HIDDEN'S WRITE-UP GCSC2022

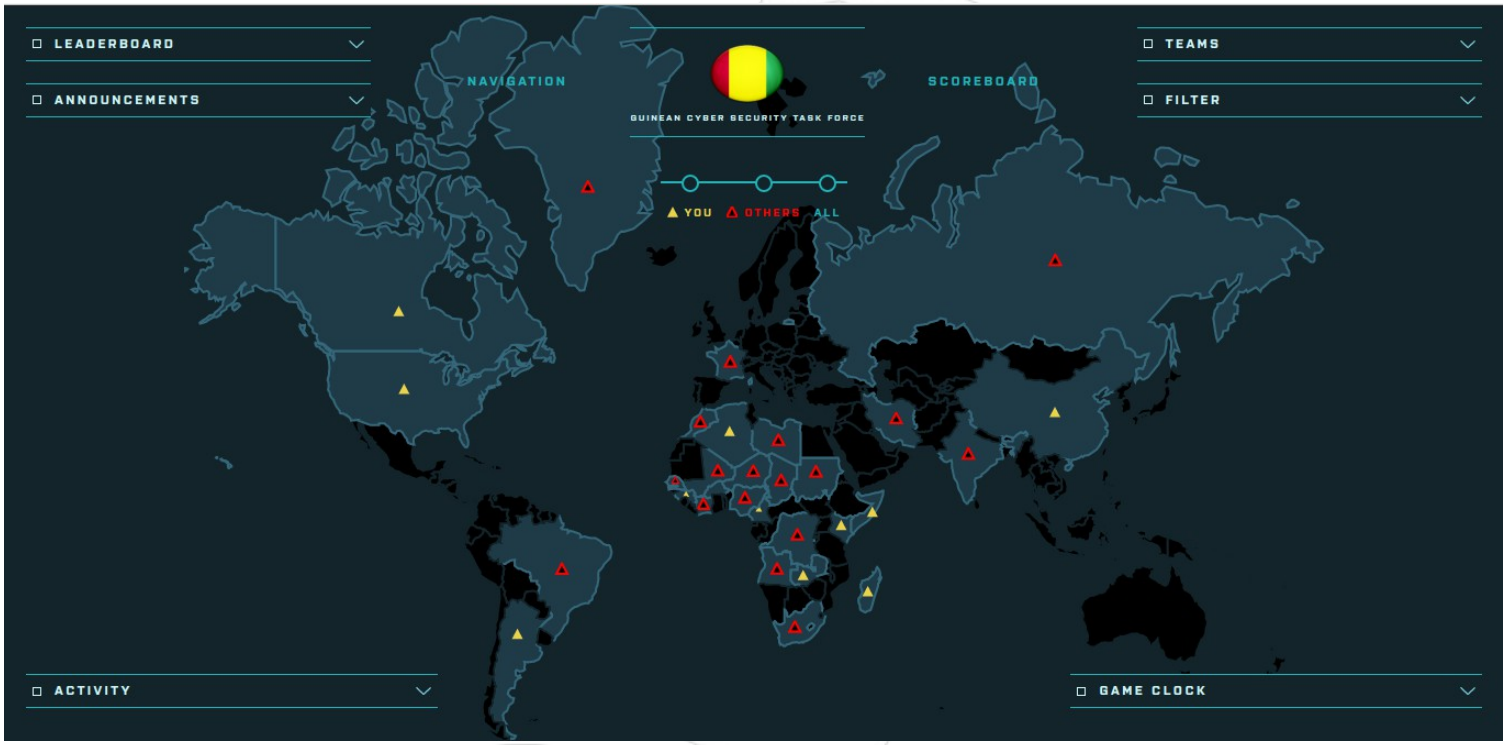


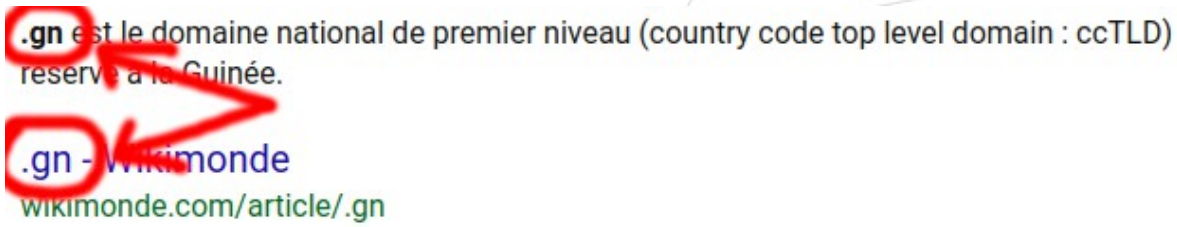
Table des matières

I. QUIZZ

a) Capture_Guinea – B.A. – BA v1

Je suis Aller sur Google taper ccTLD de la Guinée Conakry, et sur wikimonde par exemple le ".gn" qui est le domaine de la guinée

J'ai ma première réponse



En plus, toujours sur Google j'ai tapé loi relative à la Cybersécurité et la Protection des Données à caractère Personnel en Guinée

Sur le site justiceguinee.gov.gn nous avons la seconde réponse qui est "LOI L-2016-037-AN"

Pour Le fuseau horaire je savais déjà que la guinée est sur le "GMT+0" qui est la troisième réponse pour former mon flag

Flag : GCSC2022{.gn_LOI L-2016-037-AN_GMT+0}

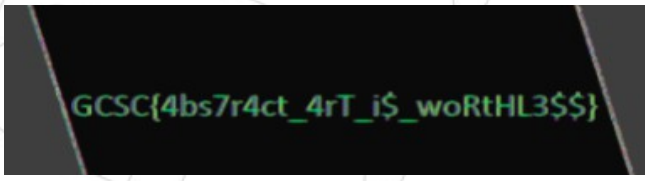
II.STEGANALYSIS

a) Capture_Cameroon – Voler des informations avec classe. Quel art !

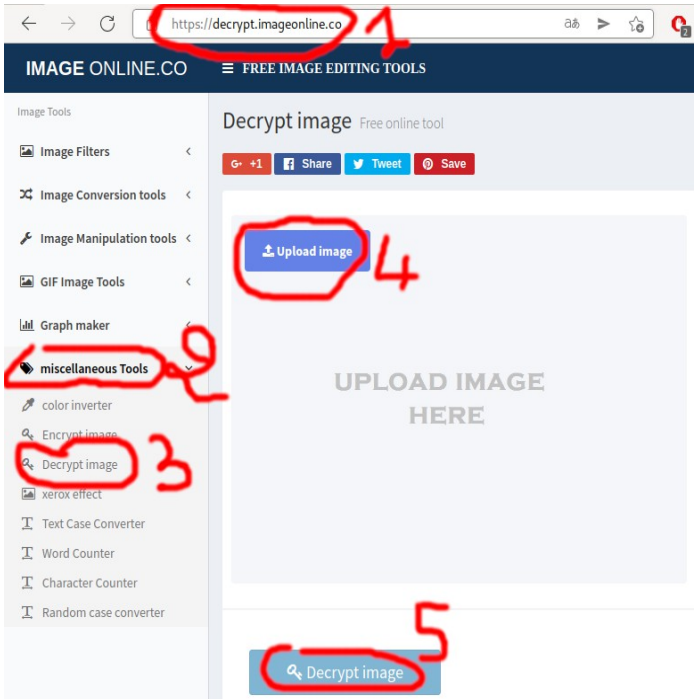
J'ai Cliqué sur Link 1 et télécharger limage art abstrait.png

Je suis aller sur le lien https://decrypt.imageonline.co dans le menu sur la gauche je clique sur miscellaneous Tools > Decrypt image

J'importe l'image en cliquant sur upload image ensuite je clique sur le bouton Decrypt qui se trouve en dessous de l'image et a la droite apparaîtra le flag à l'intérieur de l'image décryptée



Flag : GCSC2022{4bs7r4ct_4rT_i$_woRtHL3$$}



b) Capture_Chine – Sais-tu réellement programmer ?

Je Clique sur Link 1 et ça me rediriger vers la page Google drive et j'y trouve deux fichiers .txt ensuite je les télécharge

J'ai créé un fichier sur mon bureau au nom de bea et j'y mets les deux fichiers puis je renomme scrypt.py.txt en scrypt.py

À partir de visual studio code j'ouvre scrypt.py et modifie le contenu

Contenu départ

```
1  #
2  #Trouve lerreur dans un script et exé
3  #
4  #! /usr/local/bin/python  -*- coding:
5  poeme = open('poem-14février.txt')
6
7  flag=""
8  for vers in poeme:
9      vers=vers.strip()
10     lettre = line[0:1]
11     flag=flag+lettre
12
13 print flag
```

Et je la modifie ainsi

```
5  poeme = open('poeme-14février.txt')
6  flag=""
7  for vers in poeme:
8      #vers=vers.strip()
9      #lettre=line[0:1]
10     #flag=flag+lettre
11     flag += vers[0].upper()
12 print (flag)
```

Je compile et obtient

```
└─$ /usr/bin/python /home/beavogui/Bureau/bea/main.py
FLAG
CMPH
DDSQ
NUCC
PNNS
OQAC
JOOP
```

Je colle toutes les lettres sur une seule ligne et j'aurai FLAGCMPHDDSQNUCCPNNSOQACJOOP

Flag : GCSC2022{FLAGCMPHDDSQNUCCPNNSOQACJOOP}

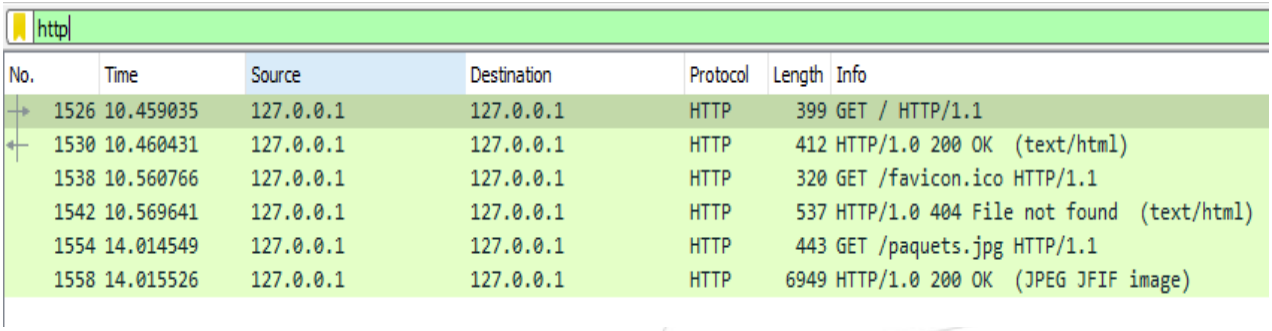
III. NETWORK SECURITY

a) Capture_Somalia – Cybertalent ! Il faut mettre le paquet… 1/2

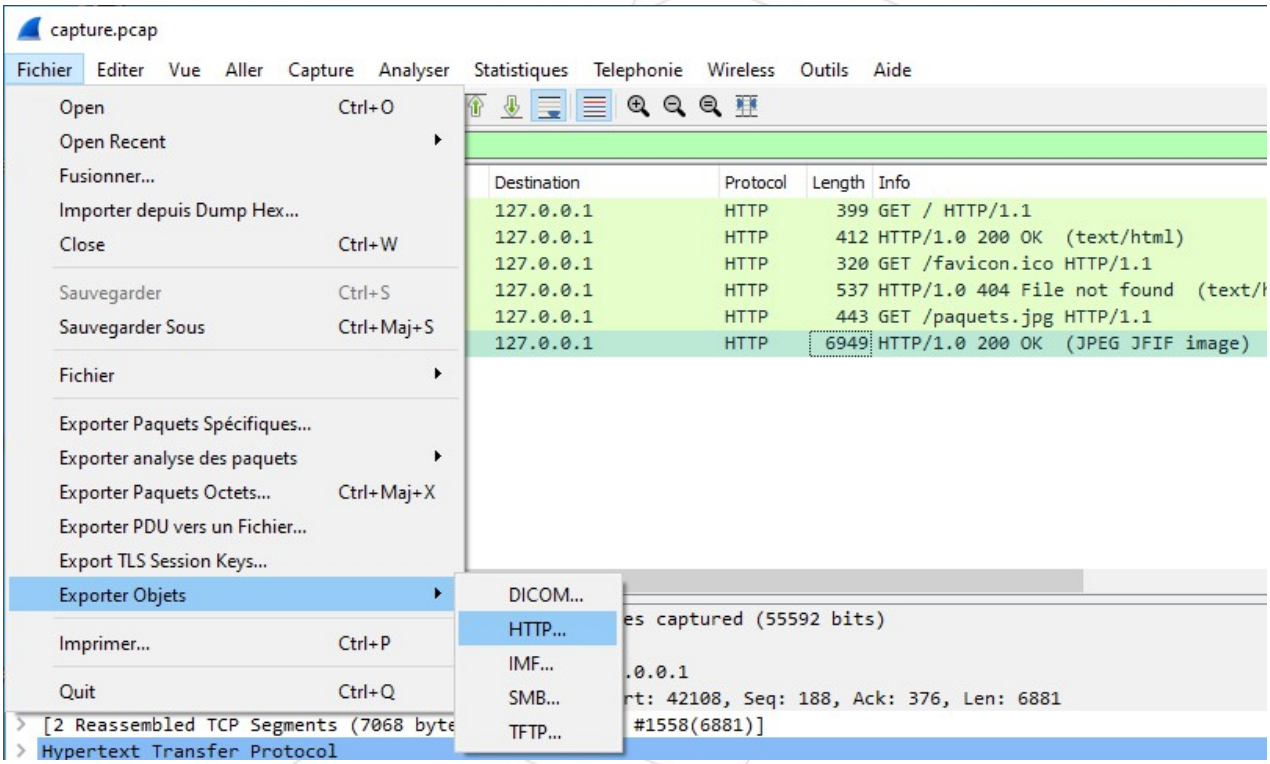
Je Clique sur Link 1 et je télécharge le fichier capture.pcap

Je l'ouvre avec le logiciel Wireshark puis je fais un Filtre par http

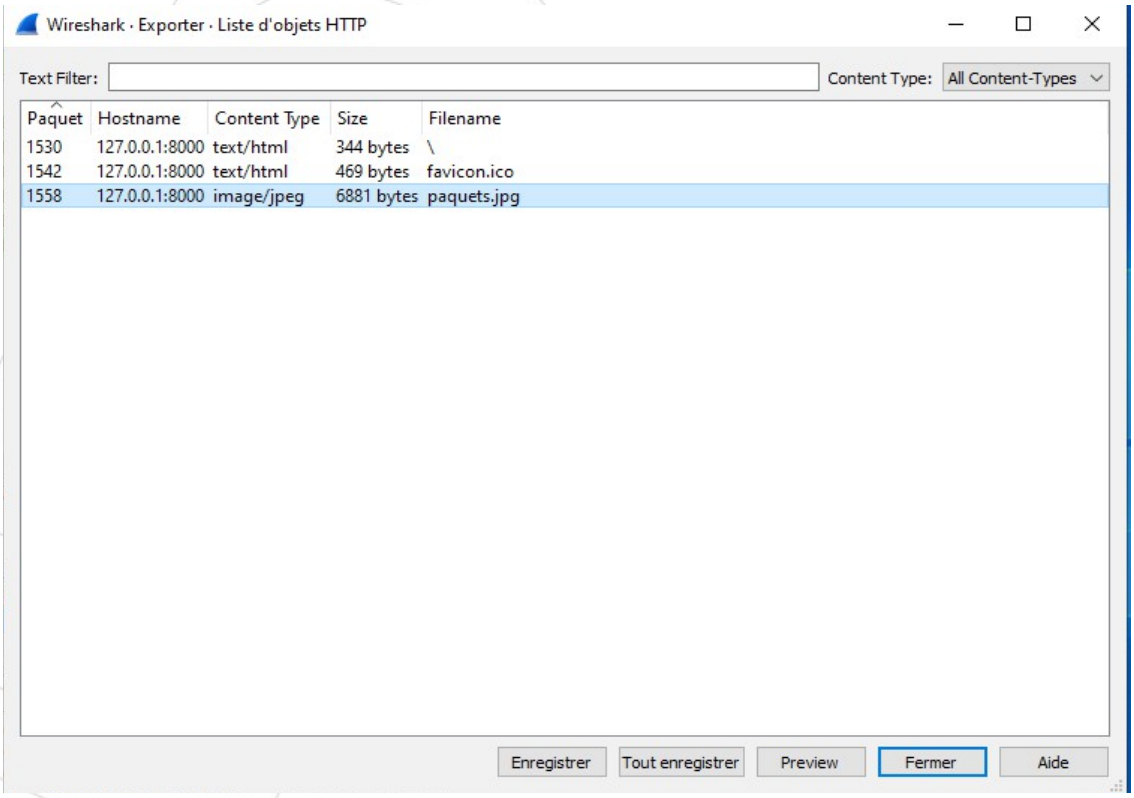
Je sélectionne "http/1.0 200 ok (JPEG JFIF image)



Je vais dans le menu fichier > exporter objets > http



Sélectionner paquet.jpg > enregistrer



Aller ouvrir votre image télécharger pour voir le flag

GCSC{ToU7_3sT_d4N$_l3$_p4Qu3t5}

Flag : GCSC2022{ToU7_3sT_d4N$_l3$_p4Qu3t5}

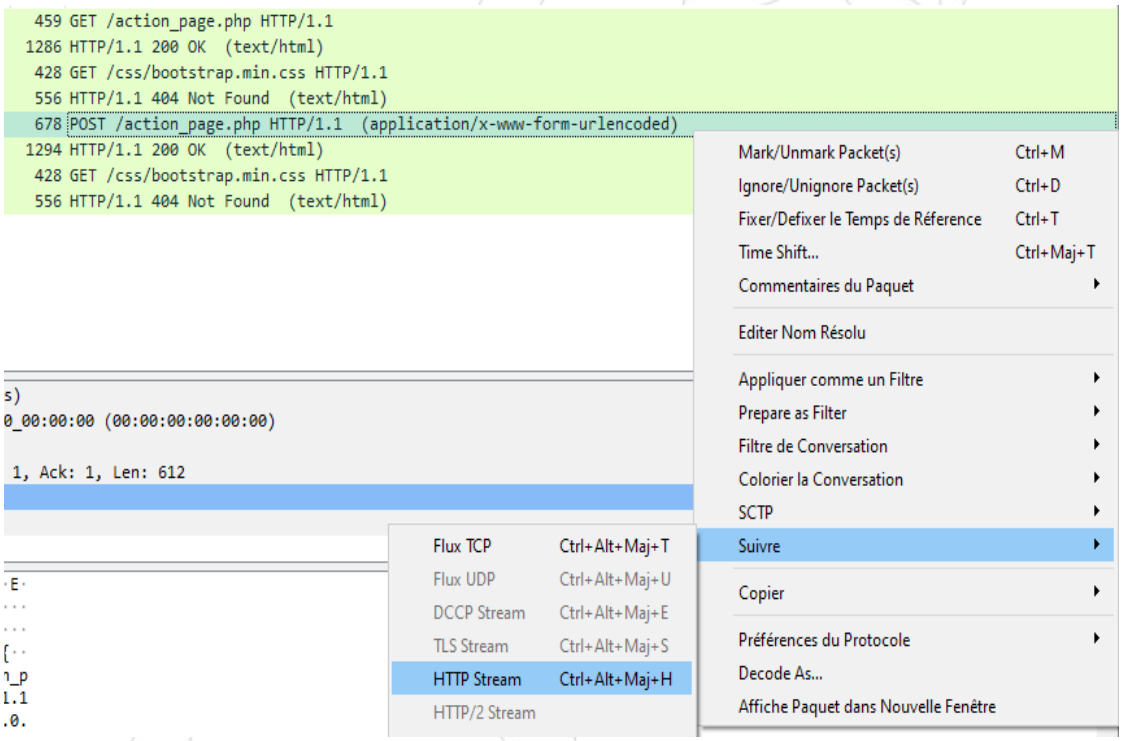
b) Capture_Zambia – Cybertalent ! Il faut mettre le paquet… 2/2

Je Clique sur Link 1 et je télécharge le fichier connexion-non-sécurisée.pcap

Je l'ouvre le avec le logiciel Wireshark puis je Filtre par http

Je Sélectionne "HTTP/1.1 (application/x-www-form-urlencoded)"

Je fais clic droit là-dessus > suivre > http Stream

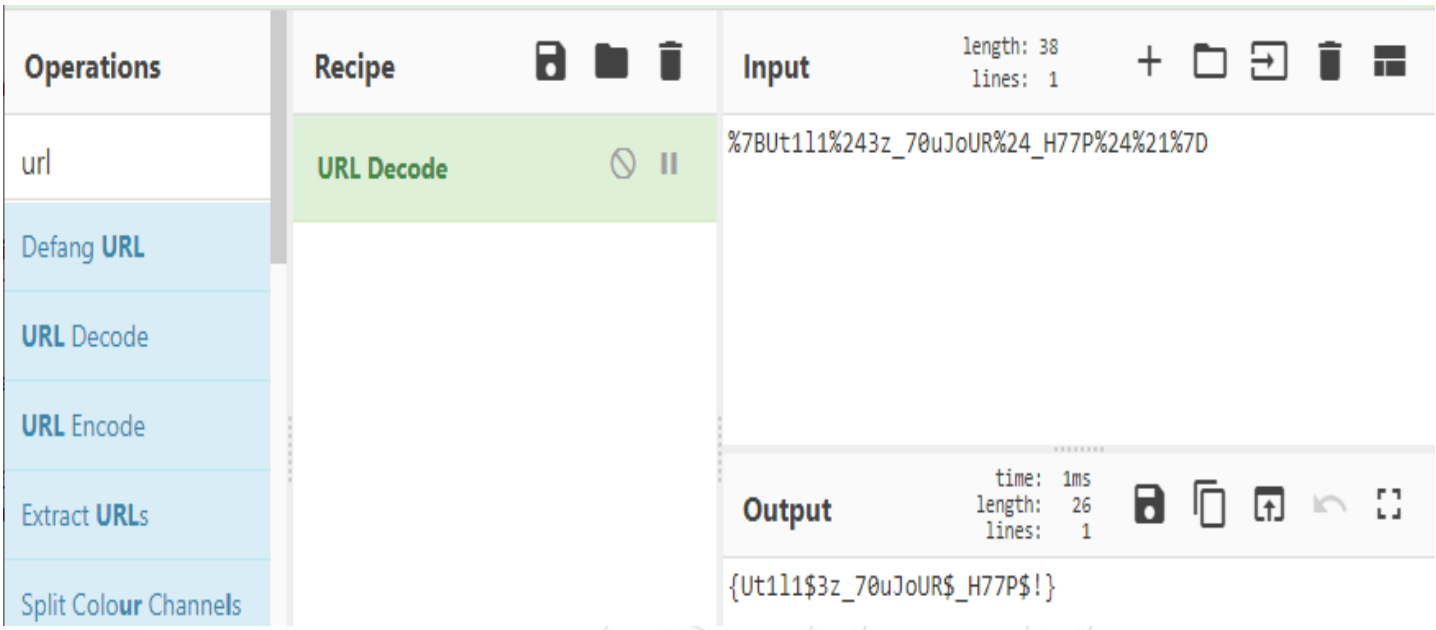


Dans la boite de dialogue qui s'affiche je sélectionne et copie le mot de passe

Puis je vais sur le site https://gchq.github.io/CyberChef/

Je Colle le texte dans input et Cherche l'opération URL Decode ensuite je la maintiens et la place dans recipe

Et le tour est joue



Flag : GCSC2022{Ut1l1$3z_70uJoUR$_H77P$!}

IV. OSINT

a) Capture_Kenya – Tout le monde est la bienvenue à la #GCSC2022

Dans cette capture il m'a suffi de me référer au mot de passe que j'avais reçu par courrier.
Si telle le cas pour cette capture en me référant des infos ci-dessous

- ➔ Pseudonyme : CyberBadCorp
- ➔ Email : cyberbadcorp@gmail.com
- ➔ Token d'inscription : 20022022

Le mot de passe est : GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022

Flag : GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}

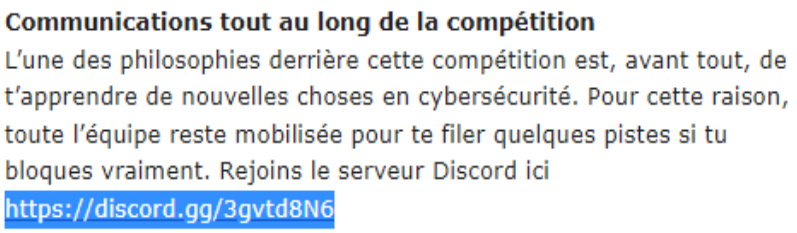
b) Capture_Madagascar – Accès au serveur discord !

Dans cette capture le flag se trouvait dans le courrier reçu de la part de GCSC

Ouvrir le courrier Guinean Cyber Security Challenge

Aller dans la section « Communications tout au long de la compétition »

Copier le lien discord qui est notre flag : https://discord.gg/3gvtd8N6



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

c) Capture_Argentine – Bonus

Il suffisait de cliquer sur hint pour avoir le flag

V. CRYPTANALYSIS

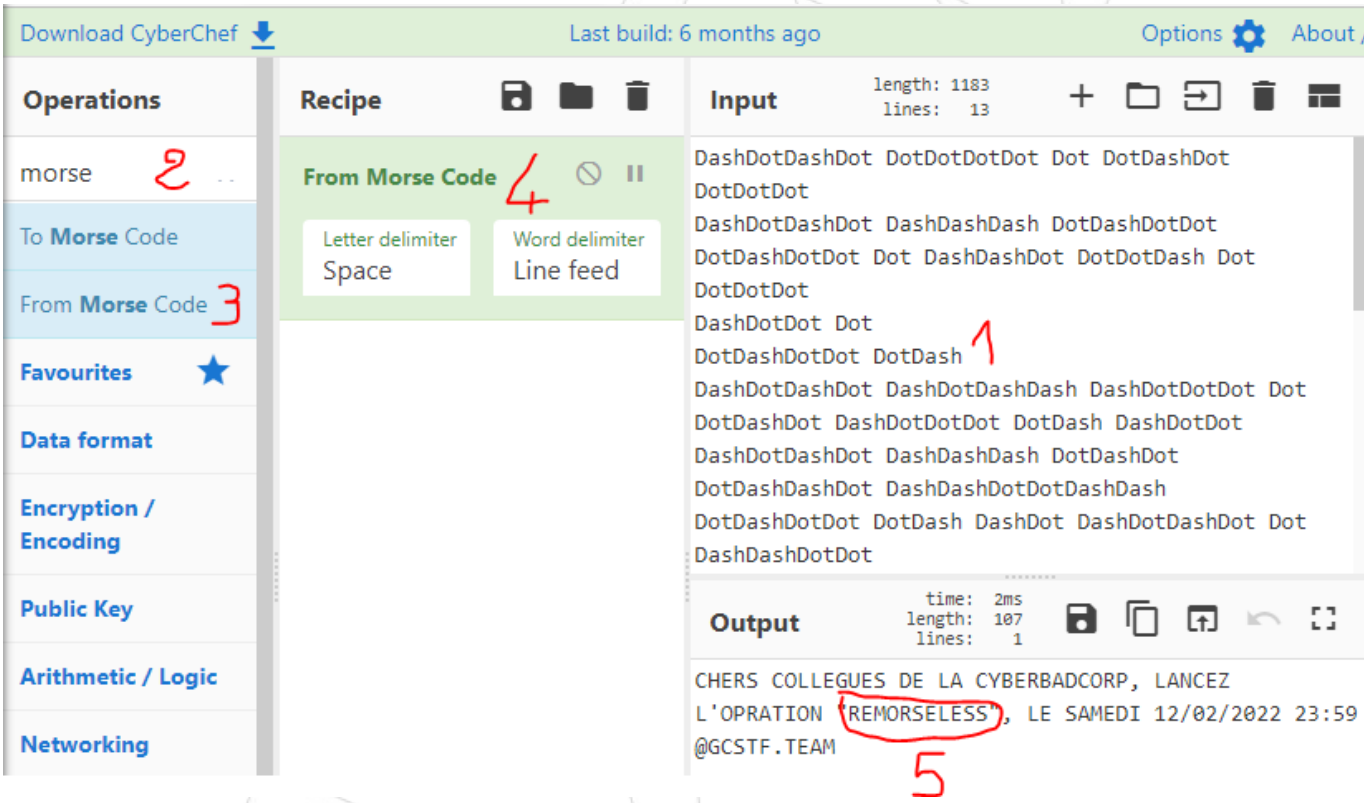
a) Capture_Algeria – Des point tiré (tirets) ?

Je clique sur Link 1 et je suis redirigé vers la page Google drive et je copie le contenu du fichier affiché

Je vais sur le site https://gchq.github.io/CyberChef/

J'y colle le texte dans input et cherche l'opération morse dans search

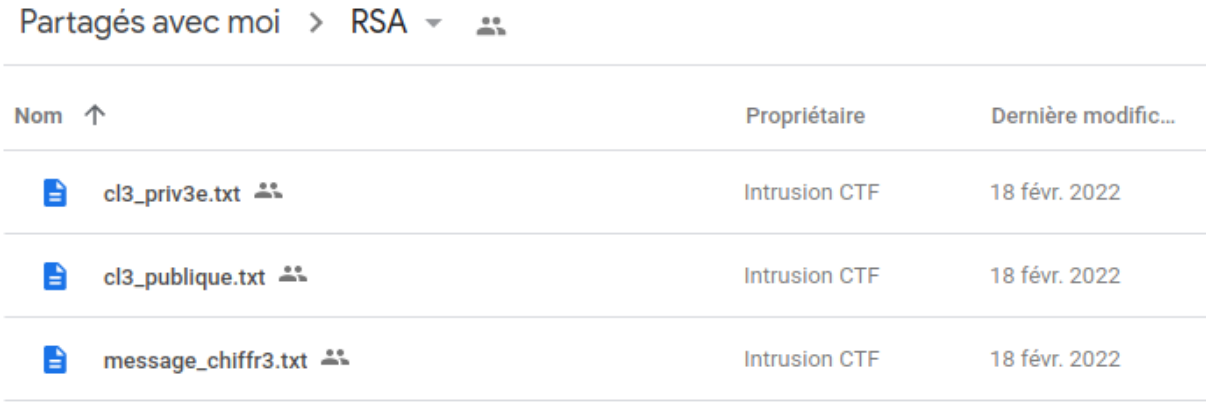
Je maintiens From morse code et le place dans recipe et le tour est joue



Flag : GCSC2022{remorseless}

b) Capture_United States – Ils vivent avec le RSA en France?

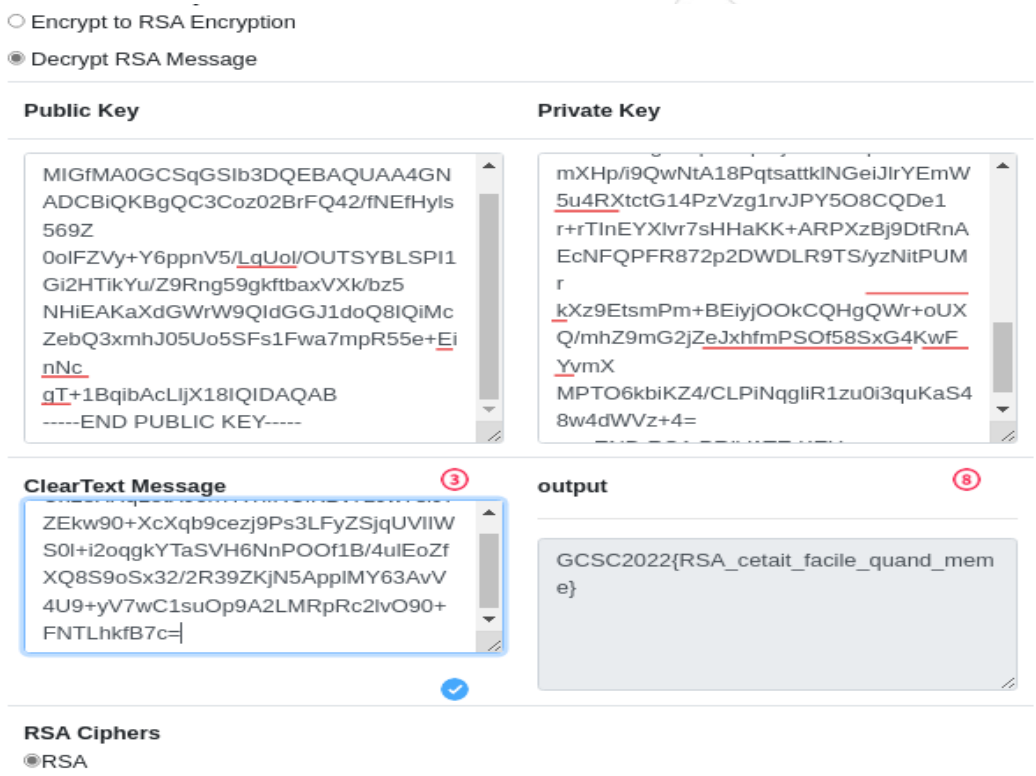
Je clique sur Link 1 et je suis redirigé vers la page Google drive ou se trouve trois fichiers dont la clé publique, la clé privée et le message chiffre



Je vais sur le site https://8gwifi.org/rsafunctions.jsp

Sélectionner Decrypte RSA Message et copier y la clé publique, la clé privée et le message chiffre

Au niveau d'output nous avons notre flag

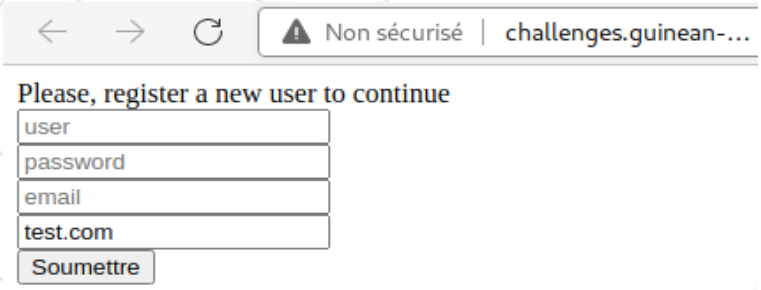


Flag : GCSC2022{RSA_cetait_facile_quand_meme}

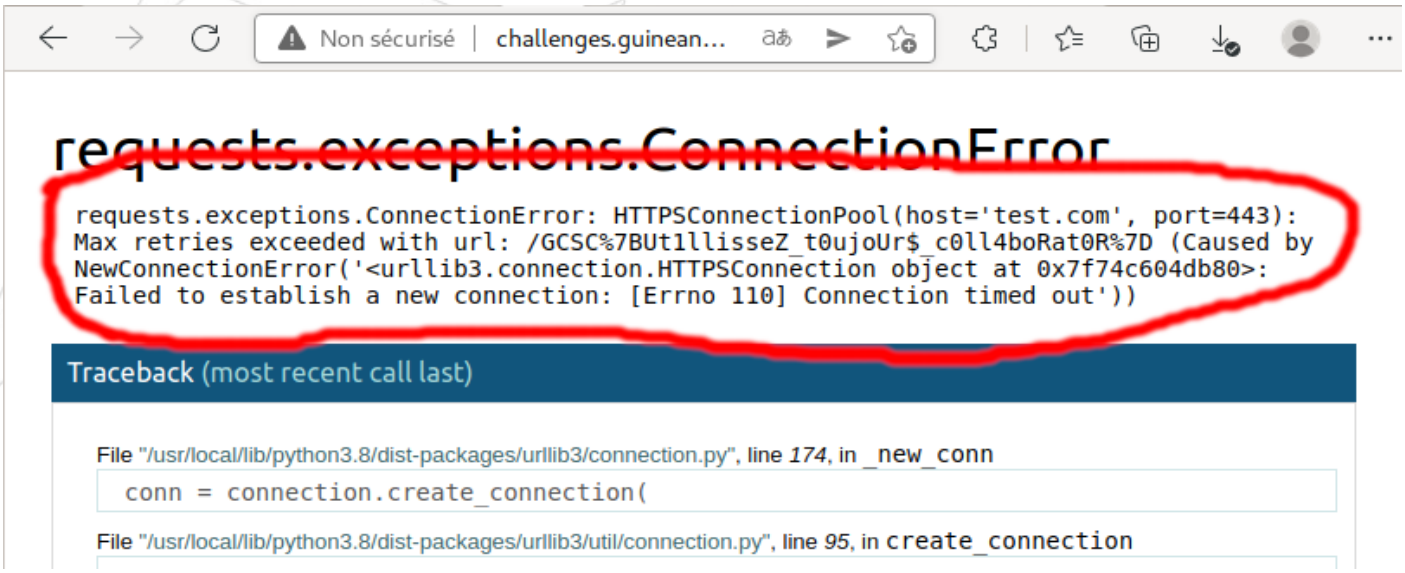
VI. WEB SECURITY

a) Capture_Canada – IP_publique x Collaborer x Interagir

Clique sur Link 1 et je suis redirigé vers une page web ou j'ai rempli les champs et soumis



Et puis une nouvelle page d'erreur va s'ouvrir et je clique sur la partie encercle



Je suis redirigé vers le flag en question

```
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}')
```

File "/usr/local/lib/python3.8/dist-packages/requests/api.py", line *75*, in get

```
return request('get', url, params=params, **kwargs)
```

File "/usr/local/lib/python3.8/dist-packages/requests/api.py", line *61*, in request

```
return session.request(method=method, url=url, **kwargs)
```

Flag : GCSC2022{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}