



Les CTFs de Cyrhades

version 2

« Un hacker, c'est quelqu'un de créatif qui réalise des choses merveilleuses. »
Tim Berners-Lee



Développé par
CYRIL LECOMTE

TABLE DES MATIÈRES

03	Présentation	08	Interface – Les CTFs
04	Configuration requise	11	Prochaines évolutions
05	Votre email	12	Remerciements
06	Interface – Le menu		



PRÉSENTATION

Parce que la sécurité de demain se construit aujourd'hui.

J'ai conçu une application dans le but de former et d'entraîner les personnes intéressées par le domaine de la cybersécurité. Avec cette application, vous pouvez déployer facilement des challenges de cybersécurité, offrant une expérience d'apprentissage pratique et immersive.

Qu'il s'agisse d'étudiants, de professionnels en reconversion ou de passionnés de sécurité informatique, "Les CTFS de Cyrhades" offre une approche pratique pour acquérir des compétences essentielles en cybersécurité. Vous devrez relever des défis concrets et résoudre des problèmes de sécurité réels où l'objectif est de récupérer un flag.

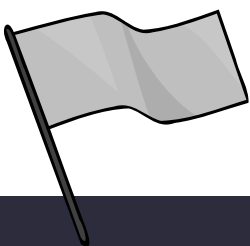
La majorité des challenges sont des environnements Docker, fournissant des scénarios réalistes de cyberattaques et de vulnérabilités. Vous pourrez exploiter ces failles et mettre en pratique les techniques des hackers.

Je propose une variété de challenges de différents niveaux de difficulté, allant des concepts de base aux cas les plus complexes.

Vous pourrez dans certains cas utiliser des plateformes d'apprentissage interactif et stimulant, favorisant et facilitant l'expérience des CTFS.

Fichier Outils Affichage Plateformes Aide						
Cryptanalyse Forensic Osint Programmation Stéganographie Web client Web serveur						
	ID	Nom	Auteur	Techno	Diffi...	Description
	1	Injection de fichier et gestionnaire de Flux FTP	Cyrhades	PHP	3	La faille LFI et RFI pousser jusqu'à l'utilisation d'un gestionnaire...
	2	Session Faible	Cyrhades	PHP	1	Attention à la gestion des id de session !
	3	Directory Traversal (Navigation dans les répertoires)	Cyrhades	NodeJS	2	On peut aller là où l'on devrait pas pouvoir aller.
	4	Faible Doctype PUG Zéro Day	Cyrhades	NodeJS PUG	3	Faible déclarée mais ignorée sur PUG
	5	Insecure Direct Object Reference et Magic Hash	Cyrhades	PHP	2	Insecure Direct Object Reference et Magic Hash en 1 CTF
	9	Affaires classées	Cyrhades	-	1	Le timestamp, c'est pas pour toute la vie en 32bits
	16	Conversation serialisée	Cyrhades	PHP	4	Ne vous laissez pas distraire par la discussion
	17	La fonction assert de PHP	Cyrhades	PHP	2	Assert à pas grand chose cette sécurité
	18	Désérialisation de cookie et Loose comparaison	Cyrhades	PHP	2	Devenez admin en émettant le cookie

Les plateformes sont associées à des centres de formations ou écoles en cybersécurité, vous devrez être éligible pour en profiter.



CONFIGURATION REQUISE

L'application "**Les CTFS de Cyrhades**"
est compatible avec les systèmes d'exploitation Windows, Mac et Linux



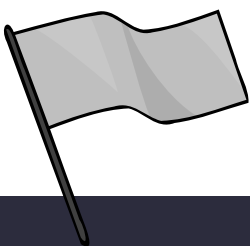
L'application "Les CTFS de Cyrhades" a été écrite en java, dans le but de la rendre multiplateforme. Il vous faudra donc Java d'installé sur votre système pour pouvoir en profiter.



La majorité des challenges nécessitent Docker, vous devrez donc avoir Docker d'installé pour pouvoir profiter de ceci.



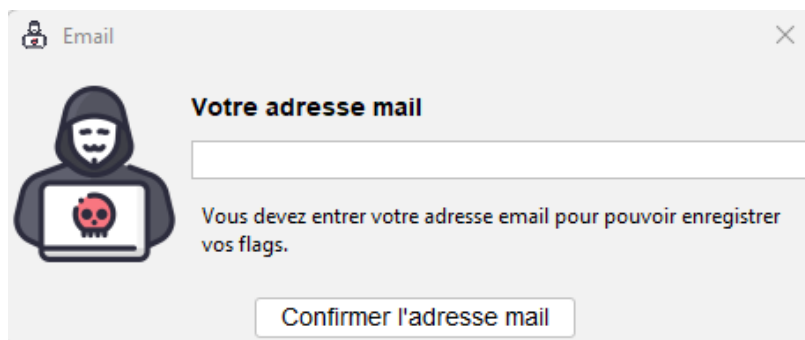
Un outil facultatif peut être utile pour les formateurs, il s'agit de Ngrok, qui permet de créer un tunnel TCP sur votre système, grâce à celui-ci vous pourrez donner accès aux étudiants qui n'ont pas la possibilité d'installer Docker.



VOTRE EMAIL

Votre adresse mail vous sera demandée au démarrage de l'application, elle est indispensable pour valider les flags. Elle n'est jamais transmise ni même utilisée pour une autre raison. Elle sert de clé de "sécurité" pour les flags, afin que les flags validés ne puissent pas être partagés entre étudiants.

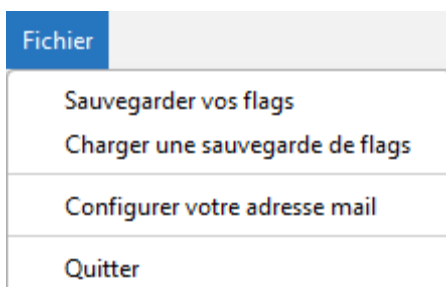
Cela est une sécurité pour éviter le partage de flags. **Rien d'autre !**



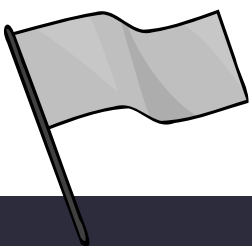
Tant que vous n'aurez pas enregistré une adresse email, la fenêtre de dialogue s'ouvrira à chaque démarrage de l'application.



De même si vous tentez de valider un flag, la fenêtre de dialogue vous demandera votre email et il vous sera impossible de saisir un flag tant que vous n'aurez pas indiqué votre email.

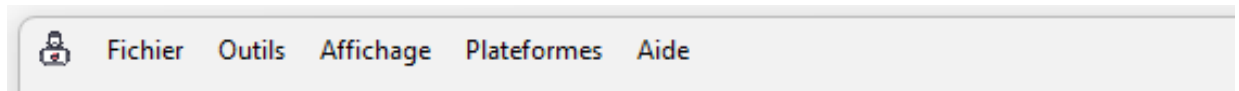


Dans le menu Fichier, vous trouverez un menu "Configurer votre adresse mail" (visible uniquement si l'adresse n'a pas été renseignée).

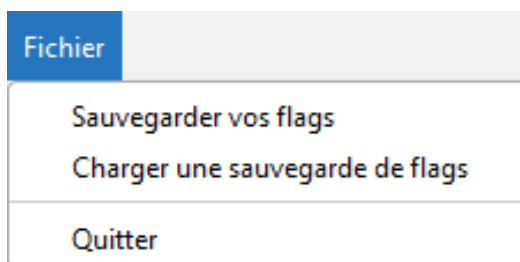


INTERFACE - LE MENU

Menu



Fichier

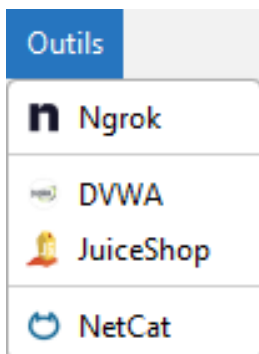


Dans le menu fichier, vous pouvez "Sauvegarder vos flags" et "Charger une sauvegarde de flags". Cela peut vous permettre de récupérer vos flags validés sur un autre système ou sur une nouvelle installation.

Vous pouvez également "quitter" l'application.

Dans le menu fichier, le menu "Configurer votre adresse mail" est visible tant que vous n'avez pas renseigné votre adresse mail.

Outils



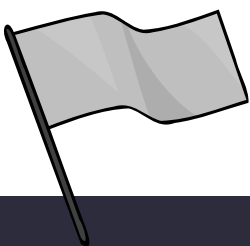
Dans le menu Outils, vous trouverez différents outils, c'est l'un des menus qui est voué à évoluer au fur et à mesure des versions.

Actuellement les outils disponibles sont :

Ngrok, permettant de créer un tunnel TCP sur la machine hôte DVWA qui est un container Docker contenant l'application WEB écrite en PHP, permettant de découvrir pour les débutants diverses failles de sécurité WEB.

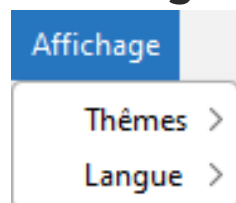
JuiceShop Site E-commerce fictif et vulnérable écrit en NodeJs utile pour pratiquer une analyse OWASP.

Netcat un outil réseau très utile et utile pour pratiquer le reverse Shell.



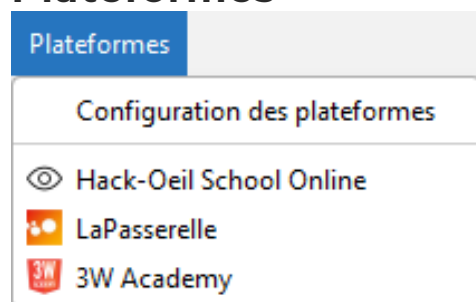
INTERFACE - LE MENU

Affichage



Le menu affichage vous permet de changer le thème de l'application Dark (foncé) ou Light (clair) ainsi que de choisir la langue souhaitée Français ou Anglais. Que ce soit au changement de thème ou de langue, cela sera enregistré, au redémarrage de l'application, vous aurez la même configuration.

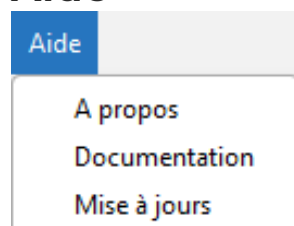
Plateformes



Le menu plate-forme permet d'ajouter et configurer une plate-forme de formation. Ces plateformes sont principalement distribuées par des centres de formations ou des écoles. Elle vous sera communiquée par votre centre de formation, si celui-ci possède une formation dédiée à la cybersécurité. Vous pourrez ensuite cliquer sur le lien de votre plate-forme pour accéder à vos cours.

Vous pouvez prendre contact avec moi si vous souhaitez ajouter votre plateforme.

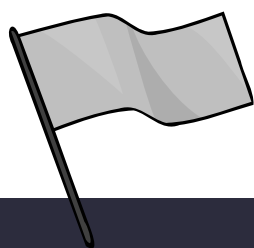
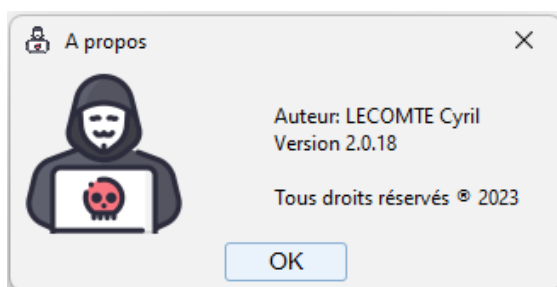
Aide



Le menu Aide, vous permet d'accéder à la partie "A propos" qui vous permettra de connaître le numéro de version actuelle de votre application.

Le sous-menu Mise à jour vous permettra de mettre à jour votre application si une mise à jour existe.

Le sous-menu Documentation vous donne accès à la documentation que vous êtes en train de lire.



INTERFACE - LES CTFS

Les catégories





Cryptanalyse	Forensic	Osint	Programmation	Stéganographie	Web client	Web serveur
--------------	----------	-------	---------------	----------------	------------	-------------



Les CTFS sont listés dans différentes catégories, quand vous vous placez sur une catégorie celle-ci est enregistrée, quand vous redémarrez l'application vous êtes automatiquement placé dans cette catégorie.

La première colonne

La première colonne peut avoir 4 états différents.

Le premier état ne peut exister que si Docker n'est pas installé sur votre système, vous devrez l'installer pour utiliser ces challenges.

	ID	Nom
	1	Injection de fichier et gestionnaire
	2	Session Faible
	3	Directory Traversal (Navigation di
	4	Faible Doctype PUG Zéro Day

	ID	Nom
	1	Injection de fichier et gestionnaire de Flux FTP
	2	Session Faible
	3	Directory Traversal (Navigation dans les répertoires)

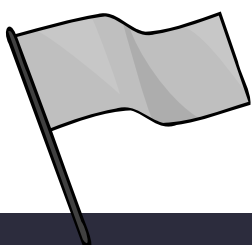
Avant de pouvoir faire un CTF vous devez le télécharger, effectivement afin de ne pas occuper de l'espace de stockage inutilement, aucun CTF n'est présent au téléchargement de l'application.

L'état sans bouton est possible uniquement dans le cas d'un container docker qui n'est pas démarré.

Le bouton de téléchargement








Le bouton de démarrage du CTF



INTERFACE - LES CTFS

L'avant dernière colonne

Description		
La faille LFI et RFI pousser jusqu'à l'utilisation d'un gestionnaire...		
Attention à la gestion des id de session !		
On peut aller là où l'on devrait pas pouvoir aller.		




Le bouton de validation de Flag



Le bouton de validation de Flag, d'un CTF déjà validé

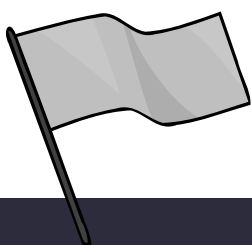
Si vous avez déjà validé un CTF, vous pouvez tout de même le revalider, cela permet principalement aux formateurs de pouvoir faire leur démonstration jusqu'à validation.



Validation de flag






Flag

Valider le Flag



INTERFACE - LES CTFS

La dernière colonne

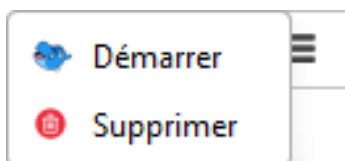
Description		
La faille LFI et RFI pousser jusqu'à l'utilisation d'un gestionnaire...		
Attention à la gestion des id de session !		
On peut aller là où l'on devrait pas pouvoir aller.		



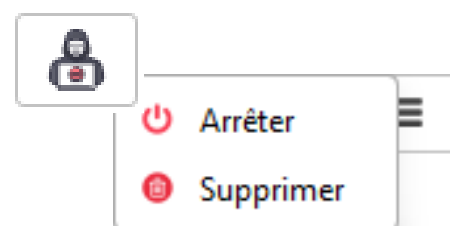
Quand vous téléchargez un CTF nécessitant docker, un nouveau bouton s'affiche en dernière colonne.

Si le CTF n'est pas démarré vous avez un bouton, pour le démarrer, mais si le CTF est démarré vous avez un bouton "Arrêter" cela aura pour effet de supprimer le container Docker du CTF. Vous pouvez également supprimer, ce qui supprimera le container docker et supprimera le CTF de votre système, libérant ainsi l'espace physique.




CTF non démarré

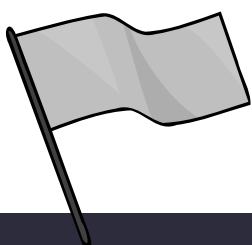


CTF démarré



Certains CTFs ne nécessitent pas docker dans ce cas seul le bouton supprimer s'affiche, après le téléchargement.

Description		
Stéganographie d'image		
Stéganographie d'image		



PROCHAINES ÉVOLUTIONS

Les challenges

Concernant les challenges eux-mêmes Il y aura bien entendu de nouveaux challenges très régulièrement.

Dans une prochaine version les flags des challenges seront différents par utilisateur, ce qui évitera la triche, on ne pourra pas valider un challenge avec le flag d'un autre utilisateur.

L'application

Ajout d'une catégorie de CTF "Divers" permettant d'ajouter des CTFs sans validation de flag, en permettant aux formateurs de paramétrer ces challenges, je possède déjà 2 CTFs qui pourraient entrer dans cette catégorie.

Ajout d'un système d'ajout de plate-forme avec une simple URL.

Ajout d'un moteur de recherche pour chercher les CTFs par mot clé

Ajouter un système de notation des CTFs (nécessite le déploiement en ligne de ma solution de formation).



REMERCIEMENTS

Je tenais à ajouter cette page de remerciements pour exprimer ma gratitude, envers les beta testeurs. Grâce à leurs retours d'expérience et à leurs suggestions, j'ai pu peaufiner les fonctionnalités et optimiser l'expérience utilisateur.

Je tiens tout particulièrement à remercier Matthieu, qui a été le premier à suivre les différentes étapes de développement et à essayer les différents CTFS proposés, malgré le fait que j'ai dû l'ennuyer plus d'une fois ^^.

Je suis également impatient d'accueillir de futurs utilisateurs, et je vous remercie par avance de l'intérêt que vous porterez à mon travail. Vos retours, suggestions et idées m'aideront à continuer à faire évoluer cette application et à offrir un produit qui répondra aux besoins et aux attentes de nos étudiants, formateurs et passionnés de cybersécurité.

Je suis ravi de partager cette application afin d'offrir des formations adaptées, et je m'engage à continuer à vous offrir une application accessible avec toujours plus de challenges.

Encore une fois, merci et amusez-vous !

Cyril LECOMTE

