02 Walkthrough

Apprenant	Date	Sujet	Nom du CTF
Michel MEIRESONNE	25/01/2023	Cryptographie Résolution	Base-Ball

Résolution

TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9

Déterminer le type de chiffrement

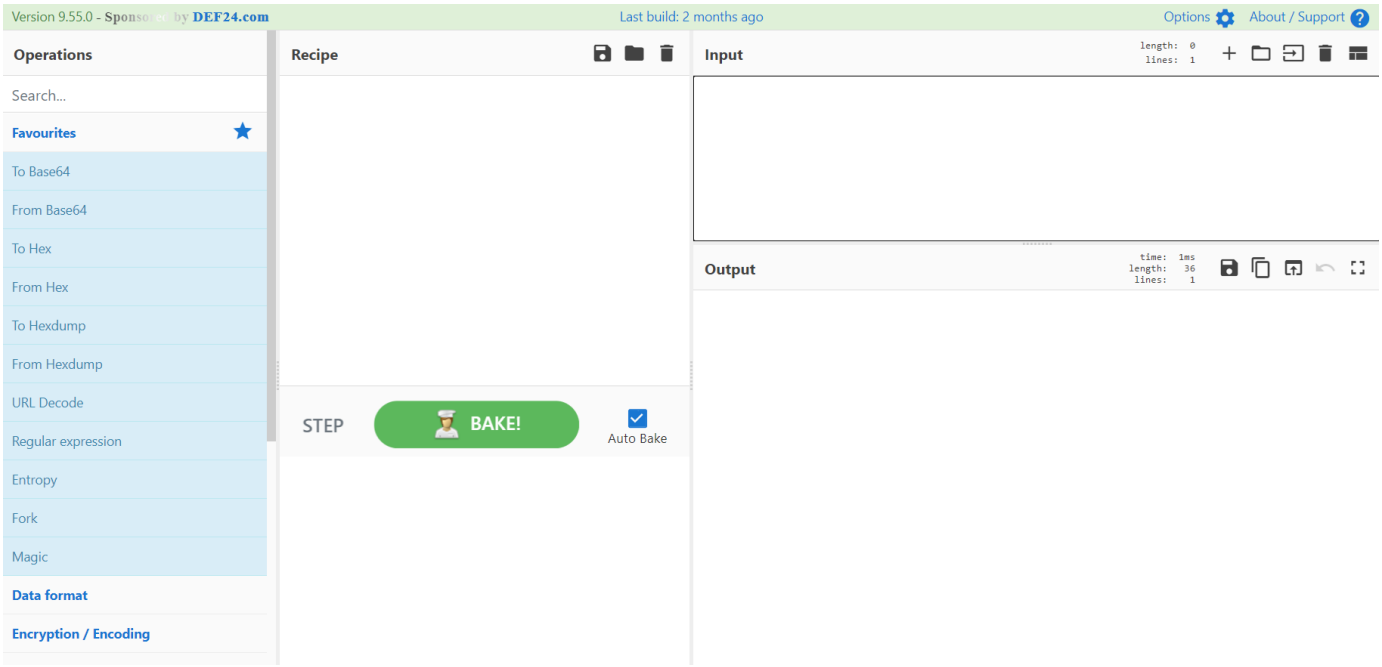
Sur Dcode on peut identifier rapidement le type.

Résolution en ligne

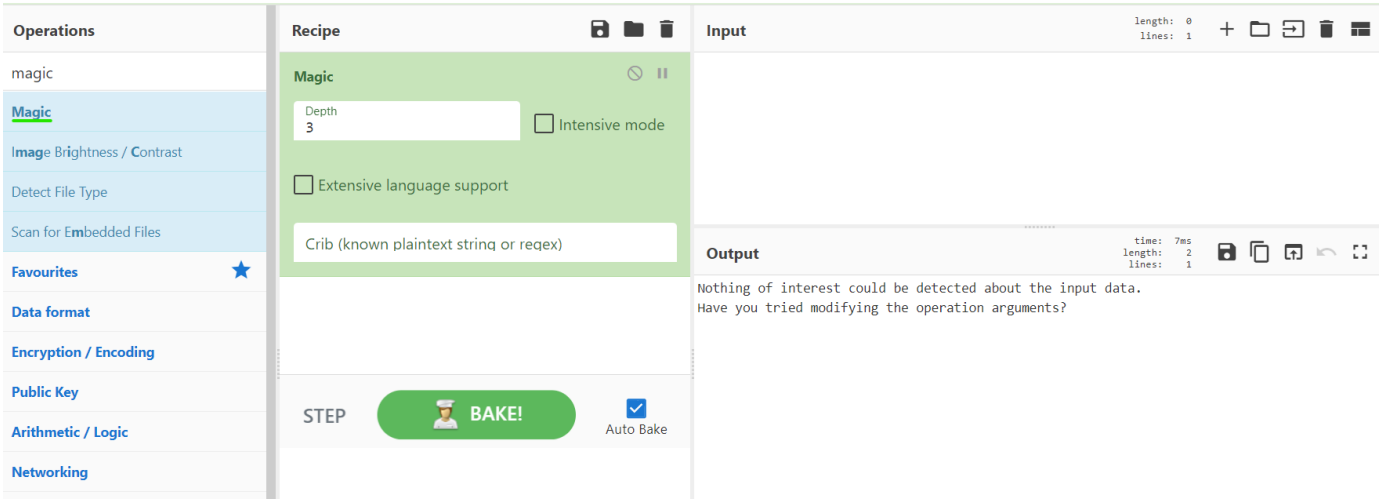
Il existe plusieurs sites pour déchiffrer, par exemple

- Cyberchief
- Dcode
- Online-toolz

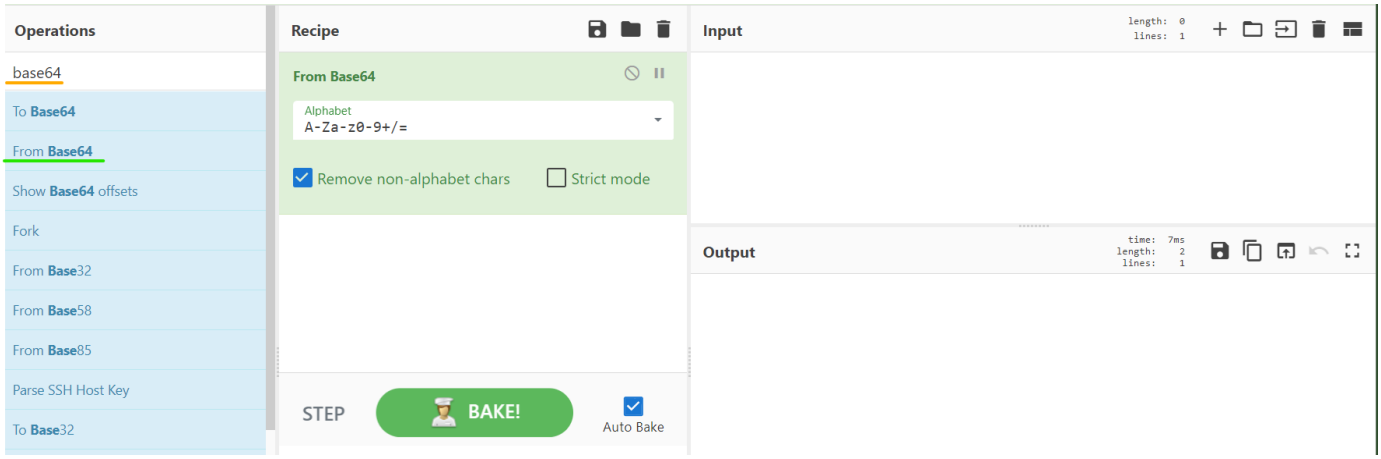
Ici on le fait avec [Cyberchief]



- **avec Magic**
  - Si le type de chiffrement est indéterminer
    Dans la partie Opération on chercher Magic, puis la fait glisser vers Recipe.



- **avec From base64**
  - Si il a trouver que c'est du base64
    Dans la partie Opération on chercher From Base64, puis la fait glisser vers Recipe.



Puis on colle le chiffré

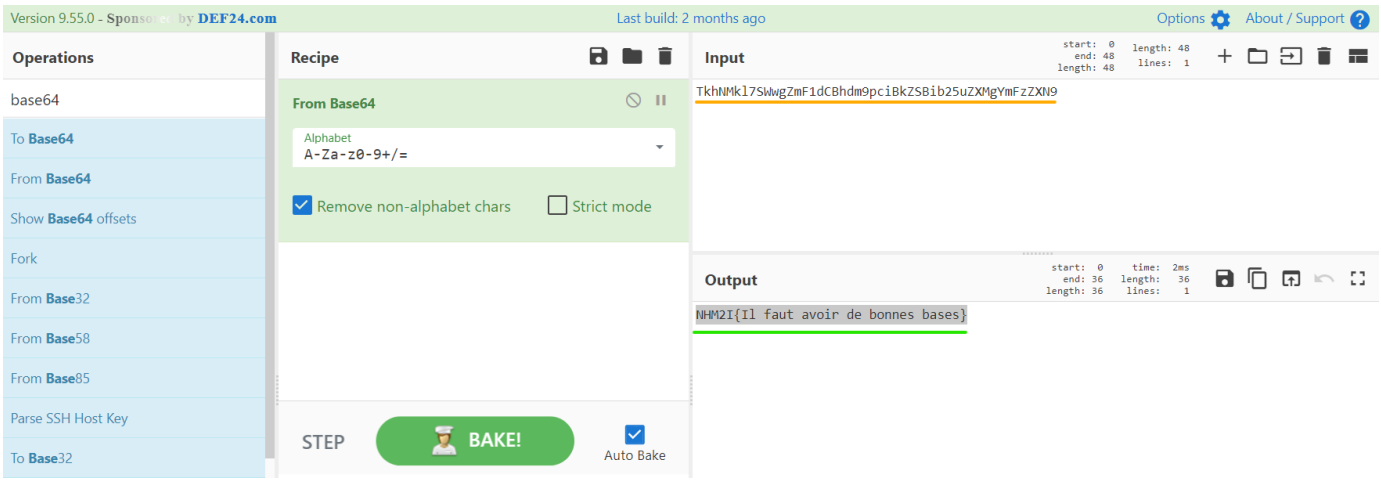
`TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9`

dans Input.

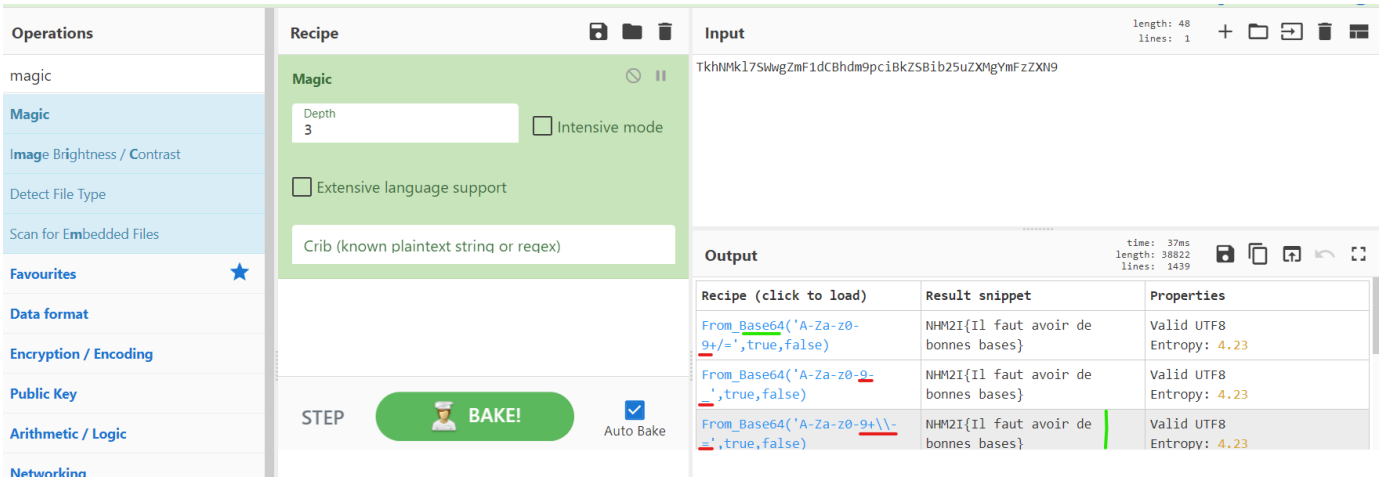
Le message déchiffré s'affiche dans Output

NHM2I{Il faut avoir de bonnes bases}

avec From base64



avec Magic



Le déchiffrement en lignes de commande

On utilise la commande

```
echo -ne TkhNMkl7SWwgZmF1dCBhdm9pciBkZSBib25uZXMgYmFzZXN9|base64
# Flag{drapeau d'initiation}
```

Bonus

Source: *https://www.dcode.fr/code-base-64*

Qu'est-ce que l'encodage Base64 ?

Base64 est un codage informatique utilisant 64 caractères pour encoder n'importe quelle chaine binaire avec du texte (il est notamment utilisé pour les emails).

Pourquoi utiliser la Base64 ?

Un message codé en Base64 contiendra uniquement des caractères ASCII imprimables ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=

Cette propriété permet de transmettre n'importe quelles données sur des systèmes originellement prévue pour ne transmettre que du texte (sans avoir à se soucier de l'encodage initial ni de la manière dont les caractères apparaitrons sur l'écran du destinataire du message)

Qu'est-ce que Base64URL ?

Base64URL est une variante de Base64 adaptée aux URL (http). Les caractères 62 + et 63 / peuvent poser des problèmes dans les URL, les remplacer alors par respectivement - et _. De plus, le = est quant à lui supprimé.

Quand Base64 a-t-il été inventé ?

La Norme RFC 2045 qui officialise Base64 date de 1996