HACKY' NOV

WRITE-UP

Hacky'Shop – Partie 1

Florian Allione

Hacky'Nov Aix-en-Provence
2022 - 2023

HACKY'NOV

Hacky'Nov est une association créée dans le cadre des YDAYS organisés par l'école YNOV qui organise chaque année un CTF afin d'initier le grand public aux différentes problématiques de cybersécurité.

L'événement est organisé par les étudiants du campus YNOV d'Aix-en-Provence et se décompose en trois parties.

La première partie est l'organisation d'un Capture The Flag (CTF). Chaque étudiant, de bachelor 1 à master 2 propose des challenges de cybersécurité, afin que les participants puissent en résoudre le maximum et gagner la compétition ! Les challenges sont axés de sorte que même les débutants puissent en résoudre un maximum tout en sachant faire plaisir aux plus expérimentés

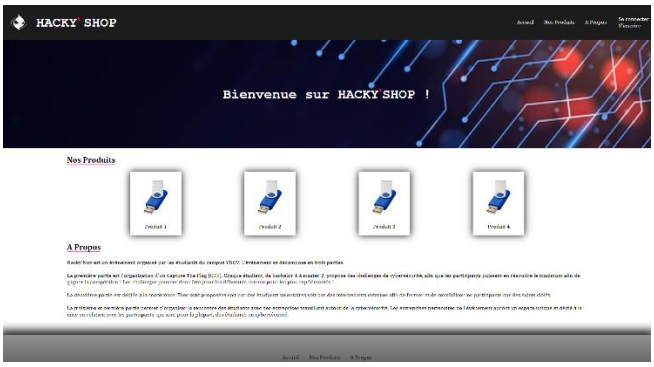
La deuxième partie est dédiée à l'organisation de conférences autour de problématiques et sujets de cybersécurité. Elles sont proposées soit par des étudiants volontaires, soit par des intervenants externes afin de former et de sensibiliser les participants sur des sujets ciblés.

La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants, qui sont pour la plupart, des étudiants en cybersécurité.

https://hackynov.fr/

Table des matières

Partie 1 : Présentation du challenge



Nom du challenge : Hacky'Shop – Partie 1

Domaine : Web

Difficulté : ★★★★★

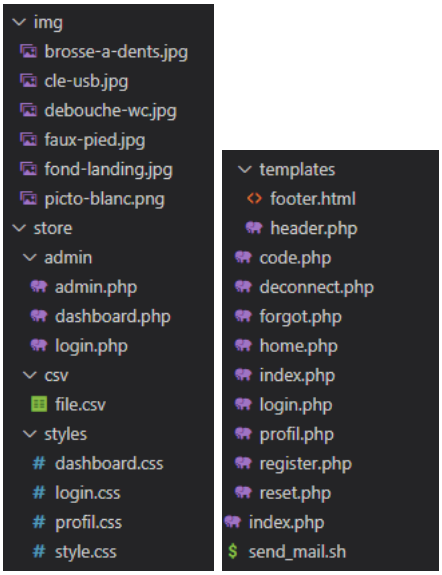
Auteur : Florian Allione

Description : Ton but est simple : Réussir à se connecter au panneau d'administration du site. Ton Flag est le mot de passe du compte administrateur.

(Note : Il est inutile d'utiliser des techniques de bruteforce. Ça ne vous servira à rien)

Partie 2 : Sources

Le challenge comporte les fichiers suivants :



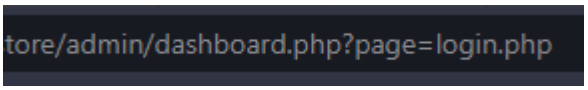
Tous les fichiers du challenge sont disponibles dans le dossier de ce write-up.

Partie 3 : Résolution

Il ne faut pas se précipiter sur le formulaire de connexion classique et d'essayer de se connecter avec le compte démo : c'est une fausse piste qui ne sert à rien dans la partie 1 de ce challenge.

Il faut au contraire bien regarder les pages et remarquer le petit lien dans le <footer> « Panneau d'administration » qui nous redirige sur un formulaire de connexion.

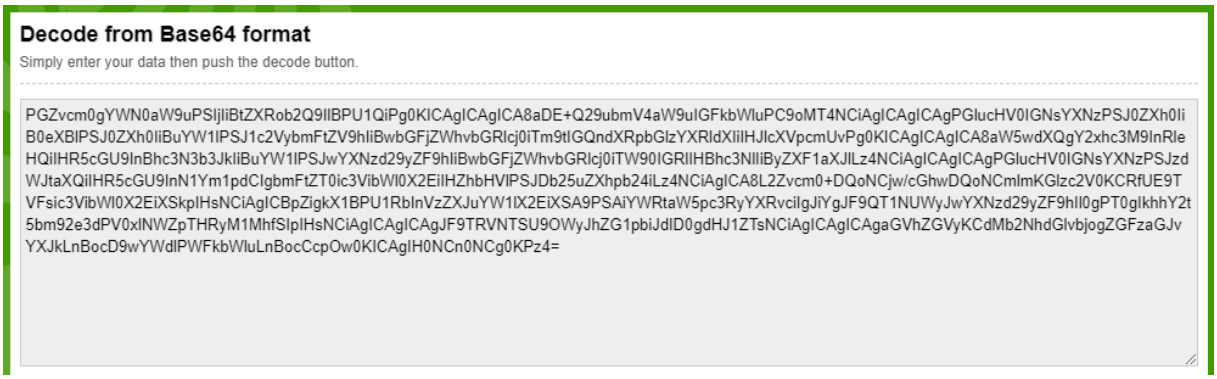
Maintenant que nous avons trouvé ce formulaire, il suffit de regarder notre URL pour se rendre compte que notre page appel un paramètre « page » qui est égale à « login.php ».

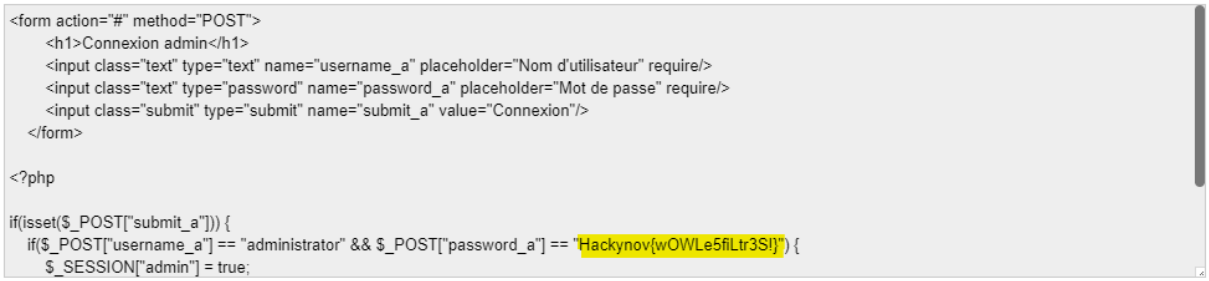


Il faut ici exploiter une faille LFI (Local File Inclusion), et plus particulièrement l'utilisation d'un filtre php pour convertir le code source de la page racine « dashboard.php » en base64.

Cela va nous permettre de voir l'intégralité du code source de notre page web (HTML + PHP).

Pour cela, on copie le code converti en base64 et on le déchiffre pour qu'il soit lisible. J'utilise ici le site https://www.base64decode.org dans l'exemple.





On retrouve alors, en clair, le login et le mot de passe du compte administrateur.

CONNEXION REUSSIE !

Flag : HN0x02{wOWLe5fiLtr3S!}