



WRITEUP OFFICIEL

‘Objectif-Eagle’

Table des matières :

I. Rappel des faits	4
II. Challenges	5
LA MISSION	5
BINGO	6
INDISCRETION	7
CALL ME MAYBE	7
OU SUIS-JE	8
HOTEL CALIFORNIA	9
VACANCES J'OUBLIE TOUT	11
CA PIQUE	12
MAUVAISE MAIN	13
PARADIS FISCAL	13
VOS PAPIERS SVP	14
BALANCE TON PORC	16
DERRIERE LECRAN	16
LE LIEU DU CRIME	17
PREMIERE EXPERIENCE	18
FIN DE PARTIE	18
DOUBLE JEU	19
UN POUR TOUS	20
UNDERCOVER	20
MARLY GOMONT	21
PING	22
PONG	22
TUTOS	23
LE MOT DE PASSE SVP	23
ATTRAPE-MOI SI TU PEUX	24
TAUPE MODELE	25
TOUT CA POUR UN PIAF	26
MAN IN THE MIDDLE	26
GRANDE VITESSE	27
SOUS CONTROLE	28
DISPARITION SUSPECTE	29
UNE LONGUE HISTOIRE	30

III. Challenges : SIDEQUEST	30
EXTRATERRITORIALITE	31
LA LOI C'EST LA LOI.....	31
CATALOGUE	32
BALANCE TON DRONE.....	32
PATTE BLANCHE	33
REAL WORLD.....	33

I. Rappel des faits

Aeroguard Technologies est une entreprise française de la BITD basée à Angoulême, qui conçoit des systèmes anti-drones adaptables sur tous types de véhicules. En parallèle, elle s'est lancée sur un projet de drone biomimétique capable d'imiter le vol d'un oiseau de type rapace, permettant des phases de plané pour le recueil de renseignements, ou de piqué pour l'attaque de cibles.

En 2022, l'entreprise présente son système de défense anti-drones lors du salon Eurosatory. Durant le salon, l'ordinateur portable du directeur R&D est volé mais des sauvegardes existant, l'entreprise ne signale pas le vol auprès de services compétents.

L'ordinateur contenait les éléments techniques du système anti-drones, mais également les premiers plans du futur prototype de drone biomimétique.

Quelques mois après le vol, Aeroguard Technologies fait l'objet d'un audit du département de la justice américaine pour infraction à la réglementation ITAR à la suite de la présentation sur un salon étranger d'un de leur modèle contenant un composant inscrit sur la liste ITAR et pour laquelle elle a oublié de faire une demande d'exportation temporaire auprès des autorités américaines. En 2023, l'entreprise est condamnée à une amende de 10 millions d'euros qui affecte considérablement ses finances.

Depuis, le climat social en interne se détériore et plusieurs cadres techniques démissionnent.

Depuis cet été, tout s'effondre pour l'entreprise. Entre les démissions et des attaques réputationnelles, Aeroguard Technologies perd 2 contrats très importants sur ses produits phares.

En septembre, une attaque informatique paralyse les systèmes d'informations. Financièrement au bord du gouffre, l'entreprise doit réagir. Son PDG commence à se poser de sérieuses questions sur la concomitance de tous les incidents qui ont affecté l'entreprise depuis plusieurs mois. Lors d'un échange au sujet du prototype du drone, il s'en ouvre auprès de son contact à la Direction des Industries de Défense à la DGA, qui décide de mettre ses équipes de réservistes sur le sujet pour en avoir le cœur net.

II. Challenges

Vous retrouverez ci-dessous la correction des challenges de l'histoire principale du CTF.

LA MISSION

Le règlement fourni dans le challenge permet de trouver les trois termes demandés.

REGLEMENT DU CTF

1/ Durée :

Ce CTF se déroule en ligne sur la plateforme <https://objectif-eagle.ctfd.io> du 14 novembre 2024 à 9h au 17 novembre 2024 à 23h59.

2/ Inscription :

Tous les participants doivent s'inscrire sur la plateforme avant la date limite d'inscription, fixée au 12 novembre 2024 à 23h59. Tous les capitaines d'équipes sans exception (et tous les joueurs solos) devront impérativement rejoindre le Discord du CTF pour ouvrir un canal de support. Toute équipe qui n'aurait pas ouvert son canal au démarrage du CTF sera désinscrite de la plateforme.

3/ Modalités :

Les participants **peuvent** concourir en équipes de 4 joueurs au maximum, ou individuellement.

4/ Challenges :

Chaque challenge rapportera un nombre de points variant en fonction du niveau de difficulté. Des hints seront disponibles sur les challenges pouvant représenter une difficulté particulière ou technique. Ces hints coûteront des points qui seront retranchés au score de l'équipe.

5/ Soumission des flags :

Les réponses **doivent** être soumises via la plateforme officielle du CTF. Les tentatives sont limitées à 3 par challenge. En cas de blocage, l'équipe ou le joueur aura la possibilité d'être débloqué par les admins pour un coût de 200 pts.

6/ Phase finale du CTF :

Lors de l'inscription, les équipes mentionnent leur disponibilité pour l'événement final qui aura lieu en présentiel à Angoulême le 27 novembre 2024. Au moment de la fin du CTF, les 10 meilleures équipes classées au scoreboard ayant indiqué leur disponibilité pour la finale auront 24h pour fournir un rapport synthétique indiquant les éléments trouvés, les liens entre les protagonistes et leur analyse. Ce rapport sera noté selon un barème de points attribués en fonction des éléments trouvés assorti d'une note bonus pour l'analyse fournie. Le résultat définitif du classement sera publié le 20 novembre à 9h00. Les 4 équipes ayant recueilli la meilleure note seront invitées par le Campus Osint à Angoulême dans le cadre de son inauguration pour y disputer la « hunt » finale. Une remise des prix aura lieu à l'issue.

7/ Code de conduite :

Aucune action **de** bruteforce ne sera tolérée sur les assets ou sur la plateforme du CTF. Aucune identité réelle n'est demandée pour l'inscription, mais les inscriptions avec des

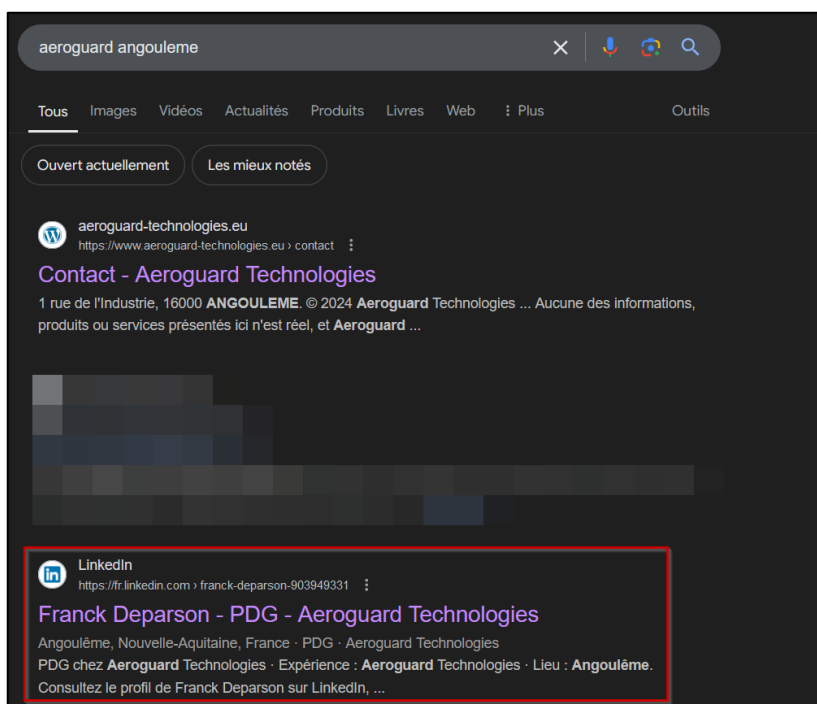
Le flag attendu était : peuvent_doivent_de

BINGO

Grâce au fichier PDF "contexte" mis à votre disposition dès le début du CTF, nous obtenons des informations sur l'entreprise victime de plusieurs attaques (cyberattaque, campagne de désinformation...)

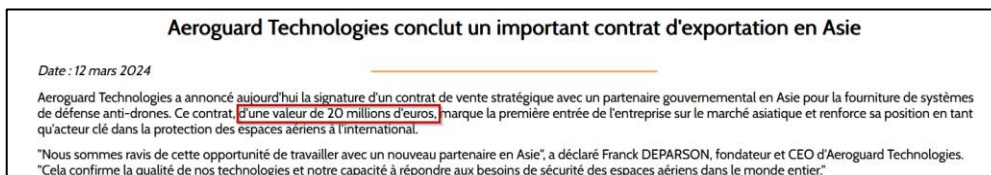
- Aeroguard est une entreprise française située à Angoulême
- Aeroguard a été victime d'une attaque informatique en septembre 2024
- ...

Grâce à une recherche Google, nous pouvons retrouver le profil LinkedIn du PDG : [Franck Deparson - PDG chez Aeroguard Technologies](#)



Après l'analyse de son profil, nous trouvons un lien vers le site web de l'entreprise : [aeroguard-technologies.eu](#). Il est également possible d'accéder au site directement via une recherche Google.

Sur la page 'News' consacrée aux actualités d'Aeroguard, nous découvrons le montant du contrat signé."



Le flag attendu était : 20 000 000

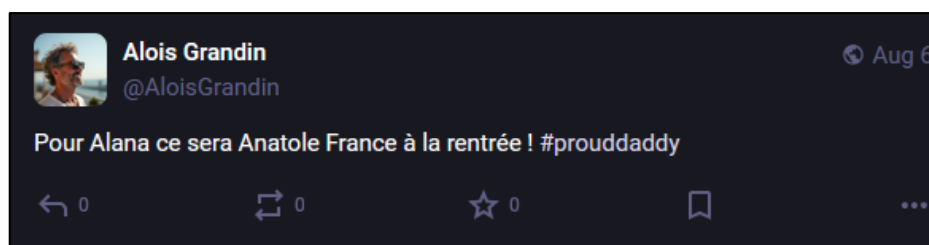
INDISCRETION

Sur le site d'Aeroguard précédemment trouvé, nous pouvons consulter la page « About us » :

<https://www.aeroguard-technologies.eu/about/>. Sur cette même page, nous retrouvons alors l'identité du directeur commercial : Alois GRANDIN



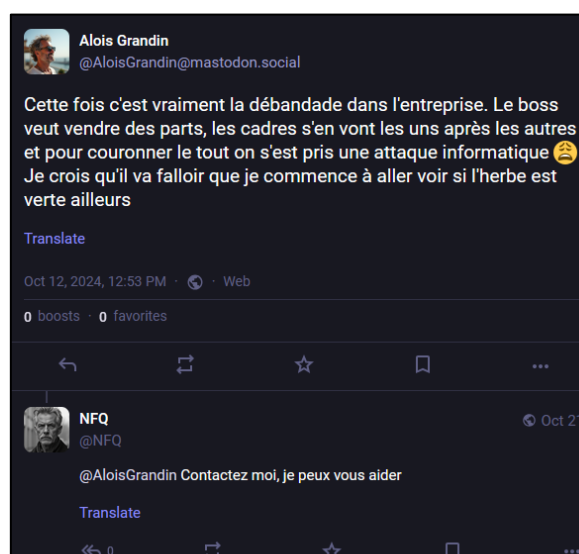
Finalement, c'est sur son compte Mastodon <https://mastodon.social/@AloisGrandin> que nous apprenons que sa fille intégrera Anatole France à la rentrée prochaine.



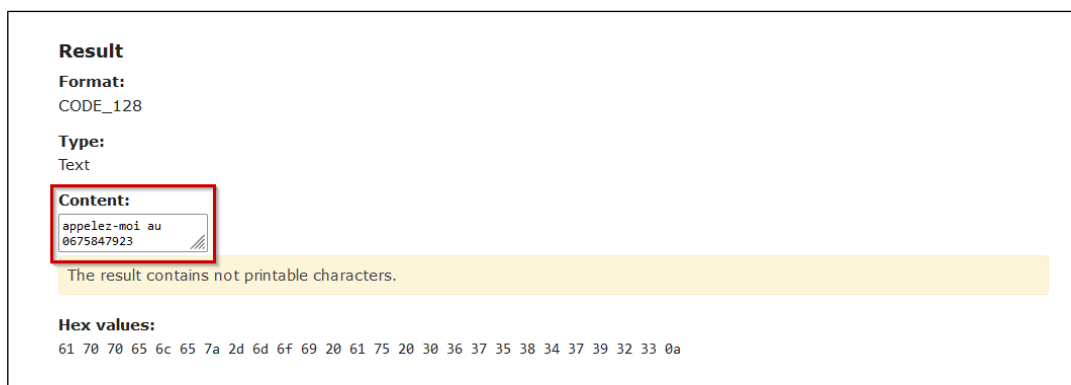
Le flag attendu était : anatole_france

CALL ME MAYBE

Sur le compte Mastodon d'Alois Grandin, nous retrouvons [un post](#) évoquant l'état d'Aeroguard. Sur ce même poste, un certain « NFQ » propose son aide.



En s'intéressant [au profil Mastodon de NFQ](#), nous retrouvons dans sa bio un lien vers une note en ligne : <https://justpaste.it/g25y5>. Pour voir ce qu'il se cache derrière le code-barre affiché, nous utilisons le site <https://www.onlinebarcodereader.com/>

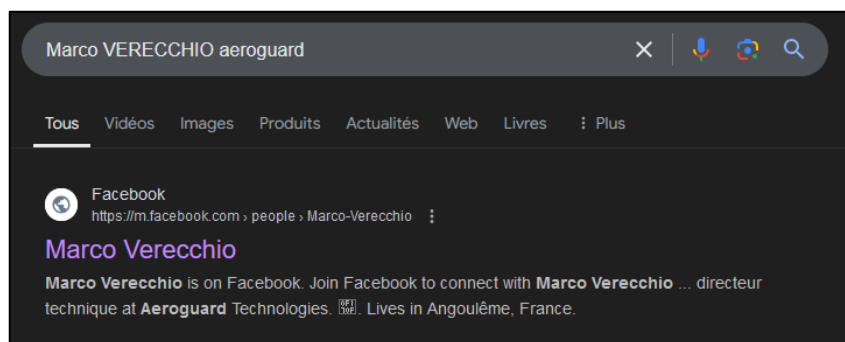


Le flag attendu était : 0675847923

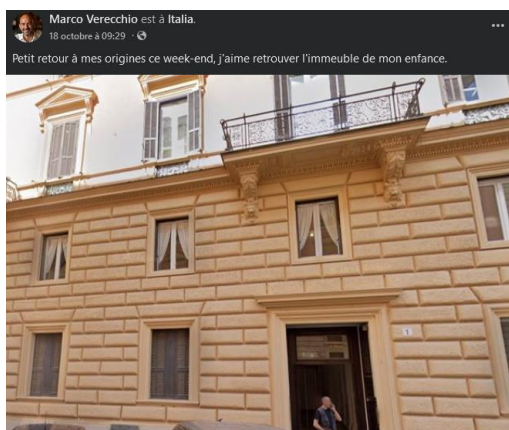
OU SUIS-JE

Pour ce nouveau challenge, nous retrouvons l'identité du directeur technique sur la page « [about](#) » du site d'Aeroguard. Il s'agit de Marco VERECCHIO.

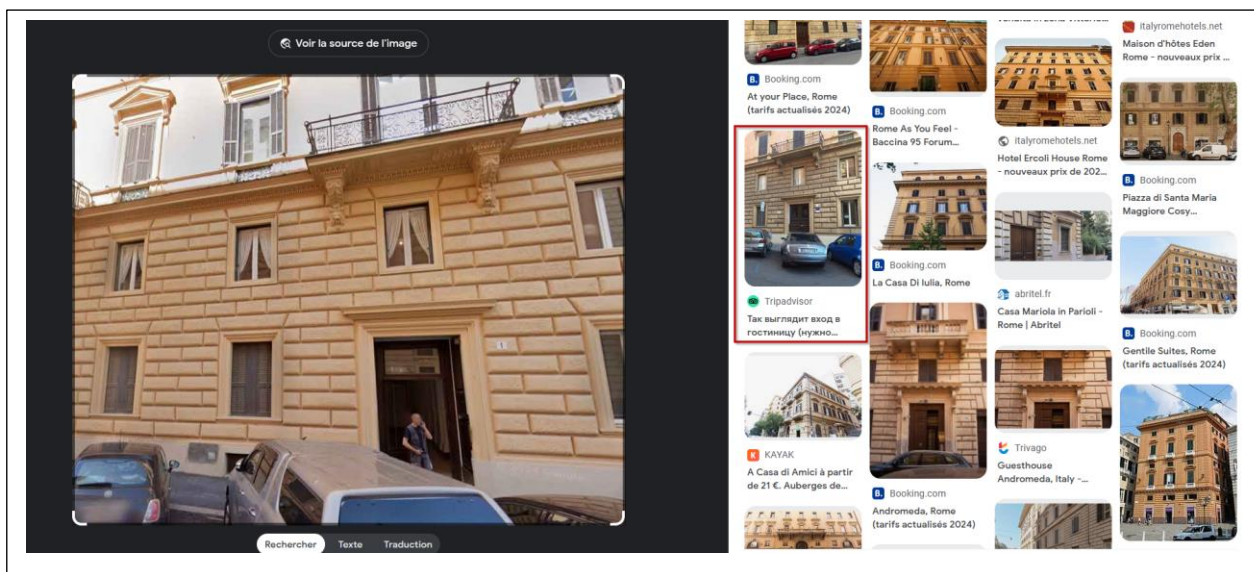
Grâce à une recherche Google, nous retrouvons le lien vers son profil Facebook : https://www.facebook.com/people/Marco-Verecchio/61566958176024/?_rdr



Un post daté du 18 octobre évoque son week-end des 19 et 20 octobre.

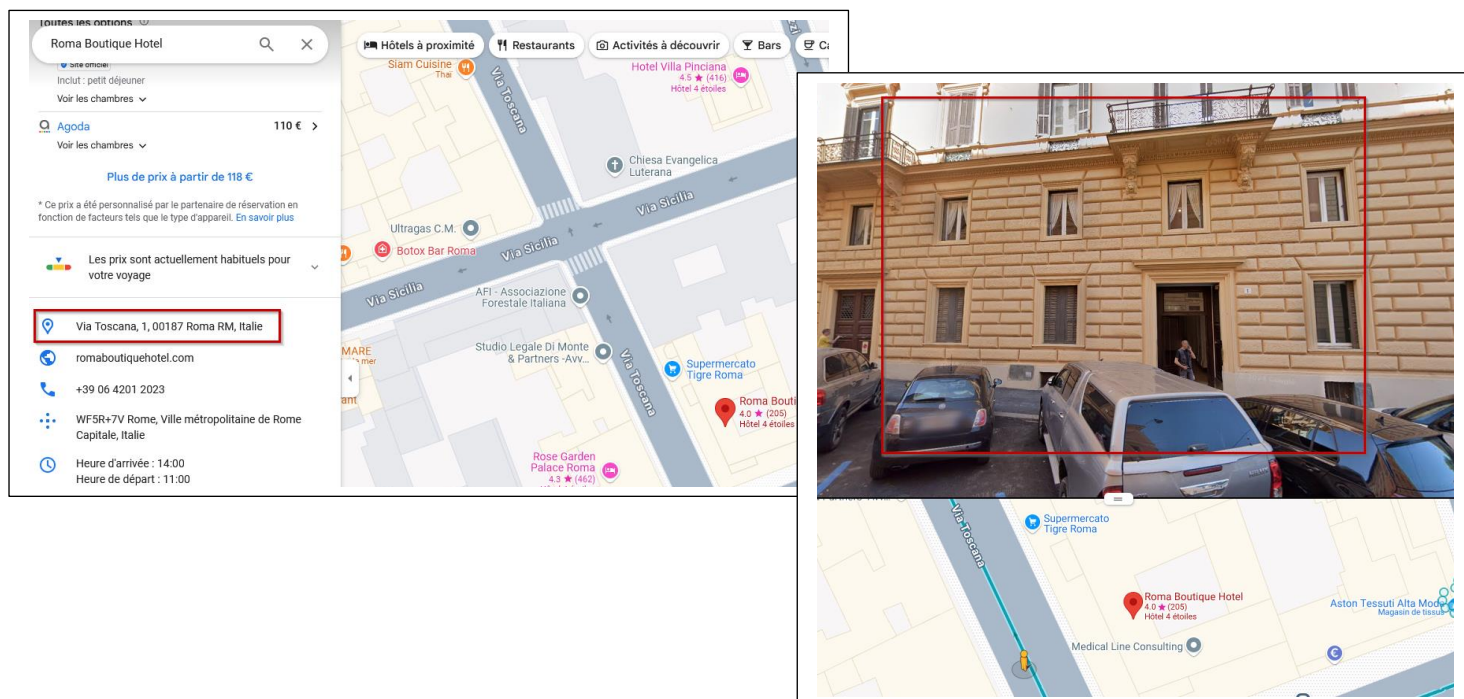


En effectuant une recherche inversée de l'image, nous trouvons un lien vers un hôtel répertorié sur TripAdvisor : https://www.tripadvisor.com/LocationPhotoDirectLink-g187791-d612667-i155007816-Roma_Boutique_Hotel-Rome_Lazio.html



Marco séjournait donc au Roma Boutique Hôtel de Rome.

En consultant Google Maps, nous pouvons confirmer cette information et obtenir l'adresse précise du lieu.

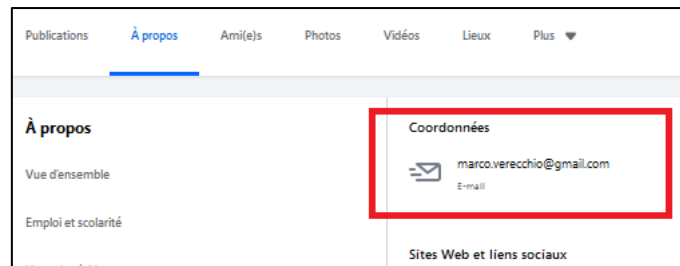


Le flag attendu était : `via_toscana_1_roma_italia`

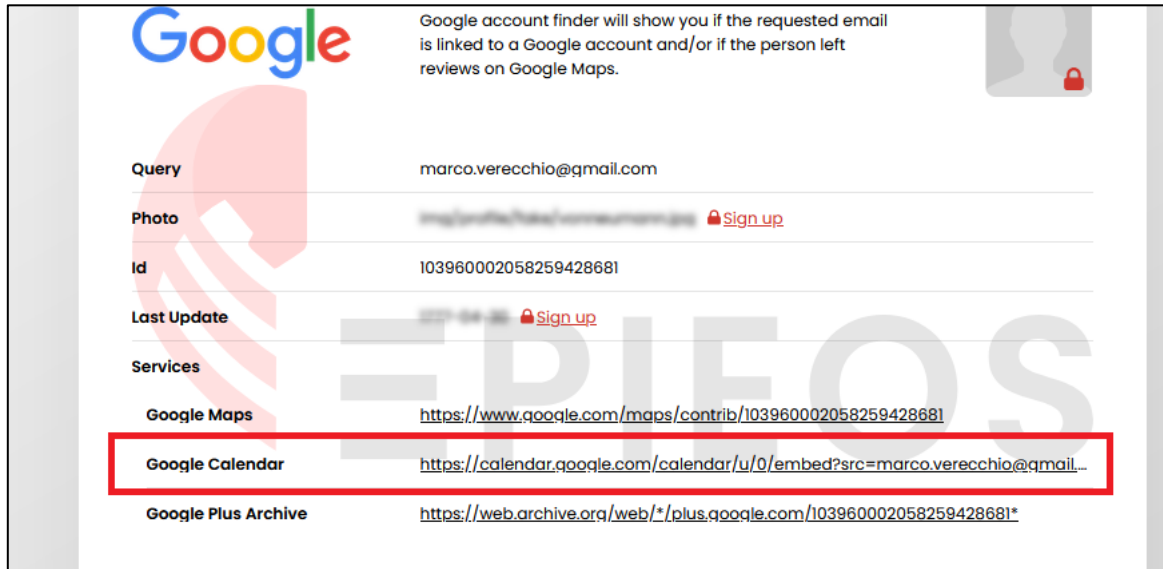
HOTEL CALIFORNIA

Nous cherchons l'hôtel dans lequel se trouvait Marco Verecchio au moment du salon Eurosatory 2022.

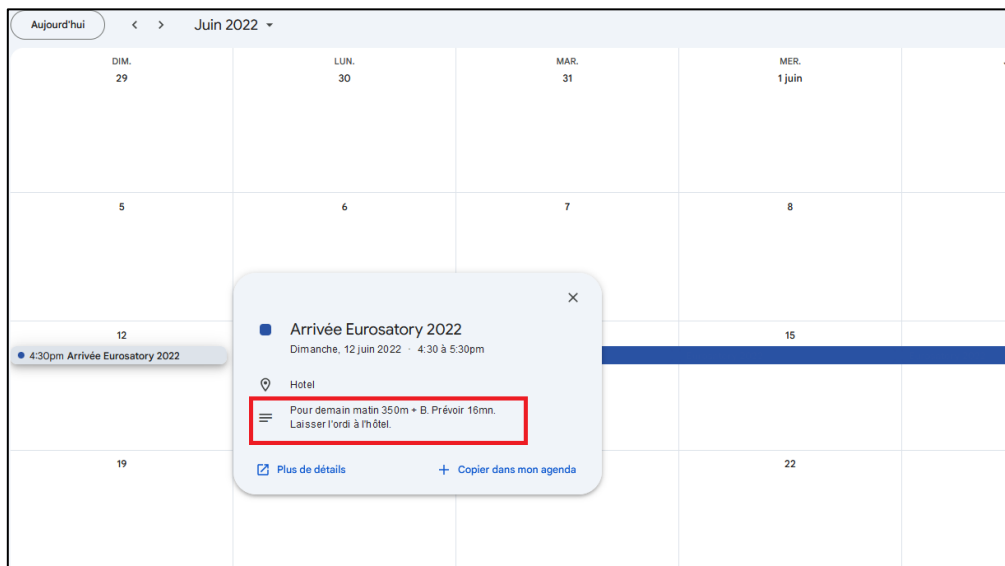
En creusant la rubrique "coordonnées" de son compte FB, on trouve un email :



Une recherche de cet email sur la version gratuite d'Epieos nous indique qu'un agenda est lié au compte.



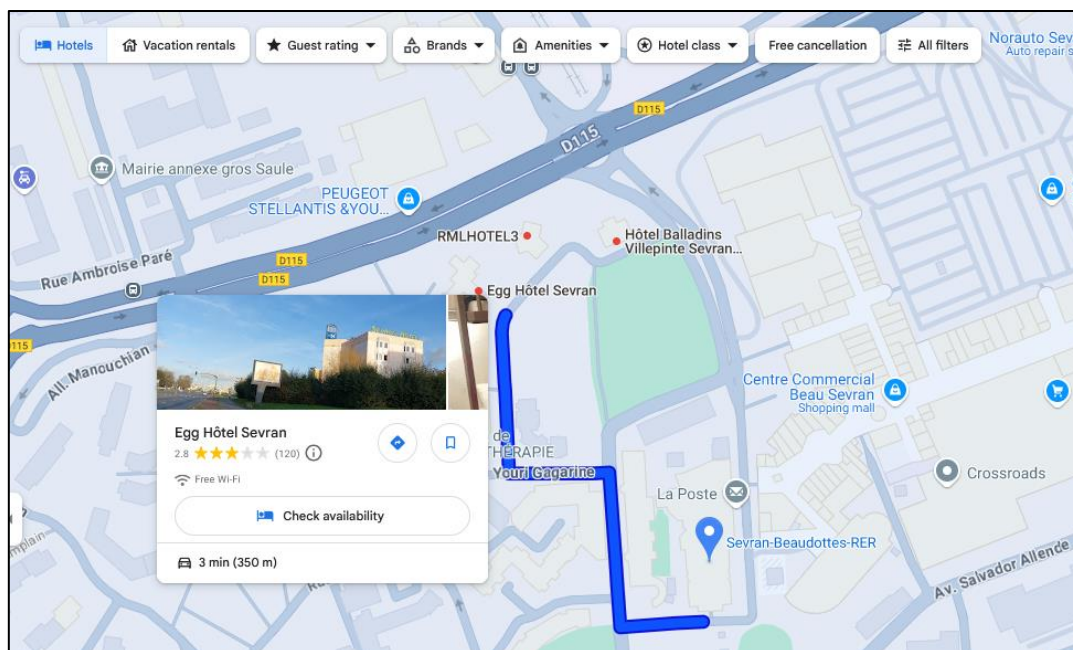
Comme Marco n'a pas paramétré son agenda en privé, ses notes sont accessibles. A la date du salon Eurosatory 2022, nous trouvons une note avec un commentaire :



Celui-ci semble indiquer un itinéraire. Faisons le trajet à l'envers depuis le Parc des Expositions, on se rend compte rapidement que le RER B dessert la zone du parc.

Il indique 16mn de trajet. Depuis le parc des expos, il y a déjà 7mn à pied pour aller au RER et le commentaire précise 350m (soit 5mn à pied). Le trajet en RER dure donc 4mn, soit au maximum 2 stations.

Le plan du RER nous indique 2 options. L'aéroport CDG TGV ou Sevran Beaudotte. Une recherche d'hôtels dans un rayon de 350m à l'aéroport ne donne qu'une possibilité qui ne correspond ni en distance, ni au format du flag. La même recherche autour de la gare du RER de Sevran nous indique en revanche 3 hôtels, dont un seul ayant précisément cette distance (et le bon format).

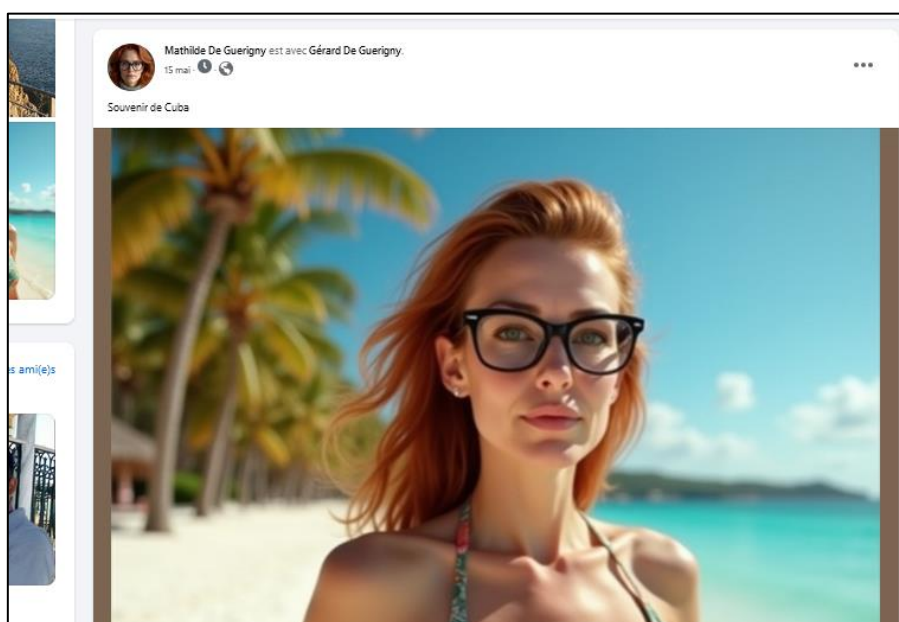


Pour être certain d'être au bon endroit on peut refaire l'itinéraire dans le bon sens depuis l'hôtel jusqu'au Parc des Expositions, on obtient bien 16mn via le RER B.

Le flag attendu était : egg_hotel_sevrans

VACANCES J'OUBLIE TOUT

Si l'on cherche les profils des employés d'Aeroguard on trouve celui de la DRH, Mathilde de Guerigny, qui semble aimer voyager. On tombe effectivement sur un voyage en mai 2024

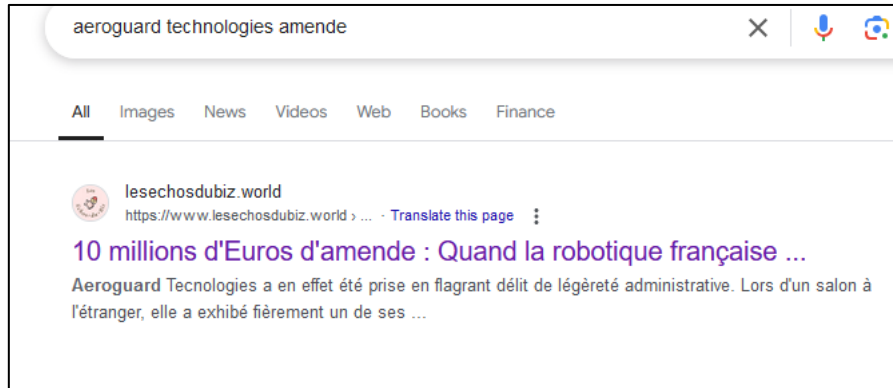


Le flag attendu était : cuba

CA PIQUE

Une recherche sur les termes “Aeroguard Technologies” et “amende” ramène un résultat :

<https://www.lesechosdubiz.world/>



On trouve rapidement notre information sur l'article en question :



Le flag attendu était : 09/12/2023

MAUVAISE MAIN

Sur son profil Facebook, Mathilde de Guerigny, directrice des ressources humaines, mentionne être mariée à Gérard de Guerigny. Le compte de Gérard montre clairement son fort intérêt pour le poker, mais aucun message menaçant n'y est visible. Il est donc nécessaire d'explorer d'autres pistes. C'est sur un forum de poker que nous trouvons un post de Gérard.



Exemple d'une recherche avancée sur Google permettant de localiser le bon forum. Toutefois, il était tout à fait possible de trouver le forum adéquat sans recourir à ce type de recherche.

La particularité de ce challenge réside dans le fait que le forum contient deux barres de recherche. Il fallait utiliser celle de la barre de navigation fixe pour retrouver un post de Gérard de Guerigny en recherchant le terme 'guerigny'.

Comment éviter la spirale... - Espace débutants - Club Poker

Club Poker > ... > Stratégie au poker > Espace débutants

19 sept. 2024 ... Salut à tous, Je suis passionné de poker depuis plusieurs années, et comme beaucoup ici, j'apprécie énormément l'excitation et la stratégie ... Avec libellé Forum et blogs

<https://www.clubpoker.net/forum-poker/topic/244037-comment-%C3%A9viter-la-spirale/>

En consultant l'article, nous découvrons qu'une personne nommée 'Hann Onymous' adopte un ton menaçant envers Gérard.

Le flag attendu était : hann_anonymous

PARADIS FISCAL

SI l'on reprend le profil LinkedIn du PDG d'Aeroguard Franck DEPARSON, un commentaire d'InnovEx Capital sur le post où il mentionne la nécessité d'ouvrir son capital attire l'attention. La page de l'entreprise renvoie sur un

site internet qui précise qu'elle est un fonds d'investissement dans les hautes technologies basée au Liechtenstein.

InnovEx Capital est un fonds d'investissement basé au Liechtenstein, spécialisé dans les technologies innovantes et d'usage dual avec un potentiel d'applications civiles et militaires. Notre mission est de soutenir les entreprises et projets qui repoussent les limites de l'innovation et créent des opportunités pour l'avenir.

Le flag attendu était : liechtenstein

VOS PAPIERS SVP

Nous avons trouvé précédemment (challenge : « PARADIS FISCAL ») le site internet de l'entreprise <https://www.innovexcapital.online/> s'intéressant à la situation Aeroguard. Sur ce site, nous retrouvons dans la page « Investors » un rapport financier de l'entreprise de 2023.



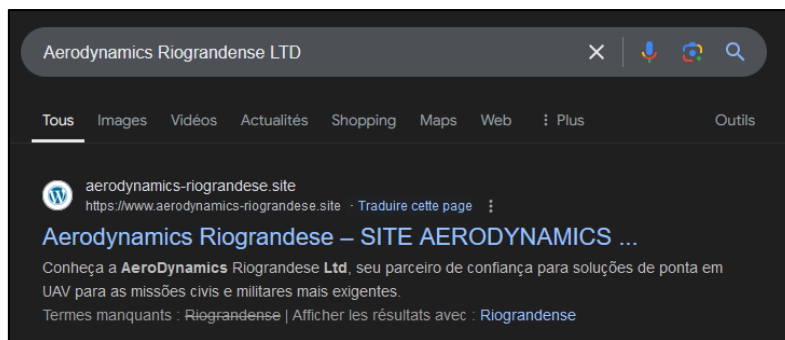
Nous pouvons alors trouver sur ce rapport, un tableau des principaux actionnaires :

3. Structure de l'Actionariat

La structure de l'actionariat d'**InnovEx Capital** au 31 décembre 2023 est la suivante :

Actionnaires	Participation (%)	Nombre d'Actions
Aerodynamics Riograndese LTD	60 %	600,000
Valtech Ventures	20 %	200,000
Global Innovations Fund	10 %	100,000
Stellar Growth Partners	10 %	100,000
Total	100 %	1,000,000

Finalement en cherchant « Aerodynamics Riograndese LTD » sur Google, nous retrouvons le lien vers le site web de cette entreprise.



Ce site est uniquement accessible depuis certains pays et est bloqué en Europe. Par conséquent, il était nécessaire d'utiliser un VPN pour obtenir une adresse IP d'un pays autorisé à se connecter au site.

Permanent link to this check report | Share on Twitter

Live server terminal

Location	Result	Time	Code	IP address
Brazil, Sao Paulo	OK	1.204 s	200 (OK)	104.21.75.174
Bulgaria, Sofia	Server error	0.099 s	403 (Forbidden)	172.67.179.180
Croatia, Sisak	Server error	0.470 s	403 (Forbidden)	172.67.179.180
Czechia, C.Budejovice	Server error	0.140 s	403 (Forbidden)	172.67.179.180
Finland, Helsinki	Server error	0.195 s	403 (Forbidden)	172.67.179.180
France, Paris	Server error	0.045 s	403 (Forbidden)	188.114.96.2
Germany, Frankfurt	Server error	0.072 s	403 (Forbidden)	188.114.96.3
Germany, Nuremberg	Server error	0.140 s	403 (Forbidden)	172.67.179.180
Hong Kong, Hong Kong	OK	0.780 s	200 (OK)	104.21.75.174
India, Chennai	OK	1.001 s	200 (OK)	104.21.75.174
India, Hyderabad	OK	0.895 s	200 (OK)	172.67.179.180
India, Mumbai	OK	0.734 s	200 (OK)	172.67.179.180
Indonesia, Jakarta	OK	0.804 s	200 (OK)	104.21.75.174
Iran, Esfahan	OK	1.041 s	200 (OK)	104.21.75.174
Iran, Karaj	OK	1.849 s	200 (OK)	172.67.179.180
Iran, Shiraz	OK	0.719 s	200 (OK)	188.114.96.6
Iran, Tehran	OK	4.332 s	200 (OK)	188.114.97.3
Israel, Netanya	OK	1.110 s	200 (OK)	188.114.96.3
Israel, Tel Aviv	OK	1.102 s	200 (OK)	188.114.96.7

Finalement, sur la page 'About' (<https://www.Aerodynamicss-riograndese.site/fr/about/>), nous découvrons l'identité du fondateur de l'entreprise, et par conséquent, l'actionnaire principal de l'entreprise InnovexCapital

Notre fondateur

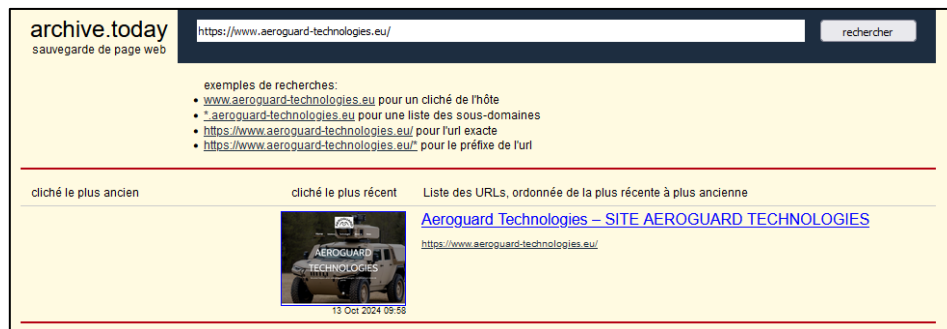


Joaquim Alveiro Dias est né il y a 52 ans dans la petite ville de San Pedro, nichée au cœur de la République de Riograndese, un pays riche en histoire et en défis. Issu d'une famille modeste, il a grandi avec un sens aigu de la détermination et un amour inébranlable pour les machines et l'ingénierie. Très jeune, Joaquim a montré un intérêt marqué pour le fonctionnement des appareils mécaniques, passant des heures à démonter et remonter tout ce qu'il trouvait.

Le flag attendu était : republique_de_riograndese

BALANCE TON PORC

Le site des Echos du Biz qui a relayé l'amende infligée par les Etats Unis a republié un article en octobre sur Aeroguard, concernant des allégations de harcèlement sexuel faites par une ancienne stagiaire. Le site d'Aeroguard ne la mentionne pas, mais comme elle ne fait plus partie de l'entreprise ce n'est pas étonnant. Cependant, une recherche d'archive donne un résultat sur archive.today, alternative à archive.org.



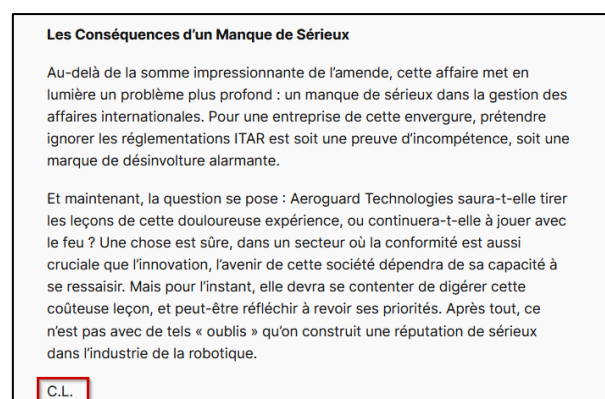
Et là nous découvrons qu'une ingénieure stagiaire travaillait à la Direction technique avec Marco Verecchio.



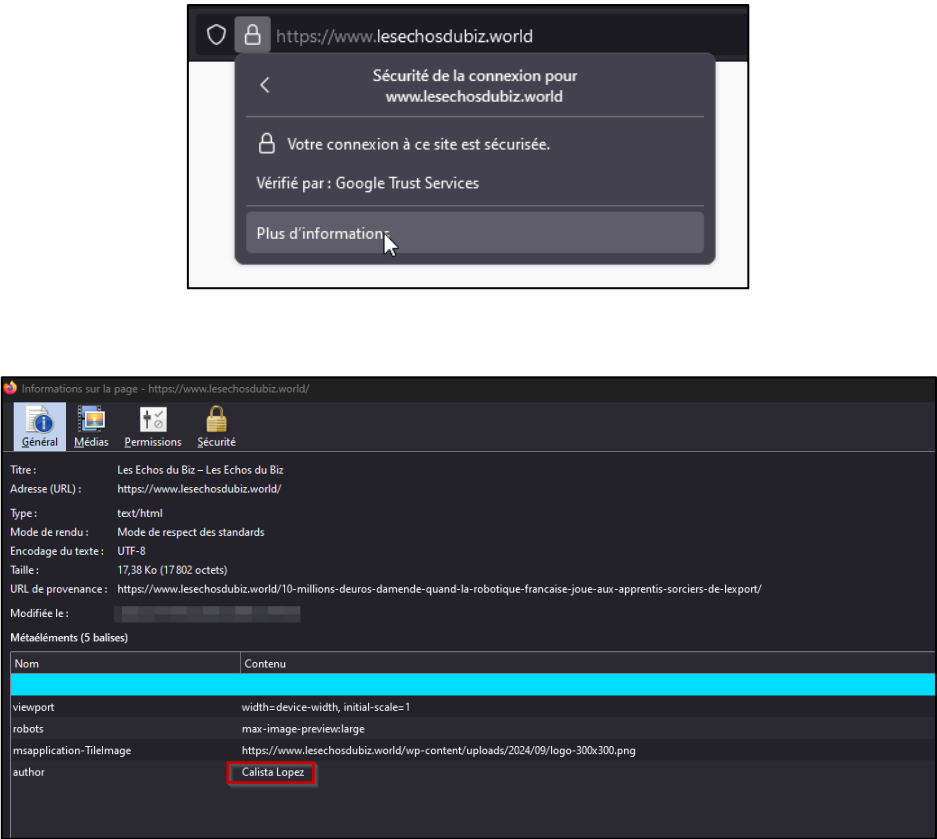
Le flag attendu était : isia_de_courselle

DERRIERE LECRAN

Pour découvrir l'identité de la personne derrière ce site de presse, nous pouvons d'abord trouver un article signé par C.L. sur le site de presse.



C'est finalement dans les informations générales du site que nous trouvons la réponse :



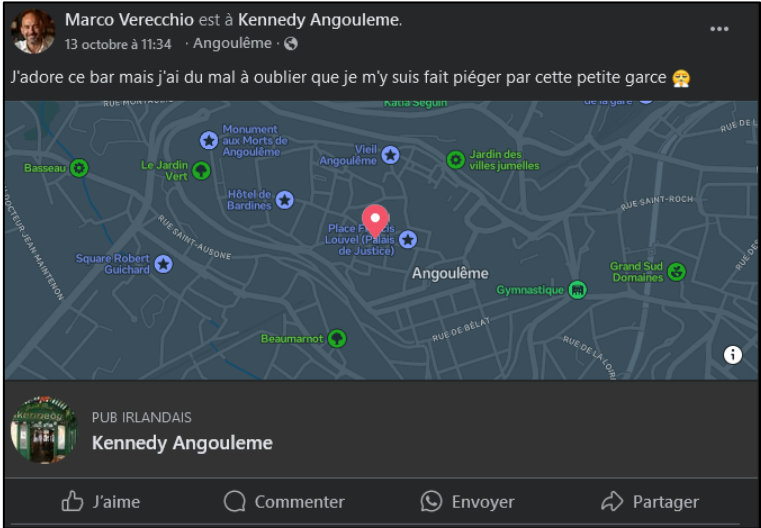
Nous pouvons également retrouver cette information dans le code source de la page d'accueil :

```
233 <meta name="author" content="Calista Lopez">
```

Le flag attendu était : calista_lopez

LE LIEU DU CRIME

Comme mentionné dans l'article disponible sur le site Echosdubiz, qui parle d'Aeroguard et d'une accusation de harcèlement sexuel, nous trouvons une photo de Marco Verecchio dans un bar. Sur le Facebook de Marco, un post révèle qu'il affirme avoir été piégé par Isia.



L'incident s'est donc déroulé au PUB Kennedy d'Angoulême. Pour obtenir le nom commercial de l'établissement, il suffit de se renseigner sur l'enseigne via Pappers :

<https://www.pappers.fr/entreprise/kennedy-479662637>


	<p>Adresse : 10 RUE TISON D'ARGENCE, 16000 ANGOULEME</p> <p>Activité : Restauration traditionnelle</p> <p>Effectif : Entre 1 et 2 salariés (donnée 2021)</p> <p>Création : 29/11/2004</p> <p>Dirigeants : Abbas Marie , Damour Didier</p>
---	---


Le flag attendu était : the_kennedy_irish_pub


PREMIERE EXPERIENCE

En ayant le nom de la personne gérant le site de presse 'Echosdubiz', Calista Lopez, nous pouvons retrouver son profil LinkedIn : <https://www.linkedin.com/in/calista-lopez-a36ba32a8/>

Expérience

**Rédactrice web**
À mon compte · Freelance
déc. 2022 - aujourd'hui · 2 ans
Paris et périphérie

**Journaliste multimédia**
Indépendant
mars 2020 - déc. 2022 · 2 ans 10 mois
Republique de Riograndese

**Assistante technologies de l'information et de la communication**
Aerodynamics Riograndese Ltd · Stage
sept. 2019 - févr. 2020 · 6 mois
Republique de Riograndese

Calista a ainsi fait une partie de sa carrière en République de Riograndese.

Le flag attendu était : republique_de_riograndese

FIN DE PARTIE

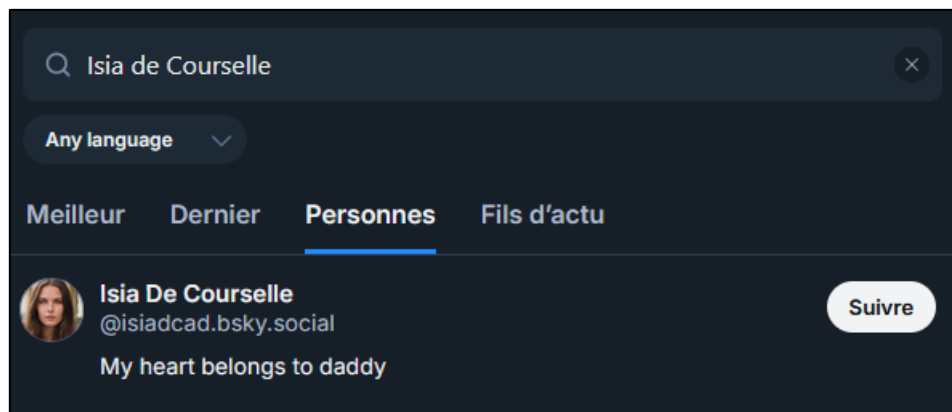
Sur le profil LinkedIn de Calista, nous pouvons trouver [un article](#) qu'elle a rédigé, intitulé 'L'Éthique du rédacteur : réflexions sur la responsabilité de la plume'. Dans cet article, elle indique que sa mission actuelle se termine en novembre de cette année.

Ce n'est pas un renoncement à la critique, mais un engagement à la pratiquer avec discernement, respect et intégrité. Parce que si la vérité est importante, la manière dont nous la disons l'est tout autant. J'ai maintenant hâte de finir ma mission actuelle en novembre, avant de me tourner vers des engagements qui auront vraiment du sens à mes yeux.

Le flag attendu était : novembre_2024

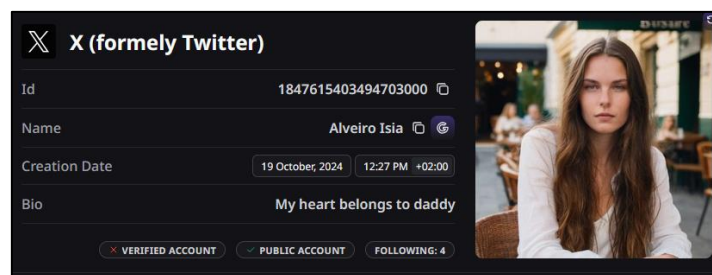
DOUBLE JEU

Nous avons précédemment identifié la stagiaire Isia De Courselle. Grâce à cette information, nous pouvons désormais retrouver son profil sur le réseau social Bluesky : <https://bsky.app/profile/isiadcad.bsky.social>

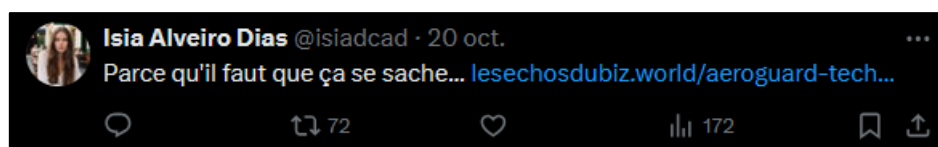


Nous avons trouvé un pseudonyme associé à son compte : isiadcad.

En utilisant un outil en ligne, nous découvrons qu'un compte Twitter utilise ce même pseudo, qu'il est également possible de trouver simplement en recherchant ce pseudonyme sur Twitter.



Nous retrouvons alors le compte twitter d'Isia : <https://x.com/isiadcad>



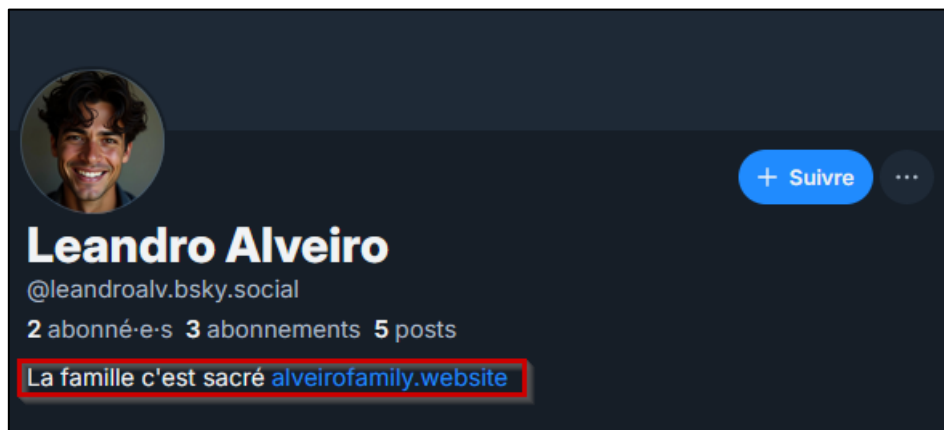
Celle-ci parle sous l'identité d'Isia Alveiro Dias

Le flag attendu était : isia_alveiro_dias

UN POUR TOUS

À partir du compte Bluesky précédemment trouvé, nous pouvons retrouver celui de son frère, Leandro Alveiro, qui a commenté l'un des posts d'Isia.

Sur le profil Bluesky de son frère, nous découvrons un blog consacré à la famille Alveiro.



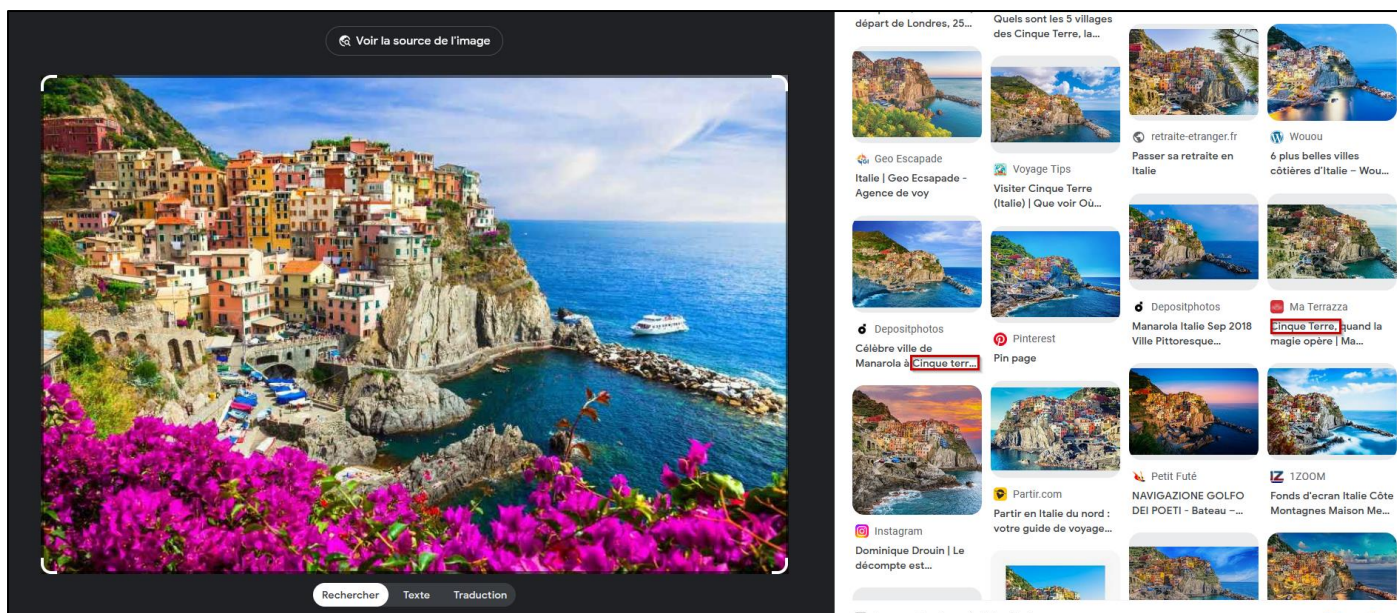
Le flag attendu était : alveirofamily.website

UNDERCOVER

Grâce au blog de la famille, nous apprenons qu'Elinor, la mère, est sollicitée par son mari pour différentes missions. En consultant le compte Bluesky d'Isia, nous retrouvons le profil Bluesky de sa mère, Elinor De Courselle : <https://bsky.app/profile/elidecourselle.bsky.social>. Nous découvrons alors un post dans lequel elle évoque les services qu'elle rend à son mari.



En faisant un reverse de l'image nous retrouvons alors le lieu :



Le flag attendu était : cinque_terre

MARLY GOMONT

Pour résoudre ce challenge, il était nécessaire d'avoir terminé les challenges 'Un pour tous' et 'Vos papiers SVP'. Grâce au challenge 'Un pour tous', vous avez trouvé un article intitulé 'Retour aux racines : Noël chez mes grands-parents en République de Riograndese', qui parle des grands-parents d'Alveiro et d'Isia, habitants de San Pedro. Enfin, avec le challenge 'Vos papiers SVP', vous découvrez que le père d'Isia et d'Alveiro est né à San Pedro.

Chaque année, je compte les jours avant notre visite à San Pedro en République du Riograndese, entre le Brésil et l'Uruguay. C'est là-bas que vivent mes grands-parents paternels, dans une région où le temps semble s'écouler différemment. Pour Isia et moi, ce voyage est plus qu'une simple escapade familiale, c'est comme un pèlerinage. Une façon de nous reconnecter à nos origines, à des valeurs que le monde moderne oublie parfois.

Notre fondateur



Joaquim Alveiro Dias est né il y a 52 ans dans la petite ville de San Pedro, nichée au cœur de la République de Riograndese, un pays riche en histoire et en défis. Issu d'une famille modeste, il a grandi avec un sens aigu de la détermination et un amour inébranlable pour les machines et l'ingénierie. Très jeune, Joaquim a montré un intérêt marqué pour le fonctionnement des appareils mécaniques, passant des heures à démonter et remonter tout ce qu'il trouvait.

Le flag attendu était : san_pedro

PING

En analysant le fichier de log mis à notre disposition, nous pouvons déterminer que l'IP ayant attaqué le site d'aeroguard le 27 septembre est la 185.217.125.225 (attaque de type injection SQL).

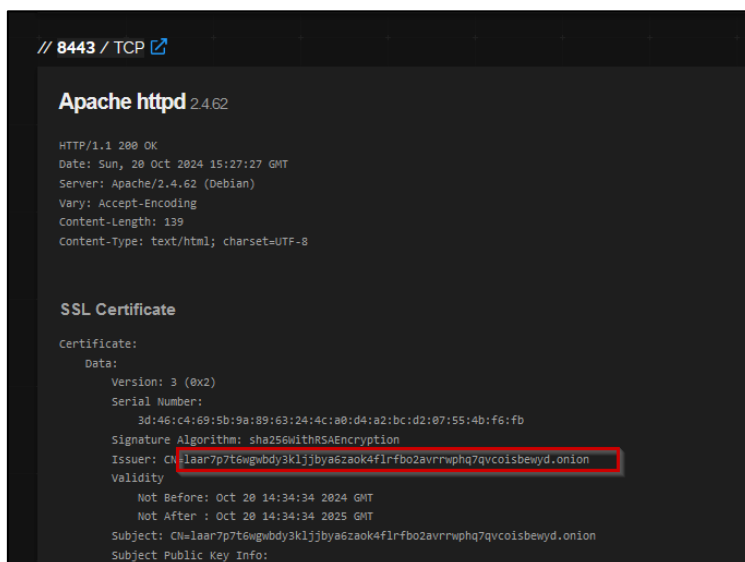
```
185.217.125.225 - - [27/Sep/2024:02:15:35 +0000] "POST /wp-admin/admin-ajax.php HTTP/1.1" 200 1413 "-" "Mozilla/5.0 (Linux; Android 13; Pixel 7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.64 Mobile Safari/537.36" "id="%20AND%205%3D0%20AND%20%28SELECT%206087%20FROM%20SELECT%20COUNT%28%2A%29%2C%28CONCAT%280x717a767071%2C%28SELECT%20%28ELT%285492%3D5492%2C1%29%29%2C0x71716b7671%2CFLOOR%28R AND%280%29%2CRAND%285346%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20--%20-")"
```

Le flag attendu était : 185.217.125.225

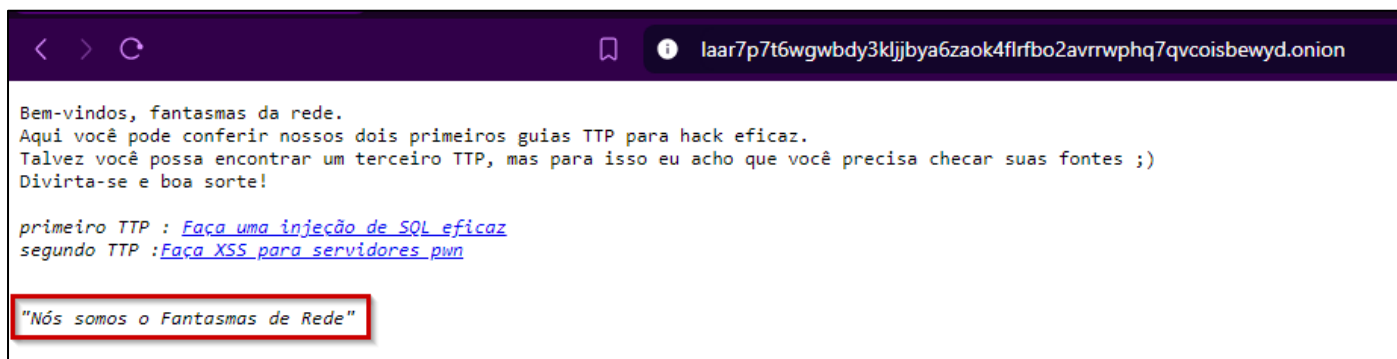
PONG

Nous allons alors nous renseigner sur l'IP précédemment trouvée. C'est sur Shodan que celle-ci est connue comme hébergeant un site .onion (TOR) : <https://www.shodan.io/host/185.217.125.225>

En analysant alors les résultats disponibles sur la page Shodan, nous retrouvons l'URL vers la page .onion :



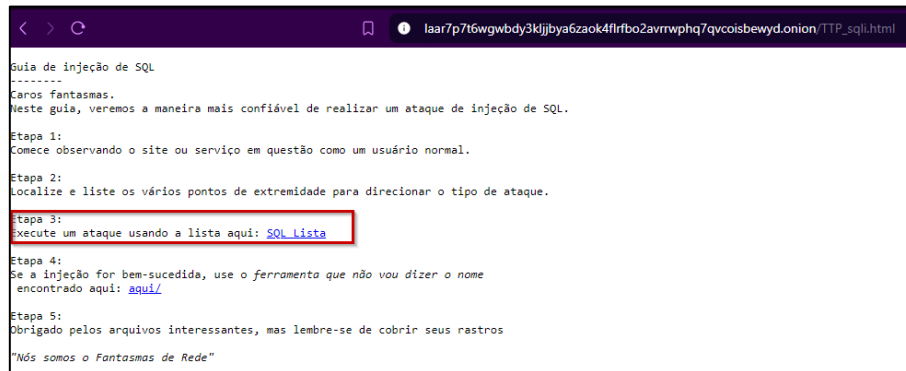
En consultant le site, nous découvrons le nom du groupe de hackers :



Le flag attendu était : fantasmas_de_rede

TUTOS

En analysant les articles disponibles sur le site .onion des hackers c'est dans leur premier « travail pratique » concernant les injections SQL que nous retrouvons l'étape relative à la liste SQL



Le flag attendu était : etape_3

LE MOT DE PASSE SVP

En analysant le code source de la page d'accueil du site .onion nous trouvons alors un commentaire en portugais évoquant la façon de rejoindre le groupe des hackers sur le clear web.

```
Bem-vindos, fantasmas da rede.
Aqui você pode conferir nossos dois primeiros guias TTP para hack eficaz.
Talvez você possa encontrar um terceiro TTP, mas para isso eu acho que você precisa checar suas fontes ;)
Divirta-se e boa sorte!

<cite>primeiro TTP : <a href="TTP_sqli.html">Faça uma injeção de SQL eficaz</a></cite>
<cite>segundo TTP :<a href="TTP_xss.html">Faça XSS para servidores own</a></cite>
<!-- junte-se a nós TTP : Parabéns. Para se juntar a nós, siga CUIDADOSAMENTE o guia na url: TTP_FANTASMAS.html -->

<cite style="color:red">"Nós somos o Fantasmas de Rede"</cite>
</pre>
</body>
</html>
```

Le code source nous invite alors à consulter la page :

http://laar7p7t6wgwbdy3kljjbya6zaok4flrfbo2avrrwphq7qvcoisbewyd.onion/TTP_FANTASMAS.html

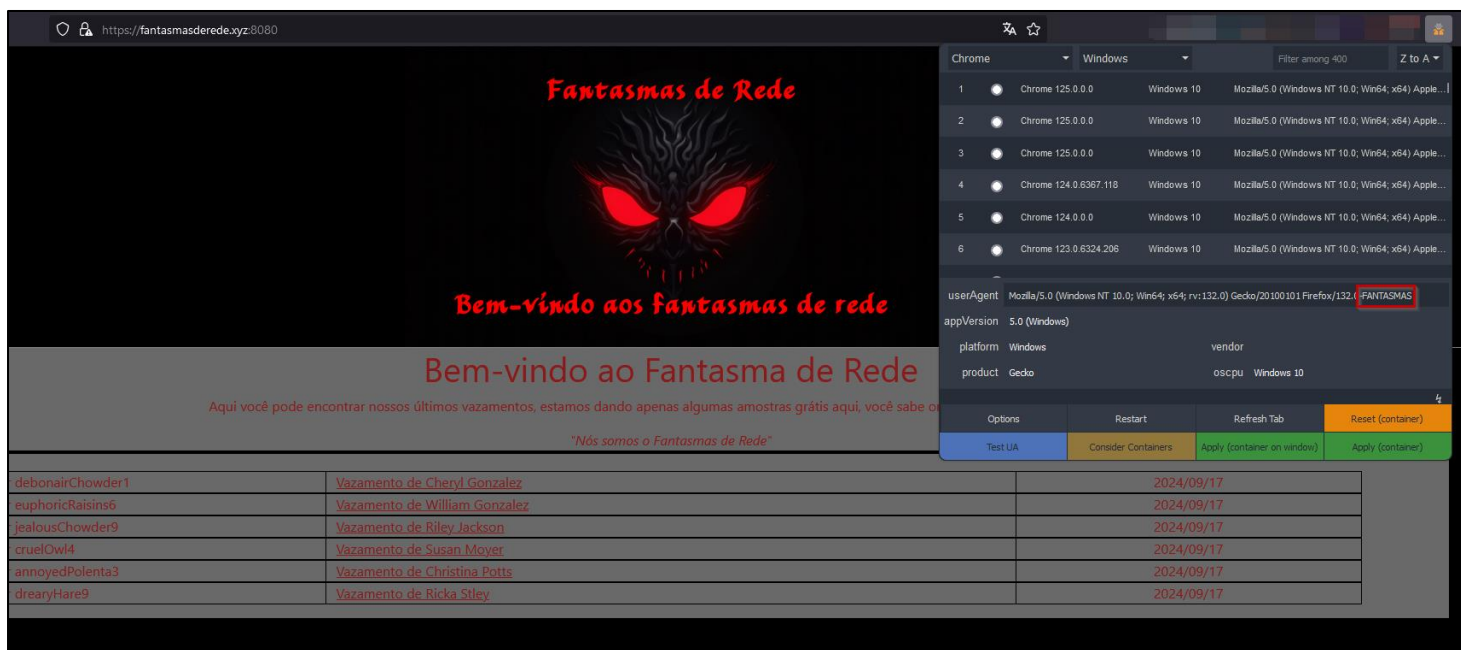
Sur cette page, nous découvrons les étapes pour rejoindre le groupe de hackers via leur site sur le clear web :

<https://fantasmasderede.xyz:8080>.

Pour cela, il faut modifier le user-agent de son navigateur et utiliser, comme expliqué dans leur guide, le user-agent 'FANTASMAS'. Si nous tentons d'accéder à leur site sans le bon user-agent, un message apparaît, indiquant que le site est en construction.



Cependant en changeant notre user-agent et en mettant « FANTASMAS », nous accédons alors au contenu du site.



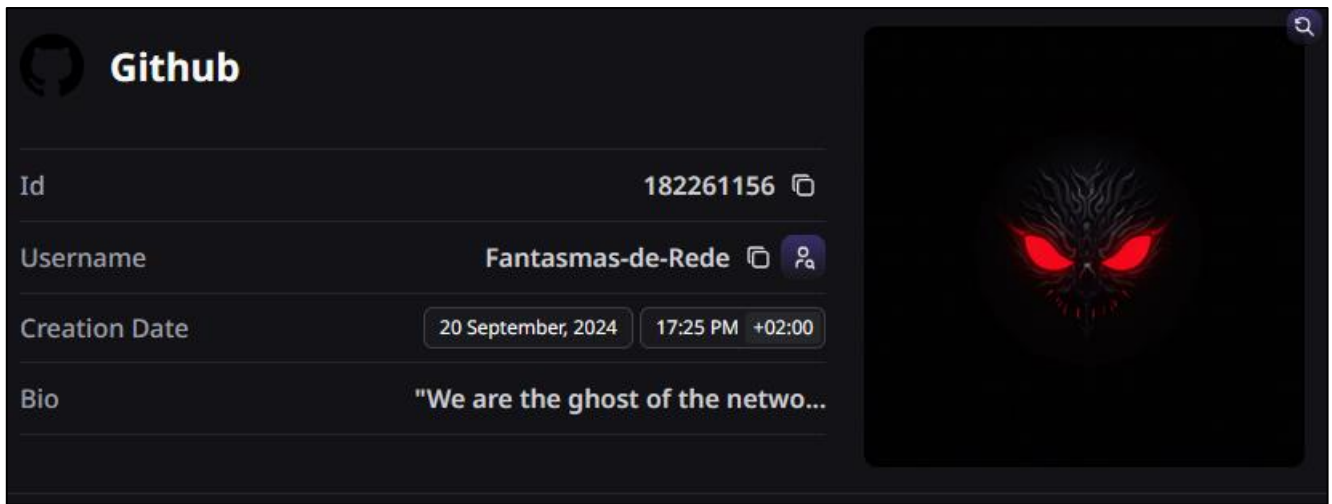
Le flag attendu était : fantasmas

ATTRAPE-MOI SI TU PEUX

En analysant le code source de la page d'accueil du site (clear-web) des hackers, nous trouvons un commentaire indiquant : 'TODO : Ajouter l'icône qui mène au profil 'Fantasmas-de-Rede'.

```
104 <!--
105 Todo : Adicione o ícone que Leva ao perfil 'Fantasmas-de-Rede'
106 -->
```

Nous savons alors qu'il nous faut chercher un profil menant à un compte 'Fantasmas-de-Rede'. En utilisant un outil en ligne, nous découvrons l'existence d'un compte GitHub sous ce pseudonyme : <https://github.com/Fantasmas-de-Rede>



(trouvable également sans outil juste avec une simple recherche du pseudo sur git-hub)

En analysant les commits du projet 'Practice' sur ce compte, nous découvrons un lien vers un profil Bluesky :<https://bsky.app/profile/leandroAlv.bsky.social>

```
▼ ransom_to_finalize.py
... @@ -1,4 +1,4 @@
1 - # Script by : https://bsky.app/profile/leandroAlv.bsky.social
1 + #script by : Fantasmas da Reye
2 2 import os
3 3
4 4 # Dossier cible
```

La personne se cachant derrière l'identité des hackers est enfaite : Leandro Alveiro, frère d'Isia (stagiaire chez Aeroguard).

Le flag attendu était : leandro_alveiro

TAUPE MODELE

En poursuivant l'analyse du site clear-web des hackers, nous trouvons dans le fichier /robots.txt (<https://fantasmasderede.xyz:8080/robots.txt>) de nouvelles URL disponibles sur le site.

```
← → 🏠 🔒 view-source:https://fantasmasderede.xyz:8080/robots.txt

User-agent: *
Disallow:
/*
/suculento/*
/amostras/*
```

En accédant au répertoire <https://fantasmasderede.xyz:8080/suculento/> nous trouvons un dossier nommé 'aeroleak' contenant de nombreux mails. Nous apprenons alors que la taupe au sein d'Aeroguard est Mathilde DE GUERIGNY (DRH chez Aeroguard). Celle-ci vend les plans du projet EAGLE en raison de problèmes financiers liés aux jeux en ligne pratiqués par son mari.

C'est alors dans le fichier « SWIFT_Wire_Transfer_Request_28743.eml » que nous retrouvons le premier virement que Mathilde a reçu datant du 22 décembre 2022.

Transaction Details:
- Order Date: December 22, 2022
- Order Number: #28743
- Amount: 5,000 EUR (five thousand euros)
- Purpose of Transfer: Provision of service

Le flag attendu était : 28743 (order number)

TOUT CA POUR UN PIAF

Toujours en analysant les différents échange de mail entre Mathilde et un certain NFQ, nous retrouvons le mail « email_75722aa178d81e0a.eml » contenant un fichier PDF et le code technique du prototype EAGLE

Nouvelles informations disponibles

Mathilde de Guerigny <mathilde.deguerigny@aeroguard-technologies.eu>
À NFQ

Schéma_drone_EBV001.pdf
161 octets

NFQ,

J'ai récupéré des schémas préliminaires du drone "Eagle". Je les joins à ce mail. Veuillez confirmer la réception et la compensation supplémentaire comme discuté.

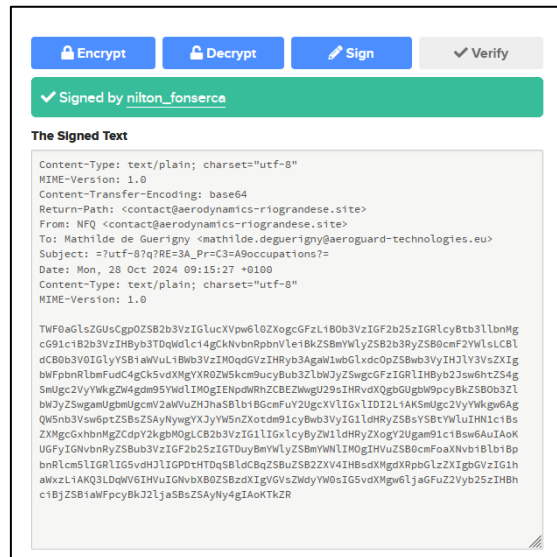
MDG

Le flag attendu était : EBV001

MAN IN THE MIDDLE

En parcourant les différents échanges sur le site des hackers, nous trouvons un mail nommé 'email_e27ff42b1f20a24e.eml' contenant une clé PGP. En ouvrant le mail avec Notepad, nous obtenons le contenu brut de celui-ci.

En nous rendant sur le site <https://keybase.io/verify> et en y entrant ce contenu brut, nous pouvons alors identifier la personne ayant signé ce mail à l'aide de sa clé PGP.



Nous retrouvons alors l'identité de « NFQ » : https://keybase.io/nilton_fonserca, Nilton Fonserca Quadros.

Pour connaître son rôle auprès de Joaquim (le chef de la famille Alveiro), nous devons retourner sur le blog familial (<https://www.alveirofamily.website/>). C'est dans l'article 'La visite de Papa en France' que nous apprenons que Nilton est le bras droit du père.

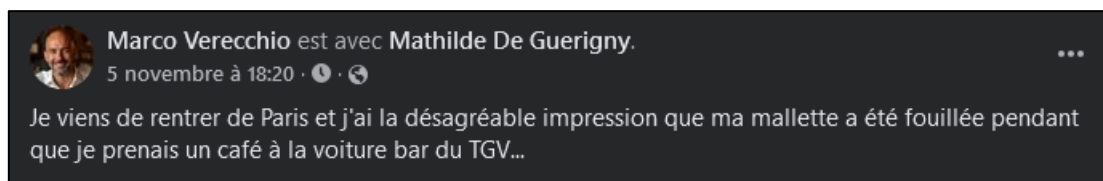
À chaque retour, c'est Nilton qui s'assure que tout se passe bien en amont. Nilton, c'est un peu comme un membre de la famille. **Il est le bras droit de mon père en France, son homme de confiance. Il gère toutes les affaires ici, que ce soit les contrats, les partenariats, ou même les réunions de dernière minute avec des clients. Mais au-delà du boulot, c'est un véritable ami de la famille. Il est présent pour nous, même quand mon père est loin.**

Le flag attendu était : nilton_fonserca_quadros_bras_droit

GRANDE VITESSE

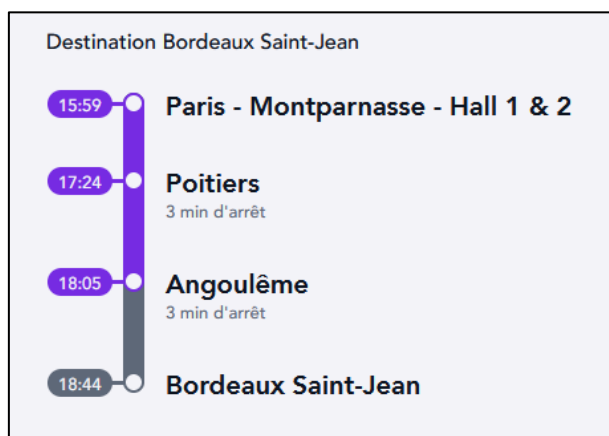
Une fois les challenges '[UNDERCOVER](#)' et '[TAUPE MODELE](#)' terminés, ce nouveau challenge se débloque.

Pour commencer, nous trouvons sur le compte Facebook de Marco Verecchio un post dans lequel il évoque un incident survenu dans le train lors de son retour de Paris, le 5 novembre à 18h12.



Pour déterminer dans quel train Marco se trouvait, nous utilisons le site : <https://signal.eu.org/rail/>.

Sachant que Marco habite à Angoulême, il a effectué le trajet Paris -> Angoulême. En consultant SNCF CONNECT, nous découvrons que la destination finale du train est 'Bordeaux Saint-Jean' et que le train généralement pris à cette heure est un TGV.



Nous effectuons ensuite une recherche sur le site Signal pour tous les trains partant le 5 novembre de la gare Paris – Montparnasse : <https://signal.eu.org/rail/tst/idfm/IDFM:71139/20241105>. Nous sélectionnons le TGV à destination de Paris – Bordeaux – Arcachon. Nous trouvons alors le train numéro 8447, qui correspond exactement à l'heure d'arrivée de Marco à Angoulême : <https://signal.eu.org/rail/train/sncf/8447>.

Horaires du train 8447

[8447 \[carte\]](#)

Circule tous les jours sauf vendredi, dimanche du 20241111 au 20241210
Sauf 20241111
Circule le 20241110

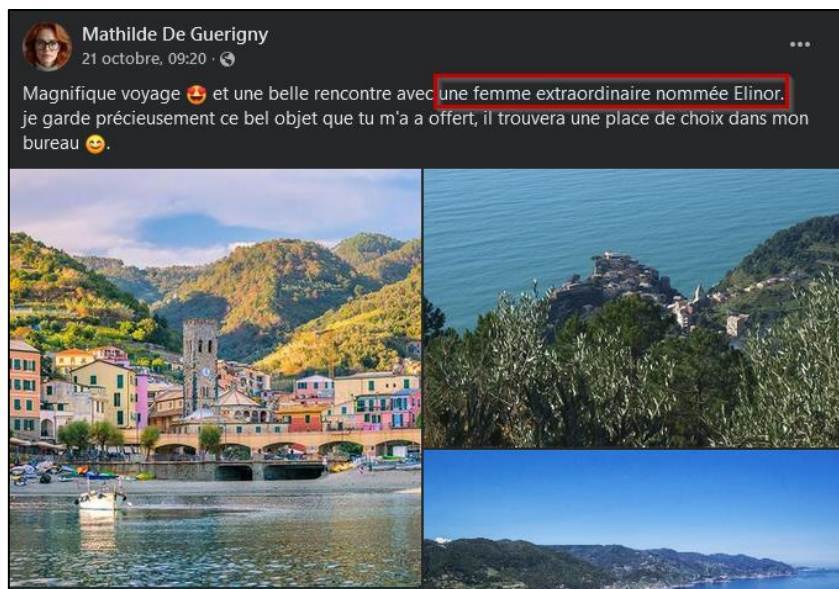
Heures du fuseau horaire Europe/Paris

Gare	Arrivée	Départ	Voie	km	V moyenne
Paris Montparnasse Hall 1 - 2		15:59:00		0.0	
Poitiers	17:24:00	17:27:00		317.8	224.3
Angoulême	18:05:00	18:08:00		431.5	179.6
Bordeaux Saint-Jean	18:44:00			545.7	190.4

Le flag attendu était : 8447

SOUS CONTROLE

En faisant le lien avec les différents challenges, nous découvrons sur le profil Facebook de Mathilde DE GUERIGNY (DRH) qu'elle a également été aux Cinque Terre en Italie pendant la même période que madame De Courselle (challenge : [UNDERCOVER](#)).



Par conséquent, on peut affirmer que Mathilde a été approchée par Elinor De Courselle lors de son voyage.

Le flag attendu était : elinor_de_courselle

DISPARITION SUSPECTE

Dans un premier temps, sur le profil Bluesky de la mère de famille, nous trouvons un post 'inquiétant', laissant entendre qu'un événement tragique s'est produit.



Cette famille semble être très connectée sur Internet. C'est ainsi que nous retrouvons l'arbre généalogique de la famille sur Geneanet : <https://gw.geneanet.org/edecourselle?n=de+courselle&oc=&p=elinor>

Vos critères
Préférences

Nom : de COURSELLE
Prénom(s) : Elinor

Modifier
Nouvelle recherche

1 résultat

Trier par Résultats

DE COURSELLE Elinor
Conjoint : ALVEIRO DIAS Joaquim
Arbre de edecourselle

Naissance 1980
Paris, Paris, France

On apprend alors que le fils Leandro Alveiro est décédé le 30 octobre 2024 lors d'un accident de moto :

<https://gw.geneanet.org/edecourselle?lang=fr&n=alveiro&p=leandro>

♂ **Leandro ALVEIRO**

- Né le 31 mars 1999 (mercredi) - Ciudad Del Sol, Republique de Riograndese
- Décédé le 30 octobre 2024 (mercredi) - Paris, France, à l'âge de 25 ans
- Pentester

Le flag attendu était : 30/10/2024

UNE LONGUE HISTOIRE

Nous avons précédemment trouvé le lien vers le site web de l'actionnaire principal de l'entreprise Innovexcapital (voir challenge 'VOS PAPIERS SVP') : <https://www.Aerodynamicss-riograndese.site/fr/>

Nous avons également trouvé le lien vers le blog familial de la famille Alveiro (challenge « un pour tous ») <https://www.alveirofamily.website/>

Sur le blog familial, dans l'article 'La visite de Papa en France', nous apprenons qu'Aerodynamics a été fondée en juillet, tandis que sur la page 'About' du site Internet d'Aeroguard (<https://www.Aerodynamicss-riograndese.site/fr/about/>), il est précisé qu'elle a été fondée en 2003.

Mon père est un homme occupé,
dirigeant une entreprise technologique en pleine expansion en
République de Riograndese du nom d'Aerodynamics Riograndese qu'il a fondée en juillet 2003.

Notre Histoire

AeroDynamics Riograndese Ltd a été fondée en 2003 par Joaquim Alveiro Dias, un passionné de mécanique et de robotique, déterminé à faire de la

Le flag attendu était : juillet_2003

III. Challenges : SIDEQUEST

Les challenges de la catégorie SIDEQUEST de l'événement n'étaient pas directement liés aux scénarios. Cependant, ils devaient tout de même être résolus pour terminer le CTF. Ces challenges font référence à des événements réels concernant certaines lois et sanctions imposées à des entreprises.

EXTRATERRITORIALITE

Grâce à une recherche Google, nous trouvons sur un site du gouvernement français un PDF évoquant les inspections des agences américaines concernant des composants ITAR :

https://www.entreprises.gouv.fr/files/files/entreprises/biens-a-double-usage/reglementation/guide_de_sensibilisation_aux_lois_americaines_de_controle_des_exportations_sgdsn.pdf

Les agences américaines en charge du contrôle des exportations mènent des inspections auprès des importateurs étrangers de biens sensibles américains ou d'origine américaine afin de vérifier le bon respect de leurs réglementations.

Cadre réglementaire	Export Administration Regulations	International Traffic in Arms Regulations
Agence américaine en charge de l'inspection	Antenne du bureau de l'industrie et de la sécurité de Francfort. Personnel détaché depuis les États-Unis dans le cadre du programme <i>Sentinel</i> .	Personnel des ambassades américaines dans le cadre du programme <i>Blue Lantern</i> .
Types de vérification	Les <i>Pre-License Checks</i> consistent en une vérification des renseignements fournis par l'importateur étranger dans sa demande de licence américaine, en amont de l'exportation du bien. Les <i>Post-Shipment Verifications</i> consistent en une vérification de l'utilisation finale du bien déclarée par l'importateur étranger dans sa demande de licence américaine après que le bien a été exporté.	Le programme <i>Blue Lantern</i> prévoit des contrôles, effectués avant ou après la délivrance d'une licence ou l'expédition d'un produit contrôlé au titre des <i>ITAR</i> .

Nous apprenons alors que ce programme s'appelle 'Blue Lantern'.

Le flag attendu était : blue_lantern

LA LOI C'EST LA LOI

Pour ce challenge, la réponse concernant l'article de loi encadrant les investissements étrangers en France est disponible sur la page du site du ministère de l'Économie : <https://www.tresor.economie.gouv.fr/services-aux-entreprises/investissements-etrangers-en-france>

Investissements étrangers en France

Procédure de demande d'autorisation et d'avis

Les relations financières entre la France et l'étranger sont libres. Par exception, dans des secteurs limitativement énumérés, touchant à la défense nationale ou susceptibles de mettre en jeu l'ordre public et des activités essentielles à la garantie des intérêts du pays, l'article L. 151-3 du code monétaire et financier soumet les investissements étrangers à une procédure d'autorisation préalable.

Le flag attendu était : L151.3_code_monetaire_et_financier

CATALOGUE

Pour ce challenge, il fallait d'abord trouver le fichier de nomenclature d'Eurosatory 2022. Grâce à une recherche Google, il est facilement accessible : <https://www.eurosatory.com/wp-content/uploads/Eurosatory-2022-Nomenclature.pdf>.

Parmi les différentes catégories, la seule qui correspondait aux activités d'Aeroguard était celle de 'Détection, Localisation, Acquisition et Leurrage'. Finalement, la sous-catégorie correspondant aux activités d'Aeroguard dans cette catégorie était : E11

Détection, Localisation, Acquisition et Leurrage	
	Détection, Localisation, Acquisition et Leurrage
E 1	Surveillance radar
E 2	Moyens d'observation de jour et de nuit (jumelles, lunettes, caméras thermiques et à intensification de lumière)
E 3	Capteurs oubliés
E 4	Dispositifs d'écoute
E 5	Dispositifs d'identification (Identification Ami/Ennemi), balises de détresse
E 6	Système d'Information Géographique - Positionnement - Navigation - Géolocalisation
E 7	Organes de visée - Commandes de pointage - Conduites de tir
E 8	Acquisition et désignation d'objectifs - Télémètres
E 9	Moyens de mesures météorologiques
E 10	Moyens topographiques
E 11	Dispositifs de détection d'alerte, de contre-mesures et de protection active
E 12	Furtivité (acoustique, thermique et électromagnétique)
E 13	Brouillage
E 14	Systèmes de poursuite de véhicules et de personnes

Le flag attendu était : E11

BALANCE TON DRONE

Pour trouver le numéro à contacter pour signaler une violation potentielle de l'ITAR (International Traffic in Arms Regulations), la réponse se trouvait sur le site gouvernemental américain du Bureau de contrôle des exportations de défense (Directorate of Defense Trade Controls - DDTC).

https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_contact_us

Contact DDTC	
DDTC Help Desk The DDTC Help Desk provides technical support to users of DDTC applications when they encounter website or system issues. These issues could include, but not limited to: DDTC Public Portal, DECCS Industry Service Portal, DECCS Enrollment and/or Log In, Passwords, Multi-Factor Authentication (MFA), Corporate Administrator (CA) Role, Registration & Licensing Roles, Registration and/or License Payments, and Functionality of Registration & Licensing online forms. Additional Note: If applicable, it is recommended that you have your registration code, license number, and/or case number readily available before calling our intake agents. Contact the DDTC Help Desk: Email (202) 663-2838 8:00am - 5:00pm	DDTC Response Team The Response Team provides non-authoritative guidance on basic regulatory and process questions and assists exporters in identifying how to get answers to more complex questions through other well-established DDTC channels. Although we cannot make determinations, we can provide you with resources that will support you in making an informed decision on issues regarding the requirements of and process for submitting Advisory Opinion and Commodity Jurisdiction requests, Registrations, and Licenses along with guidance around regulatory changes. Additional Note: If applicable, it is recommended that you have your registration code, license number, and/or case number readily available before calling our intake agents. Contact the DDTC Response Team: Email (202) 663-1282 8:00am - 5:00pm

Le flag attendu était : 202_663_1282_DDTC_response_team

PATTE BLANCHE

En cherchant sur internet « circulaire interministérielle 2012 dispositif protection », nous retrouvons un lien vers un site du gouvernement français évoquant la protection du potentiel scientifique et technique de la nation.

<https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation>

On retrouve alors un lien pour consulter une présentation du dispositif PPST :

https://www.sgdsn.gouv.fr/files/files/Nos_missions/a5-ppst-v5.pdf

• Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.
N°3415/SGDSN/AIST/PST
du 7 novembre 2012



FONCTIONNEMENT

La réglementation prévoit l'**identification des zones à régime restrictif (ZRR) abritant les activités de recherche ou de production stratégiques de l'établissement**. Il peut s'agir de bureaux, de laboratoires, de plates-formes expérimentales, etc.

Lorsqu'une personne souhaite accéder à une ZRR pour y **travailler** (travail contractuel ou relevant d'une convention de coopération, sous-traitance, etc.) une **demande d'accès** doit être formulée auprès du ministère de rattachement de l'établissement. Le ministère instruit le dossier de demande d'accès et émet un avis fondé sur une analyse technique et de sécurité dans un délai maximum de deux mois.

Le dispositif offre un espace de **dialogue privilégié entre l'établissement et son ministère de rattachement**.

AVANTAGES

- ✓ **Contraintes limitées** pour l'établissement. Aucune mesure de protection physique n'est exigée en dehors d'un espace clos. L'établissement protège sa/ses zone(s) selon ses moyens et son besoin de protection
- ✓ **Flexibilité** du dispositif pour l'entité

MISE EN ŒUVRE

Le dispositif **PPST** offre une **protection juridique et administrative** qui découle de la constitution d'une

Le flag attendu était : 3415/SGDSN/AIST/PST_PPST_ZRR

REAL WORLD

Nous pouvons trouver sur un site gouvernemental américain un article évoquant cette sanction :

<https://home.treasury.gov/news/press-releases/jy2651>. Il est alors mentionné que la société chinoise 'Redlepus Vector Industry Shenzhen Co Ltd' est impliquée dans cette affaire.

En consultant Opensanctions, nous pouvons obtenir les détails concernant cette sanction :

<https://www.opensanctions.org/entities/NK-akF9JnfsTGYz8RNRcgwhh7/>.


On y retrouve également le numéro d'enregistrement de l'entreprise : 1440300MA5HX80Y1Q.


Sur le portail officiel chinois des registres d'entreprise (<https://www.gsxt.gov.cn>), nous pouvons finalement retrouver des informations sur ce numéro d'enregistrement, notamment le nom du représentant légal :

用时0.024秒, 查询到1条信息

红兔矢量实业（深圳）有限公司

存续（在营、开业、在册）

 统一社会信用代码：91440300MA5HX80Y1Q

 法定代表人：黄英

 成立日期：2023年05月30日

注册号：

Le flag attendu était : 黄英 (Huang Ying)ⁱ

^{i i} Fin du writeup – Objectif EAGLE