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{W3lC0m3*0n*B04rD}**

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{YHqL*YlgL*YLfl}

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**

Mots de passe - Partie 2 (25 pts)

Description Agent de la Sécurité Numérique !

Grâce a votre travail, la sécurité du site à été accrue. En effet, à la place d'utiliser un mot de passe trop évident pour tout le monde, les utilisateurs doivent maintenant se connecter avec des comptes personnels.

Cependant, nous avons découvert que certaines personnes utilisent des informations personnelles trop évidentes comme mot de passe, ce qui expose nos données à des risques potentiels.

Voici les informations publiés sur les réseaux sociaux d'une employée suspectée d'utiliser un mot de passe trop faible.

- Nom: **Doherty**
- Prénom: **Alice**
- Email: **alice.doherty@exemple.fr**
- Animal de Compagnie: un chat, appelé **Moustache**
- Date d'Anniversaire: **10/05/2001**
- Couleur Préférée: **Bleu**
- Ville: **Bordeaux**

Votre mission : déterminer si les comptes utilisateurs actuels sont suffisants pour garantir la sécurité de nos trésors numériques.

Voici l'url de notre coffre-fort numérique: Coffre Fort Numérique

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

Une fuite inattendue - Partie 1 (150 pts)

Description
Votre ami a été victime d'une **fuite de données** inattendue qui a secoué le monde de la location de voitures.

Les **informations confidentielles des clients**, y compris leurs itinéraires de conduite prévus et leurs données personnelles, sont maintenant exposées au grand jour.

La situation est critique, et pour résoudre ce mystère, votre ami a pris la décision d'installer en urgence une instance de préproduction de son application afin que vous puissiez effectuer des tests de sécurité dessus.

Votre mission revêt un caractère d'urgence crucial : devenir le **“détective des données”** et plonger dans les méandres de l'application pour identifier les vulnérabilités potentielles qui ont conduit à **cette fuite de données**.

Le sort de l'entreprise de location de voitures et la confidentialité de milliers de clients dépendent de vos compétences en matière de sécurité. Gardez donc votre chapeau de détective à portée de main, car il vous faudra résoudre ce mystère sans tarder et assurer la protection des données clients avant que des dommages irréparables ne surviennent !

Votre ami est allé voir le développeur de cette application, qui vous a transmis les informations suivantes:

- Le site est développé en **NodeJS**
- La base de données utilisée est **MongoDB**

Peut-être qu'en cherchant avec ces indices sur internet vous trouverez le moyen de vous **connecter sur le site de location de voiture…**

Lien vers le site de location de voitures: Location de voitures

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 language 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.

Réédition polonaise (150 pts)

Description

Quelle puissance de calcul! Seul problème, le serveur se met soudainement à parler polonais.

Dans la même logique, répondez à **100** expressions, toujours dans un temps imparti.

À chaque étape, une suite de chaînes de caractères vous est envoyée avec les règles suivantes :

- x y renvoie x + y
- x y renvoie x - y
- x y renvoie x * y

Par exemple, la chaine de caractères **+ - 8 7 6** se lit + (- 8 7) 6. Comme - 8 7 vaut 8 - 7 = 1, l'expression finale vaut + 1 6 soit 1 + 6 = 7.

Connectez vous au même serveur **37.59.31.202** sur le port **2000** et selectionnez le challenge “2” dans le menu des challenges.

Ouverture fermeture (200 pts)

Description
Une épreuve finale de programmation vous est proposée. Vous devez évaluer la validité de **25** chaînes de parenthèses générées de manière aléatoire. Veuillez répondre par “True” si les parenthèses sont équilibrées et par “False” dans le cas contraire.

L'expression sera considérée comme valide si chaque crochet ouvert est correctement fermé avant la fin de la chaîne de caractères.

```
{()[]} est valide.
{[])(} est invalide.
```

Connectez vous au même serveur **37.59.31.202** sur le port **2000** et sélectionnez le challenge “3” 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**.

usbkey.vhd.zip
process-pcjacques.pml.zip

Bonne chance, cher détéctive !

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

securite-eclair.pcap.zip

Bonne chance dans votre quête de preuves !

Epreuves Cryptograpphie

Une histoire de colosse - Partie 1 (150 pts)

Description
La cible de votre mission se trouve devant vous: une vieille batisse de l'époque Victorienne, au sud de Londres.

Votre enquête vous mène à l'intérieur du bâtiment; Vous avez reçu l'ordre de récupérer les effets personnels d'un ancien officer anglais, qui aurait gardé des documents de l'armée chez lui.

Vous ne trouvez rien de très interessant dans un premier temps, les pièces principales et le grenier semblent calmes et rangées.

Un détail cependant vous marque: un coffre en bois, un peu en retrait, semble fermé par un cadenas. Vous réussissez à l'ouvrir avec un peu de mal en forçant.

Surprise! A l'intérieur se trouve une pochette contenant des documents... Assez étrange. Une suite de chiffres et de lettres sans vraiment de sens.

Vous décidez d'en prendre une pour analyse, avec ce qui semble être une documentation pour déchiffrer le contenu.

Voici les documents récupérés:

NOTES.pdf

et **P**

HOTOCOPIE.pdf

Peut-être que ce code secret cache des informations sur les documents que vous cherchez ?

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/hack/passtonhackdabord/epreuvespthd2024?rev=1706519053

Last update: **2024/01/29 10:04**