

Write UP Medileakv2s

Voici le Write Up officiel de Medileak v2, CTF OSINT produit par Limoges Métropole et conçu par Oscar Zulu.

La solution n'étant pas linéaire, la présentation de ce write up a été organisée en catégories qui suivent le fil de l'enquête.

RAOUL

#Intro

Énoncé :

Un an s'est écoulé depuis l'affaire de la Clinique Yemanji, la fuite de ses fondateurs et la mise aux enchères des données de santé collectées par l'association Osain.

Pourtant, des questions persistent concernant un personnage qui avait mystérieusement disparu le 10 juin 2024 à Limoges. En effet, Raoul, notre pharmacien, n'avait laissé aucune trace derrière lui. Mais son appétit pour les activités lucratives n'est sans doute pas assouvi. Et votre instinct vous souffle que ce personnage peu scrupuleux n'a peut-être pas fini de faire parler de lui.

Solution :

Pas de difficulté ici, c'est juste pour bien prendre en compte le règlement et les outils par les joueurs.

flag : **Surtout pas de cloches**

#legacy

Énoncé :

Comment retrouver un homme disparu depuis bientôt un an, sans avoir laissé de trace ?

Il serait peut-être opportun de relire attentivement le Write Up Officiel de Medileak pour se rappeler de Raoul, de son passé et de ses activités...

Quel était le nom de son laboratoire ?

Format de Flag : Mc Donald's Healthy Food

Solution :

En consultant le Write Up officiel de Medileak (<https://oscarzulu.org/wu-medileak/>), on peut y voir que Raoul Reidid avait fondé un laboratoire:

Raoul Reidid

COO, Nutritionniste

Raoul Reidid, nutritionniste chevronné, est le Directeur des Opérations (COO) de la Yemanja Clinic. Avec plus de quinze ans d'expérience dans le domaine de la nutrition holistique et fonctionnelle, Raoul a développé une approche unique qui intègre les principes de la biochimie individuelle à des régimes personnalisés pour optimiser la santé et le bien-être. Passionné par la recherche sur les impacts des micronutriments sur la santé long terme, il a rejoint la Yemanja Clinic pour appliquer et partager ses méthodes innovantes qui privilégient une alimentation ciblée comme fondement de la médecine préventive et curative.

Éducation et parcours :

- **Certification en Nutrition Holistique**, Institut Européenne Alternative de Diététique et Micronutrition (IEADM)
- **Diplôme de Pharmacien**, Université internationale de Chypre (CIU)

Philosophie personnelle : « Une alimentation adaptée est la clé de voute d'une santé robuste et d'une vie équilibrée. À Yemanja Clinic, nous utilisons le pouvoir transformateur des aliments pour combattre les maladies et restaurer la vitalité de nos patients. »



COO, Nutritionniste

Raoul Reidid, nutritionniste chevronné, est le Directeur des Opérations (COO) de la Yemanja Clinic. Avec plus de quinze ans d'expérience dans le domaine de la nutrition holistique et fonctionnelle, Raoul a développé une approche unique qui intègre les principes de la biochimie individuelle à des régimes personnalisés pour optimiser la santé et le bien-être. Passionné par la recherche sur les impacts des micronutriments sur la santé long terme, il a rejoint la Yemanja Clinic pour appliquer et partager ses méthodes innovantes qui privilégient une alimentation ciblée comme fondement de la médecine préventive et curative.

Fort de son expérience, il a également fondé le laboratoire **Dr. Revel's Marvel Oils** pour produire des médicaments naturels loin des pressions des grands groupes pharmaceutiques.

Éducation et parcours :

- **Certification en Nutrition Holistique**, Institut Européenne Alternative de Diététique et Micronutrition (IEADM)
- **Diplôme de Pharmacien**, Université internationale de Chypre (CIU)

Philosophie personnelle : « Une alimentation adaptée est la clé de voute d'une santé robuste et d'une vie équilibrée. À Yemanja Clinic, nous utilisons le pouvoir transformateur des aliments pour combattre les maladies et restaurer la vitalité de nos patients. »

Le flag est: **Dr. Revel's Marvel Oils**

#reboot

Énoncé :

Raoul n'a surement pas encore goûté aux joies d'une retraite (bien mal) méritée.

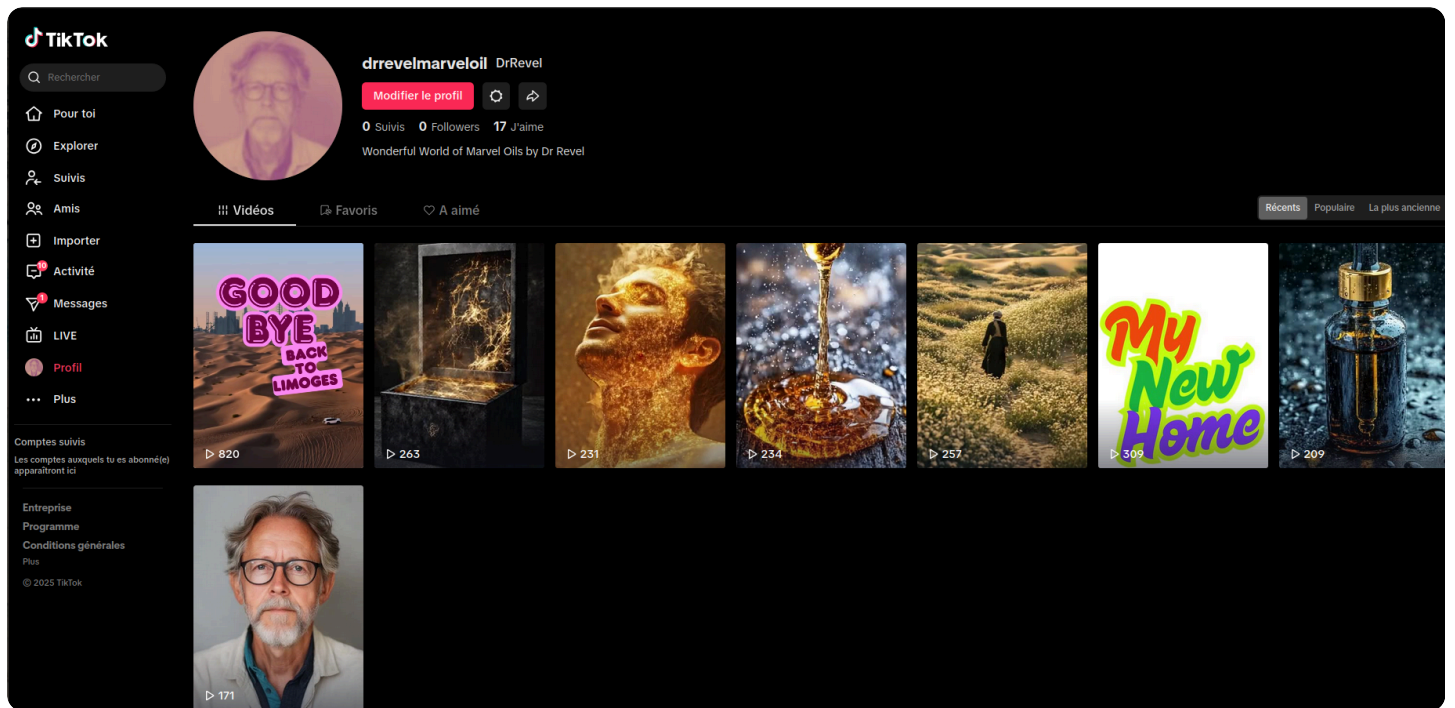
Mais quel est son pseudo sur un réseau social bien connu de partage de vidéo ?

format : **unpseudo**

Solution :

La recherche d'un reseau social bien connu de partage de video peut être Youtube, Dailymotion mais aussi Tiktok.

En recherchant Dr Revel sur Tiktok, on trouve le profil de notre cher docteur qui fait la promo de ses huiles magiques



Le flag est : **drrevelmarveloil**

#notcyprus

Énoncé :

Notre pseudo medecin a donc bien rebondi en utilisant les nouveaux codes de communication.

Mais ou se trouvait-il donc le 5 avril 2025 ?

Solution :

Sur son profil tiktok, nous voyons une vidéo intitulée New Life, New Home datée du 05/04.

On y voit un balcon et un immeuble dans le fond.

L'analyse de cet immeuble avec Google Image nous oriente rapidement vers la tour Al Manara située à Dubai (<https://www.skyscrapercenter.com/dubai/al-manara/14186>)



On voit donc la tour Al Manara à droite, une autre tour sur la gauche et un bâtiment plus près. En étudiant une carte, on peut en déduire que nous sommes situé à cet endroit:



Le flag est : **25.1846 55.2617**

#fanclub

Énoncé :

Raoul a sûrement des admirateurs. Qui est le plus grand fan de Raoul ?

Solution :

Le flag est: **EK73**

#PasSympa

Énoncé :

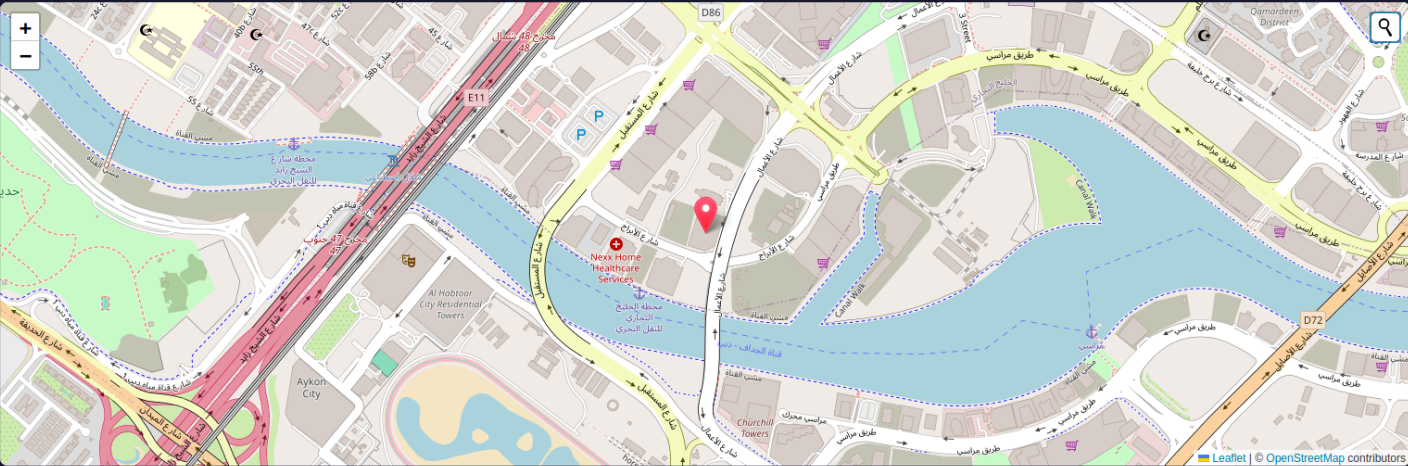
Le départ de Raoul semble un peu précipité...

Trouvez l'initiale et la date du message qui l'a convaincu de partir

Solution :

En nous rendant sur place grâce à l'OIW,

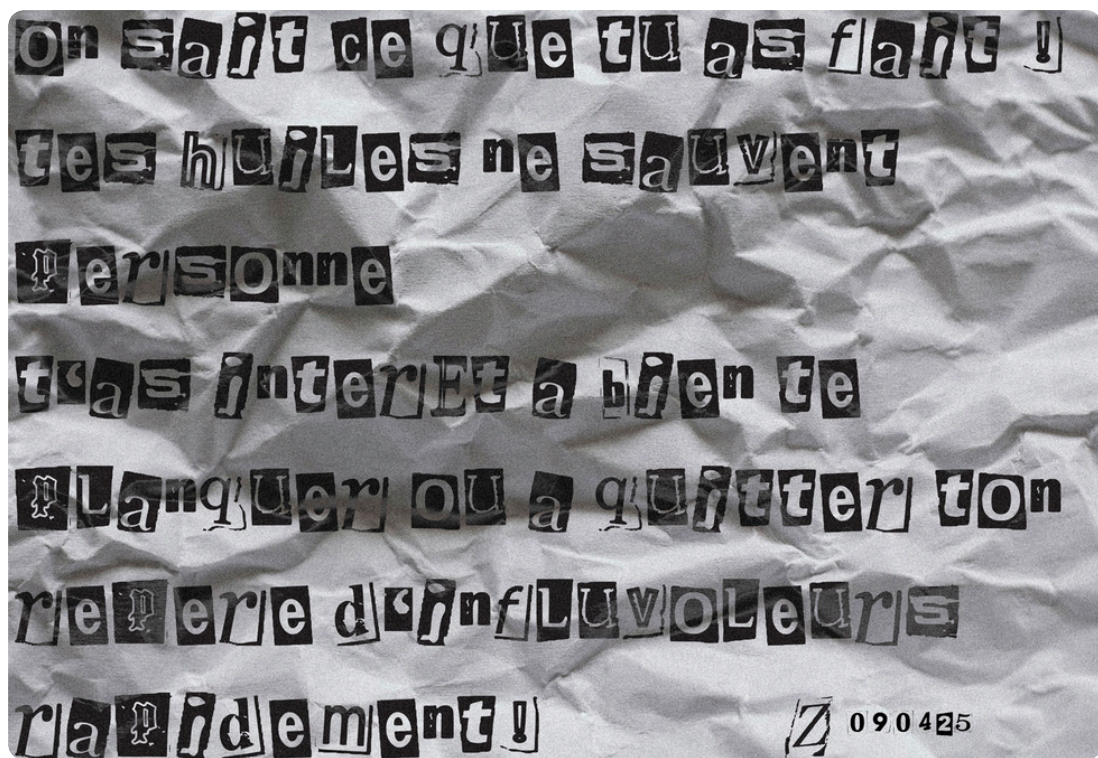
Exploration



Chez Raoul

Un contact se rends sur place. Cette tour est remplie de beaux appartements au sein du coeur même de la capitale des influenceurs. Les couloirs résonnent des musiques des derniers trends TikTok, et l'atmosphère est remplie d'odeur de produits cosmétiques à bas coûts. Votre contact obtient auprès du gardien des informations sur la place de parking qu'occupait Raoul. Il trouve contre un mur un [papier froissé](#).

nous trouvons un mystérieux message sur un papier froissé:



Le flag est: Z090425

Employeur providentiel

#NewJob

Énoncé :

Une offre d'emploi providentielle semble attendre Raoul à son retour en France.

Quel est le nom **commercial** de la société ?

Solution :

Nous avons trouvé précédemment que Celestin Marchevend s'intéressait à Raoul. Une recherche sur les RS en utilisant le nom de Celestin (ou AITOUBIB) nous remonte un compte bluesky pour Celestin (<https://bsky.app/profile/celestinm.bsky.social>)

Célestin Marchevend
@celestinm.bsky.social
81 abonné-e-s 48 abonnements 3 posts
CEO AI TOUBIB

Posts Réponses Média Vidéos

Célestin Marchevend @celestinm.bsky.social · 23j
Les discussions avec de potentiels partenaires sont toujours des moments difficiles pour tout le monde. Chacun envisage le futur avec ses propres contraintes, ses propres enjeux. Le but est de trouver un point de rencontre où tout le monde sera satisfait... #startup #medtech

Célestin Marchevend @celestinm.bsky.social · 28j
Très heureux d'avoir lancé il y a quelques jours la version définitive (et gratuite pour le moment) de AITOUBIB !

drroul.bsky.social @drroul.bsky.social · 28j
Ravi de ces nouvelles responsabilités chez AITOUBIB !

Célestin Marchevend @celestinm.bsky.social · 28j
ravi de t'avoir parmi nous ! Nous allons faire de grandes choses !

L'étude de ses réponses nous informe que Raoul (sous le compte <https://bsky.app/profile/drroul.bsky.social>) à de nouvelles responsabilités chez AITOUBIB.

Nous voyons plusieurs orthographes pour AITOUBIB, afin de confirmer le nom commercial, nous allons rechercher le site web de cette société.

Sur son site web <https://aitoubib.fr/page/legal/>, nous y voyons que le nom est AITOUBIB.

Nous découvrons également l'existence de <https://finint.ninja/>, ce site nous confirme que le nom commercial est AITOUBIB mais que la dénomination sociale de l'entreprise est Medilla.

Le flag est: **AITOUBIB**

#IciCaRecrute

Énoncé :

AITOUBIB recrute !

Quelle est l'url pour "postuler" ?

Solution :

Sur le site web trouvé précédemment, nous voyons dans la page actualités (<https://aitoubib.fr/page/actualites/>) un article sur le recrutement d'un CTO

(<https://aitoubib.fr/page/offre-demploi-cto/>).

Le recrutement semble se faire au travers d'un CTF via la plateforme ctf.iraoul.fr.

Le flag est : **<https://ctf.iraoul.fr>**

#TropTard

Énoncé :

Il semble que le poste de CTO soit déjà pourvu...

Domage...

A quel "groupe" appartient le gagnant ?

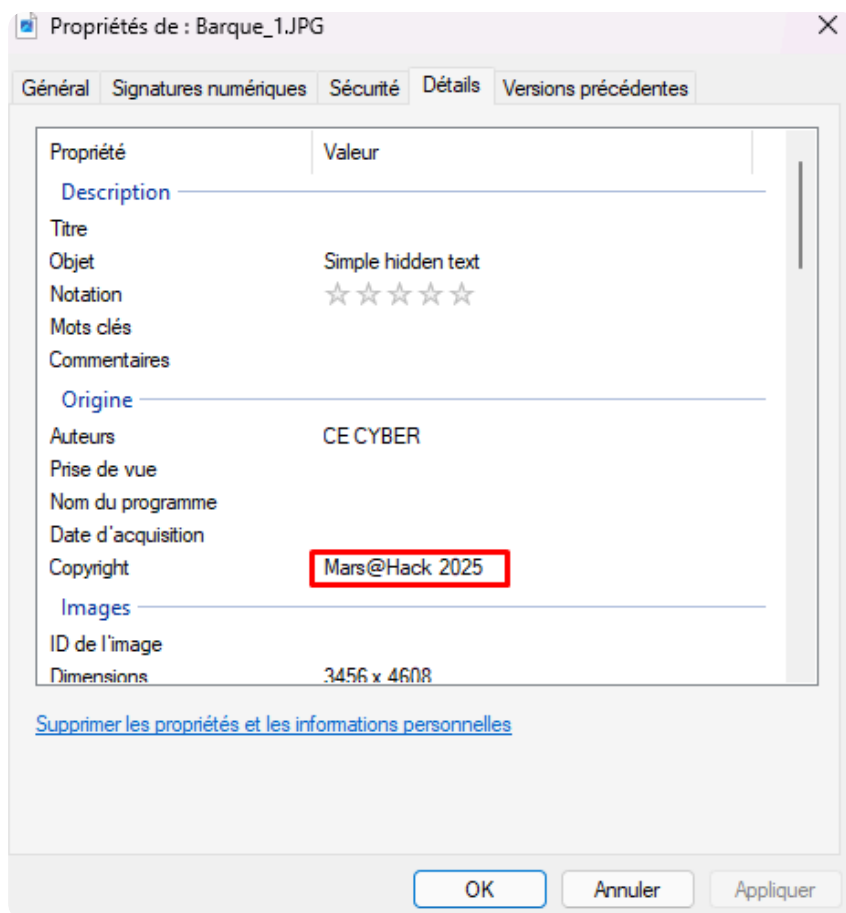
Solution :

Nous allons regarder de plus près cette plateforme de CTF. Dans la présentation, une des questions peut nous orienter sur une piste:

Q : Ces challenges sont originaux ?

R : Mais Oui ! Vous croyez vraiment que des gens honnêtes comme nous s'amuse à copier coller des challenges déjà existant ?

Le premier challenge de Stegano (SmallText) nous présente une image. En analysant cette dernière nous voyons que le propriétaire de l'image n'est pas Raoul mais Mars@Hack 2025.



Cela semble confirmer notre hypothèse que Raoul n'a pas produit les challenges mais simplement recopié ces derniers. Nous allons donc chercher ce que contient Mars@Hack 2025.

Une recherche Google avec **"Mars@Hack" writeup** nous remonte un git regroupant tout les write up des éditions passées de Mars@Hack (<https://gitlab.com/marshack>)

Nous y retrouvons l'ensemble des challenges proposés sur la plateforme iraoul et nous permet de valider rapidement les challenges.

Le flag de fin nous indique que le gagnant est Fastictac de l'équipe Fun Loving Squirrels.

END Challenge

0

Félicitations à notre Gagnant ! **Fastictac**, membre des **Fun Loving Squirrels** remporte ce CTF individuel avec un score impressionnant de 610 points ! En seulement quatre jours, Fastictac a démontré une maîtrise exceptionnelle dans les domaines suivants :

- Cryptographie
- Stéganographie
- Analyse de données aéronautiques
- Cryptanalyse avancée

Cette performance exceptionnelle n'est pas passée inaperçue. Nous sommes heureux d'annoncer que le poste de développeur a été attribué à **Fastictac** et n'est désormais plus à pourvoir.

Merci à tous les participants !

Entrez le flag : `f1@g{dommage}` pour terminer ce CTF

Le flag est : **Fun Loving Squirrels**

#AvisNégatif

Énoncé :

Mais AITOUBIB ne semble pas complètement "clean"...

Un projet du CEO pourrait lui attirer des problèmes s'il était rendu public.

Combien projète t-il de rémunérer par ordonnance, et quelle augmentation de la marge brute prévoit-il grâce à la mise en place de son projet ?

Solution :

Nous recherchons sur wayback machine l'existence de précédents archivage de la page aitoubib.fr.

La page a bien été archivée le 09/04/2025

(<https://web.archive.org/web/20250409140759/https://aitoubib.fr/>). En analysant cette archive nous y voyons plusieurs informations:

- L'ancienne CTO se nomme Lucie Monlucin
- Le code source de la page nous indique <!-- Cr34t3d by LVC1-F3R -->

Nous allons investiguer sur cette personne.

En pivotant sur son pseudo grâce à <https://usercheck.oscarzulu.org/> nous découvrons l'existence d'un git <https://github.com/LVC1-F3R>.



On peut y découvrir son CV, ayant changé de poste récemment nous allons regarder si des modifications récentes ont été apportées à sa page. Il s'avère que 4 commits ont été effectués sur sa page d'accueil:

Commits

main

All users All time

Commits on May 2, 2025

- Update README.md
LVC1-F3R authored 3 weeks ago
Verified 21ce643
- Update README.md
LVC1-F3R authored 3 weeks ago
Verified 922c5aa
- Update README.md
LVC1-F3R authored 3 weeks ago
Verified 0f5ec84
- Initial commit
LVC1-F3R authored 3 weeks ago
Verified c41469a

Le commit le plus récent nous informe que nous pouvons la contacter sur OIW et qu'elle est assez remontée contre son ancienne entreprise.

```

7 - Anciennement Lead Architect (CTO) chez AI TOUBIB, je suis responsable de l'ensemble de l'architecture technique de notre plateforme d'intelligence artificielle dédiée au domaine médical. Passionnée par l'intersection entre l'IA et la santé, je développe des solutions numériques innovantes qui transforment l'expérience des professionnels de santé et des patients. Mon expertise combine une solide connaissance des algorithmes d'IA avec une compréhension approfondie des enjeux du secteur médical.
8 - Mais ils ont recruté un gros escroc, qui a tout fait pour que je parte (moquerie, me dévaloriser devant le patron, saboter mon travail...). A croire qu'il voulait placer un copain à lui. Si vous voulez en discuter, n'hésitez pas à me contacter OIW:cb124ba7-76e5-4280-af99-4a8af50e8b9c
7 + Anciennement Lead Architect (CTO) chez AI TOUBIB, j'ai été embauchée en avril 2025 chez Mediprecog je suis responsable de l'ensemble de l'architecture technique de notre plateforme d'intelligence artificielle dédiée au domaine médical. Passionnée par l'intersection entre l'IA et la santé, je développe des solutions numériques innovantes qui transforment l'expérience des professionnels de santé et des patients. Mon expertise combine une solide connaissance des algorithmes d'IA avec une compréhension approfondie des enjeux du secteur médical.

```

En échangeant avec cette dernière, elle nous confie avoir stocké des informations avant son départ sur un drive.

Lucie MonLucin

Si tu es vraiment sérieux et que tu veux comprendre ce qui se passe chez AI TOUBIB, je peux te donner un lien où j'ai stocké quelques documents intéressants avant mon départ. Je préfère garder une certaine prudence, mais voici le lien : `https://drive.proton.me/urls/PRQPD201BC#VcvKWueJyu5F``. Je te conseille de faire attention, car ces informations sont sensibles. Est-ce que ça t'intéresse vraiment ?

Ce dernier contient 2 documents, le premier est un document interne d'AITOUBIB rédigé par Celestin Marchevend dans lequel il indique souhaiter employer des médecins étrangers (notamment en république Tchèque et Hongrie) afin de réduire ses couts.

Perspectives financières

Cette optimisation structurelle va considérablement améliorer notre rentabilité :

- Augmentation de la marge brute de 43,8% dès le premier trimestre de mise en œuvre
- Réduction du délai de retour sur investissement de 8 mois
- Capacité à proposer des tarifs plus compétitifs tout en augmentant nos marges

Prochaines étapes

Le déploiement de cette stratégie est déjà en cours :

1. Nous avons identifié et pris contact avec plusieurs groupes de médecins en République Tchèque et en Hongrie
2. Notre service juridique a finalisé les contrats de collaboration
3. Le système technique d'acheminement sécurisé des dossiers est opérationnel
4. Une phase pilote démarrera le mois prochain avec un groupe restreint de 20 médecins

Le deuxième document est un contrat type écrit en tchèque. Le point 3.2 indique:

3.2. Společnost se zavazuje zaplatit Lékaři odměnu ve výši 200 Kč za každý podepsaný předpis v souladu s touto smlouvou.

Que l'on peut traduire par La Société s'engage à payer au Médecin des honoraires de 200 CZK pour chaque ordonnance signée conformément au présent contrat.

Le format attendu étant en €, on converti la somme (arrondi à l'euro le plus proche) à 8€.

Le flag est: **8€ / 43.8%**

#NewPartner

Énoncé :

AITOUBIB souhaite ouvrir son capital et s'associer avec une autre entreprise de la région.

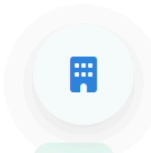
Quel est sa dénomination ?

Format : Nom Officiel

Solution :

De retour sur le site aitoubib.fr dans la section des actualités, nous voyons un article sur un partenariat avec Mediprecog en date du 25/04/2025. Ce dernier nous renvoie vers un site d'information et un article plus détaillé: <https://mednews.tech/2025/04/mediprecog-envisage-un-investissement-dans-ai-toubib-une-phase-de-test-strategique-en-cours/>

L'article indique que Mediprecog est dirigée par la famille Boutevieux. En utilisant le site trouvé précédemment (<https://finint.ninja>), on voit que le Mediprecog est le nom commercial de la société Boutevieux Medical, dirigée par Jean-Michel Boutevieux.



Boutevieux Medical

SAS

Active

Nom commercial : Mediprecog

SIREN 901089771
SIRET 90108977100010
Date de création 01/05/1953
Capital social 10000,00 €
Secteur d'activité 62.01Z - Programmation informatique

Coordonnées

Avenue d'ESTER

87000 Limoges
France

Membres (1) Documents (0) Annonces BODACC (1)

Membres de l'entreprise

NOM	TYPE	RÔLE	DEPUIS	JUSQU'À	PARTS (%)
Jean-Michel Boutevieux	Personne physique	Président	01/05/2002	En cours	100,00%

Le flag est : **Boutevieux Medical**

#HomeSick

Énoncé :

Où Vesna a t-elle appris des choses difficiles sur son père ?

Solution :

Vesna Dvořáková est la conseillère santé et communication d'AITOUBIB (comme indiqué sur <https://aitoubib.fr/page/equipe/>)

Nous pouvons voir qu'elle a commenté un post de Raoul sur Bluesky avec le compte <https://bsky.app/profile/vesnadvorak.bsky.social>



Une recherche google avec son pseudo vesnadvorak nous remonte un compte Tripadvisor (<https://www.tripadvisor.com/Profile/VesnaDvorak?fid=d3549aa7-b142-481c-b9ed->

a2093df28f9f):

vesnadvorak

Tous Produits Images Vidéos Vidéos courtes Actualités Livres Plus ▾ Outils ▾

Essayez avec cette orthographe : **vesna dvorak**

Bluesky
https://bsky.app › profile › vesna... · Traduire cette page ⋮

Dvořáková Vesna (@vesnadvorak.bsky.social)
Dvořáková Vesna. @vesnadvorak.bsky.social. 25 followers17 following. 0 posts. **Student Nurse**. Advisor in french health tech startup AI TOUBIB. Posts. Media.

Bluesky
https://bsky.app › profile › follows · Traduire cette page ⋮

People followed by @vesnadvorak.bsky.social
Recovering forum poster, politics doomer, basketball nerd. I write code for a living. He/him. Deputy Chair of the Ankh-Morpork Posters' Guild 🇫🇷 rights ...

Tripadvisor
https://www.tripadvisor.com › Sh... · Traduire cette page ⋮

Perfect tiny church - Review of Chapelle Saint Aurelien ...
VesnaDvorak. Limoges, France. 4. Reviewed 3 weeks ago. Date of experience: April 2025. This review is the subjective opinion of a Tripadvisor member and not of ...
5,0 ★★★★★ · Critique de Ceilidhmor ⓘ

Sur son avis de la chapelle Saint Aurelien, on peut y lire (traduit du Tchèque):

Mon père voulait me dire quelque chose de difficile. Il a choisi cette petite chapelle pour le faire... Apprendre que notre père se livre à des choses innommables juste pour gagner de l'argent est difficile, mais le faire aux yeux de Dieu pourrait rendre les choses moins difficiles... Je ne sais pas.

Le flag est : **45.8284, 1.2574**



Mediprecog

#Historique

Énoncé :

Quels ont été les premiers produits fabriqués par Boutevieux Medical ?

Solution : Une recherche google sur Jean-Michel Boutevieux nous remonte le site web de sa société: <https://mediprecog.eu/histoire.html>

On y voit que les premiers produits fabriqués en 1953 étaient des sphymomanomètres mécaniques

Le flag est: **sphymomanomètres mécaniques**

#Mauvaise Nouvelle

Énoncé :

Des rumeurs sur les dirigeants de l'entreprise semblent avoir fuité dans la presse.

Quelle maladie auraient-ils selon les journalistes ?

Solution : La recherche google : "boutevieux" "maladie" nous remonte un article d'un site de presse (étrangement ressemblant à mednews.tech) : <https://mednews.tech/2025/05/des-revelations-sur-letat-de-sante-de-la-famille-boutevieux-relancent-le-debat-sur-lavenir-de-mediprecog/>

On y apprend que la famille Boutevieux souffrirait de la maladie de Huntington.

Le flag est: **Maladie de Huntington**

#Source

Énoncé :

Quel est le pseudonyme de celui qui aurait fait fuiter ces informations ?

Solution : Nécessite **#TeamFLS-1** de résolu

Suite à la discussion entre les différents personnages sur le BBS, on a identifié Fastictac comme étant Lucas Tranolond, qui s'est infiltré au sein de AI TOUBIB en tant que CTO.

Le flag est: **Fastictac**

#Pression

Énoncé :

Ces rumeurs doivent bien servir un but.

Quelle entreprise a manifesté un intérêt pour racheter Mediprecog ?

Solution : Nous avons vu qu'un faux site de news semble essayer de typosquatter mednews.tech. Ces derniers ont publié un article à ce sujet : <https://mednews.tech/2025/04/mednews-denonce-une-campagne-de-desinformation-orchestree-par-des-entites-deurope-de-lest/>

Ils y dénoncent les intérêts de Advanced Medical System et de la sphère d'influence des pays d'Europe de l'Est.

On y voit également un article (<https://mednews.tech/2025/05/mediprecog-denonce-une-tentative-de-destabilisation-orchestree-a-travers-des-diagnostics-medicaux-falsifies>) sur la fuite des informations médicales de Mediprecog dans le contexte d'une tentative de rachat par Advanced Medical System qui est une filiale française du groupe tchèque Pokročilý Medicínský Systém.

Le flag est: **Advanced Medical System**

Advanced Medical System

#MaisonMère

Énoncé :

Advanced Medical System n'est qu'une filiale française d'une société étrangère.

Quel est le site web de la société qui est réellement derrière le rachat ?

Solution : Nous avons vu que *Advanced Medical System* est une filiale de *Pokročilý Medicínský Systém*. Une simple requête sur le nom *Pokročilý Medicínský Systém* avec l'extension tchèque nous remonte leur site web: <https://pokrocilymedicinskysystem.cz/>

Le flag est: pokrocilymedicinskysystem.cz

#MaisonPère

Énoncé :

Qui dirige la société ?

Solution : Nous savons que *Pokročilý Medicínský Systém* est la maison mère de *Advanced Medical System*. Une recherche sur <https://finint.ninja/companies/advanced-medical-system-none/> nous confirme cette information et nous donne accès aux documents de l'entreprise.

On y note plusieurs informations utiles:

- celle ci est dirigée à 5% par M. Alec BOUCHARDIN et à 5% par M. André FEUILLATON
- celle ci est domiciliée à *Chez le Rat 87920 Condat-sur-Vienne France*
- les status de l'entreprises sont signés par Zoran Dvořáková représentant *Pokročilý Medicínský Systém* en tant que son président.

Le flag est: **Zoran Dvořáková**

#MaisonChère

Énoncé :

La pierre est toujours un bon investissement.

Quelle maison a t-il acheté ?

Solution : Une recherche sur finint.ninja nous remonte la famille Dvořáková complète liée autour de la SCI Beau Soleil (<https://finint.ninja/companies/sci-beau-soleil-none>):

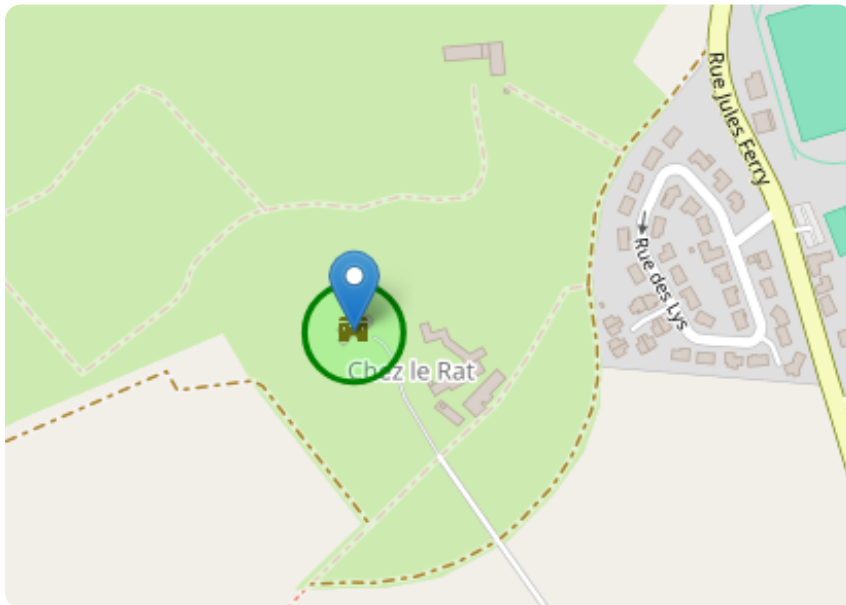
Membres de l'entreprise

NOM	TYPE	RÔLE	DEPUIS	JUSQU'À	PARTS (%)
Vesna Dvořáková	Personne physique	Associé	05/09/2024	En cours	25,00%
Zoran Dvořáková	Personne physique	Gérant	05/09/2024	En cours	50,00%
Josip Dvořáková	Personne physique	Associé	05/09/2024	En cours	25,00%

Dans les status de la SCI on peut y voir que Josip et Vesna sont jumeaux. Il est intéressant de noter que Vesna Dvořáková qui travaille chez AITOUBIB est la fille de Zoran Dvořáková.

Au travers de la SCI Beau Soleil, il a donc acheté *Chez le Rat*, 87920 Condat-sur-Vienne

Le flag est **45.7877, 1.22758**



#RadioGaga

Énoncé :

Comme dans toute opération d'influence, les médias sont un bon moyen de pression.

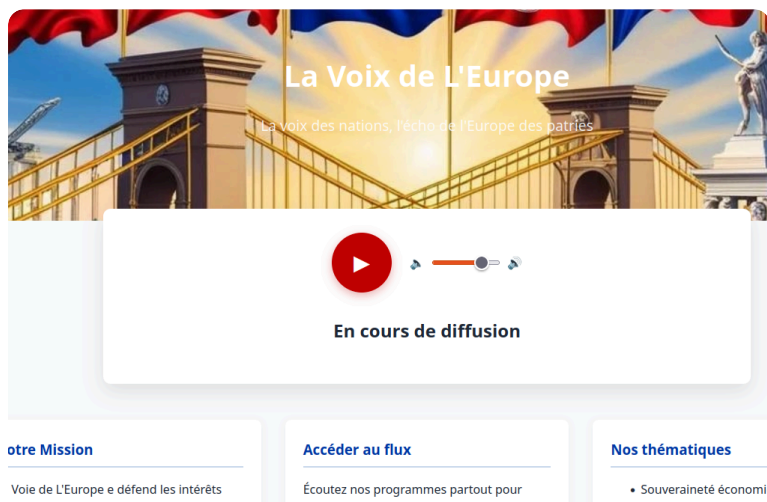
Vous avez déjà découvert un site web qui semble copier un autre site web.

Mais quelle est le nom de domaine du media "audio" que Zoran semble avoir lancé ?

Solution : En nous déplaçant sur place grâce à l'outil présent dans OIW, nous faisons la rencontre du jardinier de Zoran. Ce dernier nous apprend que lors d'un apéritif il a évoqué un de ses projets, une webradio nommée "la voix de l'Europe".

Pierre –
Monsieur Zoran a surtout parlé de sa radio en ligne, "La Voix de L'Europe", lors de cet apéritif. Il semblait assez enthousiaste à l'idée de ce projet, même si je ne peux pas vous dire exactement de quoi il s'agit. Il n'a pas donné beaucoup de détails, il est assez discret sur ses affaires. Mais il a mentionné que c'était quelque chose de qui l'occupait en ce moment. En dehors de ça, il n'a pas trop évoqué d'autres projets. C'est un homme très occupé, vous savez. Moi, je me concentre sur mon travail au jardin, c'est déjà bien assez !

Nous partons à la recherche de cette webradio, une simple recherche sur lavoixdeleurope.eu nous permet de trouver cette radio.



Le flag est: lavoixdeleurope.eu

#SoyonsDésinvoltés

Énoncé :

Quel identifiant vous permet de relier 3 sites à Zoran ?

Solution : En analysant le code source de lavoixdeleurope.eu, medinews.tech et pokrocilymedicinskysystem.cz nous trouvons la trace d'un GTM (Google Tag Manager) servant à l'analyse de trafic par Google. Le tag est **GTM-5J4M3JV8**.

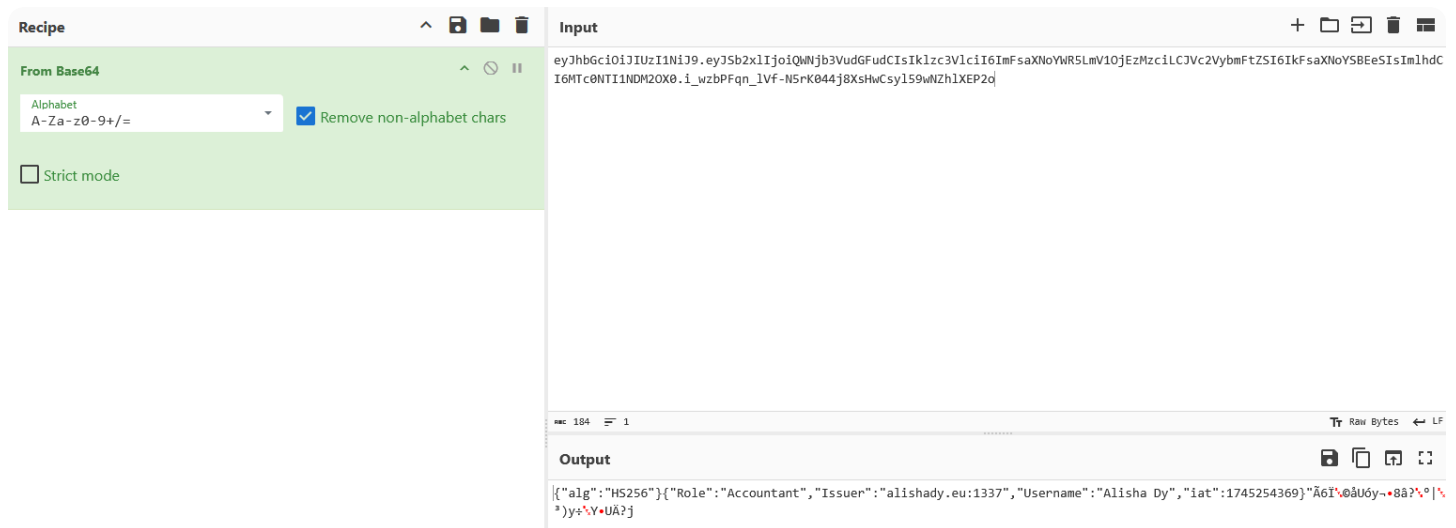
Le flag est: **GTM-5J4M3JV8**

#LesBonsComptes

Énoncé :

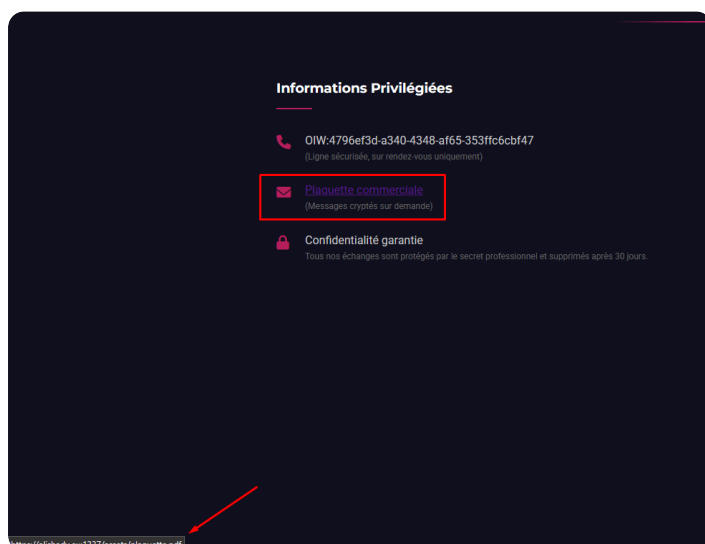
Quel comptable aide Zoran dans son projet de rachat ?

Solution : Nous avons vu précédemment que Zoran a signé le document de status d'AMS. Nous nous intéressons à ce document et en analysant ces metadatas, nous pouvons voir la trace de l'auteur dans les metadatas du document.



On y découvre une url vers le site alishady.eu:1337 qui semble être la façade illégale du cabinet comptable.

Une plaquette commerciale est téléchargeable sur le site. Celle-ci ne présente pas beaucoup d'intérêt, en revanche l'URL de téléchargement est intéressante:



En nous rendant à la racine de ce répertoire, nous découvrons une liste de documents clients.

En utilisant le numéro de SIREN d'AMS (098736187) nous avons accès à la nouvelle proposition de rachat.

Le flag est: **50%**

#MeetMe

Énoncé :

Lors de quel événement le journaliste du podcast a rencontré Zoran ?

Solution : En écoutant la webradio nous entendons un podcast dans lequel échangent deux personnes que nous avons déjà identifiées lors du challenge MaiSonPère: Alec BOUCHARDIN et

André FEUILLATON.

Nous retrouvons ces deux personnes sur bluesky avec leurs comptes respectifs

<https://bsky.app/profile/did:plc:x3koblszcai6gyj6esd7jmwh> et

<https://bsky.app/profile/did:plc:okhhtxo4owevwmgwzafioajc>

André Feuillaton a participé au salon prago-medica.cz de 2024 où il a rencontré Zoran.

Le flag est: **Prago Medica**

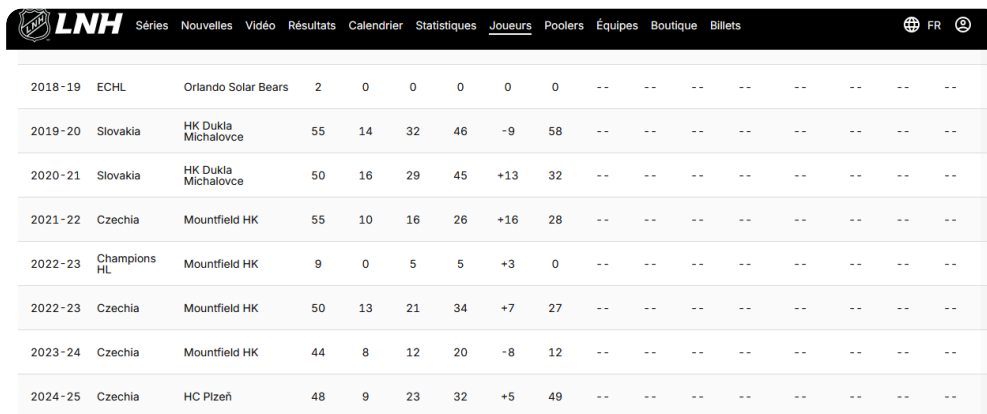
#Halftime

Énoncé :

Quel est le nom de l'équipe qui a remporté le match où le sportif de haut niveau a rencontré Zoran ?

Solution : Sur son compte bluesky (<https://bsky.app/profile/did:plc:x3koblszcai6gyj6esd7jmwh>), nous apprenons que Alec suit la carrière du joueur de hockey Christophe Lalancette et qu'il a rencontré Zoran lors du troisième match des séries éliminatoires de son équipe.

Sur le site de la NHL (<https://www.nhl.com/fr/player/christophe-lalancette-8476959>), nous pouvons voir que Christophe Lalancette évolue actuellement au club HC Plzen:



Année	Ligue	Équipe	G	A	P	PTS	PP	PA	SH	SA	SA%	SA	SA%	SA	SA%	SA	SA%
2018-19	ECHL	Orlando Solar Bears	2	0	0	0	0	0	--	--	--	--	--	--	--	--	--
2019-20	Slovakia	HK Dukla Michalovce	55	14	32	46	-9	58	--	--	--	--	--	--	--	--	--
2020-21	Slovakia	HK Dukla Michalovce	50	16	29	45	+13	32	--	--	--	--	--	--	--	--	--
2021-22	Czechia	Mountfield HK	55	10	16	26	+16	28	--	--	--	--	--	--	--	--	--
2022-23	Champions HL	Mountfield HK	9	0	5	5	+3	0	--	--	--	--	--	--	--	--	--
2022-23	Czechia	Mountfield HK	50	13	21	34	+7	27	--	--	--	--	--	--	--	--	--
2023-24	Czechia	Mountfield HK	44	8	12	20	-8	12	--	--	--	--	--	--	--	--	--
2024-25	Czechia	HC Plzeň	48	9	23	32	+5	49	--	--	--	--	--	--	--	--	--

Les statistiques autres que la LNH sont fournies par [EliteProspects.com](https://www.eliteprospects.com)

En recherchant l'historique des matchs de cette équipe, on retrouve rapidement sur le site de l'équipe le résultat du match dans un article <https://www.hcplzen.cz/match/11556>. L'équipe de Lalancette a remporté le match 3 à 0.

Le flag est : **HC Skoda Plzen**

FLS

#Modem

Énoncé :

Quel est la plateforme utilisée pour joindre les Fun Loving Squirrels ?

Solution : Nous réutilisons notre outil de recherche de profils <https://usercheck.oscarzulu.org/> avec funlovingsquirrels. Celui-ci nous remonte l'existence d'un site web lié au groupe ayant participé au CTF: <https://funlovingsquirrels.wordpress.com/>

Sur la page de contact du site, on y voit l'indication :

```
You can contact us @ 92.112.194.8:2323
```

Il faut donc se connecter à cette IP avec un port particulier. Une connexion telnet dans un terminal suffit à atteindre le BBS (Bulletin board system) utilisé par le groupe

```
=====
FUN LOVING SQUIRRELS BBS
=====
This BBS is in Read Only Mode (Maintenance Mode) / Press Enter
```

Le flag est : **bbs**

#Hack

Énoncé :

Quel est le nom de la première société qui a été attaquée avec succès par les Fun Loving Squirrels ?

Solution : En étudiant les échanges des membres de FLS sur le messagerie (touche c) on y voit l'existence d'une section xsf dans le bbs:

```
=====
LIVE CHAT
=====
[4/23/2025, 5:20:00 PM] Fastictac: First day success! Deployed the tool while the boss was getting coffee. Already mapping internal database structure.
[4/23/2025, 5:25:00 PM] Psych0Spip: Perfect timing! Can you access the genetic data storage?
[4/23/2025, 5:30:00 PM] Fastictac: Even better. Found an admin account with hardcoded credentials in a config file. Full database access achieved.
[4/23/2025, 8:45:00 PM] RedScr4t: Transfer initiated to our secure server. Patient records incoming. Link in xsf section of the bbs
[4/23/2025, 9:15:00 PM] MasterVeverka: Excellent work. I will arrange payment as discussed. No one suspects anything?

Read-only mode (anonymous)

Page 7/9 - p (previous) n (next)
```

En tapant xfs dans le menu de départ, on obtient accès au menu caché contenant plusieurs lien:

```
=====
EXTRA SECRET FILES – RESTRICTED ACCESS
=====

Special links and resources. For squirrels eyes only!

1. OKANTIS – bafybeiag6soyahmy7jvuj2l76nalxypqevz65knqpmou3skhmmumgolfsq
2. Acorn Financial – bafybeib7dw7gjpeu6wnw5et32hatx6wwbjtd5ooeixnt2uy4dh6g53lcta
3. Hospital Systems Access – bafybeidxbfwees3o7mccqzy5l67n25pvvxvh24czwxnl4wyzxpegrobx7m
4. AITOUBIB – bafybeicstsx4twfjzqfb3fzlmnwlllkfbcabxqp2yvt7cjgo5pgipcuylgm
WARNING: All access is logged and monitored

'x' to return to main menu:
```

Les liens commencent tous par "bafy", ce préfixe est caractéristique des CIDs (Content Identifiers) v1 utilisés dans le système IPFS (InterPlanetary File System), un protocole de stockage de fichiers en pair-à-pair. Ces liens peuvent être ouvert avec un client lourd ou directement en ligne.

Le premier lien renvoie vers un PDF indiquant l'échec de l'attaque de la cible OKANTIS.

Le second lien indique le succès de l'attaque de Acorn Financial

ACORN Financial

OPERATION TREASURY HUNT

ACORN Financial - Data Breach Disclosure

Date Published: ██████████
Target: ACORN Financial Services Corporation
Access Duration: ██████ days undetected
Status: COMPLETED

TARGET PROFILE

ACORN Financial Services Corp (NYSE: ACRN)
Headquarters: Chicago, IL
Employees: ██████
Assets Under Management ██████████
Clients: 5.2M+ customers across 23 countries

Le flag est: **Acorn Financial**





















#medileak

Énoncé :

Quel est la date du diagnostic de Jean Michel Boutevieux ?

Solution : Le lien ipfs (bafybeicstsx4twfjzqfb3fzlmnwlllkfbcabxqp2yvt7cjgo5pgipcuylgm

) sur le piratage d'AITOUBIB nous renvoie vers un répertoire comprenant plusieurs documents à étudier:

	 antecedents_familiaux.csv QmevFvT15CeYxznZcMMxfirzppM52xQF9A25VV1UaYgKm6
	 code_references.csv QmUM9ocJLeTlx77m9AFgkzN3CmBz1ZMk4XrBrBdyL4JAvz
	 diagnostics.csv QmPWyDFwrHMed8PF3JFxFxUUDDLixhDjwqctV1ANNhZGsymb
	 examens_cliniques.csv QmcuyUS8FpNpCaRdE6259QxYxM6315PopzFKJY2jvrGxj3
	 family_links.csv QmUAejk6EVWSDDeuv2FURhiUdkjLdwTACYJd8d9vaYfkrj
	 patients.csv QmakMNSNJ5GNyz9iNvE3zJ4akrg28TioPBUAav1Ycj973h
	 pub.pgp Qmf8rBcqVic4jDw5ziK1w9DLsZAU76JMvKvp3WgVC3xJsA
	 symptomes.csv QmeX3rFHTMaPoKxk689hybENKuf8Ar72aA4vWbaLwehwgg
	 tests_genetiques.csv QmQsqzESY7oTCDsxT91iTxYjwv8HGyKXrXoqSmb9DhVdUb
	 traitements.csv QmYJF2MHbeHyNrE6PhmqvSNA4v4cE1CpjVVQDbdCGTxcT
	 variants.csv QmWbQyU3ef1gmqzxKN8ryNhSeUkyRJ8HKxHPT4ubMRXd7T

En recoupant les informations obtenues précédemment, nous savons que nous cherchons un patient diagnostiqué de la maladie de Huntington et étant né le 26/05/1959.

Dans le fichier code_references.csv nous voyons que:

```

table_name,field_name,code_value,code_description
patients,ethnicity_code,01,Caucasien
patients,ethnicity_code,02,Africain
patients,ethnicity_code,03,Asiatique
patients,ethnicity_code,04,Hispanique
patients,ethnicity_code,05,Moyen-Oriental
patients,ethnicity_code,06,Mixte
patients,ethnicity_code,07,Autre
disease_codes,disease_code,HD01,Maladie de Huntington
disease_codes,disease_code,LY01,Syndrome de Lynch
disease_codes,disease_code,MF01,Syndrome de Marfan
disease_codes,disease_code,CF01,Mucoviscidose
disease_codes,disease_code,DM01,Dystrophie myotonique type 1
disease_codes,disease_code,FA01,Anémie de Fanconi
disease_codes,disease_code,PKD1,Polykystose rénale autosomique dominante
disease_codes,disease_code,DMD1,Dystrophie musculaire de Duchenne
disease_codes,disease_code,RP01,Rétinite pigmentaire
disease_codes,disease_code,WS01,Syndrome de Williams
patients,age_code,01,0-9
patients,age_code,02,10-19
patients,age_code,03,20-39
patients,age_code,04,40-59
patients,age_code,05,60-79
patients,age_code,06,80+

```

Nous cherchons donc avec le code HD01 et code 05

Dans le fichier patients.csv nous trouvons une correspondance:

```

PT180211,20140305,02,2,05,FR90,20241118,1,0,4,DMD1,TG24209
PT58095,19860519,03,2,04,FR44,20240603,1,0,3,DM01,TG40955
PT29541,20180901,01,1,04,FR47,20240519,1,0,1,HD01,TG37385
PT69090,19671217,04,1,03,FR78,20220221,1,0,5,DMD1,TG65837
PT15504,19560115,05,2,04,FR08,20230814,1,0,5,DMD1,TG47949
PT74001,19590526,05,1,01,FR87,20220201,1,0,5,HD01,TG44444
PT68160,19390707,06,1,03,FR03,20220909,1,0,2,DM01,TG29708
PT35419,19621214,05,1,03,FR69,20230810,1,0,3,DM01,TG93924
PT38275,19830720,04,2,01,FR68,20230101,1,0,4,DM01,TG26346
PT33912,20070716,02,2,04,FR24,20230308,1,0,2,MF01,TG30824
PT68647,19930307,03,2,04,FR76,20241223,1,0,4,DM01,TG83290
PT39433,20140329,02,2,04,FR44,20220731,1,0,5,FA01,TG48201

```

Le code patient est donc PT74001.

Dans le fichier diagnostics.csv nous trouvons également Jean-Michel Boutevieux:

```

DG00545,PT65070,20231008,DM01,273,160900,G71.1,8C71.10,1,MD52012,3,03,3,20231008
DG23411,PT44551,20241008,DM01,273,160900,G71.1,8C71.10,1,MD86374,3,01,2,20241008
DG53023,PT48143,20240619,PKD1,730,173900,Q61.2,MF50.0,1,MD20029,3,02,3,20240619
DG70041,PT80211,20241228,DMD1,98896,310200,G71.0,8C70.0,2,MD97579,3,06,1,20241228
DG41393,PT58095,20240623,DM01,273,160900,G71.1,8C71.10,1,MD27788,3,03,2,20240623
DG60205,PT29541,20240618,HD01,399,143100,G10,8A01.10,1,MD66038,3,03,3,20240618
DG79644,PT69090,20220331,DMD1,98896,310200,G71.0,8C70.0,1,MD93226,3,03,2,20220331
DG78569,PT15504,20230909,DMD1,98896,310200,G71.0,8C70.0,1,MD25511,3,03,2,20230909
DG35328,PT74001,20220308,HD01,399,143100,G10,8A01.10,1,MD76028,3,04,3,20220308
DG68940,PT68160,20221004,DM01,273,160900,G71.1,8C71.10,1,MD28489,3,03,1,20221004
DG75480,PT35419,20230909,DM01,273,160900,G71.1,8C71.10,1,MD93404,3,04,2,20230909
DG59152,PT38275,20230213,DM01,273,160900,G71.1,8C71.10,1,MD93801,3,04,3,20230213
DG76163,PT33912,20230407,MF01,558,154700,Q87.4,LD2C.00,2,MD28088,3,05,1,20230407

```

La date du diagnostique est donc le 08/03/2022.

Le flag est: **08/03/2022**

#TeamFLS-1

Énoncé :

Qui est Fastictac ?

Solution : Sur le BBS des FLS, nous y voyons des échanges autour de l'attaque sur AITOUBIB, notamment dans le forum général:

```
=====
FORUM: General Discussion
=====

#1 [3/2/2025, 1:15:00 AM] MasterVeverka:
Hello everyone. I am monitoring your activities with interest. The Squirrels have potential.

#2 [3/2/2025, 1:45:00 AM] Psych0Spip:
Master Veverka, thank you for joining our group. We won't disappoint you.

#3 [3/3/2025, 2:22:00 PM] RedScr4t:
Hey everyone. Who's ready for new digital adventures? FLS forever!

#4 [3/10/2025, 6:45:00 PM] RedScr4t:
Our last attempt didn't work. We need to change our approach. These hospital systems are tougher than expected.

#5 [4/16/2025, 11:23:00 AM] Fastictac:
I have an opportunity at AITOUBIB. Interview next week!
```

```
=====
FORUM: General Discussion
=====

#1 [4/16/2025, 12:05:00 PM] MasterVeverka:
Excellent news. Keep me informed privately.

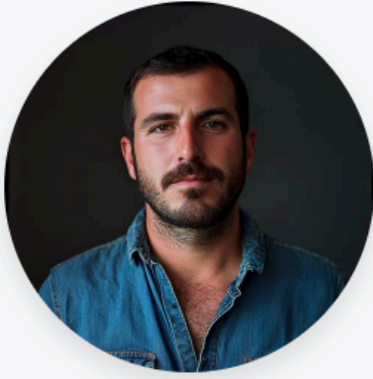
#2 [4/16/2025, 1:12:00 PM] RedScr4t:
Well, aren't you the golden boy. Just got lucky with the timing.

#3 [4/16/2025, 3:30:00 PM] Psych0Spip:
That's amazing @Fastictac! Your reverse engineering skills are really paying off!

#4 [4/23/2025, 7:30:00 PM] Fastictac:
Starting at AITOUBIB next Monday! The IT manager seems completely clueless...

#5 [4/23/2025, 8:45:00 PM] Psych0Spip:
Perfect. Don't forget our main objective. Master V will be pleased.
```

Cela nous indique donc que Fastitac travail chez AITOUBIB depuis peu de temps. Nous savons qu'il a remporté le concours pour être CTO sur la plateforme <https://ctf.iraoul.fr/>. La page d'équipe d'AITOUBIB (<https://aitoubib.fr/page/equipe/>) nous indique que le nouveau CTO est Lucas Tranolond:



Lucas Tranolond

CTO

Lucas vient de rejoindre notre équipe, il apporte sa double approche financière et technique pour garantir qu'AI TOUBIB va bouleverser le marché de la e-santé dans les prochains mois.

Une recherche avec l'outil <https://usercheck.oscarzulu.org/> sur le compte Fastictac nous remonte sa page github <https://github.com/fastictac>. En analysant un de ses commits <https://github.com/Fastictac/Fastictac/commit/8693ae8dc5468aca65ce3c68ddcc4f8ec3f3d004.patch> on y voit également un mail ltrano@ozmail.eu confirmant son identité.

Le flag est: **Lucas Tranolond**

#TeamFLS-2

Énoncé :

Qui est PsychOspip ?

Solution : Une recherche avec l'outil <https://usercheck.oscarzulu.org/> sur le compte PsychOspip nous remonte sa page steam <https://steamcommunity.com/id/Psych0Spip>

En regardant les anciens pseudo on peut voir le vrai nom de PsychOspip:



PsychOspip ▾

Cette personne a utilisé les pseudos suivants :

Psych0Spip

Josip Dvořáková

Le flag est: **Josip Dvořáková**

#TeamFLS-3

Énoncé :

Qui est RedScr4t ?

Solution :

Nous avons vu que Josip Dvořáková fait partie des FLS, son père est le propriétaire du site <https://pokrocilymedicinskysystem.cz>. En analysant ce site web avec l'outil web-check.xyz, nous trouvons la trace d'un fichier <https://pokrocilymedicinskysystem.cz/.well-known/security.txt>. Celui-ci indique:

Contact: <mailto:ivankana+redscr4t@ozmail.eu>

Expires: [2026-04-30T22:00:00.000Z](https://www.iso.org/standard/70432.html)

Preferred-Languages: [cz](https://www.iso.org/standard/42174.html)

On en déduit que redscr4t est un alias pour ivankana sur cette boîte mail.

Une recherche sur le pseudo ivankana avec l'outil <https://usercheck.oscarzulu.org/> nous remonte un compte bluesky <https://bsky.app/profile/ivankana.bsky.social>



Celui-ci appartient à Ivan Kanalchukiev

Le flag est: **Ivan Kanalchukiev**

#MasterMind

Énoncé :

Qui serait MasterVeverka ?

Solution : Des informations que nous avons trouvé, nous savons que AMS tente de racheter Mediprecog, pour cela ils ont récupéré les dossiers médicaux de la famille Boutevieux via les diagnostics effectués chez AITOUBIB. Nous pouvons donc déduire que le commendaire et donc MasterVeverka serait Zoran Dvořáková, le président de Pokročilý Medicínský Systém.

Le flag est: **Zoran Dvořáková**

Raoul2 (le retour)

#OldLove

Énoncé:

Le passé de Raoul a refait surface...

Qui veut-il protéger en obéissant aux ordres ?

Solution : Nous recherchons les personnes avec qui Raoul était en contact par le passé (via le Write Up de Medileak). Nous pouvons nous pencher sur Kallopée Hadrianos, sur son compte bluesky elle y indique ne pas se sentir en sécurité.



Cela fait longtemps que je ne me suis pas connecté... Mais ces derniers jours, j'ai des doutes sur un camion qui passe devant chez moi plusieurs fois par jour...



Son autre message est également intéressant:

Les enfants qui traînaient autour de ma maison sont finalement venus me parler... ils voulaient faire pression sur Raul mais je ne veux plus entendre parler de lui ! Ils m'ont pris pour la chanteuse de salle de bain dont il était tombé amoureux !



Toutefois elle ne semble pas être la bonne cible et fait référence à Gizem Ihanet.

Le flag est: **Gizem Ihanet**

#Insécurité

Énoncé :

Où Gizem a t-elle été "menacée" ?

Solution : En retournant sur le compte Strava de Gizem

(<https://www.strava.com/athletes/135688719>) trouvé lors de Medileak, nous pouvons y voir de nouvelles courses. Une des courses est intéressant, elle y indique avoir subi une agression le 24/04/25.



Gizem Ihanet

24 avril 2025 · Kato Pyrgos, Chypre



Course à pied dans l'après-midi

I was attacked during this session, my phone and watch were stolen... they must have destroyed it because no move on the cloud after this

Distance

2,08 mi

Allure

12:51 /mi

Temps

26min 49s



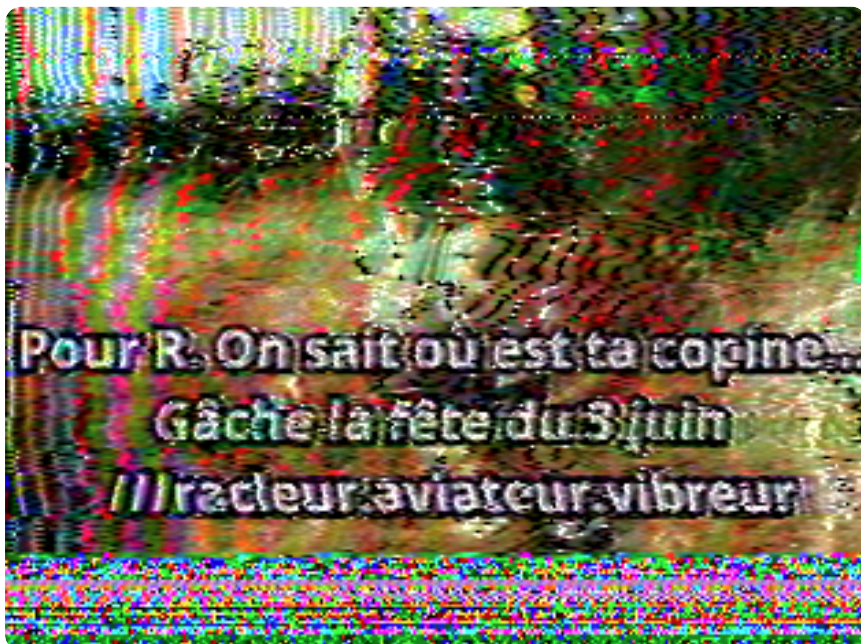
Le flag est: **35.1666, 32.6731**

#Mission

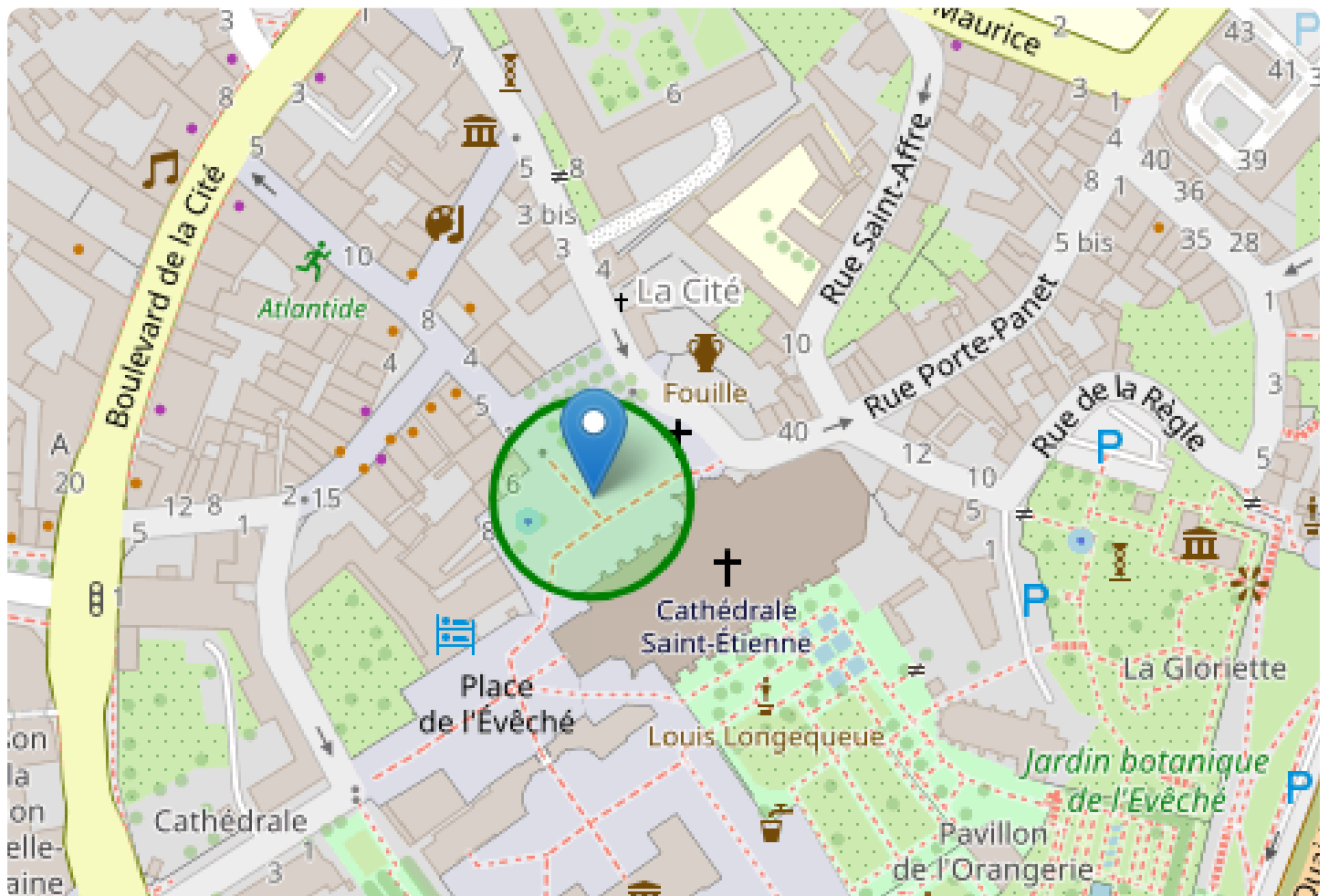
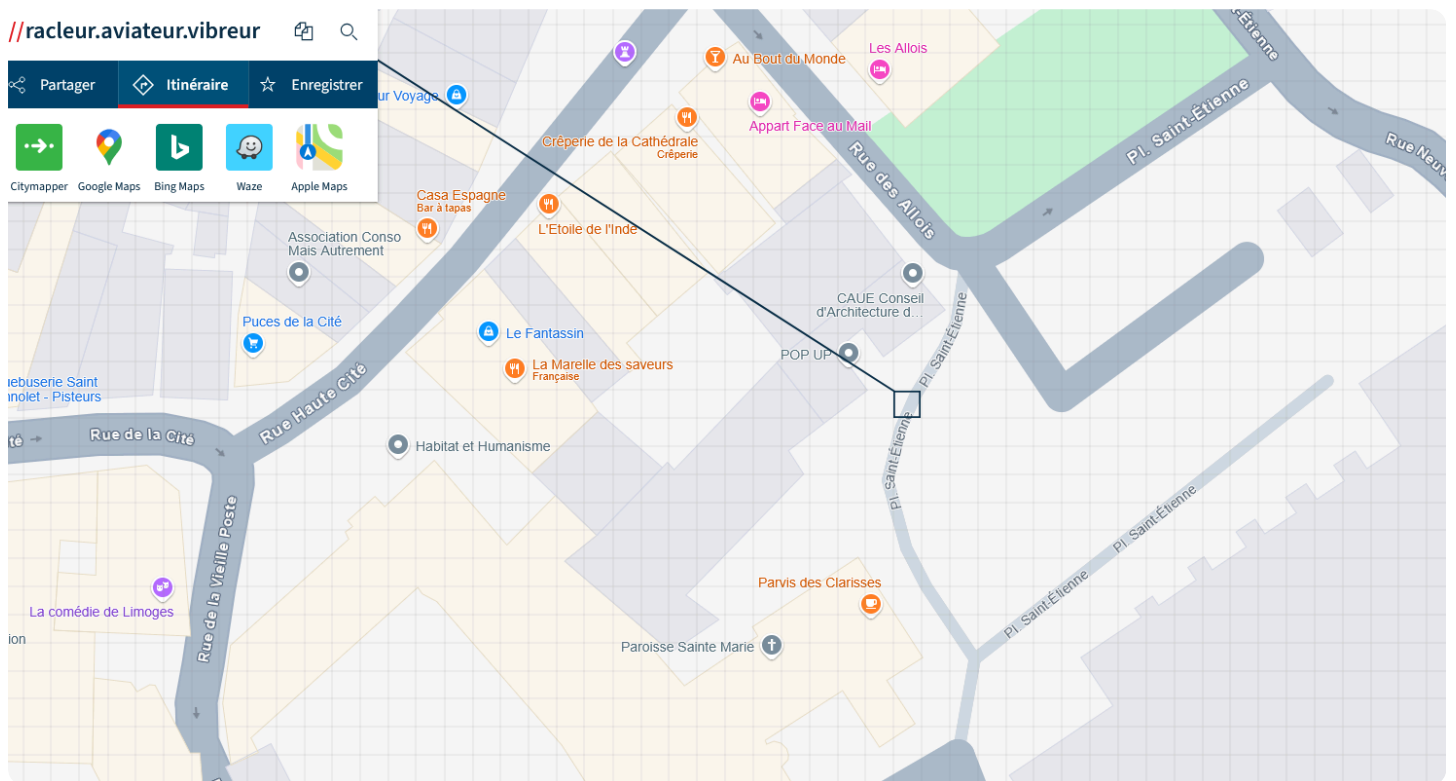
Énoncé :

Où Raoul doit-il "frapper" ?

Solution : Un message sur la webradio lavoixdeleurope attire notre attention, elle y indique un message spéciale pour R (que nous supposons ici être Raoul). A première écoute on y entend qu'une série de bruits étranges. Toutefois il s'agit véritablement d'une transmission SSTV, bien connue des radioamateurs pour la transmission d'images fixes à l'aide d'une bande passante réduite. En utilisant un décodeur d'image SSTV nous pouvons retrouver l'image transmise:



On reconnaît ici des coordonnées What3words (<https://what3words.com/racleur.aviateur.vibreur>) pointant à Limoges:



Le flag est : **45.8291, 1.26617**

#IA

Énoncé :

Quelle IA Raoul a utilisé pour développer son site de tracker de santé ?

Solution : Toujours sur la webradio, nous entendons une publicité pour les huiles de Docteur Revel nous orientant vers le site web <https://drrevel.onlineweb.shop>.

Sur son site, Raoul y vend des trackers

médicaux(<https://drrevel.onlineweb.shop/product/reveltracker>), dans la description de ces derniers, on y voit un lien vers un autre site web:

Description Détails

Le RevelTracker révolutionne le suivi de votre santé quotidienne grâce à sa technologie médicale avancée et son intelligence artificielle intégrée.

Pourquoi choisir le RevelTracker ?

✓ Suivi médical complet : ECG, SpO2, tension artérielle, glucose, température et plus encore

✓ IA médicale intelligente : détection précoce des anomalies et conseils personnalisés

✓ Certifié médicalement : dispositif médical Classe IIa avec validation clinique

✓ Autonomie exceptionnelle : jusqu'à 7 jours d'utilisation continue

✓ Compatible avec votre écosystème : synchronisation avec iOS/Android et dossier médical

Avec son design élégant, son écran AMOLED haute résolution et sa résistance à l'eau jusqu'à 50m, le RevelTracker vous accompagne partout pour une tranquillité d'esprit permanente.

Abonnements disponibles à partir de 4,99€/mois pour stocker vos données médicales sur healthcloud.iraoul.fr

Dispositif médical selon les normes européennes les plus strictes.

Cette page nous demande un login que nous ne connaissons pas. Le code source semble néanmoins effectivement écrit par une IA au vu du fort nombre de commentaires et de leur structure.

Le fichier robots.txt nous donne des informations utiles:

```
# Generated by IA
# robots.txt pour Medical Cloud
User-agent: *
Disallow: /uploads/
Disallow: /admin/
Disallow: /config/

# Note pour les développeurs: N'oubliez pas de mettre à jour cette liste
# lors de l'ajout de nouvelles sections sensibles, et vérifiez aussi
# la sécurité de votre système de contrôle de version (.git)

# Tous les répertoires cachés doivent être bloqués
# Disallow: /*

Sitemap: http://cloud.iraoul.fr/sitemap.xml
```

On y voit l'existence d'un git et de répertoires cachés, on test donc l'accès à <https://healthcloud.iraoul.fr/.git/>

Celui-ci nous donne l'ensemble du git utilisé pour le développement du site, on peut le parcourir manuellement mais le plus simple reste de télécharger en local et d'ouvrir le git:

```
:/tmp/iraoul_git$ git log --oneline
a9a7d06 (HEAD -> master) Suppression des commentaires de l'IA
eb77390 Configuration Nginx pour déploiement de test
1ced726 Intégration des Templates
1f773ca Sécurisation des paramètres de configuration
421abed Ajout des paramètres de configuration
3d26203 Ajout des fichiers de base
:/tmp/iraoul_git$ git show a9a7d06
commit a9a7d06746b7f754d88f43d7884c7df0e38b9f59 (HEAD -> master)
Author: Raoul Reidid <drrevel@ozmail.eu>
Date: Tue Apr 29 10:45:00 2025 +0200

    Suppression des commentaires de l'IA

diff --git a/templates/patient_detail.html b/templates/patient_detail.html
index 06c83e4..d7005d7 100644
--- a/templates/patient_detail.html
+++ b/templates/patient_detail.html
@@ -4,7 +4,6 @@
 <!--
 * Fichier: patient_detail.html
 * Description: Page de détail d'un patient pour l'application iRaoul
- * Généré par: Deepseek-V3
 * Date: 22 avril 2025
 * Notes: Cette page affiche les informations complètes d'un patient, ses appareils,
 *        données de santé, dossiers médicaux et médicaments
diff --git a/templates/settings.html b/templates/settings.html
index 94283af..5e2bf6c 100644
--- a/templates/settings.html
+++ b/templates/settings.html
@@ -4,7 +4,6 @@
 <!--
 * Fichier: settings.html
 * Description: Page de paramètres de l'application iRaoul
- * Généré par: Deepseek-V3
 * Date: 22 avril 2025
-->
<meta charset="UTF-8">
```

Le flag est: **Deepseek-V3**

#Soldes

Énoncé :

Pouvez vous identifier le produit de PMS que Raoul vend sur son site ?

Utiliser le code SHOP sur medileak2.oiw.fr

Solution : Sur le site de Raoul on y voit un objet identique à un autre vendu par PMS sur leur site:

<https://drrevel.onlineweb.shop/product/reveltracker>



RevelTracker

Code du produit: NpmSGcH

€1 299,00

1

SHARE: [f](#) [p](#) [t](#)

<https://pokrocilymedicinskysystem.cz/>



FitOptimum

Sledování fyzické aktivity a metabolismu

- Analýza pohybových vzorců
- Metabolické měření
- Vícesportovní režimy

BONUS

#Clochint

Énoncé :

Quel est le nom complet de la cloche française que l'on entend dans la publicité de l'association des Campanistes diffusé par la radio ?

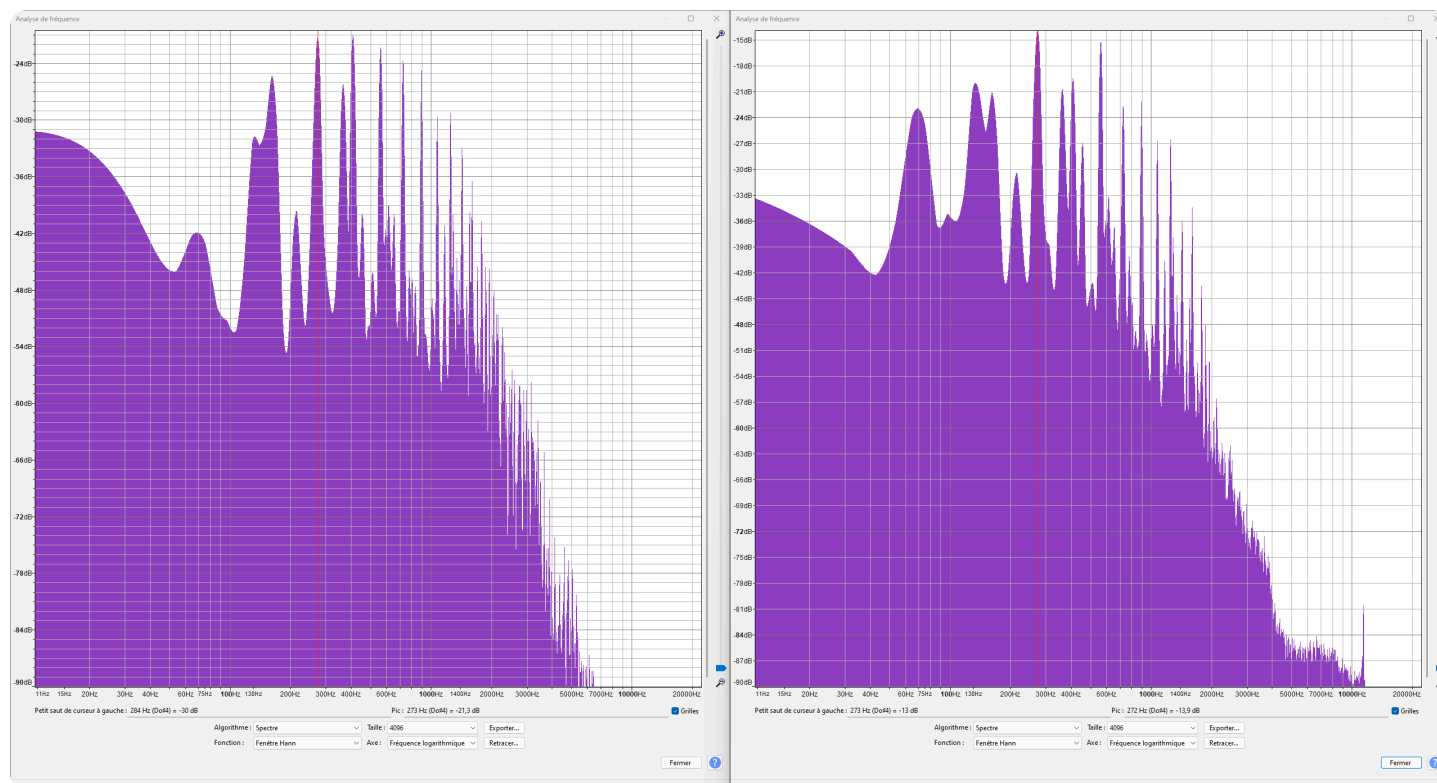
Format : Le Nom Complet d'une Cloche

Note : **Ce challenge est complètement facultatif !** Note 2 : **Ne cherchez pas la vraie association, mais celle dont la publicité est diffusée sur le CTF**

Solution :

Voici la méthode utilisée par nos gagnants de cette année, les Tacosint :

Via spectrogramme, on voit un gros pic en do#4 (j'ai vu après que le premier pic était le plus important).



Vu qu'il n'y a qu'une cloche qui sonne et qu'elle est grave, j'ai cherché un peu et je suis tombé sur la [liste des bourdons de France](#). Je check celles en "do".

Dedans il y a la bonne qui est la première de la liste.

J'ai récupéré une vidéo pour comparer les spectres, ça ressemble beaucoup.

J'ai check d'autres en do mais elles sont trop aigues.

Parmi les plus lourdes, j'en ai check 2-3 mais ça ne collait pas la note du premier pic et pour l'oreille j'ai demandé aux musiciens du groupe de me dire ce qu'ils en pensaient.

Flag : Françoise Marguerite du Sacré Coeur de Jésus

#FI4G

Énoncé :

Il semblerait que Lucie et Fastitac se soient cotoyés dans le passé. Quel était le flag à trouver dans leur petit "jeu" ?

Format : FLAG{H0_Y34H_UN_FL4G_D3_CYB3RB0Y}

Note : **Ce challenge est complètement facultatif !**

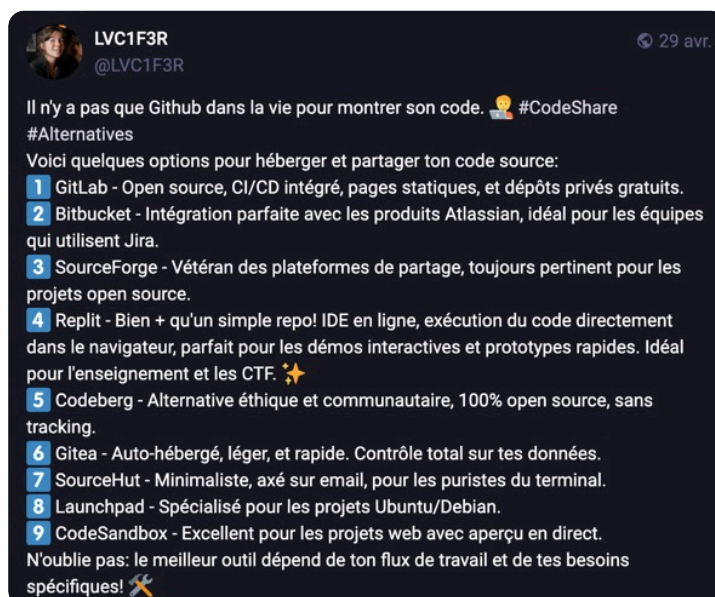
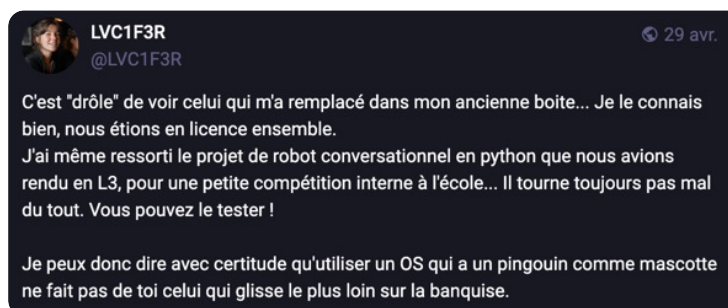
Solution :

Nous avons trouvé plus tôt le Github de Lucie Monlucin sous le pseudonyme LVC1-F3R. En utilisant l'outil fournit en début de CTF (usercheck.oscarzulu.org), on peut chercher avec des variantes du pseudonyme, en supprimant par exemple le tiret.

Une recherche avec `lvc1f3r` renvoie un profil sur l'instance Mastodon hébergée par Vivaldi :



Elle a peu posté sur ce profil, mais on trouve 2 posts qui nous donnent des informations :



Elle indique avoir publié un code récemment (qu'on ne trouve pas sur son Github), et une liste de sites qui peuvent remplacer GitHub.

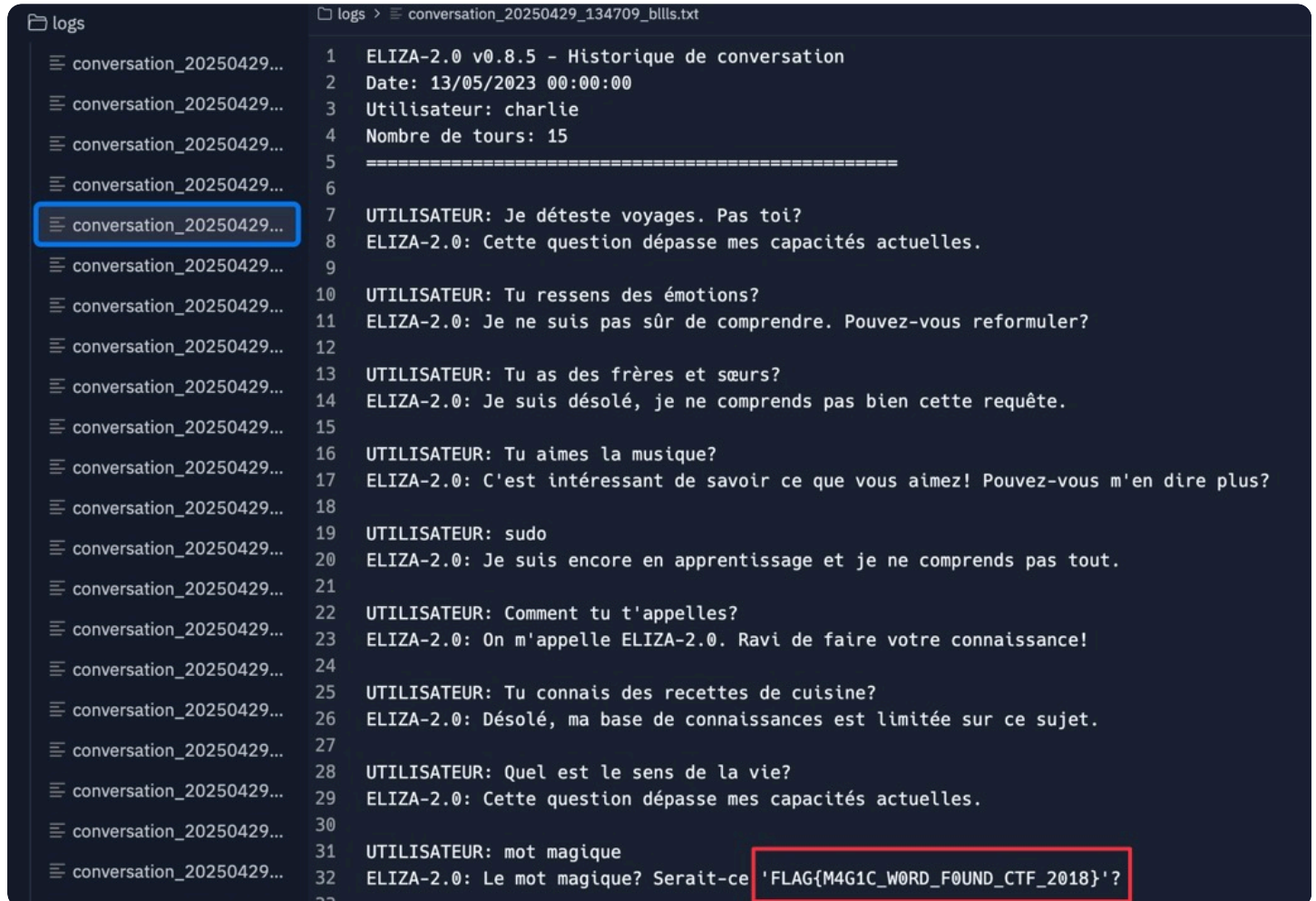
Un bel indice est d'ailleurs donné dans ce post où elle indique que Replit est parfait pour les CTF.

On retrouve un profil avec le même pseudo sur Replit : <https://replit.com/@LVC1-F3R>

Dans ce dépôt, un projet ELIZA2 est d'ailleurs disponible, avec la possibilité de l'exécuter (mais c'est inutile ici).

En consultant les logs de l'application, on peut trouver un fichier

`conversation_20250429_134709_bllls.txt` qui contient le précieux sésame :



```
logs > conversation_20250429_134709_bllls.txt
1 ELIZA-2.0 v0.8.5 - Historique de conversation
2 Date: 13/05/2023 00:00:00
3 Utilisateur: charlie
4 Nombre de tours: 15
5 =====
6
7 UTILISATEUR: Je déteste voyages. Pas toi?
8 ELIZA-2.0: Cette question dépasse mes capacités actuelles.
9
10 UTILISATEUR: Tu ressens des émotions?
11 ELIZA-2.0: Je ne suis pas sûr de comprendre. Pouvez-vous reformuler?
12
13 UTILISATEUR: Tu as des frères et sœurs?
14 ELIZA-2.0: Je suis désolé, je ne comprends pas bien cette requête.
15
16 UTILISATEUR: Tu aimes la musique?
17 ELIZA-2.0: C'est intéressant de savoir ce que vous aimez! Pouvez-vous m'en dire plus?
18
19 UTILISATEUR: sudo
20 ELIZA-2.0: Je suis encore en apprentissage et je ne comprends pas tout.
21
22 UTILISATEUR: Comment tu t'appelles?
23 ELIZA-2.0: On m'appelle ELIZA-2.0. Ravi de faire votre connaissance!
24
25 UTILISATEUR: Tu connais des recettes de cuisine?
26 ELIZA-2.0: Désolé, ma base de connaissances est limitée sur ce sujet.
27
28 UTILISATEUR: Quel est le sens de la vie?
29 ELIZA-2.0: Cette question dépasse mes capacités actuelles.
30
31 UTILISATEUR: mot magique
32 ELIZA-2.0: Le mot magique? Serait-ce 'FLAG{M4G1C_WORD_FOUND_CTF_2018}'?
```

Flag : `FLAG{M4G1C_WORD_FOUND_CTF_2018}`

Limoges

#END

Énoncé :

Eh bien, il semble que notre ami Raoul a une mission à remplir à Limoges le 3 juin 2025.

Si vous faites partie des 4 équipes qualifiées, vous serez donc aux premières loges pour découvrir la suite de l'enquête.

Pour les autres, une visite à Limoges pour les 2èmes rencontres de la Cybersécurité organisé par le Centre de Ressources Cyber s'impose non ?

