



Writeups Capture The Flag

#GCSC2022

Writeups rédigé par *NGOUNOU Loic Kopper* participant au CTF
ID : *kitronghd*

Sommaire

1. Capture_Madagascar – Acces au serveur discord

La resolution de ce challenge s'est fait pas la récupération du lien de discord. Le lien correspondant est celui qui apparait lors du survol du lien tout à gauche du navigateur qui est *discord.gg/3gvtd8N6*.

Le format du flag est donc : *GCSC2022{ discord.gg/3gvtd8N6}*

capture_Madagascar – Acces au serveur discord!

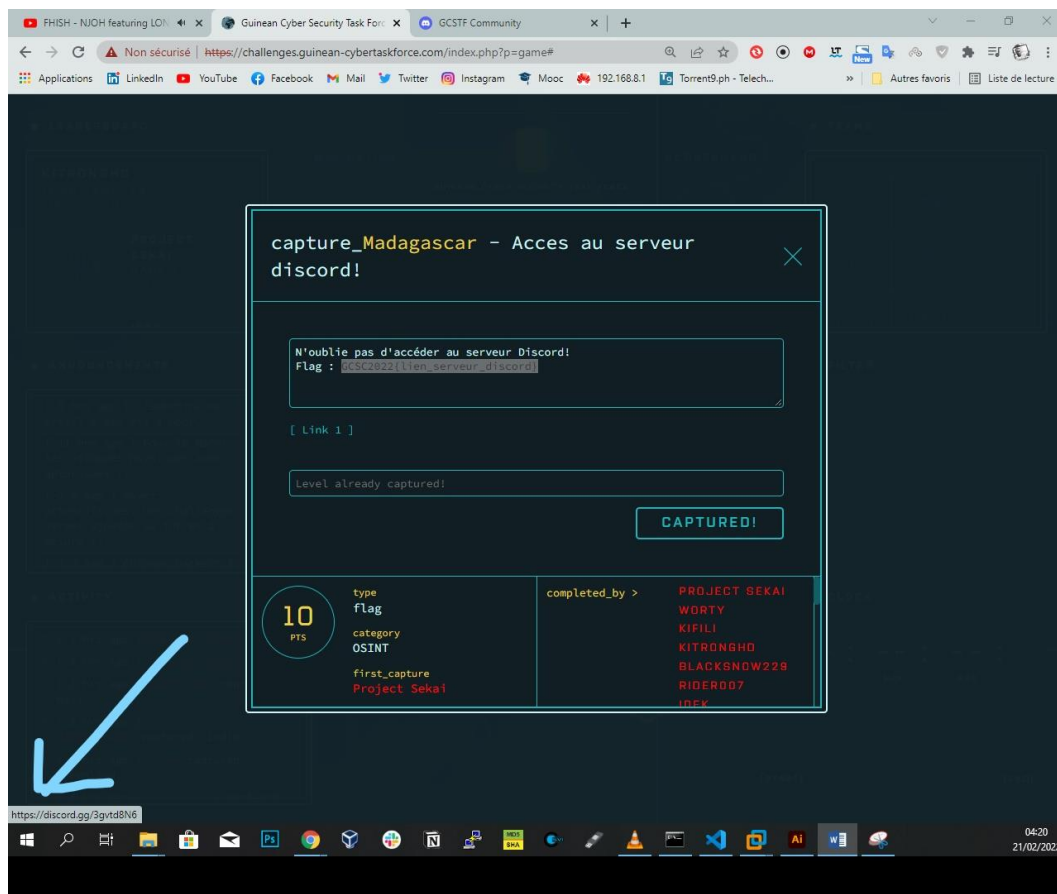
N'oublie pas d'accéder au serveur Discord!
Flag : GCSC2022{lien_serveur_discord}

[Link 1]

Level already captured!

CAPTURED!

| | | | |
|-----------|---------------|----------------|---------------|
| 10 PTS | type | completed_by > | PROJECT SEKAI |
| | flag | | WORTY |
| | category | | KIFILI |
| | OSINT | | KITRONGHO |
| | first_capture | | BLACKSNOW229 |
| | Project Sekai | | RIDER007 |
| | | | IDEK |



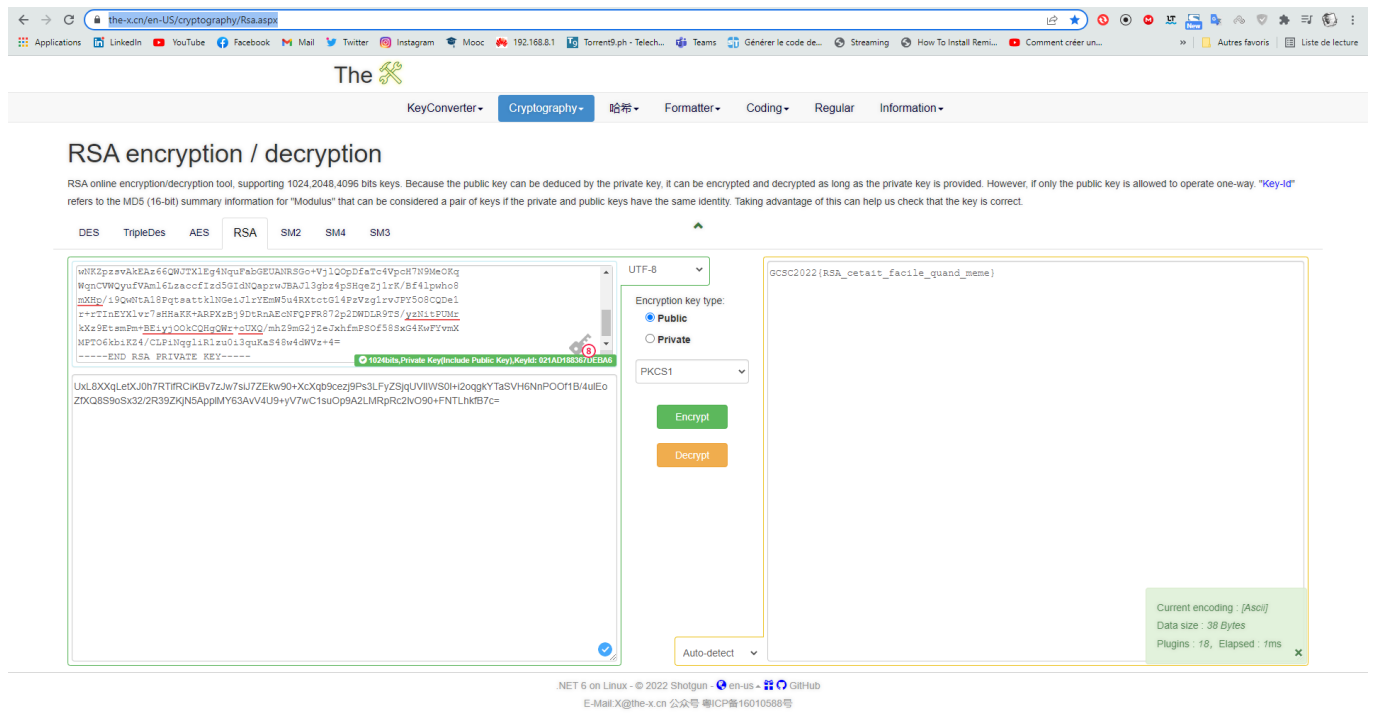
2. Capture_Argentina- Bonus

Ce challenge était un bonus pour l'effort fournis . le flag était dans le Hint.



3. Capture_United States – Ils vivent avec le RSA en France ?

La résolution de ce challenge s'est fait avec l'outil <https://the-x.cn/en-US/cryptography/Rsa.aspx> qui m'a permis de cracker le chiffrement RSA grace à la **clé privée** et le **message chiffré**.



capture_United States - Ils vivent avec le RSA en France?

On te donne le cryptosystème utilisé : message, clé privée et clé publique.

[Link 1]

Level already captured!

CAPTURED!

| | | |
|------------------------------|---|---|
| <div>20</div> <div>PTS</div> | <div>type</div> <div>flag</div> <div>category</div> <div>Cryptanalysis</div> <div>first_capture</div> <div>idek</div> | <div>completed_by ></div> <div>LEOX</div> <div>PROJECT</div> <div>SEKAI</div> <div>RMD723</div> <div>THEGARLICFLAG</div> <div>KITRONGHD</div> <div>OFSHILL</div> |
|------------------------------|---|---|

4. Capture_China - Sais-tu réellement programmer ?

Ce challenge consistait à retrouver le flag contenu dans un programme python contenant des erreurs de code. L'erreur était au niveau de la variable *line* qui n'avait pas été déclarer et j'ai également ajouter des parenthèses à la fonction *print*. J'ai donc remplacer avec la viable vers qui était défini puis j'ai eu le flag.

```
hello.py x script.py 2 poem-14février.txt
hello.py > ...
1 #
2 #Trouve l'erreur dans un script et exécute-le pour avoir le flag
3 #
4 #!/usr/local/bin/python -*- coding: UTF-8 -*-
5 poeme = open('poem-14février.txt')
6
7 flag=""
8 for vers in poeme:
9     vers=vers.strip()
10     lettre = vers[0:1]
11     flag=flag+lettre
12
13 print(flag)
```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL

Python + - [] [X] [^] [X]

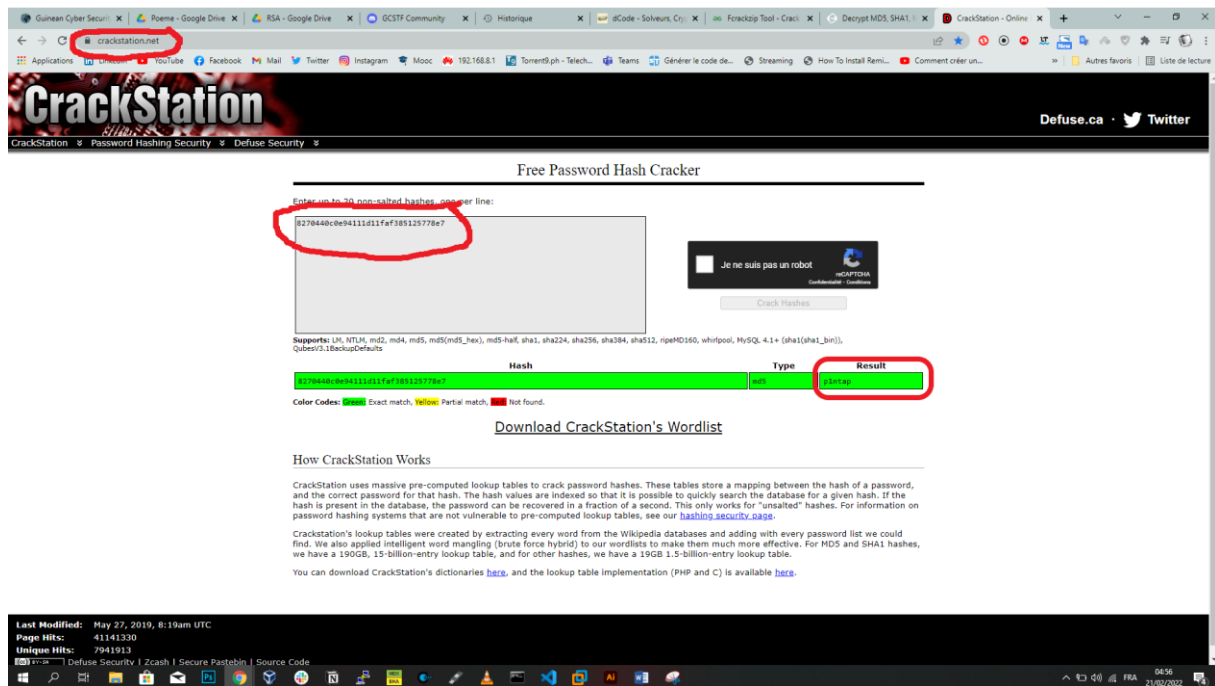
```
    lettre = line[0:1]
NameError: name 'line' is not defined. Did you mean: 'slice'?
PS C:\Users\Kopper_ng\Documents\CTF> & C:/Users/Kopper_ng/AppData/Local/Programs/Python/Python310/python.exe c:/Users/Kopper_ng/Documents/CTF/hello.py
FLAGCMPHDDSQNUCCPNNNSQACJOOP
PS C:\Users\Kopper_ng\Documents\CTF> & C:/Users/Kopper_ng/AppData/Local/Programs/Python/Python310/python.exe c:/Users/Kopper_ng/Documents/CTF/hello.py
FLAGCMPHDDSQNUCCPNNNSQACJOOP
PS C:\Users\Kopper_ng\Documents\CTF> & C:/Users/Kopper_ng/AppData/Local/Programs/Python/Python310/python.exe c:/Users/Kopper_ng/Documents/CTF/hello.py
FLAGCMPHDDSQNUCCPNNNSQACJOOP
PS C:\Users\Kopper_ng\Documents\CTF> [ ]
```

Ln 10, Col 23 Spaces: 4 UTF-8 CRLF Python [] [X]



5. Capture_Nigeria – Mot de passe d'une applicationétrange

J'ai résolu ce challenge avec beaucoup de sourire car il m'a fait découvrir plein de d'étape di déchiffrement. j'ai uploadé la bd sur <https://inloop.github.io/sqlite-viewer/> puis j'ai ensuite récupéré chaque Hash que j'ai cracker sur <https://hashes.com/en/decrypt/hash> . Après avoir eu le hash md5, je me suis rendu sur <https://crackstation.net/> pour avoir le texte en clair. J'ai répété la même méthode pour tous les autres utilisateurs jusqu'à avoir leurs différents mot de passe.



6. Capture_Kenya – Tout le monde est la bienvenue à la #GCSC2022

7. Capture_Chad – clé de déchiffrement ou de décryptage

8. Capture_Kenya – Tout le monde est la bienvenue à la #GCSC2022

Ce challenge consistait à faire de l'OSINT pour déterminer le mot de passe du Hacker de la CyberBadCorp. Après combinaisons du mot de passe reçu en email et des informations du hacker le flag est le suivant GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022

capture_Kenya - Tout le monde est la bienvenue à la #GCSC2022



Wow, quel acharnement contre notre pays!

Les membres de la CyberBadCorp se sont aussi inscrits à la compétition "Guinean Cyber Security Task Force" pour la saboter.

Très malheureusement pour eux, l'équipe "Guinean Cyber Task Force" a mis en place toutes les mesures pour les en empêcher.

Nous avons identifié un compte et te transmettons quelques informations pour deviner son mot de passe.

- pseudonyme : CyberBadCorp
- email : cyberbadcorp@gmail.com
- token d'inscription : 20022022

Flag: GCSC2022{mot_de_passe}

Level already captured!

CAPTURED!

10

PTS

type

flag

category

OSINT

first_capture

Project Sekai

completed_by >

PROJECT SEKAI

POULLO

RMD723

KITRONGHD

WHITEHORSE224

SOUL2MANE

WORTY