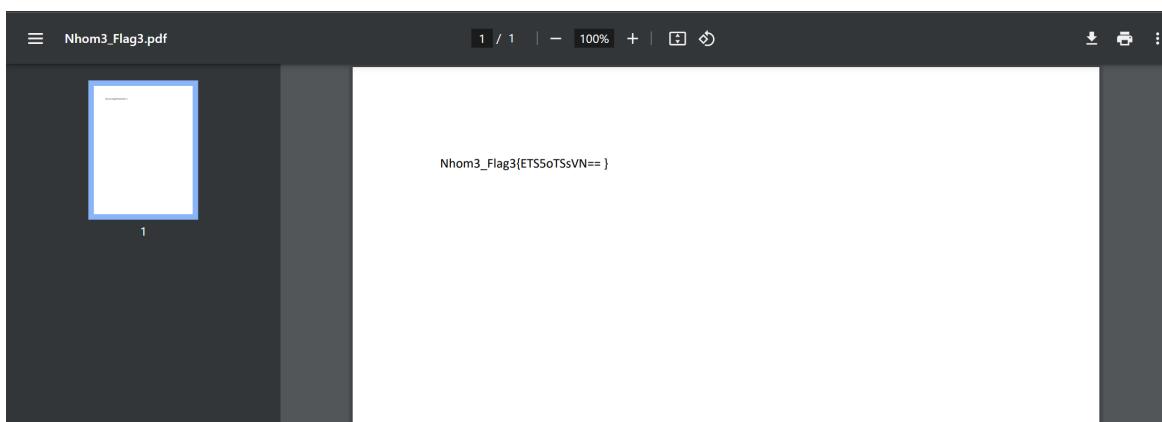
So we just need to decrypt it using Cyberchef and get the zip password

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like Vigenère Decode, Vigenère Encode, JA3Server Fingerprint, and HASSH Server Fingerprint. The main area has a 'Recipe' section titled 'Vigenère Decode' with a 'Key' field containing 'SOLVECRYPTO'. The 'Input' field contains 'UFJJKXQZQUNB' and the 'Output' field shows 'CRYPTOISFUN'. At the bottom, there's a 'BAKE!' button and an 'Auto Bake' checkbox.

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

Name	Date modified	Type	Size
445378635_432025583030901_24668179...	6/11/2024 8:47 AM	WinRAR archive	4 KB
Flag3cuoicungwithPhillHarvey..png	6/11/2024 8:46 AM	PNG File	9 KB
Nhom3_Flag3.pdf	6/11/2024 7:54 AM	Chrome HTML Do...	157 KB

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:

Download CyberChef [Download](#)

Last build: 5 days ago - Version 10 is here! Read about the new features [here](#)

Operations 440

**Caesar**

**Caesar Box Cipher**

**Cartesian Product**

**ROT13**

Rotate lower case chars

Rotate upper case chars  Rotate numbers

Amount  
13

**From Base64**

Alphabet  
A-Za-z0-9+=

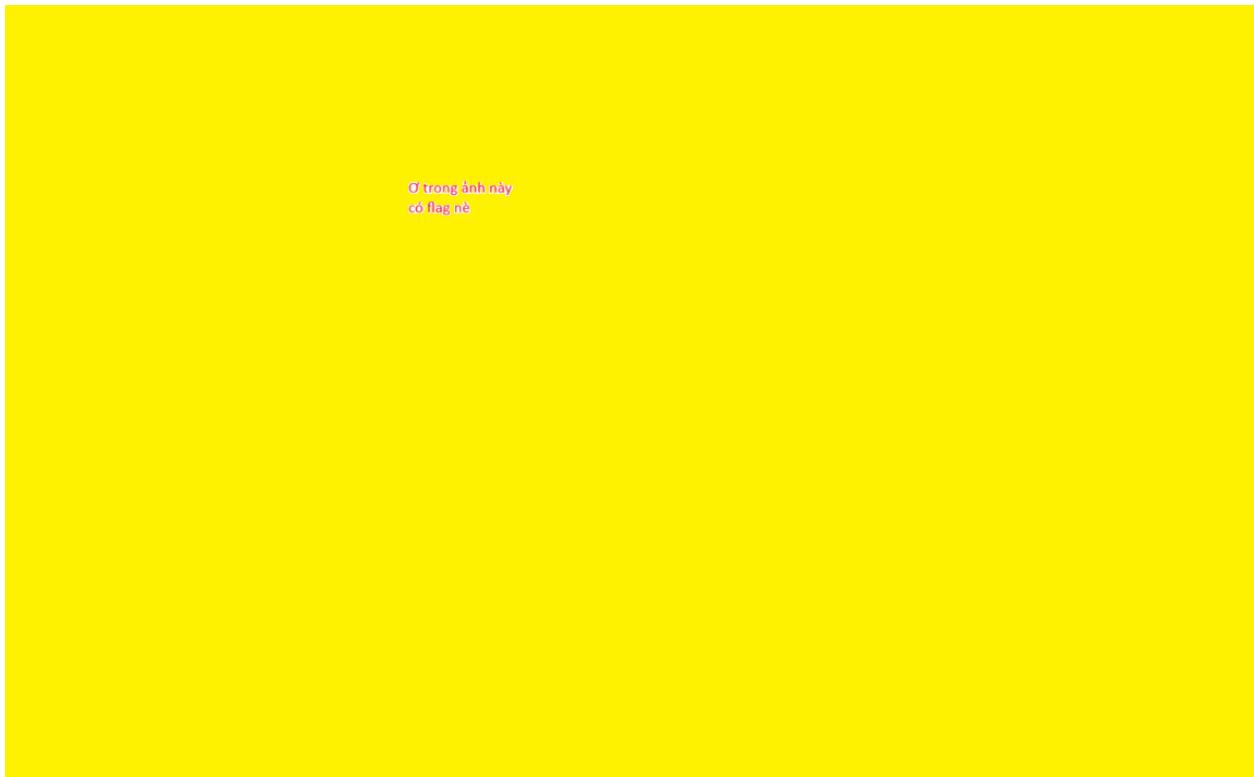
Remove non-alphabet chars  Strict mode

Input  
ETSS5oT5sVN==

Output  
Dayla\_

Raw Bytes LF

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

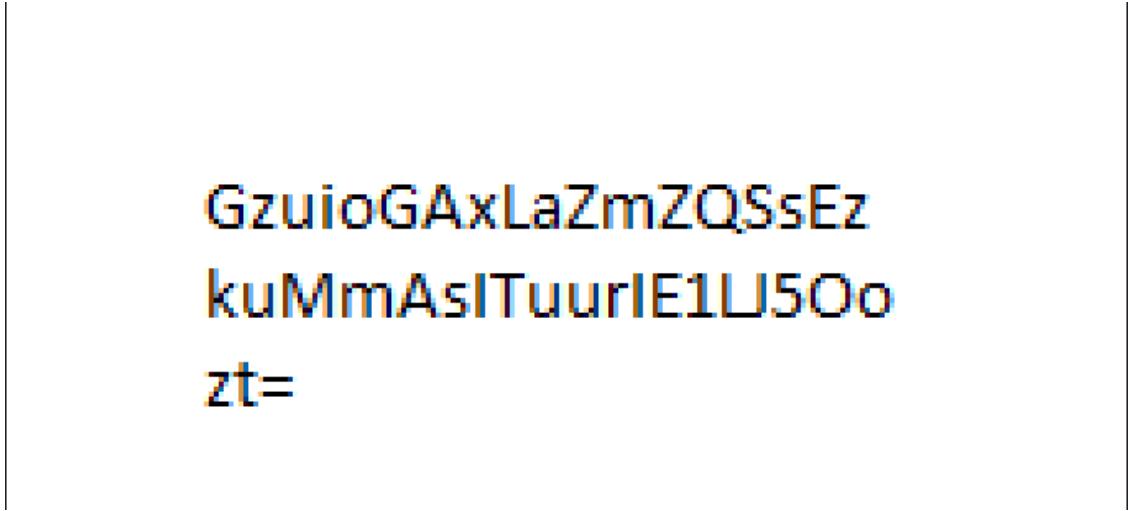


Nothing fancy. The only information I can get in the image is when I look at its metadata, I got the comment `flagcuoicungcuaFlag3`.

ExifTool	
Filter	Adaptive
Interlace	Noninterlaced
SRGBRendering	Perceptual
Gamma	2.2
Comment	flagcuoicungcuaFlag3
PNG-PHYS	
PixelsPerUnitX	4724
PixelsPerUnitY	4724

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:



GzuioGAxLaZmZQSsEz  
kuMmAsITuurlE1LJ5Oo  
zt=

Just like the [pdf](#) file, decode and got the last part of flag

Download CyberChef [Download](#)

Last build: 5 days ago - Version 10 is here! Read about the new features [here](#)

Operations      440

Recipe      ^

Input

Base

To Base

From Base

To Base32

To Base45

To Base58

To Base62

To Base64

To Base85

To Base92

From Base32

From Base45

From Base58

From Base62

From Base64

ROT13

Rotate lower case chars

Rotate upper case chars  Rotate numbers

Amount  
13

From Base64

Alphabet  
A-Za-zA-Z0-9+=

Remove non-alphabet chars  Strict mode

Output

GzuiogAxLaZmZQSSezkuMmAsITuurIE1LJ50ozt=

nhom3dbs301\_Flag3\_ThayTuanAnh

STEP Auto Bake

Raw Bytes CRLF (detected)

sec 42    2    38-39 (1 selected)    Raw Bytes CRLF (detected)

sec 29    1    29    Raw Bytes CRLF (detected)

1ms    Raw Bytes CRLF (detected)

▶ **Flag 3:** Nhом3\_Flag3{Dayla\_Nhom3dbs301\_Flag3\_ThayTuanAnh}