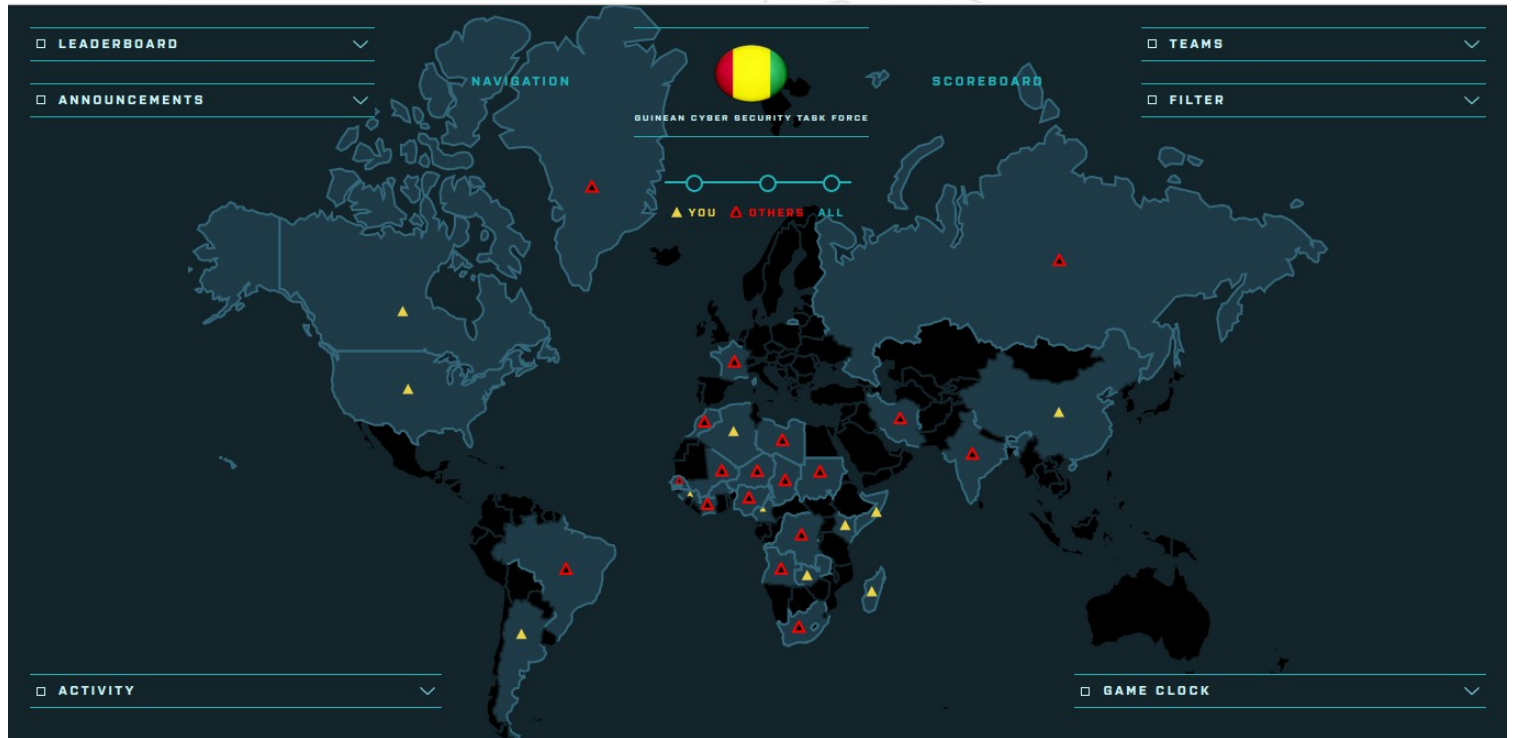




# HIDDEN'S WRITE-UP GCSC2022



## Table des matières

I. QUIZZ.....	2
a) Capture_Guinea – B.A. – BA v1.....	2
II. STEGANALYSIS.....	2
a) Capture_Cameroon – Voler des informations avec classe. Quel art !.....	2
b) Capture_Chine – Sais-tu réellement programmer ?.....	3
III. NETWORK SECURITY.....	3
a) Capture_Somalia – Cybertalent ! Il faut mettre le paquet... 1/2.....	3
b) Capture_Zambia – Cybertalent ! Il faut mettre le paquet... 2/2.....	5
IV. OSINT.....	6
a) Capture_Kenya – Tout le monde est la bienvenue à la #GCSC2022.....	6
b) Capture_Madagascar – Accès au serveur discord !.....	6
c) Capture_Argentine – Bonus.....	7
V. CRYPTANALYSIS.....	7
a) Capture_Algeria – Des point tiré (tirets) ?.....	7
b) Capture_United States – Ils vivent avec le RSA en France?.....	7
VI. WEB SECURITY.....	8
a) Capture_Canada – IP_publicue x Collaborer x Interagir.....	8

# I. QUIZZ

## a) Capture\_Guinea – B.A. – BA v1

Je suis Allé 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

**.gn** est le domaine national de premier niveau (country code top level domain : ccTLD) réservé à la Guinée.

**.gn - Wikimonde**  
[wikimonde.com/article/.gn](https://wikimonde.com/article/.gn)

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](https://justiceguinee.gov.gn) nous avons la seconde réponse qui est “LOI L-2016-037-AN”

**LOI L-2016-037-AN Relative à la Cybersecurite et la ...**

<https://justiceguinee.gov.gn/laws/loi-l-2016-037...>

LOI L-2016-037-AN Relative à la Cybersecurite et la Protection des données à caractère personnel

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}**

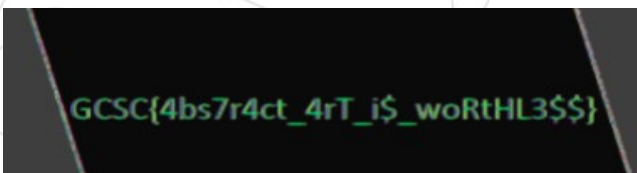
# II. STEGANALYSIS

## a) Capture\_Cameroon – Voler des informations avec classe. Quel art !

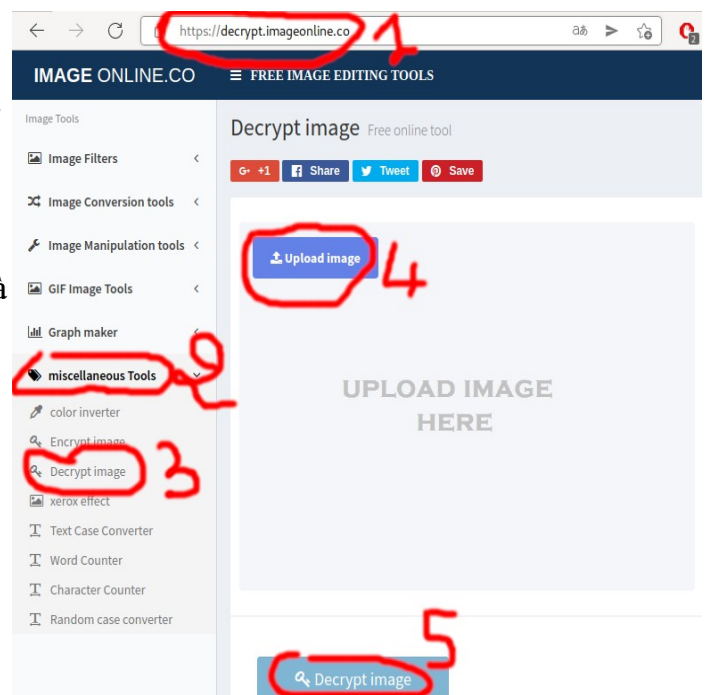
J'ai Cliqué sur Link 1 et télécharger l'image art abstrait.png

Je suis allé 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 à 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('poem-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

```
l-$ /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

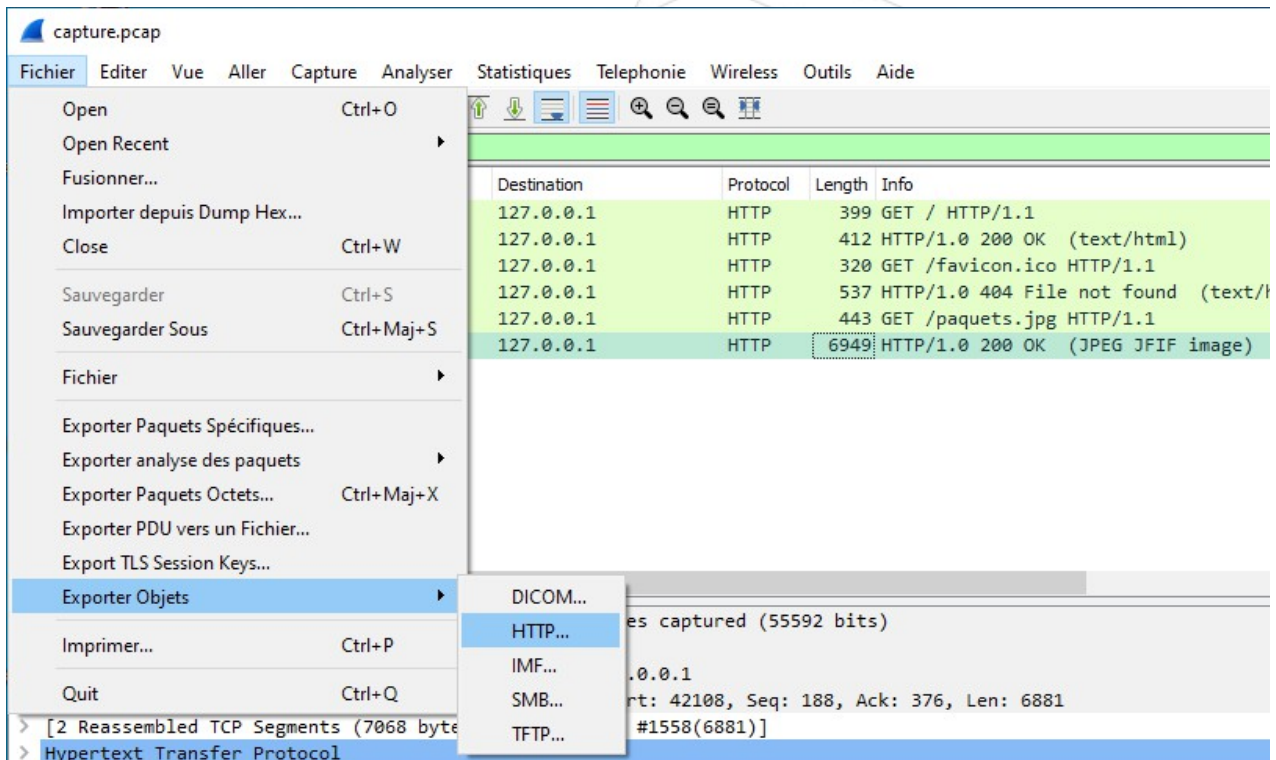
Je Clique sur Link 1 et je télécharge le fichier capture.pcap

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

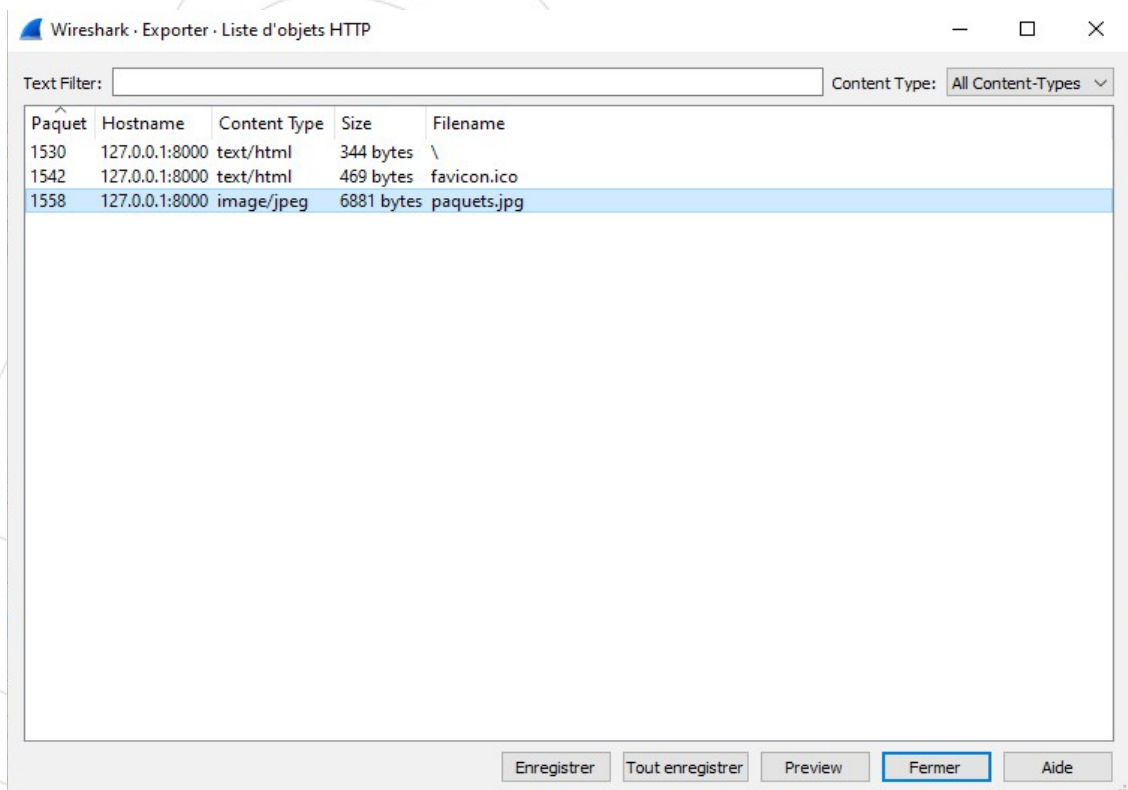
Je sélectionne "http/1.0 200 ok (JPEG JFIF image)"

No.	Time	Source	Destination	Protocol	Length	Info
1526	10.459035	127.0.0.1	127.0.0.1	HTTP	399	GET / HTTP/1.1
1530	10.460431	127.0.0.1	127.0.0.1	HTTP	412	HTTP/1.0 200 OK (text/html)
1538	10.560766	127.0.0.1	127.0.0.1	HTTP	320	GET /favicon.ico HTTP/1.1
1542	10.569641	127.0.0.1	127.0.0.1	HTTP	537	HTTP/1.0 404 File not found (text/html)
1554	14.014549	127.0.0.1	127.0.0.1	HTTP	443	GET /paquets.jpg HTTP/1.1
1558	14.015526	127.0.0.1	127.0.0.1	HTTP	6949	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\$\_I3\$\_p4Qu3t5}

**Flag : GCSC2022{ToU7\_3sT\_d4N\$\_I3\$\_p4Qu3t5}**

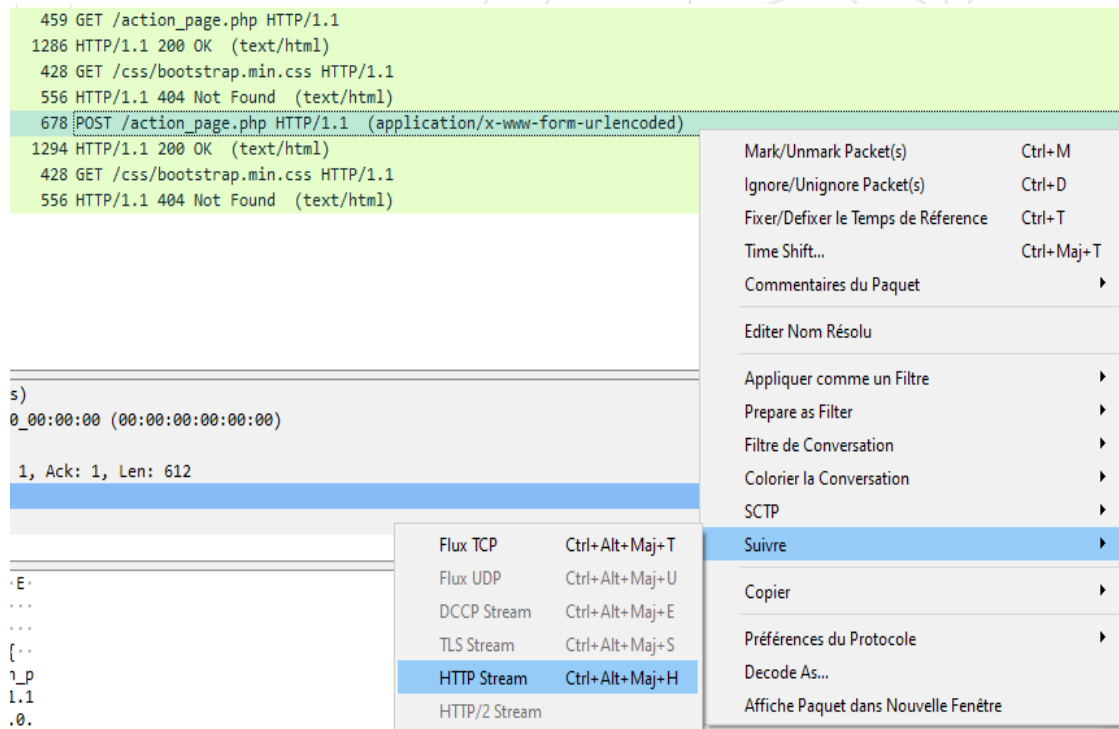
## b) Capture\_Zambia – Cybertalent ! Il faut mettre le paquet... 2/2

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 boîte de dialogue qui s'affiche je sélectionne et copie le mot de passe

```
Origin: http://127.0.0.1:34001
DNT: 1
Connection: keep-alive
Referer: http://127.0.0.1:34001/action_page.php
Cookie: PHPSESSID=uv65t4im8jpsbohgihnj4r6qou
Upgrade-Insecure-Requests: 1

username=GCSC&password=%78Ut1l1%243z_70uJoUR%24_H77P%24%21%7D&login=HTTP/1.1 200 OK
Date: Sun, 06 Feb 2022 11:17:59 GMT
Server: Apache/2.4.46 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
```

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 joué

Operations	Recipe	Input
url	URL Decode	%7BUT111%243z_70uJoUR%24_H77P%24%21%7D
Defang URL		
URL Decode		
URL Encode		
Extract URLs		
Split Colour Channels		

Output
{Ut111\$3z_70uJoUR\$_H77P\$!}

**Flag : GCSC2022{Ut111\$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

#### Guinean Cyber Security Challenge



**Equipe GCSTF** <contact... 19 févr. 2022 21:14 (il y a 2 jours) ☆ ↩ ⋮  
À moi ▾

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

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

#### Communications tout au long de la compétition

L'une des philosophies derrière cette compétition est, avant tout, de t'apprendre de nouvelles choses en cybersécurité. Pour cette raison, toute l'équipe reste mobilisée pour te filer quelques pistes si tu bloques vraiment. Rejoins le serveur Discord ici

<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 joué

Download CyberChef Last build: 6 months ago Options About

**Operations**

- morse 2
- To Morse Code
- From Morse Code 3
- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking

**Recipe**

From Morse Code 4

Letter delimiter: Space Word delimiter: Line feed

**Input** length: 1183 lines: 13

DashDotDashDot DotDotDotDot Dot DotDashDot  
DotDotDot  
DashDotDashDot DashDashDash DotDashDotDot  
DotDashDotDot Dot DashDashDot DotDotDash Dot  
DotDotDot  
DashDotDot Dot  
DotDashDotDot DotDash 1  
DashDotDashDot DashDotDashDash DashDotDotDot Dot  
DotDashDot DashDotDotDot DotDash DashDotDot  
DashDotDashDot DashDashDash DotDashDot  
DotDashDashDot DashDashDotDotDashDash  
DotDashDotDot DotDash DashDot DashDotDashDot Dot  
DashDashDotDot

**Output** time: 2ms length: 107 lines: 1

CHERS COLLEGUES DE LA CYBERBADCORP, LANCEZ  
L'OPRATION REMORSELESS, LE SAMEDI 12/02/2022 23:59  
@GCSTF.TEAM 5

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 chiffré

Partagés avec moi > RSA

Nom ↑	Propriétaire	Dernière modif...
cl3_priv3e.txt	Intrusion CTF	18 févr. 2022
cl3_publique.txt	Intrusion CTF	18 févr. 2022
message_chiffr3.txt	Intrusion CTF	18 févr. 2022

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 chiffré

Au niveau d'output nous avons notre flag

☐ Encrypt to RSA Encryption  
☒ Decrypt RSA Message

**Public Key**

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3Coz02BrFQ42/fNEfHyls569Z0oIFZVy+Y6ppnV5/LqUoL/OUTSYBLSP1Gi2HTikYu/Z9Rng59gkftbaxVXk/bz5NHIEAKaXdGWRW9QIdGGJ1doQ8IQiMcZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+Ei  
nNc  
qT+1BqibAcLijX18IQIDAQAB  
-----END PUBLIC KEY-----
```

**Private Key**

```
mXHp/i9QwNtA18PqtsattkiNGeiJlrYEmW5u4RXtctG14PzVzg1rvJPY5O8CQDe1r+rTlnEYXlvr7sHHaKK+ARPxzBj9DtRnAEcNFQPFR872p2DWDLR9TS/yzNitPUMr  
kXz9EtsmPm+BEiyjOOKCQHgQWr+oUXQ/mhZ9mG2jZeJxhfmPSOf58SxG4KwFYymXMPTO6kbiKZ4/CLPiNqgliR1zu0i3quKaS48w4dWVz+4=
```

**ClearText Message**

```
ZEkw90+XcXqb9ceZj9Ps3LFyZSjqUVIiW  
S0H+i2oqgkYTaSVH6NnPOOf1B/4ulEoZf  
XQ8S9oSx32/2R39ZKjN5ApplMY63AvV  
4U9+yV7wC1suOp9A2LMRpRc2lvO90+  
FNTLhkfB7c=
```

**output**

```
GCSC2022{RSA_cetait_facile_quand_mem  
e}
```

**RSA Ciphers**

☒ RSA

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

← → ↻ ⚠ Non sécurisé | challenges.guinean-...

Please, register a new user to continue

user

password

email

test.com

Soumettre

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

← → ↻ ⚠ Non sécurisé | challenges.guinean... ⌨ ▶ ⚙ ⭐ ⛶ ⬇ 👤 ...

# requests.exceptions.ConnectionError

```
requests.exceptions.ConnectionError: HTTPSConnectionPool(host='test.com', port=443):  
Max retries exceeded with url: /GCSC%7BUt1llisseZ_t0ujoUr$_c0ll4boRat0R%7D (Caused by  
NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f74c604db80>':  
Failed to establish a new connection: [Errno 110] Connection timed out'))
```

Traceback (most recent call last)

File "/usr/local/lib/python3.8/dist-packages/urllib3/connection.py", line 174, in \_new\_conn

```
conn = connection.create_connection(  
    host, port, timeout=self.timeout, source_address=source_address)
```

File "/usr/local/lib/python3.8/dist-packages/urllib3/util/connection.py", line 95, in create\_connection



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}**