



WRITE-UP

Hacky'Shop – Partie 2

Florian Allione

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.

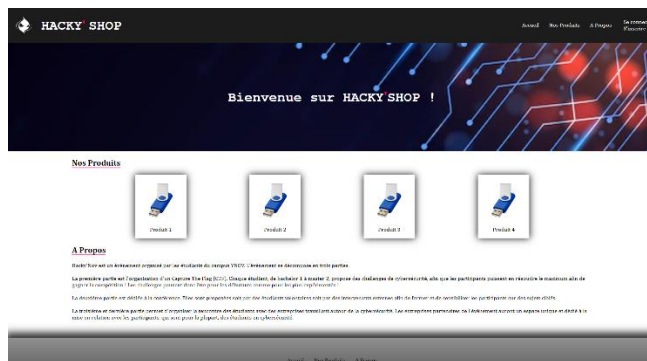
La troisième et dernière partie permet d'organiser la rencontre des étudiants avec des entreprises travaillant autour de la cybersécurité. Les entreprises partenaires de l'événement qui sont en majorité de grands acteurs du domaine, auront un espace unique et dédié à la mise en relation avec les participants,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

<https://hackynov.fr/>

Table des matières

Partie 1 : Présentation du challenge	4
Partie 2 : Sources	4
Partie 3 : Résolution.....	5

Partie 1 : Présentation du challenge



Nom du challenge : Hacky'Shop – Partie 2

Domaine : Web

Difficulté : ★★☆☆☆

Auteur : Florian Allione

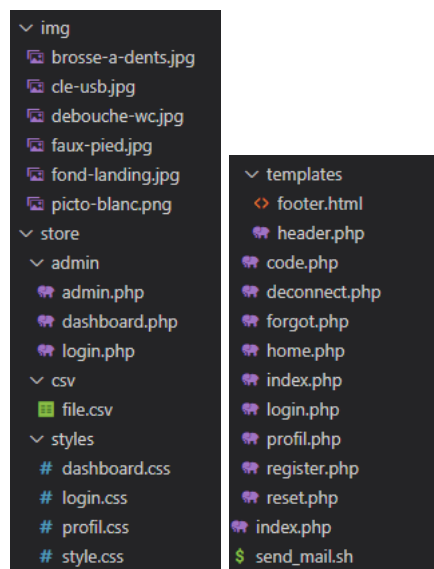
Description : A partir de ce qui a été réalisé dans la **partie 1** : Réussir à se connecter au compte de ta cible et récupérer le "FLAG" sur sa page profil. Ta cible est l'utilisateur ayant

l'ID numéro 6.

(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

Dans la partie 1 de ce challenge, tu as réussi à te connecter au panneau d'administration du site. En y retournant tu vas tomber sur un tableau des utilisateurs du site.

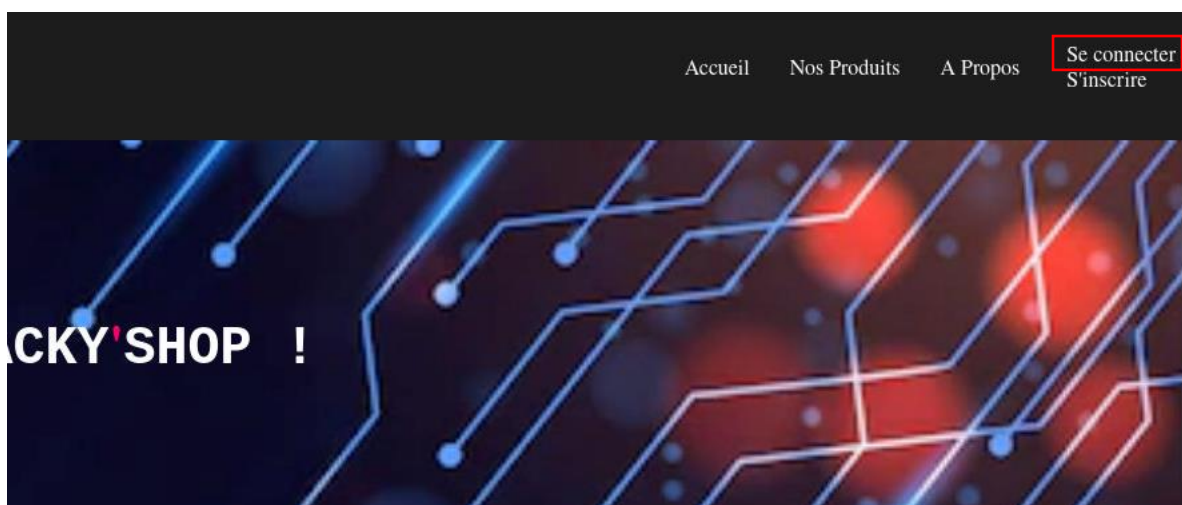
 **HACKY'SHOP - DASHBOARD**

Liste des utilisateurs

ID	Username	Email
1	demo123	compte@demo.hn
2	PierrotleFou	pierre.lepongecarre@patrick.com
3	taz	tazlediable@tazmanic.tz
4	EmmaCaréna	carena.emma@dance.com
5	FlyingSteel	xxflyx@tresor.tv
6	HackyFlag	hacky.patate@trobeau.hn
7	ElTigre	elfamoso@tigre.to
8	HackStone	stone.stone@stone.st
9	FrEagle	laigle@vent.fr

Le but est de se connecter au compte qui a pour ID, 6. On voit ici que l'utilisateur a pour nom d'utilisateur « **HackyFlag** » et pour e-mail « **hacky.patate@trobeau.hn** ». Ces informations sont à noter, elles nous serviront plus tard.

La partie admin ne nous intéresse plus, nous avons récupéré les informations dont nous avons besoin. Il faut maintenant aller sur le formulaire de connexion du site.



Cliquer sur « **Mot de passe oublié ?** » puis rentrer votre adresse mail de votre compte. Si vous n'avez pas créé de compte, créez-en un et revenez à cette étape.

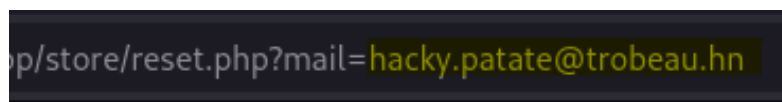


Tu vas ensuite recevoir un mail avec le code de vérification. Il te suffit de le renseigner dans le formulaire et de valider.



On nous propose donc de modifier notre mot de passe. Mais avant de le faire, nous allons faire une petite manipulation afin de changer, non pas notre mot de passe de compte, mais le mot de passe du compte de notre cible.

Dans l'URL, tu peux voir un paramètre « mail » qui est égale à ton email. Nous allons modifier la valeur de ce paramètre par l'adresse de notre cible que nous avons récupéré sur le panneau administrateur. Veille bien un refresh la page une fois que tu as modifié le paramètre, pour qu'il soit bien pris en compte.



A partir de là, tu peux entrer le mot de passe que tu veux et te connecter au compte de ta cible en utilisant la paire « Nom d'utilisateur » (HackyFlag) et le « Nouveau mot de passe ».

Une fois connecté, rendez-vous sur le profil du compte pour récupérer ton Flag !



Flag : HN0x02{r3iNIT*mDP!!0Uf}