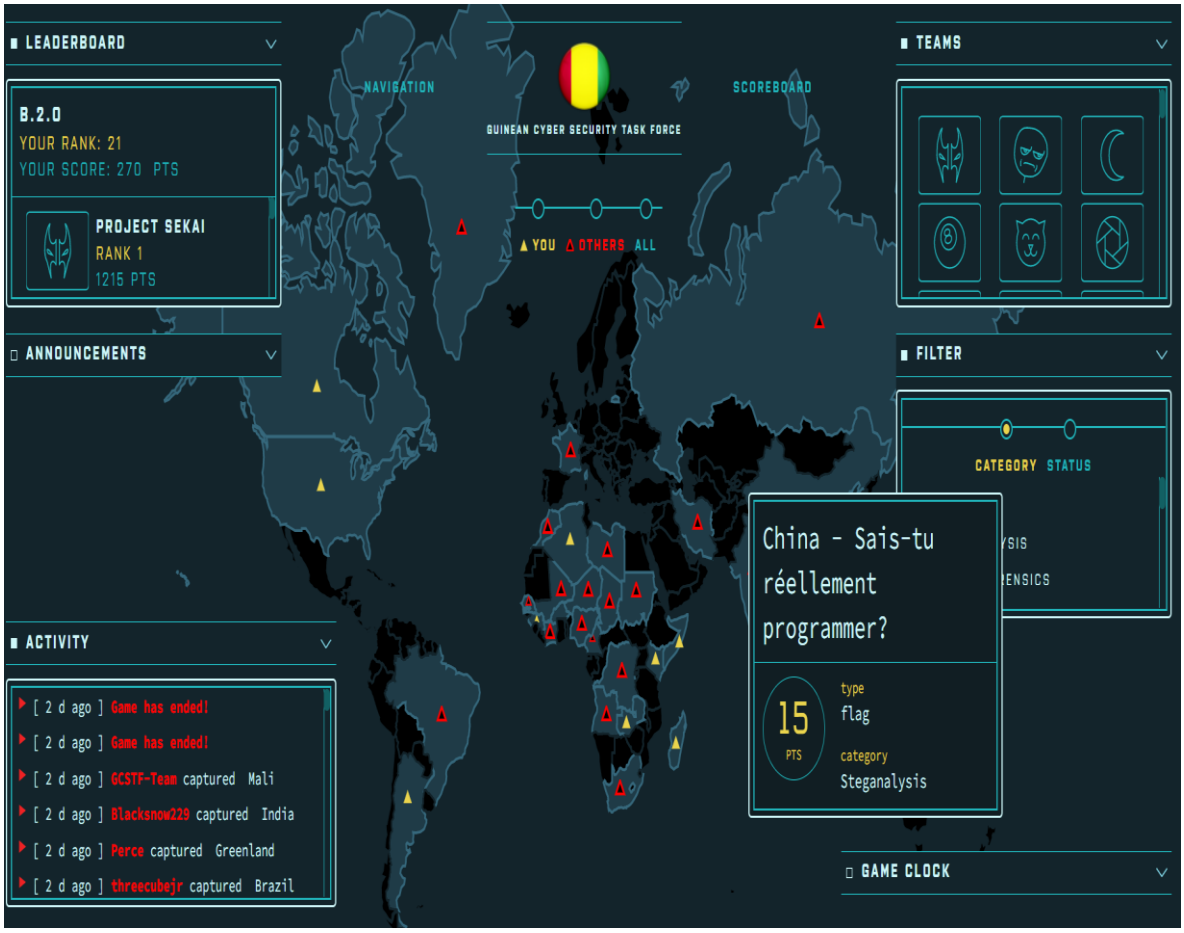
WRITEUP DU CHALLENGE GCSC2022

Dimanche, 20 février 2022 de 00h à 23h59 soit 24h

Après réception de nos identifiants, mots de passe et lien du site : https://challenges.guinean-cybertaskforce.com/, je me suis connecté et commencer à voir les différents types de challenge qu'il y avait et surtout choisir par quoi commencer pour maximiser mes points et gagner en temps, en voyant les défis, j'ai eu peur car je n'avais pas de connaissances techniques sur plusieurs types de défi tel que :

- Steganalysis
- Digital forensic…

En plus j'ai commencé à m'intéresser à la cybersécurité en octobre 2021 donc je me disais que ce n'est pas fait pour moi, le niveau est élevé mais comme on le dit : < c'est en se jetant dans l'eau qu'on apprend à nager > alors j'ai commencé par lire quelques défis pour voir ce que je pourrais faire



Je me suis déjà inscris donc il faut faire quelque chose ou du moins essayer tout en sachant qu'il y a plein de chose que je vois et que je ne connais même pas.

J'ai commencé par *MADAGASCAR* qui demandait d'accéder au serveur discord, ce que j'ai fait et j'ai eu 10 points.

Le flag c'est :

GCSC2022{https://discord.gg/3gvtd8N6}

Comment tu as eu ce flag ?

Je l'ai inventé./.

Non je blague, il était dans le mail envoyé par l'équipe **Equipe GCSTF** contacts@guinean-cybertaskforce.com

Je l'ai trouvé après avoir parcouru tout le site sans rien voir, j'ai vérifié le mail et puis bingo

J'ai rejoint le discord de GCSC, avec eux nous avons échanger tout le long de la journée et c'était géniale de voir à quel point les gens étais concentré et beaucoup passionné par la cybersécurité.

Le flag c'est :

GCSC2022{https://discord.gg/3gvtd8N6}

Le premier défi étant gagné, alors au suivant.

Les differents categories était :

1. CRYPTANALYSIS
2. DIGITAL FORENSICS
3. MISCELLANEOUS
4. MOBILE SECURITY
5. NETWORK SECURITY
6. NONE
7. OSINT
8. QUIZ
9. QUIZZ
10. REVERSE ENGENEERING
11. SCRIPTING
12. STEGANALYSIS
13. WEB SECURITY

Ensuite je me suis tourné vers le défi ***KENYA*** demandait de retrouver le mot de passe après avoir obtenu quelques informations tel que mentionné sur la figure ci-dessous

Bon, en tant que patriote, je ne pouvais pas accepter qu'on sabote un tel évènement national surtout sur un sujet de sécurité national.

Problème identifié : pas de lien à télécharger.

En observant très bien les infos que je connais du hacker,

- Pseudonyme
- Email
- Token d'inscription

En sachant déjà qu'ils nous ont infiltrés.

J'ai eu une impression de déjà vu, et ça m'a rappelé comment je m'étais loguer sur ce site.

Le mot de passe est une combinaison de ces trois éléments cités

Ci-dessus :

GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}

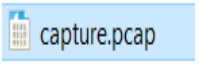
Après tout on le dit souvent : * **le diable se trouve dans les détails *.**

Allons maintenant dans le défi ***SOMALI*** où l'ANSSI-Guinée a récemment exigé aux cybercafés opérant sur toute l'étendue du territoire Guinéen de mettre en place des mesures garantissant l'authentification, la traçabilité, l'imputabilité/la non-répudiation de l'usage des appareils de leurs parcs informatiques.

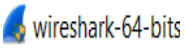
Etant en charge de l'analyse des captures réseaux bimensuels de certains cybercafés de la capitale, tu décides de commencer ta journée par celle-ci.

En fin, on me parle de RESEAU, je ris seulement pour ce que je m'apprête à les faire subir (haha)

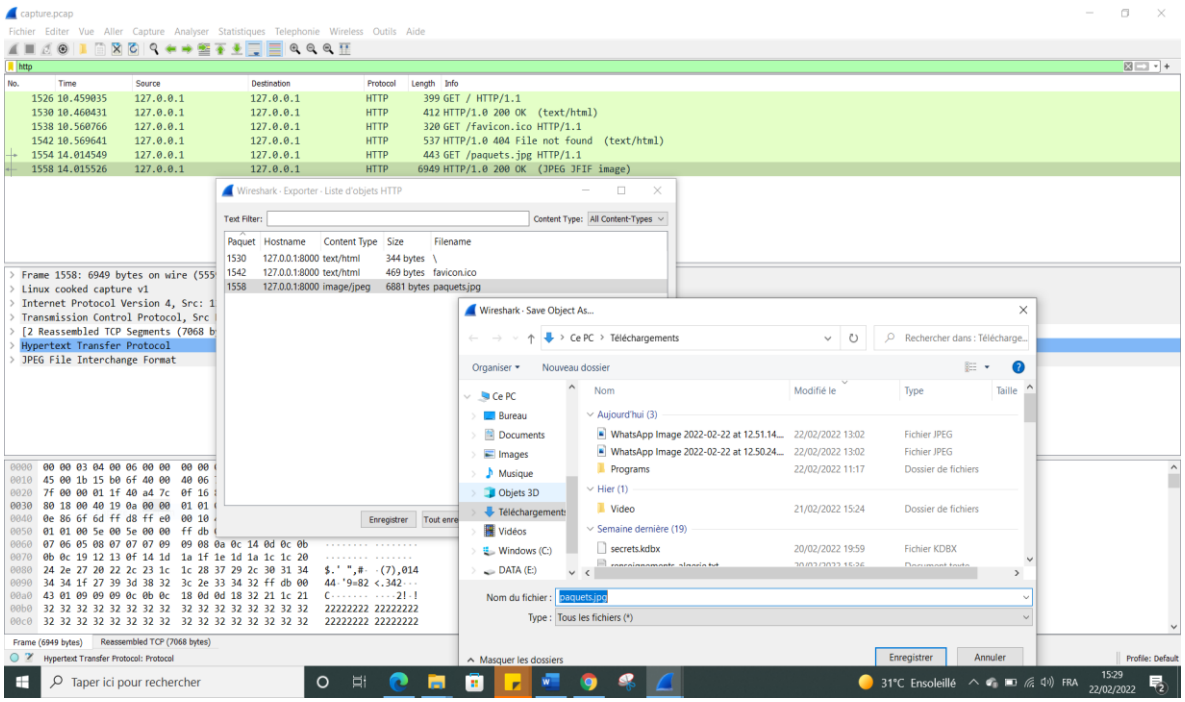
Je clique sur le Link 1 pour télécharger la ressource disponible, c'est un fichier .pcap,



ce qui veut dire il doit être analyser par un analyseur réseau, alors je choisi un outil qu'on appel

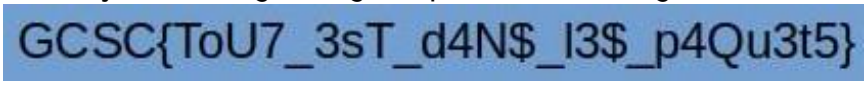


Pour l'ouvrir.



Explication 1 j'ouvre le fichier, je filtre par http, j'exporte l'objet en http puis je sélectionne le paquet pour l'enregistrer.

Ensuite j'ouvre l'image enregistré pour trouver le flag



alors le flag à insérer est :

GCSC2022{ToU7_3sT_d4N$_l3$_pQu3t5}. Alors je le prends, je le mets sur la case demandé (vous pouvez vérifier vous-même sur l'image).

Vous avez vu combien de fois j'ai souffert ? tout ça pour 10 points seulement.

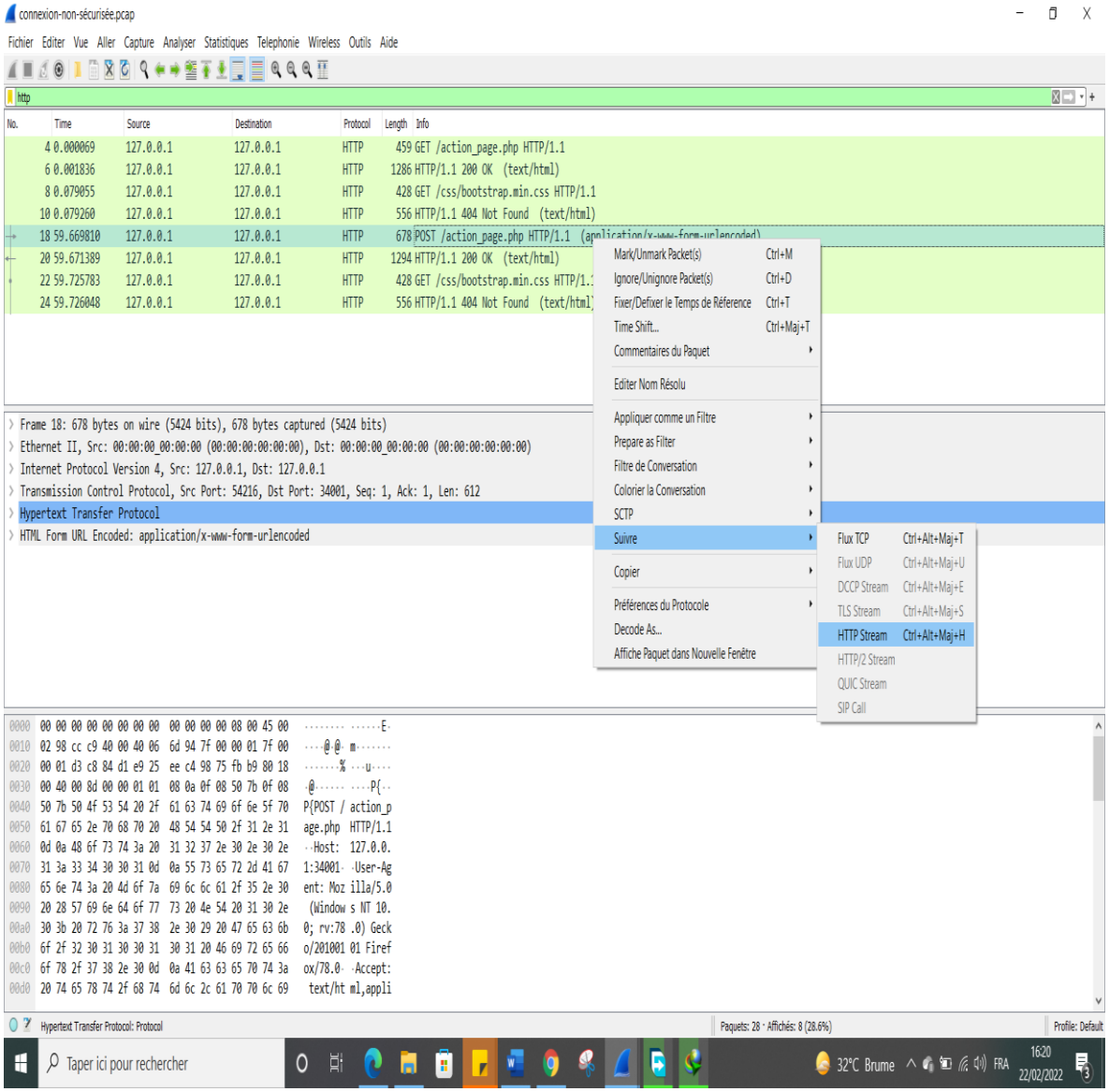
Bon, allons voir ce qu'il y a en *ZAMBIE*, il parait qu'il fait moins chaud laba, car la connexion n'est pas sécurisée.

Je télécharge la ressource fournie par le lien Link 1 pour retrouver un fichier pcap qui a pour nom :

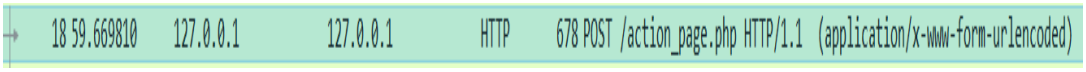
Ouvrons ce fichier avec Wireshark et filtrons le trafic en http car nous savons déjà ce que nous cherchons.

- Mot de passe, nom d'utilisateur et le message

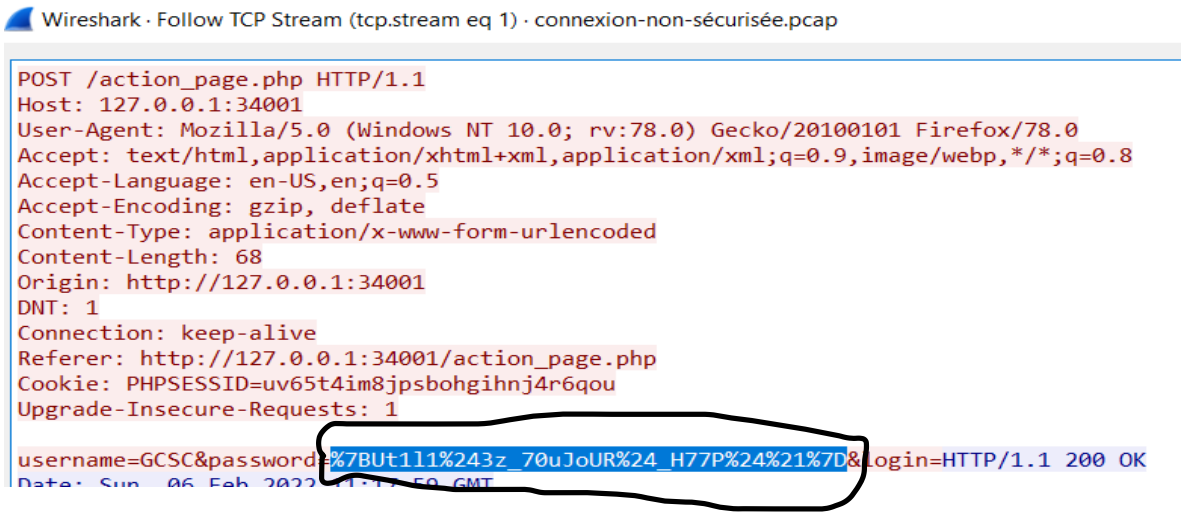
En gros nous cherchons le formulaire ou l'url.



- Sélectionnons là où le formulaire est mentionné

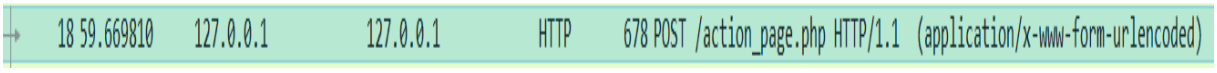


comme indique les actions sur l'image de la capture et suivons le flux

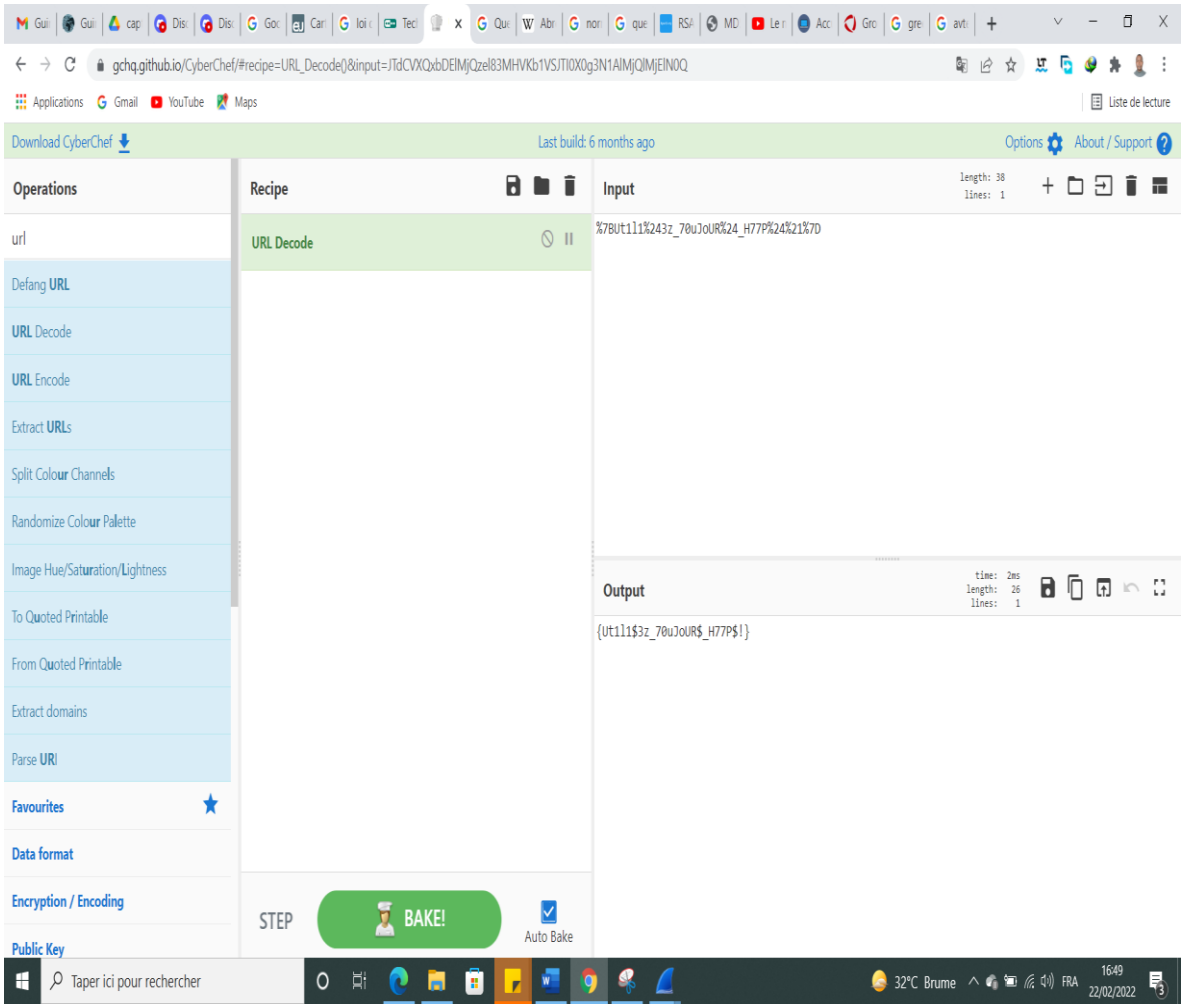


Sélectionnons ce qui se trouve sur le password, nous remarquons qu'il est codé et même alors il nous faut un outil pour le décodé, mais quel outil utilisé ? surtout il s'agit de quel type d'encodage ?

Je me suis tellement taper des vidéos sur YouTube, tellement d'écriture sur le canal discord de l'évènement, sans parler du nombre de gens que j'ai appelé pour me guider et je commençais même à somnoler tout en observant cette image



Et paf, **CYBERCHEF** est magique et commence à opérer sa magie. Je vous le montre (hahaha)



Il sélectionna le mot de passe crypté, alla sur l'outil Cyberchef et décoda le code en utilisant l'opération url décode, il prit le code (qui s'avère être le flag) {Ut1l1$3z_70uJoUR$_H77P$!} et le colla sur la case :

GCSC2022{Ut1l1$3z_70uJoUR$_H77P$!}.

NB : CYBERCHEF je ne te lâcherai plus, promis.

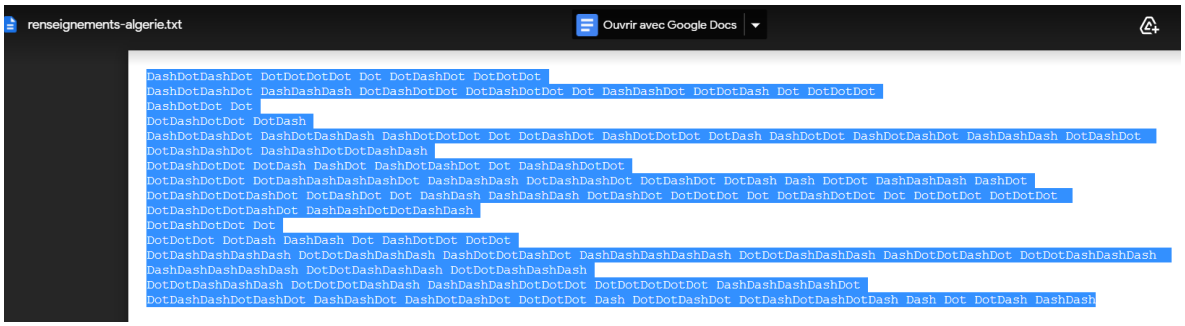
J'obtiens les 20 points après plus de 2h de torture. QUELLE GALERE !

Bon, le coté positif, j'ai eu un ami que je crois qu'on va beaucoup travailler ensemble, merci mon super ami CYBERCHEF.

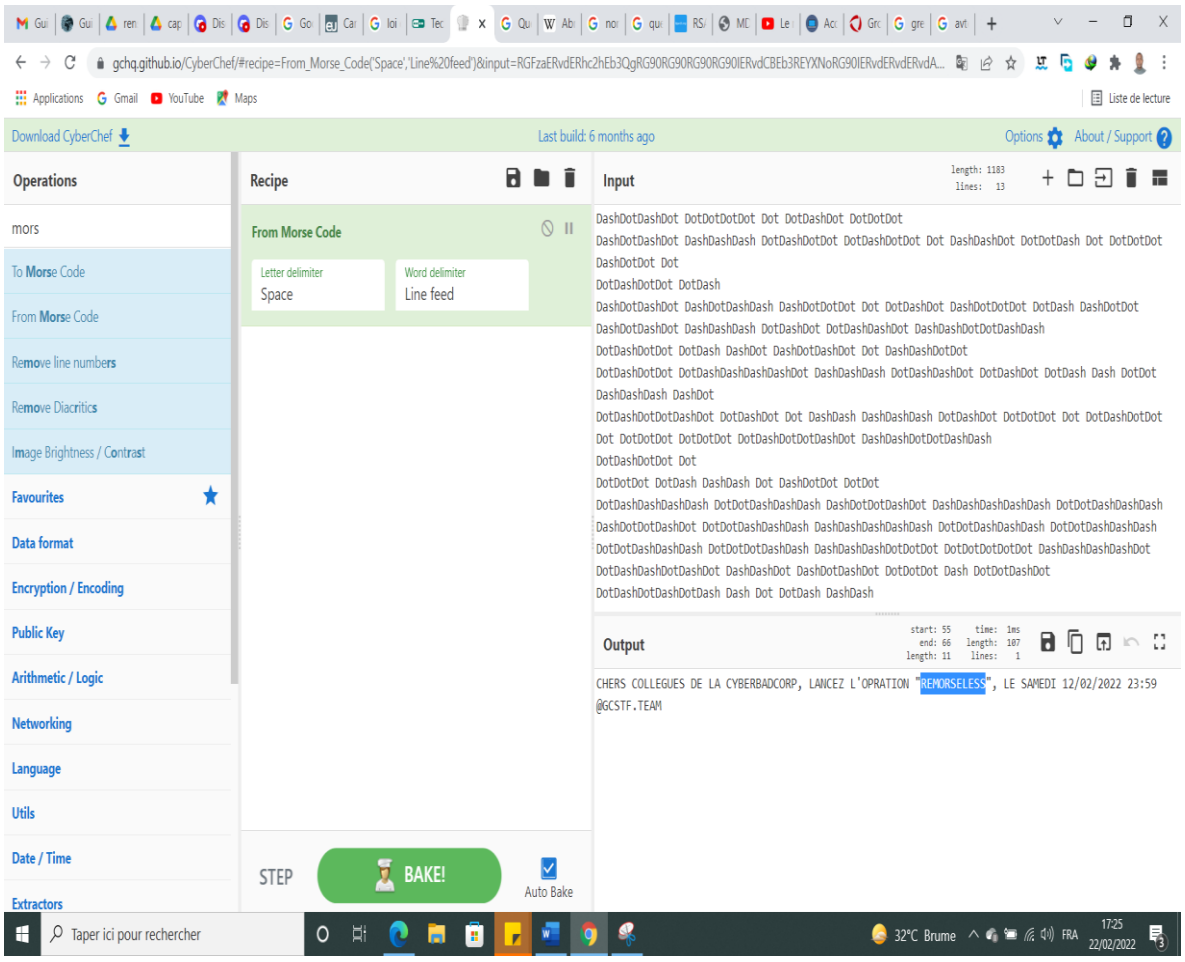
Nous continuâmes notre aventure (pour l'Europe ? mon œil) pour le challenge et nous atterrîmes en *ALGERIE* où

La ressource sur le lien Link 1 à télécharger était tellement bizarre que j'ai failli appeler l'équipe GCSC pour leur dire que leur renseignement était erroné./.

Mais en fait, il s'agissait d'un message crypté par les services de renseignements Algériens (enfin, je crois). Voyez par vous-même



Il s'agit d'un message en morse donc il faut le (démorser ou bien ?) décrypter alors je fais appel à mon nouveau super ami cyber chef, je lui explique mon problème et il m'aide

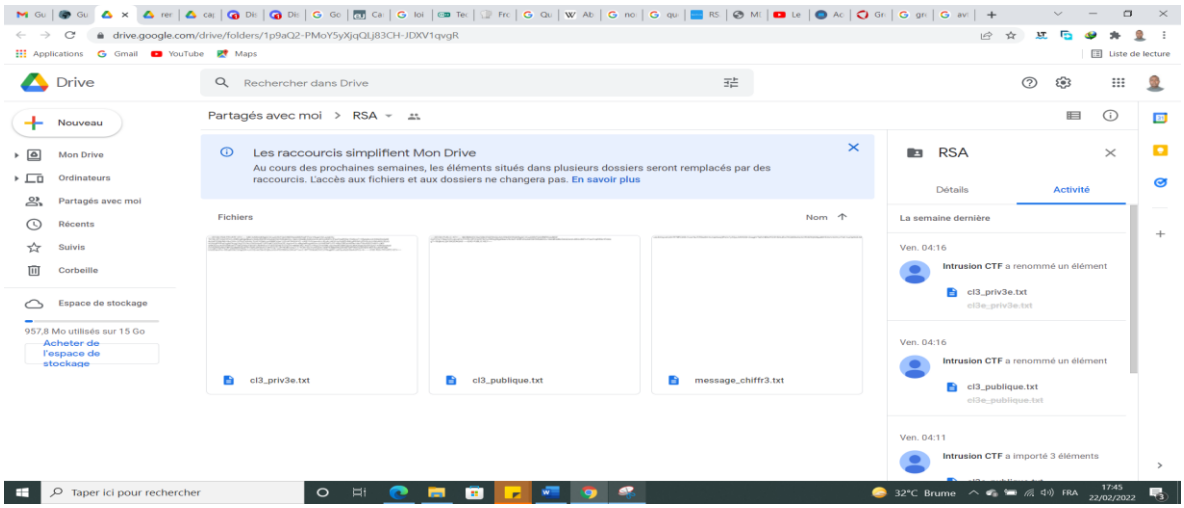


Comme on vient de voir, le nom de l'opération est : remorseless.

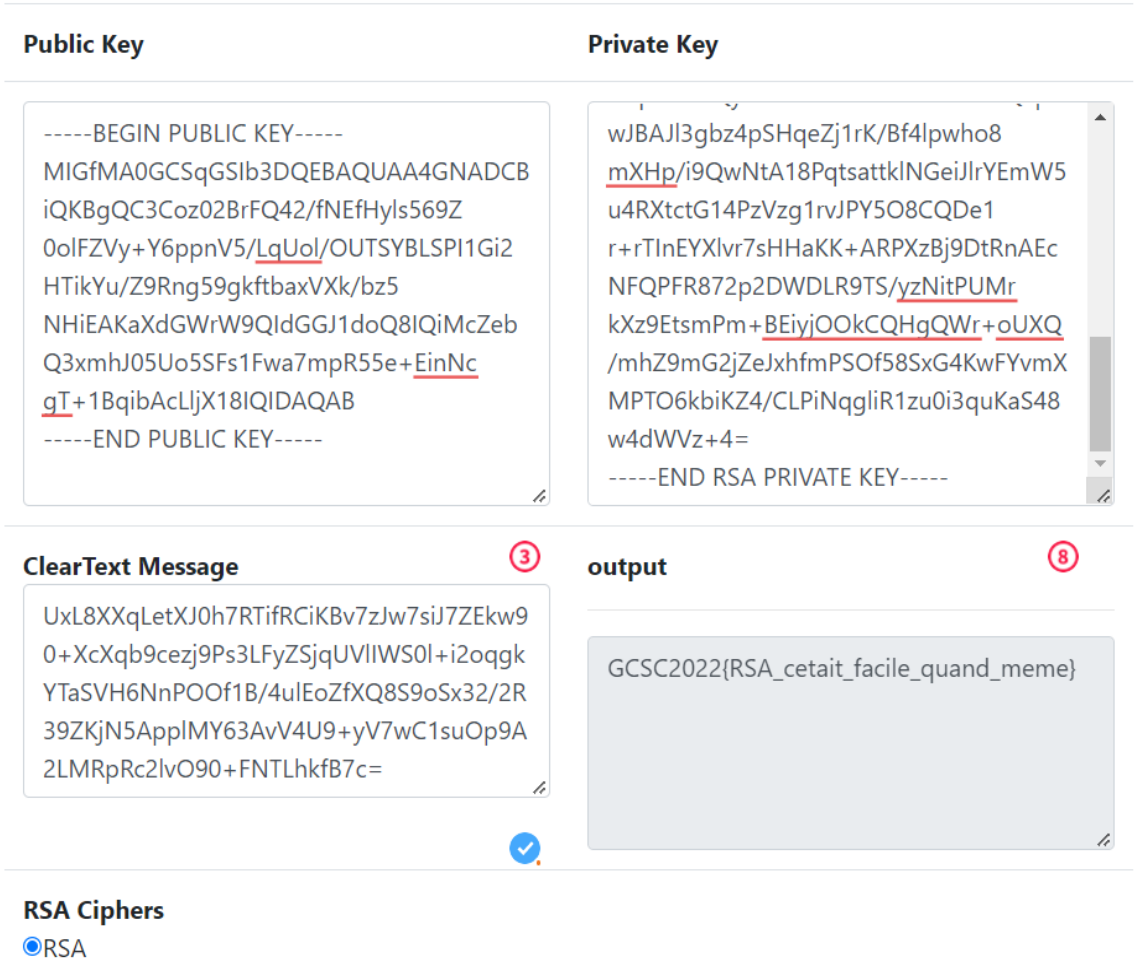
GCSC2022{remorseless}.

J'obtiens mes 10 points puis je continue mon chemin pour continuer mon aventure hors de l'Afrique, histoire de me mesurer aux autres aussi haahahahahh.

Aux usa, c'est un problème de cryptanalyse, on vous donne un message chiffré, une clé publique, une clé privée et on vous dit de décrypter le message. On fait comment ?



Il faut qu'on trouve un outil spécialisé dans le chiffrement indiqué, pour cela nous allons au site https://8gwifi.org/rsafunctions.jsp, on copie les clés et le message chiffré pour obtenir la sortie



Alors le flag est : GCSC2022{RSA_cetait_facile_quand_meme}

Après les USA, faisons un tour au ***CANADA***

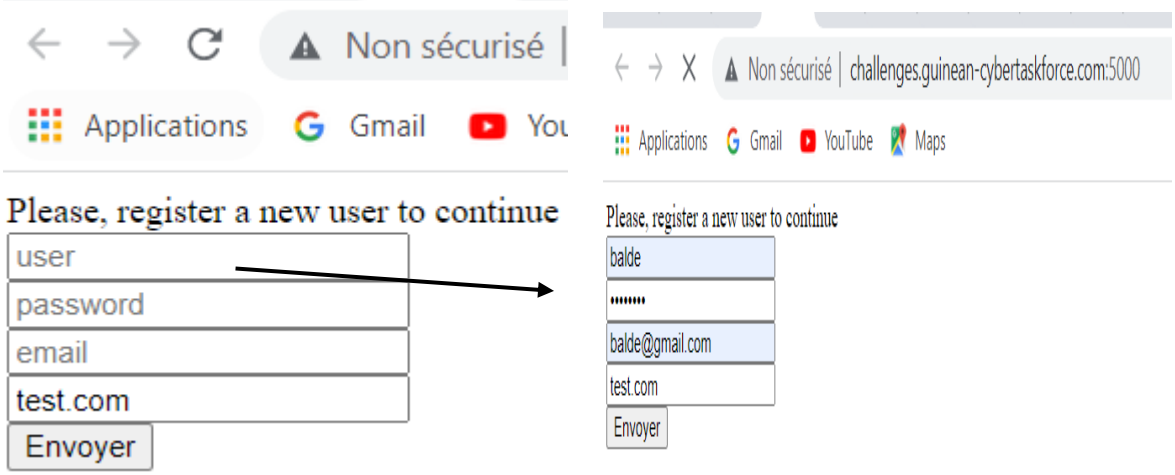
IL y a 2 liens comme ressources disponibles.

Le premier lien nous envoie vers un formulaire de connexion pendant qu'on a aucun identifiant pour ce site.

Le deuxième lien, bizarre, nous envoie écouter le Song de la fouine (trois mots) de l'album bénédiction.

Il va falloir nous dire à quoi sert cette musique dans ce CTF ?

Mais en attendant je kiffe le son grave.



---

j'ai rempli au hasard le formulaire et après un temps il y a une page d'erreur qui s'affiche

```
    response = self.full_dispatch_request()
File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1518, in full_dispatch_request
    rv = self.handle_user_exception(e)
File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1516, in full_dispatch_request
    rv = self.dispatch_request()
File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1502, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**req.view_args)
File "/app/app.py", line 32, in register
    r = requests.get('http://'+url+'/GCSC{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}')
[console ready]
>>>
File "/usr/local/lib/python3.8/dist-packages/requests/api.py", line 75, in get
```

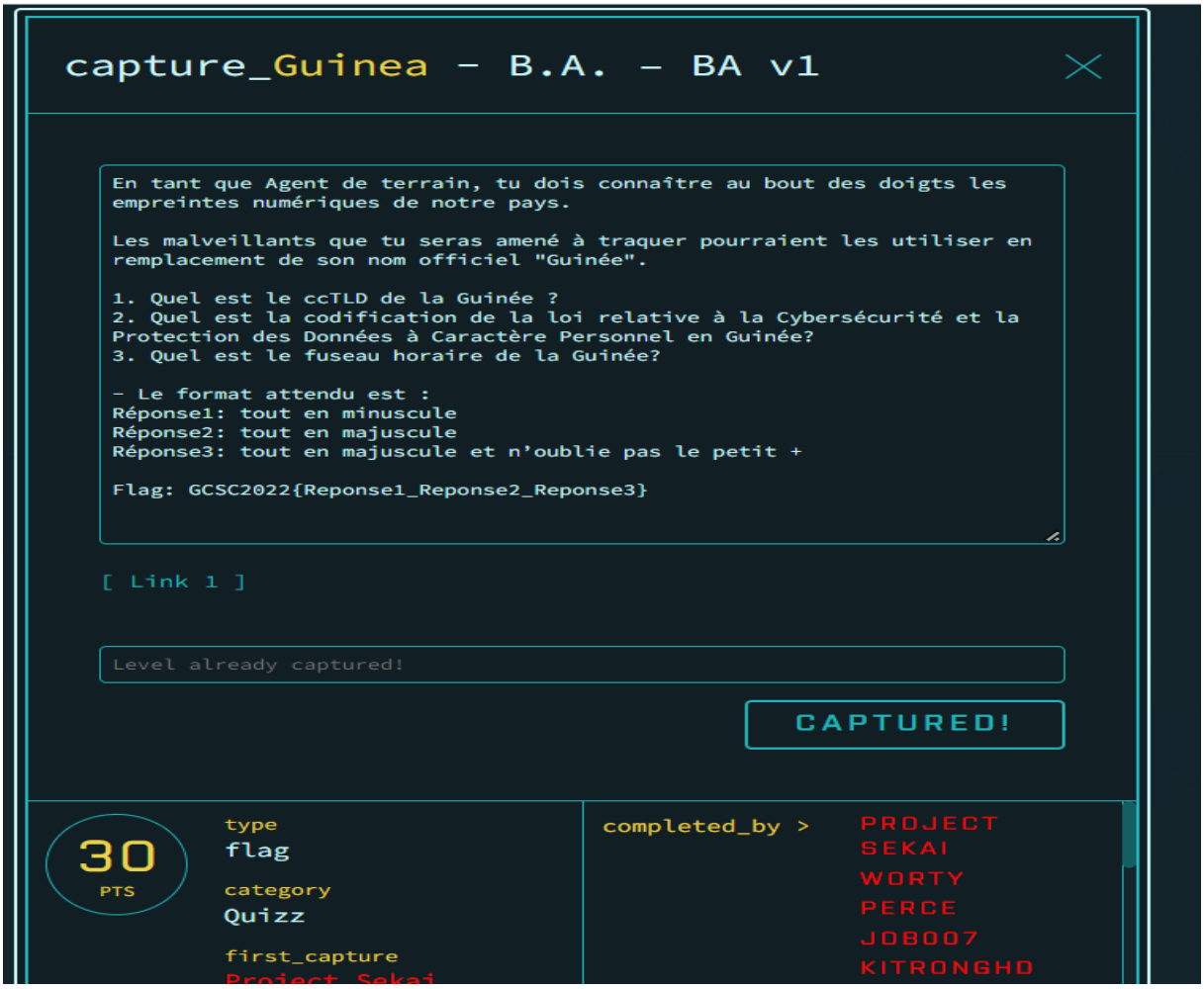
En observant bien la page d'erreur on remarque quelque chose qui ressemble au flag

```
r = requests.get('http://'+url+'/GCSC{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}')
```

Le résultat sera : **GCSC2022{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}**

J'ai obtenu les 150 points prévus pour ce challenge.

Revenons un peu en Afrique



Il s'agit d'effectuer des recherches, pour connaitre bien les lois du pays ***LA GUINEE***

1. Le ccTLD de la Guinée est le : • gn
2. La codification de la loi relative à la cybersécurité en Guinée et la protection des données à caractère personnel est la LOI L-2016-037-AN
3. Le fuseau horaire de la Guinée est le GMT+0 ou UTC+0

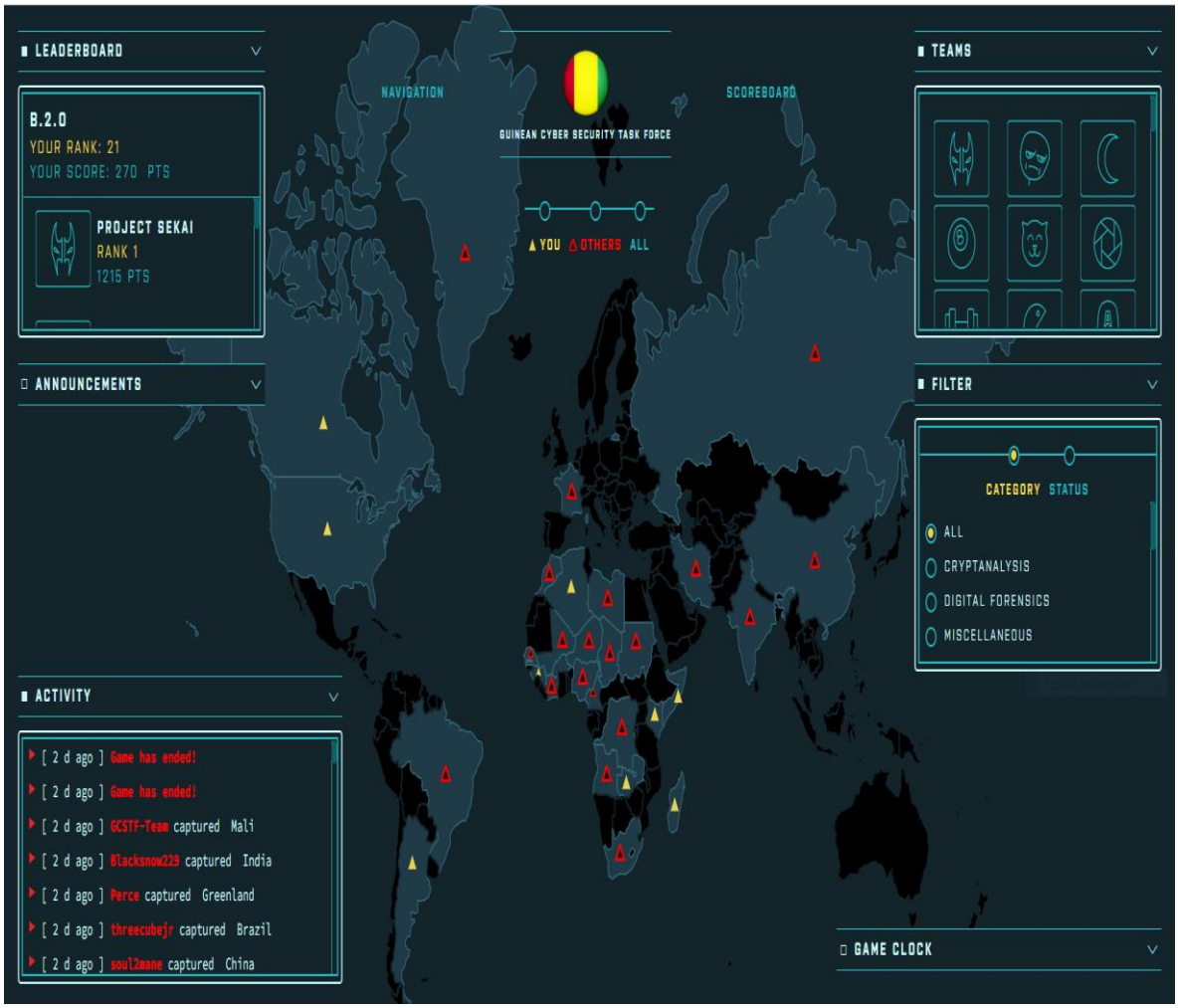
Le flag est : GCSC2022{.gn_LOI L-2016-037-AN_GMT+0}

Ce challenge était coté à 30 points et puis paf je l'ai obtenu

Pour finir allons en ***ARGENTINE***

Enfin c'était un bonus, il faut juste cliquer sur le hint et puis bam

GCSC2022{For_your_effort}



J'ai terminé avec 270 points et classé 21eme sur l'ensemble des participations et j'en suis fier car :

1. C'est le premier CTF que j'ai effectué de ma vie et j'espère que j'en ferai d'autres ;
2. C'est le premier writeup que j'effectue aussi, je m'excuse pour les erreurs de fond ou de forme que vous allez relever dans ce document et si possible je suis ouvert à toutes suggestions ou recommandations ;
3. Ça fait moins de 6 mois depuis que j'ai commencé à m'intéresser réellement à la cybersécurité donc moins de 6 mois d'expériences.

Remerciement

Je remercie du fond du cœur l'ensemble des organisateurs de cet évènement car c'est très important de mesurer son niveau et surtout d'avoir une communauté qui partage la même passion. Pour moi c'était un apprentissage du début à la fin sur l'ensemble de ce que j'ai pu faire et pour le reste, j'apprendrai.

Grâce à vous j'ai obtenu une liste de compétence que je dois apprendre et j'espère que je reviendrais plus fort l'année prochaine ou lors de votre prochain CTF.

- Je voudrais vous demander une séance de résolution de l'ensemble de ces défis et prière de m'informer pour que j'assiste ou je participe