

# Les épreuves de Passe ton hack d'abord 2024

## Epreuves Introduction

### Bienvenue (10 pts)

#### Description

Ce challenge permet à l'étudiant de "flagger" son premier challenge en comprenant le but et le format à rechercher.

Voici le flag à rentrer dans la barre de réponse: **FLAG{W3IC0m30nB04rD}**

### Ceux qui respectent le règlement

#### Description

C'est super important de lire le règlement !

### Ave César (10 pts)

**Description** Un message a été transmis entre les romains. Un bon gaulois se doit de le déchiffrer.

Voici le message: IODJ{YHqLYlgLYLf}

### Moby-Dick (50 pts)

**Description** Ce challenge repose sur la communication en morse.

Un animal veut vous parler:

... - . . . - . . . . / . . . . . / - - . . . . . / - . . . / . . . . . / . . . . . - . . . / - - . . / - . . . . . . . . / - . . . / . . . . . . . . / . . . . . - . . . . .

### Mot de passe - Partie 1 (25 pts)

#### Description

Bienvenue, Agent de la Sécurité Numérique !

Vous avez été mandaté pour enquêter sur la **robustesse du mot de passe** qui protège nos données précieuses.

Votre mission: déterminer si le mot de passe actuel est suffisamment fort pour garantir la sécurité de nos trésors numériques.

Voici l'url de notre site: [Coffre Fort Numérique](#)

Astuce: il semble que ce mot de passe soit dans la **liste des mots de passe les plus utilisés en France en 2022**

### Protégez la fusée blanche (50 pts)

#### Description

Votre ami est sur le point de partager la première photo de sa nouvelle acquisition, la "Fusée Blanche", sur les réseaux sociaux. Cependant, il veut **s'assurer que personne ne puisse localiser son appartement**, craignant le vol de son précieux vélo. Il est particulièrement ravi de pouvoir tester la "Fusée Blanche" dans le *vélodrome* situé juste en dessous de chez lui.

Votre ami est conscient que les appareils photo numériques enregistrent souvent des informations dans les métadonnées des images, telles que la date, l'heure, les coordonnées GPS, le modèle de l'appareil, et même parfois le nom du photographe. Il craint que des données sensibles soient involontairement incluses dans ces métadonnées, ce qui pourrait compromettre la sécurité de son fidèle destrier.



## Epreuves Web

### Transformers (50 pts)

#### Description

Un confident au sein des cercles énigmatiques de l'Association Française Anti-Robot (AFAR) vous transmet en secret des murmures inquiétants : le sanctuaire numérique de l'organisation est actuellement plongé dans l'ombre de la maintenance. Son appel à l'aide résonne comme une invocation, sollicitant vos compétences d'investigateur averti pour veiller sur la renaissance digitale en cours, en particulier contre les assauts furtifs des robots, considérés comme des ennemis jurés dans cette guerre invisible. Vous êtes également convié à scruter les recoins numériques pour déceler tout effet de bord énigmatique pendant cette période nébuleuse.

Votre confident laisse entendre que l'AFAR a déployé une mystérieuse mécanique, pour verrouiller l'accès aux robots sur leur précieux site. En tant qu'investigateur vêtu d'ombre et de secrets, votre mission consiste à percer les voiles numériques, à explorer les méandres des codes cryptiques, et à assurer la protection sacrée du sanctuaire virtuel de l'AFAR.

Le site de l'AFAR est disponible [ici](#). Format du flag: **FLAG{ }**

### C'est à qui (150 pts)

#### Description

Un nouveau service en ligne, MesBilletsDAvion, permet de stocker et centraliser les billets d'avion pour faciliter la présentation aux aéroports.

Il s'agit d'une application en accès bêta conçu par votre ami Rémi Droit, développeur web, pour le compte d'une compagnie aérienne. Rémi a activement participé au développement du produit en tant que responsable technique de la solution. Il insiste sur le fait que celle-ci est totalement sécurisée et ce malgré quelques fonctionnalités manquantes.

Après une conversation avec lui, il vous dit:

"Je suis sûr que mon appli est bien conçue! Pour te le prouver, je t'autorise à auditer le service. J'ai renseigné mon billet d'avion pour Londres à l'intérieur. Si tu arrives à scanner mon billet d'avion à ma place, je serais surpris! Je suis convaincu que tu n'y arriveras pas!"

Montrez-lui que son application n'est pas sécurisé. Il vous a donné un contrat permettant de tester la sécurité de l'application.

Le contrat contenait un compte utilisateur à utiliser pour effectuer les tests de sécurité:

Utilisateur: **betatest**

Mot de passe: **LeMotDePasseDuCompteDeBetaTest@2024!**

Lien vers le site de gestion de billets d'avions: [MesBilletsDavion](#)

## Epreuves Programmation

### PX92 ou TI-83 ? (100 pts)

#### Description

Un service nous demande d'évaluer des expressions mathématiques mais le temps à l'air limité.

Afin de communiquer avec lui, vous devrez établir une connexion à l'adresse **37.59.31.202** sur le port **2000**, en utilisant par exemple le module socket du langage de programmation Python.

Votre mission, si vous l'acceptez, consiste à envoyer par cette connexion, dans le temps imparti, les résultats des 100 calculs qui vous seront successivement soumis. Réussissez cette épreuve pour continuer à lui parler.

Connectez vous au serveur et sélectionnez "1" dans le menu des challenges.

## Epreuves OSINT

### Trouvez l'agent - Partie 1 (100 pts)

#### Description

Cher agent,

Vous êtes sur le point de vous embarquer dans une **mission secrète** des plus insolites. Un mystérieux agent secret vous a donné rendez-vous dans un parc pour vous confier une mission capitale. Cependant, il aime jouer avec **les énigmes**, et pour vous guider jusqu'à ce lieu de rendez-vous, il a envoyé une photo du parc.

Le parc en question est un endroit que seuls les initiés peuvent identifier. Votre mission, si vous l'acceptez, est de **déchiffrer les indices cachés dans cette image** pour trouver le parc. Soyez prêt à répondre à l'ultime question : **"Où se trouve ce lieu de rendez-vous secret ?"**

La réponse est le **nom du parc** dans sa langue d'origine, en minuscules, sans accents et sans espaces.

Bonne chance, cher agent !



## Epreuves Reverse

### Git quoi ? (150 pts)

#### Description

Un employé de l'entreprise **SecureNet Guardians** est soupçonné d'avoir transféré des données sensibles vers le darkweb sous le pseudonyme **DarkW1zard**. Bien que nous ayons identifié son alias, aucune trace des données exfiltrées n'a été repérée.

Nous avons découvert un logiciel suspect sur l'ordinateur du suspect, mais son accès reste verrouillé. Votre expertise en **Python** et en **cryptographie** est cruciale dans ce contexte.

Nos premières investigations nous ont remonté qu'il est très actif dans l'open source, et notamment sur **github**.

Votre mission consiste à déchiffrer le contenu du fichier **flag.notes**.

Format du flag: FLAG{L33t\_C0de}

## Epreuves Forensique

### À la Poursuite du Virus Maudit (150 pts)

#### Description

Jacques LaFuite, l'expert en voitures de sport, s'est retrouvé dans une situation délicate en matière de cyber. Il a malencontreusement infecté tous les ordinateurs de ses amis Alain et Michael avec un code malveillant. Apparemment, sa passion pour les moteurs ne se traduit pas en compétences informatiques !

Vous êtes appelé à la rescousse pour débusquer ce code malveillant et créer un antidote salvateur. Votre mission consiste à localiser la source d'infection sur la clé USB **USBKey.vhd** et à analyser les traces du processus sur le PC Windows de Jacques via le fichier **Process-PCJacques.PML**.

Bonne chance, cher détective !

## Epreuves Réseau

### Opération Sécurité E-clair (150 pts)

#### Description

Bienvenue, Détective,

**ShoppingCompany** a besoin de votre flair pour renforcer sa sécurité en ligne! Dans le cadre de cette mission confidentielle, l'entreprise a volontairement mis à votre disposition une capture réseau pour que vous puissiez identifier les failles de sécurité.

Votre mission, si vous l'acceptez (et nous sommes convaincus que vous le ferez), consiste à explorer les échanges d'e-mails au sein du réseau de ShoppingCompany. Concentrez-vous sur l'identification des problèmes de sécurité dans le **système de messagerie**.

Il vous faudra chercher des anomalies ou toute activité qui pourrait compromettre la confidentialité et l'intégrité des communications de l'entreprise. Vous pourrez vous aider d'un outil fort pratique permettant de faire de l'analyse réseau: **Wireshark**

ShoppingCompany compte sur vous pour résoudre ce défi de manière astucieuse et créative. Montrez-nous que vous avez le talent de détective nécessaire pour renforcer leur **sécurité en ligne** !

Voici le lien pour télécharger la capture réseau: [securite-eclair.pcap](#)

Bonne chance dans votre quête de preuves !

From:

/ - Les cours du BTS SIO

Permanent link:

[/doku.php/hack/passtonhackdabord/epreuvespthd2024?rev=1706439283](#)

Last update: 2024/01/28 11:54

