

Projet Sécurité: CTF



GROUPE	BACKDOOR	Solution
PHASE 1	DEVELOPPEMENT CTF	CRYPTO
NIVEAU	MOYEN	

Ce CTF contient 4 Flag

Flag 1:

En inspectant la page on repère que le flag a été chiffré en utilisant un chiffrement en décalage 10

172.10.80.221/crypto_moyen/

Défi 1: Bienvenue dans le chat!

PVKQ*♠V1knwsxs}~|k~o△|■

[Suivant](#)

Inspector

```
<div class="content white-text">
  <h1>Défi 1: Bienvenue dans le chat!</h1>
  <p>
    <!--decalage 10-->
    PVKQ*♠V1knwsxs}~|k~o△|■
  </p>
  <a class="blue-button" href="page2.html">Suivant</a>
</div>
</body>
</html>
```

html > body.black-bg > div.content.white-text > h1

Layout

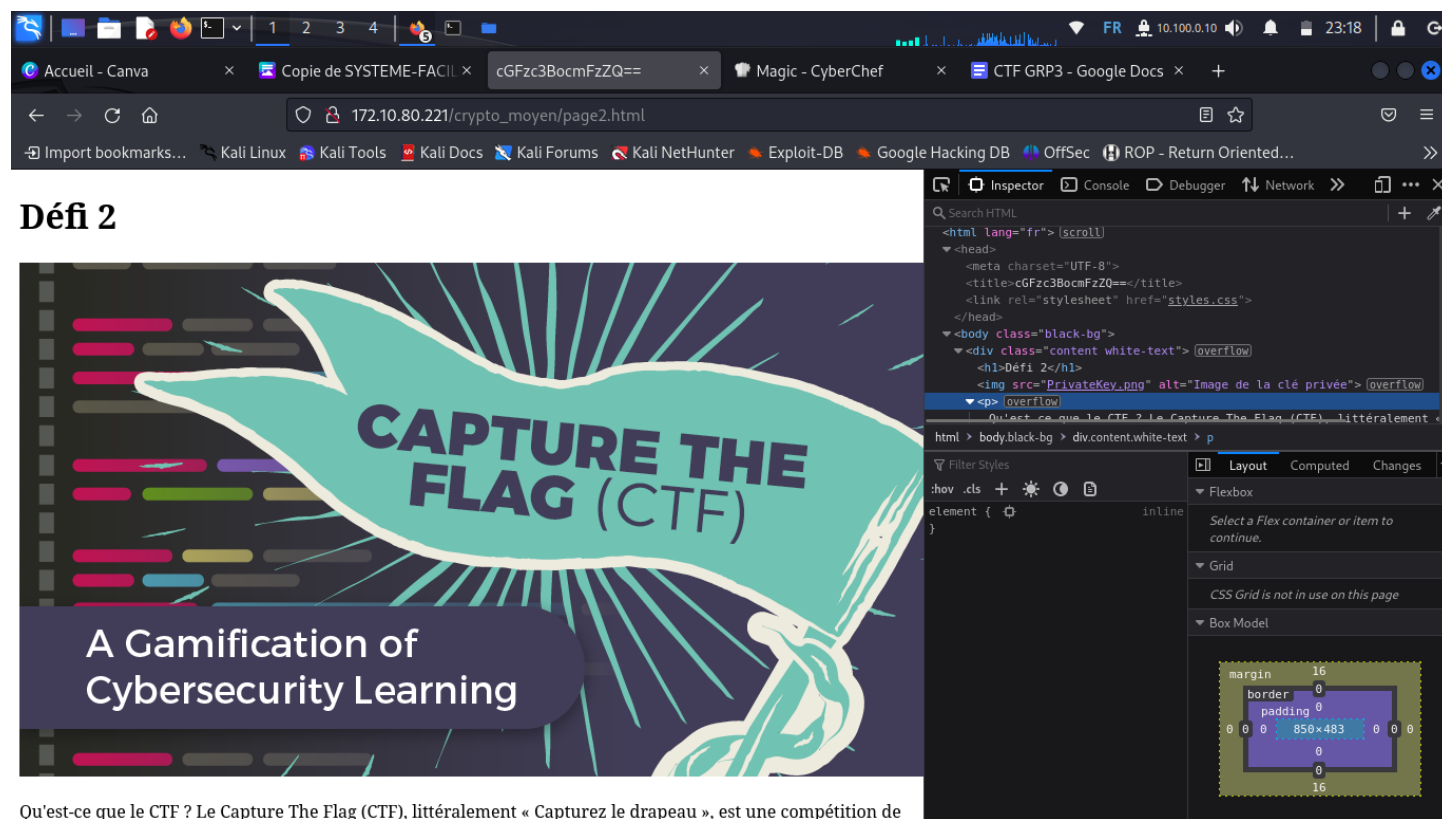
margin 0
border 0
padding 0
0 0 0 850x128.433 0 0 0

En utilisant un site en ligne de déchiffrement nous pouvons facilement retrouvé le flag :

FLAG {L'administrateur}

Flag 2:

On inspecte le site web:



Défi 2

Qu'est-ce que le CTF ? Le Capture The Flag (CTF), littéralement « Capturez le drapeau », est une compétition de

Nous pouvons remarquer qu'il s'agit d'un chiffrement asymétrique par la présence de clé privée. Nous devons récupérer 3 informations:

- La clé privée (image)
- passphrase (head)
- le chiffré (en commentaire)

1/ La clé privée : Stéganographie image

Accueil - Canva x Copie de SYSTEME-F / x cGFzc3BocmFzZQ== x RSA Decrypt - CyberC x Online Steganography x From Base64 - CyberC x

https://manytools.org/hacker-tools/steganography-encode-text-into-image/go/

Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec ROP - Return Oriented...

Image to Byte array

Une visite immersive étonnante.

Here it is!

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQCuDP+0AGaroAd5HcJh+ENQ4BHYv50omzq+9uJ5Lms5P9hd009U
4RchQt/vkTvWQueyu3hhNmWZoE0Bw520nmS+GHu1ARcvYCrotaLNSR80i3Z67Rmp
IeXz30929jn30Hxou+WwQdsuUVH6cNDjL+YD6Ucw/dRzGIGvqi rawvE6eQIDAQAB
AoGACuTxBpADhAJcvRuWj4YL9AI0HeuMraQoCtsMKDtXrhF3hKdmsYWSu7cFkqK
7UzPycRLFpeur/n8r+00mQD7WEjdWziehN2MqxMmqmz0C4FgUB3D3N5vnKFZBMVL
7VYes0srxzLvpsnDbHlzIa2M8a4UYd1YmGP7orzCX13KXgUCQQDhiJu2ZMnCid5m
U5r2FW4Jn9r4xgTQ2ryeldX/KIuP3hclvMRtBmSjyT93H6j8ijTB52vrFkclSUOK
J5oMQHYtAkeAxyP980C2XLmHvkGtNx6iYstS+1ZqafHnd0idQJ8RJ6VsW2YrTfs
PEDugWmt0uvuPaIxe5KILQ3Q0IcwNeQw/QJAbUdva5qkdEDL01kRTcmmbriPMX9p
V/WUzVaWwTLZJNwc66kii7aCuoyr1sGddPhWdnnXZqG00LcrfVwXB1j5QJABvb1
ntA4j09WmqZFjxzmDmpfuHjrm2T0R1/HKfhhaIRvXWmuaIE8BM5/1Pso/xaHNZG7
zc3UjkkbHAplLqAM/QJABpZ01NY4stUhuEXI+XUDf0hZSGiQ53m8FUMPgRzbq7uT
cxwSr5ofarnwxU4ZpON42wf7CqcfdsRqt1sbAew5wA==
-----
```

The past few weeks you may have seen a server error or two on the steganography tool. These intermittent errors were a byproduct of the recent server move and have now been fixed.

July 15, 2022
[Phasing out hosting server after \(almost\) 10 years](#)

After having been running steadily on the previous server for almost ten(!) years, it became time to retire that machine. So, ManyTools has now been moved to a shiny new hosting cluster. You may/should notice some speed improvements. In case you notice any problems or irregularities I'd be happy if you notify me so I can check on them.

September 27, 2017
[Exit Coinhive \(in-browser bitcoin mining\)](#)

Thank you for your feedback on our (brief) browser based bitcoin mining. This like a nice way to support this but turned out to be far too much for our visitors. So we've removed it. Our apologies for the

Full-stack observability drives value with IT tool consolidation. solarwinds READ EBOOK

2/Passphrase:

Download CyberChef Last build: 21 hours ago - Version 10 is here! Read about the new features here Options About / Support ?

Operations Recipe Input

Search...

Favourites ★

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

From Base64

Alphabet A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP BAKE! ☒ Auto Bake

cGFzc3BocmFzZQ==

Output

passphrase

3/ On déchiffre le message:

The screenshot shows the CyberChef web application. The 'Recipe' tab is selected, displaying a sequence of operations: 'From Base64' and 'RSA Decrypt'. The 'Input' field contains a long Base64-encoded string. The 'Output' field shows the decrypted result: 'FLAG { Bobby }'. The interface includes various operation buttons on the left, a central recipe editor, and a right-hand panel for input/output and raw bytes.

FLAG { Bobby }

Flag 3:

On inspecte la page web

The screenshot shows a web browser displaying the HTML source code of a page. The page title is 'Défi 3'. The HTML structure includes a head section with meta tags and a body section with a black background. The main content area contains a paragraph about cryptography and a button labeled 'Précédent'. The browser's developer tools are open, showing the HTML structure and the 'Layout' tab.

On remarque qu'il s'agit d'un chiffrement symétrique aes on a besoin de la clé qu'on retrouve dans l'image et le message chiffré.

1/ Stéganographie image

Steganography Online

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Browse... aeskey.png

Decode

Hidden message

la clé de chiffrement de la troisième partie du mot de passe

Input

2/ Déchiffrer :

CyberChef

Last build: 21 hours ago - Version 10 is here! Read about the new features here

Options About / Support

Operations

Recipe

AES Decrypt

Key

la clé de chiffrement de la troisième partie du mot de passe

HEX

IV

HEX

Mode

ECB

Input

Hex

Output

Raw

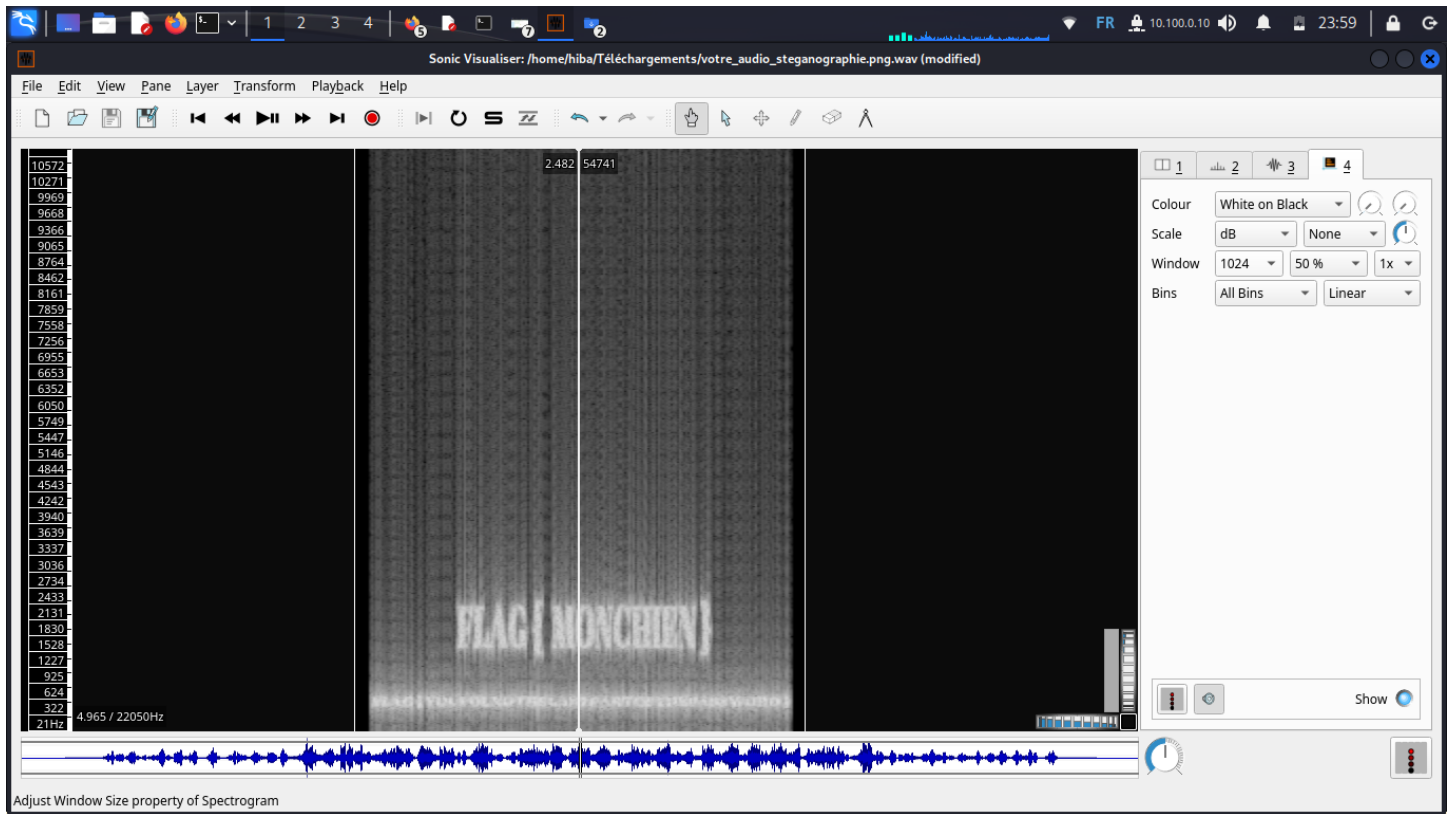
Input

5ee03b70361f511b91f6263bcd5c9f1

Output

24.01.2024

FLAG 4+5:



FLAG { MONCHIEN }

FLAG { YOUFOUNDTHELASTPARTOFTHEPASSWORD }