CTF GCSC 2022 — Write-up

Pseudo : P0ull0

La **Guinean Cyber Security Challenge (GCSC)**, est la première et plus grande compétition nationale d'hacking éthique et de cybersécurité en République de Guinée. Elle est organisée par l'association **Guinean Cyber Security Task Force.**

La **GCSC** s'est déroulé le dimanche **20 Février 2022 de 00h00 à 23h59**, soit 24h de challs, en explorant les techniques d'intrusion les plus récentes.

Dans ce write-up, j'explique comment j'ai pu résoudre les différents types de challenges du CTF (Web, Stegano, OSINT, Crypto, …).

Merci à toutes l'équipe de **GCSTF** pour l'organisation de cet évènement et pour la gestion du CTF !

Les challenges

Guinea — Quizz : B.A — BA v1

```
En tant que Agent de terrain, tu dois connaître au bout des doigts les
empreintes numériques de notre pays.

Les malveillants que tu seras amené à traquer pourraient les utiliser en
remplacement de son nom officiel "Guinée".

1. Quel est le ccTLD de la Guinée ?
2. Quel est la codification de la loi relative à la Cybersécurité et la
Protection des Données à Caractère Personnel en Guinée?
3. Quel est le fuseau horaire de la Guinée?

- Le format attendu est :
Réponse1: tout en minuscule
Réponse2: tout en majuscule
Réponse3: tout en majuscule et n'oublie pas le petit +

Flag: GCSC2022{Reponse1_Reponse2_Reponse3}
```

Énoncé quizz Guinée

Ici, il était de question de répondre à des questions, pour répondre à ces différentes questions, j'ai fait des recherches sur Google afin d'obtenir le flag.

Loi L2016–037-AN

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

Madagascar — OSINT : Accès au serveur Discord

Énoncé Chall Madagascar

Ce premier challenge était un petit cadeau de la part des organisateurs pour nous familiariser avec la plateforme, il fallait tout simplement indiquer le lien du serveur Discord fourni. :)

Somalia — Network Security : Il faut mettre le paquet ...1/2

```
Les membres de la CyberBadCorp en sont conscients. Alors, ils font
souvent recours aux cybercafés.

Or, 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.

Plus concrètement, il s'agit d'identifier les utilisateurs, de
journaliser les actions et superviser l'ensemble des flux entrants et
sortants de chaque poste.

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

Y a t'il quelque chose dans ces paquets qui mettraient en péril la
sécurité nationale?
```

Énoncé chall Somalia

Sur ce challenge, nous avions une capture réseau, avec Wireshark nous pouvons facilement observer le trafic réseau capturé, en ouvrant le fichier avec Wireshark on constate que le client a demandé une image au serveur.

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)

En exportant les ressources de type **HTTP** (file -> export objects -> HTTP) nous pouvons consulter les ressources qu'il a consultées et là, en ouvrant l'image, on obtient le flag.

GCSC{ToU7_3sT_d4N$_l3$_p4Qu3t5}

Zambia - Network Security : Il faut mettre le paquet ...2/2

```
Tu décides de continuer l'analyse des captures réseaux des cybercafés de
la capitale que tu as commencé dans le Challenge Somalie.

Cette fois-ci, tu remarques qu'un membre de la CyberBadCorp présent dans
ce cybercafé ce jour-là, s'est rendu sur le darkweb où il a passé la
commande de nombreuses armes de guerre.

Retrouve son nom d'utilisateur, son mot de passe et surtout le message de
la commande.

Flag: GCSC2022{flag_ici}
```

Énoncé chall Zambia

Pour ce second challenge de réseau, nous avions également une capture réseau à analyser, d'après le titre du fichier, il s'agit d'une connexion non sécurisée donc toutes les données qui y transitent sont en clair.

```
Apply a display filter ... <⌘/>
| Time | Source | Destination | Protoc | Length | Info
4 0.000069   127.0.0.1   127.0.0.1   HTTP   459   GET /action_page.php HTTP/1.1
6 0.001836   127.0.0.1   127.0.0.1   HTTP   1286  HTTP/1.1 200 OK  (text/html)
8 0.079055   127.0.0.1   127.0.0.1   HTTP   428   GET /css/bootstrap.min.css HTTP/1.1
10 0.079260  127.0.0.1   127.0.0.1   HTTP   556   HTTP/1.1 404 Not Found  (text/html)
18 59.669810 127.0.0.1   127.0.0.1   HTTP   678   POST /action_page.php HTTP/1.1  (app
20 59.671389 127.0.0.1   127.0.0.1   HTTP   1294  HTTP/1.1 200 OK  (text/html)

  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
> Content-Length: 68\r\n
  Origin: http://127.0.0.1:34001\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Referer: http://127.0.0.1:34001/action_page.php\r\n
> Cookie: PHPSESSID=uv65t4im8jpsbohgihnj4r6qou\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://127.0.0.1:34001/action_page.php]
  [HTTP request 1/2]
  [Response in frame: 20]
  [Next request in frame: 22]
  File Data: 68 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "GCSC"
v Form item: "password" = "{Ut1l1$3z_70uJoUR$_H77P$!}"
    Key: password
    Value: {Ut1l1$3z_70uJoUR$_H77P$!}
```

En analysant les données HTTP, on voit clairement les identifiants transmis (méthode POST) au serveur, le flag ici correspond au mot de passe : ***{Ut1l1$3z_70uJoUR$_H77P$!}***

South Africa — Stegano: Au super marché

```
Tu fais de la filature depuis plusieurs semaines sur un membre actif de
la CyberBadCorp.

Tous les jours, il se rend dans cette même enseigne pour faire ses
courses.

Tu as remarqué qu'il prend assez de temps dans le rayon des céréales.

Pointilleux sur les détails, tu décides de prendre une séquence photos
des produits de ce rayon pour les analyser.

Sans surprise, tu trouves que cette image est un peu particulière à vue
d'œil.

Arriveras-tu à trouver des informations qui feront avancer ta mission?

Flag: GCSC2022{flag_ici}
```

Énoncé chall South Africa

Sur cette épreuve, nous avions cette image ci-dessous à analyser :

En faisant un zoom sur l'image, on observe des codes-barres, je décide d'ouvrir cette image de type SVG avec Firefox pour télécharger les codes-barres et ainsi essayer de trouver ce qui sache derrière.

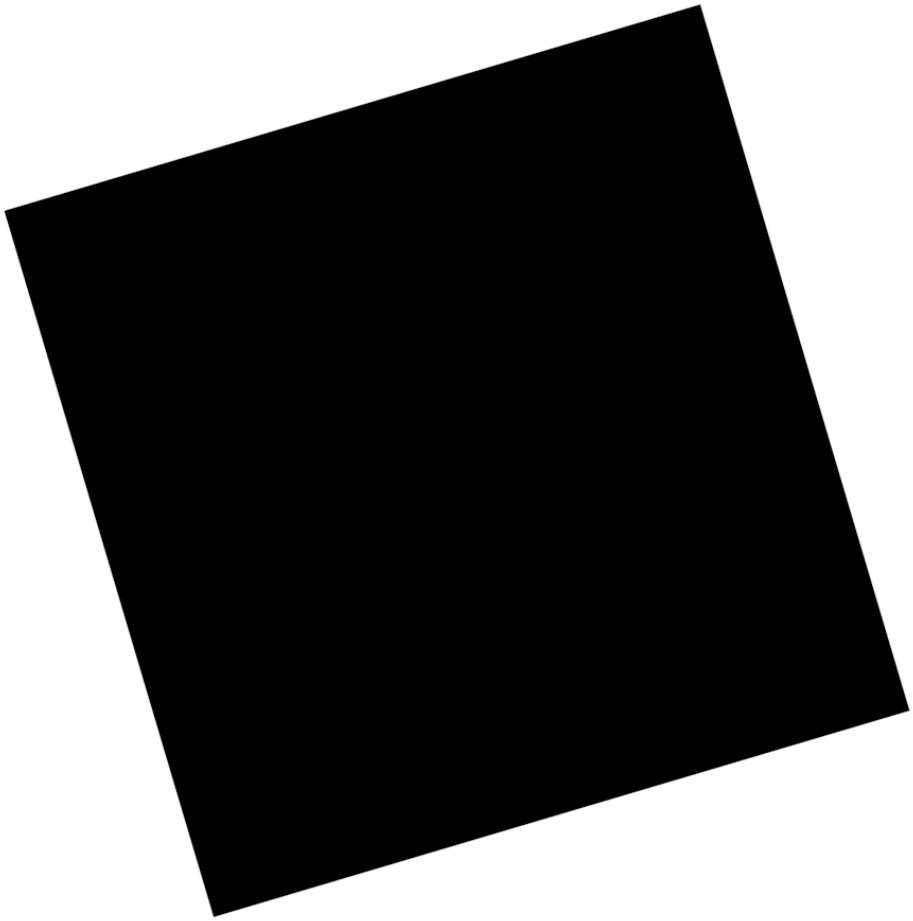
Après avoir téléchargé les codes-barres, j'utilise un outil en ligne pour le déchiffrer et là nous avons le flag.

Cameroon — Stegano : voler les informations avec classe. Quel art !

```
Cette nuit encore, un nouvel incident de sécurité s'est produit du côté
de la préfecture de Kankan.

Apres avoir eu un accès au SI, le malveillant tente d'exfiltrer des
informations par l'envoi d'une image d'apparence anodine.

Il semble que c'est la technique utilisée par la CyberBadCorp avant que
tu ne rejoignes le rang des cybercombattants guinéens.

Analyse attentivement cette image et trouve l'information exfiltrée.

Flag: GCSC2022{flag_ici}
```

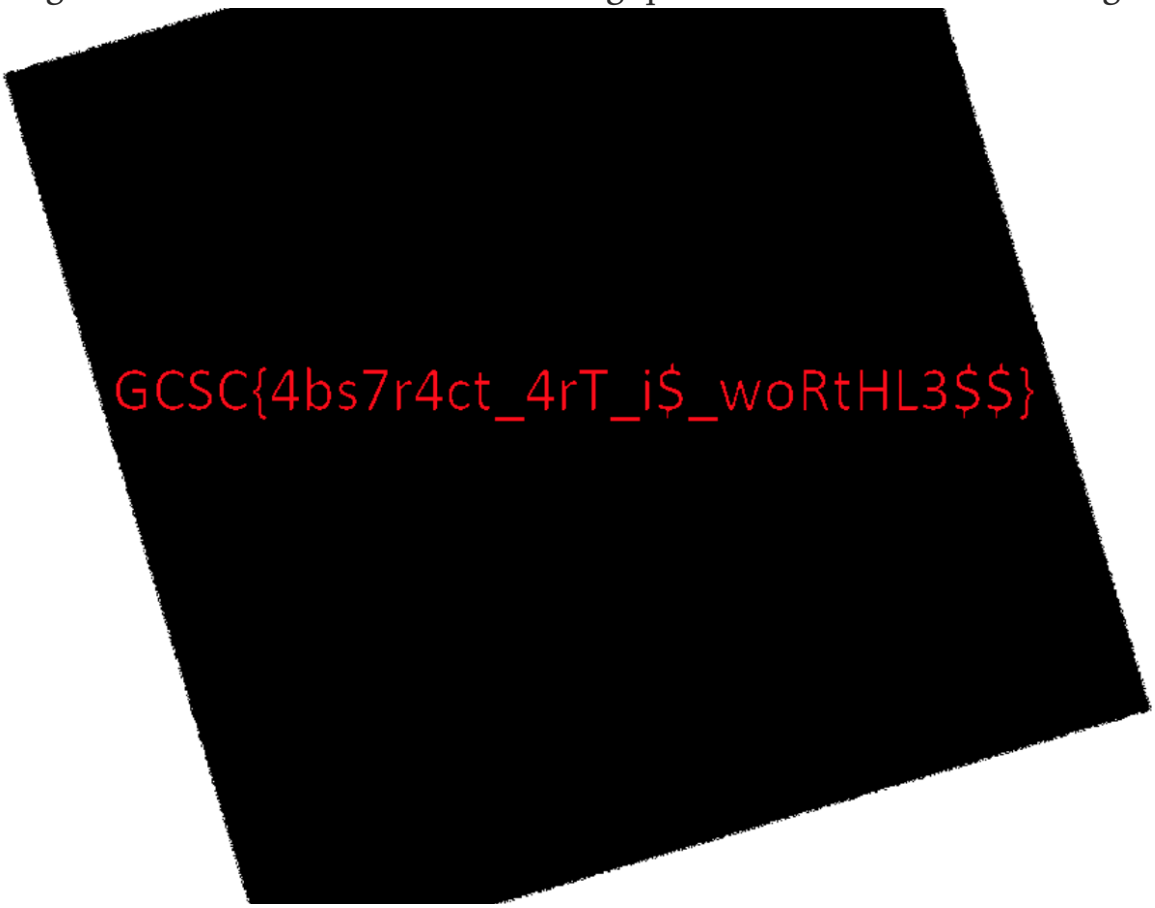
Énoncé chall Cameroon

Pour cette autre épreuve de stegano, nous avions aussi une image à analyser :



Art abstrait

Comme on le constate, nous ne voyons que du noir sur cette image, mais est-ce réellement le cas ? Pour ce type de challenge, j'utilise en général Aperi'Solve qui est une plateforme en ligne qui effectue une analyse des couches sur l'image qui comporte plusieurs outils de stegano comme zsteg, steghide, outguess, exiftool, binwalk, foremost et strings. En analysant l'image avec cet outil on découvre le flag qui se trouve sur ce filtre rouge.



Flag chall Cameroon

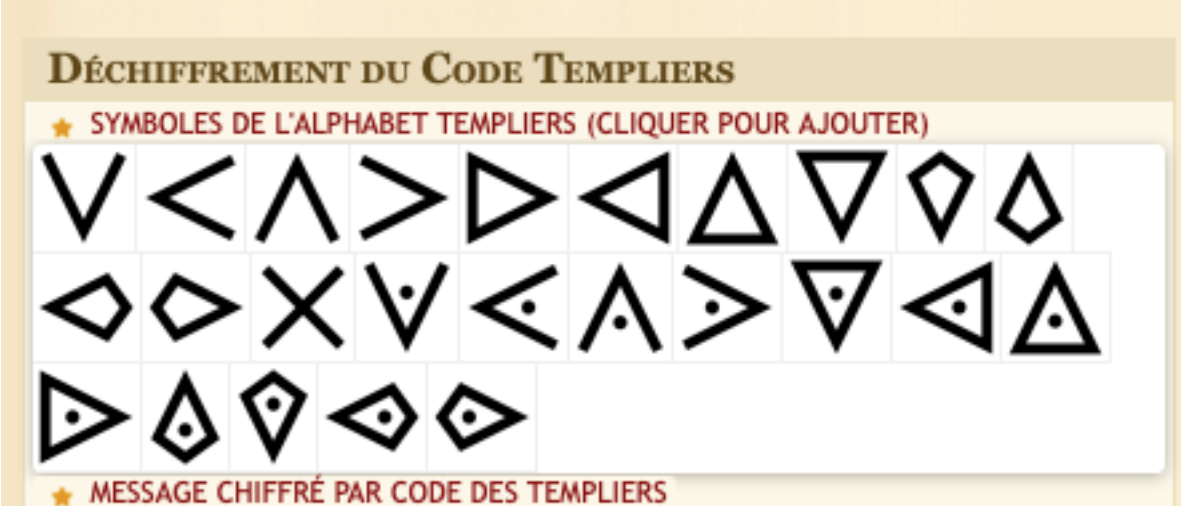
Lybia — Crypto : c'était quoi le trésor des templiers

```
Ouh! Ce sont des génies ces petits malins.

Que voulait dire ce membre fuité de la CyberBadCorp aux nouvelles
recrues?

Flag: GCSC2022{mot1_mot2_mot3}
```

Énoncé chall Lybia

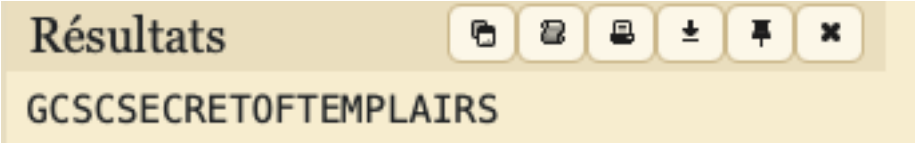
Message templiers

Ici, nous avons un message à décrypter, mais quel type de chiffrement est utilisé ici ? Je demande cela à notre ami à tous (Google), et là, je tape “ message templier” j’ouvre le premier lien, et je tombe sur un outil que j’ai l’habitude d’utiliser pour chiffrer et déchiffrer des messages :



Chiffrement templiers

Je recopie les symboles qui sont sur l’image pour obtenir le message chiffré :



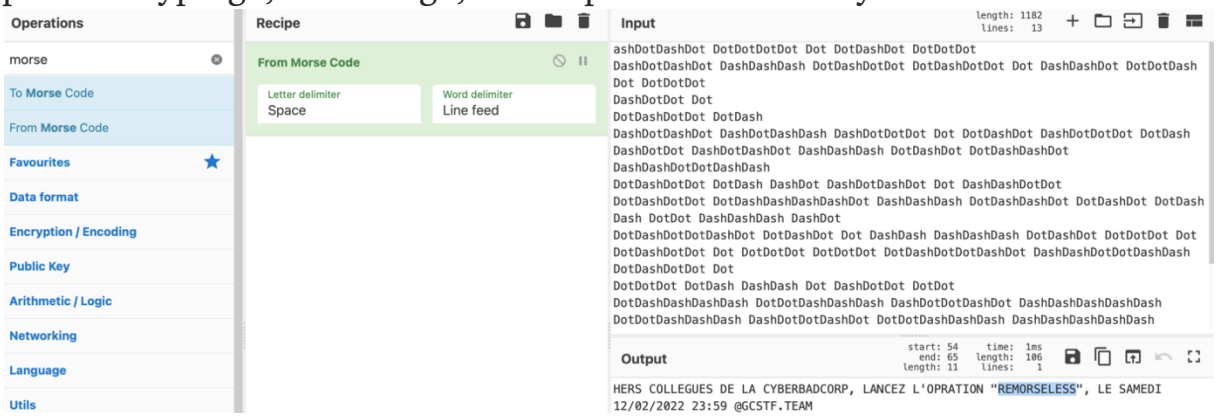
Algeria — Crypto : Des points tirés (tirets)

```
La CyberBadCorp vient de recruter un stagiaire débutant pour développer
son malware.

Ce dernier ayant appris la cryptographie sur le tas, il pense bien
dissimuler les informations sur la prochaine attaque.

Retrouve le nom de l'opération dans le fichier ou lien joint et préviens
tes collègues.

Flag : GCSC2022{minuscule(nom_de_loperation)}
```

Énoncé chall Algeria

```
ashDotDashDot DotDotDotDot Dot DotDashDot DotDotDot
DashDotDashDot DashDashDash DotDashDotDot DotDashDotDot Dot
DashDashDot DotDotDash Dot DotDotDot
DashDotDot Dot
DotDashDotDot DotDash
DashDotDashDot DashDotDashDash DashDotDotDot Dot DotDashDot
DashDotDotDot DotDash DashDotDot DashDotDashDot DashDashDash
DotDashDot DotDashDashDot DashDashDotDotDashDash
DotDashDotDot DotDash DashDot DashDotDashDot Dot DashDashDotDot
DotDashDotDot DotDashDashDashDashDot DashDashDash DotDashDashDot
DotDashDot DotDash Dash DotDot DashDashDash DashDot
DotDashDotDotDashDot DotDashDot Dot DashDash DashDashDash
DotDashDot DotDotDot Dot DotDashDotDot Dot DotDotDot DotDotDot
DotDashDotDotDashDot DashDashDotDotDashDash
DotDashDotDot Dot
DotDotDot DotDash DashDash Dot DashDotDot DotDot
DotDashDashDashDash DotDotDashDashDash DashDotDotDashDot
DashDashDashDashDash DotDotDashDashDash DashDotDotDashDot
DotDotDashDashDash DashDashDashDashDash DotDotDashDashDash
DotDotDashDashDash
DotDotDashDashDash DotDotDotDashDash DashDashDashDotDotDot
DotDotDotDotDot DashDashDashDashDot
DotDashDashDotDashDot DashDashDot DashDotDashDot DotDotDot Dash
DotDotDashDot DotDashDotDashDotDash Dash Dot DotDash DashDash
```

Sur ce challenge de crypto, nous avions ce message ci-dessus à déchiffrer, n'ayant aucune idée de quel type de chiffrement dont il pourrait s'agir, je fais une recherche sur Google aussi et je découvre que c'est de l'Alphabet Morse, je décide donc d'utiliser ***Cyberchef*** qui est une application web pour le cryptage, l'encodage, la compression et l'analyse des données.



Cyberchef — Morse

en collant le message en Morse, l'application nous donne directement le message correspondant, le flag correspond ici au nom de l'opération "**remorseless**"

USA — Crypto : Ils vivent avec le RSA en France

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


Indice: -5 points
Flag: GCSC2022{flag_ici}
```

Énoncé challenge USA

Sur cette nouvelle épreuve de cryptographie, un indice est donné dans le titre "**RSA**" et l'énoncé nous fait part d'une clé privée et d'une clé publique, donc on peut en déduire qu'il s'agit d'un chiffrement asymétrique de type **RSA** qui utilise une paire de clés composée d'une *clé publique* pour chiffrer et d'une *clé privée* pour déchiffrer des données confidentielles.

De plus sur le lien fourni sur ce chall, nous avions une clé privée, une clé publique et d'un message chiffré, donc reste plus qu'à déchiffrer le message, j'ai trouvé un outil en ligne qui permet de déchiffrer tout cela en fournissant le contenu des clés ainsi que le message, à la fin du processus nous avions le flag.

Public Key

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNAD
CBiQKBgQC3Coz02BrFQ42/fNEfHyIs569Z
0olFZVy+Y6ppnV5/LqUol/OUTSYBLSPI1Gi2
HTikYu/Z9Rng59gkftbaxVXk/bz5
NHiEAKaXdGWrW9QIdGGJ1doQ8IQiMcZe
bQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNc
gT+1BqibAcLljX18IQIDAQAB
-----END PUBLIC KEY-----

Private Key

mXHp/i9QwNtA18PqtsattklNGeiJlrYEmW
5u4RXtctG14PzVzg1rvJPY5O8CQDe1
r+rTlnEYXlvr7sHHaKK+ARPXzBj9DtRnAE
cNFQPFR872p2DWDLR9TS/yzNitPUMr
kXz9EtsmPm+BEiyjOOkCQHgQWr+oUX
Q/mhZ9mG2jZeJxhfmPSOf58SxG4KwFY
vmX
MPTO6kbiKZ4/CLPiNqgliR1zu0i3quKaS4
8w4dWVz+4=
-----END RSA PRIVATE KEY-----

ClearText Message

UxL8XXqLetXJ0h7RTifRCiKBv7zJw7siJ7
ZEkw90+XcXqb9cezj9Ps3LFyZSjqUVlIW
S0l+i2oqgkYTaSVH6NnPOOf1B/4ulEoZfX
Q8S9oSx32/2R39ZKjN5ApplMY63AvV4
U9+yV7wC1suOp9A2LMRpRc2lvO90+F

output

GCSC2022{RSA_cetait_facile_quand_meme}

RSA — Decrypt

Congo Kinshasa — Crypto : Hasher, c'est crypter

```
Un de nos agents du service de contre-espionnage a mis la main sur un
fichier crypté de la CyberBadCorp.

Aide-le à accéder à son contenu.

Flag: GCSC2022{flag_ici}
```

Énoncé chall Congo Kinshasa

Ici, nous avions en pièce jointe un fichier crypté de type "***kdbx***", pour avoir un peu plus d'info sur ce fichier j'utilise la commande "file" suivi du nom du fichier pour obtenir d'avantages d'informations et là, je vois qu'il s'agit d'une base de données de mot de passe ***Keepass***.

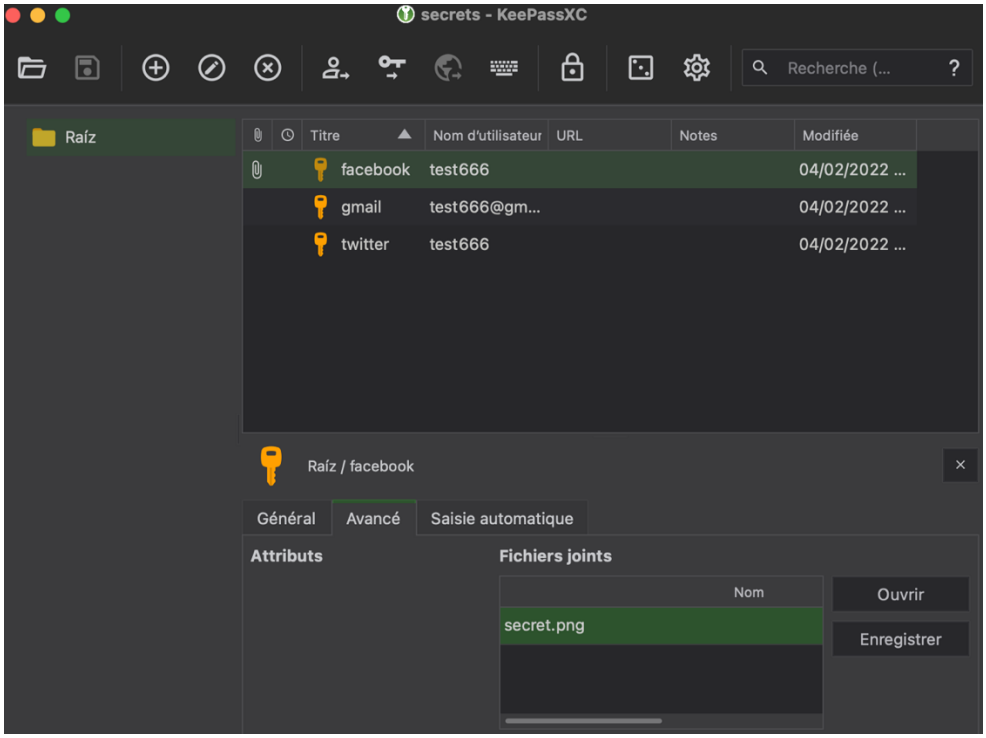
```
root@kali:~/Téléchargements# file secrets.kdbx
secrets.kdbx: Keepass password database 2.x KDBX
root@kali:~/Téléchargements#
```

kdbx file type

En essayant d'ouvrir ce fichier avec l'application Keepass, on me demandait un mot de passe pour accéder à la base de donnée, donc l'objectif ici est de cracker ce mot de passe, en faisant des recherches sur internet, je tombe sur un article qui montre comment cracker cette base de donné avec l'outil "***Keepass2john***", la première étape consiste à obtenir le hash du mot de passe stocké sur le fichier ensuite avec "***John the Ripper***" (outil conçu pour aider à trouver des mots de passe faibles par brute force) trouvé un mot passe dans le dictionnaire (rockyou.txt) qui pourrait correspondre au hash obtenu précédemment et la bingo !!!! J'obtiens le mot de passe : "***rellik000***", reste plus qu'a découvrir le contenu de la BD.

```
root@kali:~/Téléchargements# keepass2john
ch2.dmp       ch2.tbz2      output/       secrets.kdbx
root@kali:~/Téléchargements# keepass2john secrets.kdbx > keepasshash.txt
root@kali:~/Téléchargements#
root@kali:~/Téléchargements# cat keepasshash.txt
secrets:$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71bfb*4b76a74e00b23ed3ffe5c3a10afcafc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738
bba52abb75844796*417247c7668f1b979932dadb055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fadc57b12c32411b863593430aae2647cb30e437a3ab350b
root@kali:~/Téléchargements# john --worlist=rockyou.txt keepasshash.txt
Created directory: /root/.john
Unknown option: "--worlist=rockyou.txt"
root@kali:~/Téléchargements# john --wordlist=rockyou.txt keepasshash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 30 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
fopen: rockyou.txt: No such file or directory
root@kali:~/Téléchargements# john --wordlist=rockyou.txt keepasshash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 30 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rellik000        (secrets)
1g 0:00:00:15 DONE (2022-02-20 10:14) 0.06365g/s 51687p/s 51687c/s 51687C/s rellim11..rell101
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@kali:~/Téléchargements#
```

Keepass2john



Contenu secrets.kdbx

En ouvrant la database avec le mot passe trouvé précédemment, je ne trouve rien de particulier qui pourrait correspondre au flag, mais je constate qu'il y a une image enregistrée sur l'identifiant Facebook, je décide donc de l'enregistrer et de consulter celle-ci et là, j'obtiens le flag…

GCSC{4uCUn_7roUv3r4_C3t_MoT_D3_P45$3}

Flag chall Congo Kinshasa

Chad — Crypto : Clé de déchiffrement ou décryptage

```
Mon Dieu! Le pire est arrivé.

Déterminé à faire tomber la CyberBadCorp, à tout prix, tu as
malencontreusement cliqué sur un lien laissé exprès dans le téléphone que
tu as analysé.

Cela a crypté uniquement ton rapport d'avancement sur ladite mission.

Retrouve vite la clef de déchiffrement et continue a les traquer.

Flag: GCSC2022{flag_ici}
```

Énoncé chall Chad

Sur cette autre épreuve de crypto nous avions un fichier zip à déchiffrer, avec “***fcrackzip***” je crack le mot de passe en utilisant le dictionnaire de mot de passe “***rockyou.txt***”, mot de passe obtenu, j’ouvre le fichier zip, ainsi, j’obtiens le flag.

```
root@kali:~/Téléchargements# fcrackzip -u -D -p rockyou.txt note.zip


PASSWORD FOUND!!!!: pw == Catsandcows
root@kali:~/Téléchargements#
```

Bruteforce avce fcrackzip

```
note.txt
GCSC{p4$sw0rD_cr4ck1nG_br34kZ_GPUs}
```

Contenu note.txt

Nigeria — Misc : Mots de passe d’une application étrange

```
Les régions minières du pays attirent de plus en plus la CyberBadCorp.

Trois de leurs membres décident de s'installer dans la région de Kamsar
afin de dépouiller le plus d'entreprises d'exploitation.

En cours de chemin, ils s'arrêtent un moment dans un village pour manger
et se reposer avant de reprendre la route. Ils en profitent aussi pour
recharger leurs appareils dans un télécentre.

Le gérant du télécentre, agent secret, dumpe le contenu de leurs
téléphones qu'il te transmet à des fins d'analyse pour des questions de
sécurité nationale.

Lors de tes analyses, tu remarques qu'à un moment donné, tous les trois
ont utilisé le même téléphone pour se connecter à une application de
messagerie instantanée étrange.

Tu as vite retrouvé la base de données reliée à cette application.
Maintenant, trouve leurs mots de passe.
```

Énoncé chall Nigeria

Pour cet autre type de challenge, nous avions une base de données à analyser, ne sachant pas quel type de base données dont il pourrait s’agir,

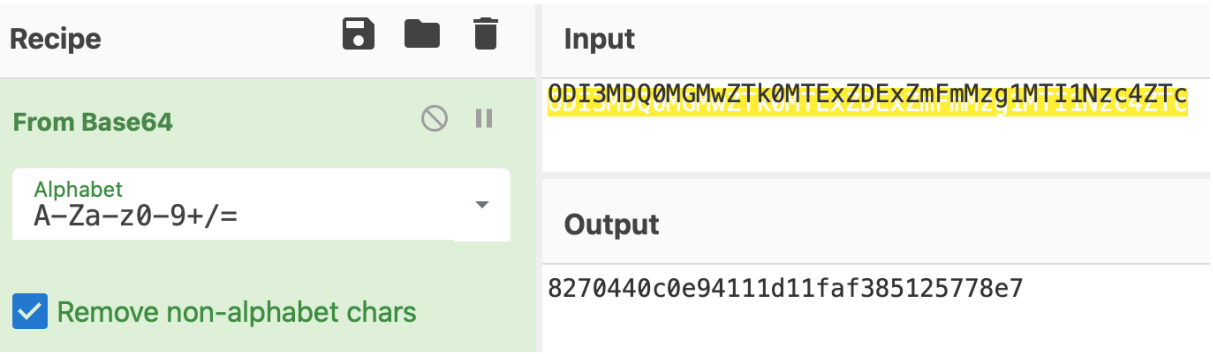
j'arrive à déterminer qu'il s'agit d'une base de données "***SQLite***" avec la commande "***file***".En ouvrant la base de données avec "***SQLite3***" je découvre qu'il n'y a qu'une seule table présente "***users***", à mon avis, il s'agit des identifiants d'utilisateurs, et le flag ici correspond aux 3 mots de passe des utilisateurs. Avec un outil en ligne, j'arrive à déterminer qu'il s'agit d'un hash en BASE64.

```
root@kali:~/Téléchargements# file db-mobile-application.db
db-mobile-application.db: SQLite 3.x database, last written using SQLite version 3028000
root@kali:~/Téléchargements# sqlite3 db-mobile-application.db
SQLite version 3.36.0 2021-06-18 18:36:39
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> SELECT * FROM users;
John|ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc=
Marie|NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK
Luc|NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK
sqlite>
```

Sqlite3

BASE64 — Hash type

J'utilise donc Cyberchef pour décoder le message, mais là encore, j'obtiens un autre message hashé, je réitère la même procédure pour déterminer le hash, et je découvre qu'il s'agit de MD5.



Cyberchef — From BAS64

✔ **Possible identifications:** Decrypt Hashes

```
8270440c0e94111d11faf385125778e7 - Possible algorithms: MD5
```

MD5 — Hash type

8270440c0e94111d11faf385125778e7 : **p1ntap**

Trouvé en 0.214s

MD5 decrypt

Je réussis à trouver le mot de passe hashé en MD5, je réitère le même process pour les 2 autres utilisateurs :

```
ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc - 8270440c0e94111d11faf385125778e7 - p1ntap
NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK - 41d538a71b2aa6004d53423771041c9c - fd1972
NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK - 4efcdac85c6c494b3cef8781cc639805 - AdDiCtIoN
```

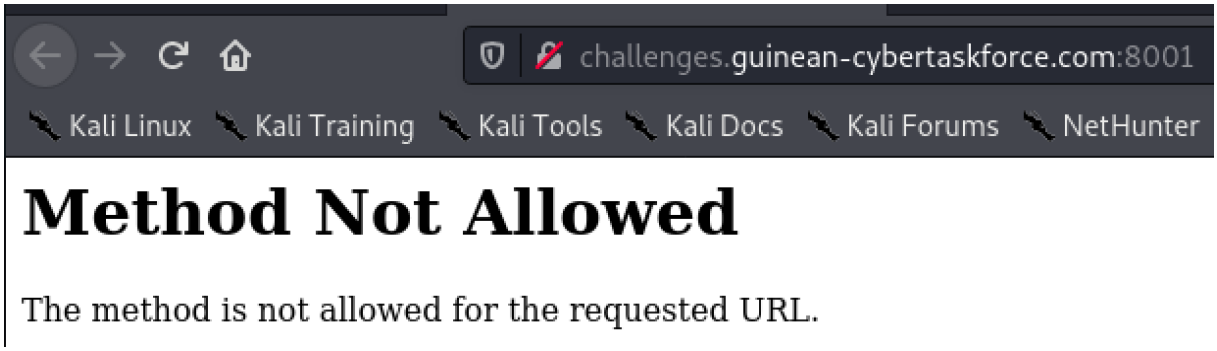
Mots passe déchiffrés

Russia — Web Security : On n’est d’accord que la méthode des hackers n’a rien d’ordinaire

```
La CyberBadCorp s'est rendue compte de ton intrusion dans leur Système
d'Information à la suite de ton succès dans le challenge France.

Ils ont pris de nouvelles méthodes, que dis-je? de nouvelles mesures de
sécurité.

Rappelle-toi : la GCSC t'aidera à passer de l'autre côté de la force :
devenir un hacker éthique.

Indice: -5 points
Flag: GCSC2022{flag_ici}
```

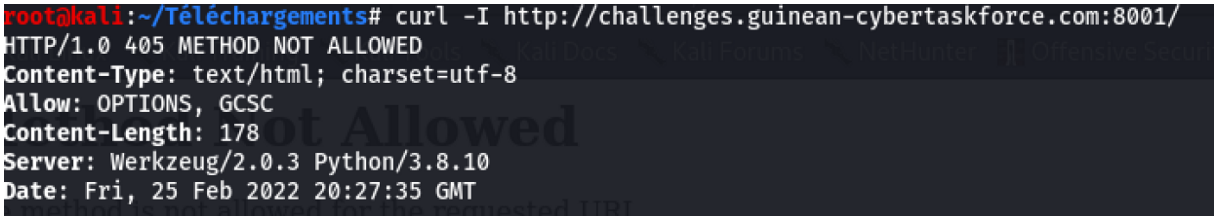
Énoncé chall Russie

Pour cette épreuve de sécurité web, nous avions un lien qui nous renvoyait sur un lien qui nous disait que la méthode utilisée n’était pas autorisée.



Method Not Allowed

Avec la commande “curl” je détermine qu’elles sont les méthodes autorisées sur ce serveur Web et je découvre que nous avons 2 méthodes autorisés uniquement : **OPTIONS** et **GCSC**



Method allowed

J’essaie donc de consulter le serveur web avec la méthode GCSC en utilisant BURP, mais aucune piste qui pourrait renvoyer au flag.

BURP -GCSC

Je décide alors d’utiliser l’indice donné (-5 points) et là, je découvre un texte en hexadécimal, que je déchiffre ensuite, qui correspond à “flag”.

Indice Hexa

Je consulte donc le répertoire “/flag” sur le serveur web avec la méthode GCSC pour sûrement obtenir le flag de challenge… Bingo !!!

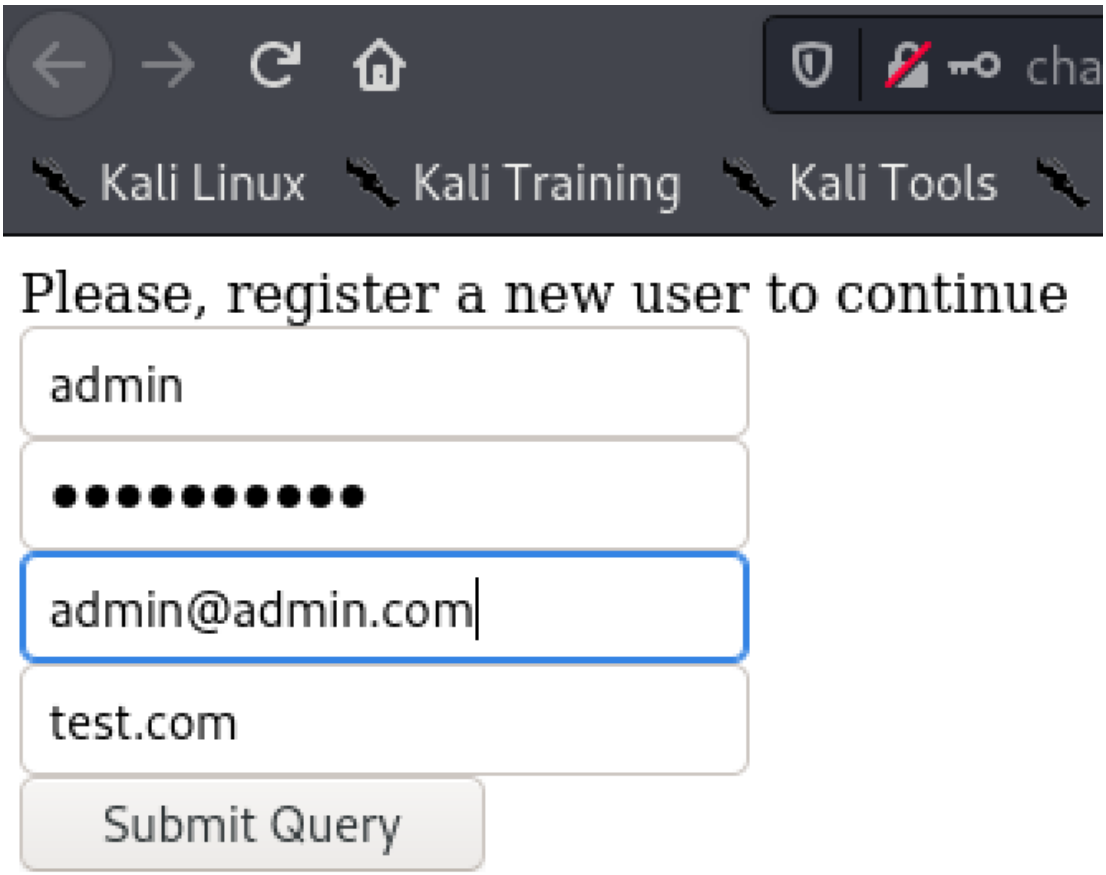
BURP — GCSC : flag

Canada — Web Security : IP_Publique x Collaborer x Interagir

```
Houhou!

On te présente ce formulaire du site web en cours de construction.

Interagit avec le serveur de la CyberBadCorp et trouve-lui un usage non
sollicité.

Indice: -5 points
Flag: GCSC2022{flag_ici}
```

Énoncé chall Canada

Cette nouvelle épreuve de sécurité Web nous renvoie sur une page, ou on peut saisir des identifiants, je décide donc d'interagir avec celle-ci pour observer le résultat, je saisis des identifiants choisis par hasard, et après un petit moment de chargement de la page, j'obtiens des erreurs…



Web page chall Canada

```
        #return "Please, provide your username, password, email and personal website"
    if len(passwd) < 8:
        return "S'il vous plait, votre mot de passe doit etre de 8 caractères ou plus"
        #return "Please, make sure that your password is at least 8 characters long"
    if url != "":
        r = requests.get('http://'+url+'/GCSC{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}')
        if (r.status_code != 200):
            return "Website not found"
        else:
            return "Registering new user, please wait...<br><br> Oops! Something happened and we couldn't register your user. Please, contact the
site administrator, or try again later", 200

[console ready]
>>>
```

Flag chall Canada

Flag : GCSC{Ut1llisseZ_t0ujoUr$_c0ll4boRat0r}