WRITE-UP

LeBlog - Web

Dorine MANN

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 : LeBlog

Domaine : Web

Difficulté : ★ ★ ★ ★ ★

Auteur : Dorine Mann

Description : Vous êtes chargé d'enquêter sur la disparition d'une amie perdu de vu depuis plusieurs années.

Celle-ci vous a envoyé un message où elle sollicite votre aide avec un lien vers son blog, mais avant de pouvoir lui demander plus d'informations, vous apprenez qu'elle a disparu.

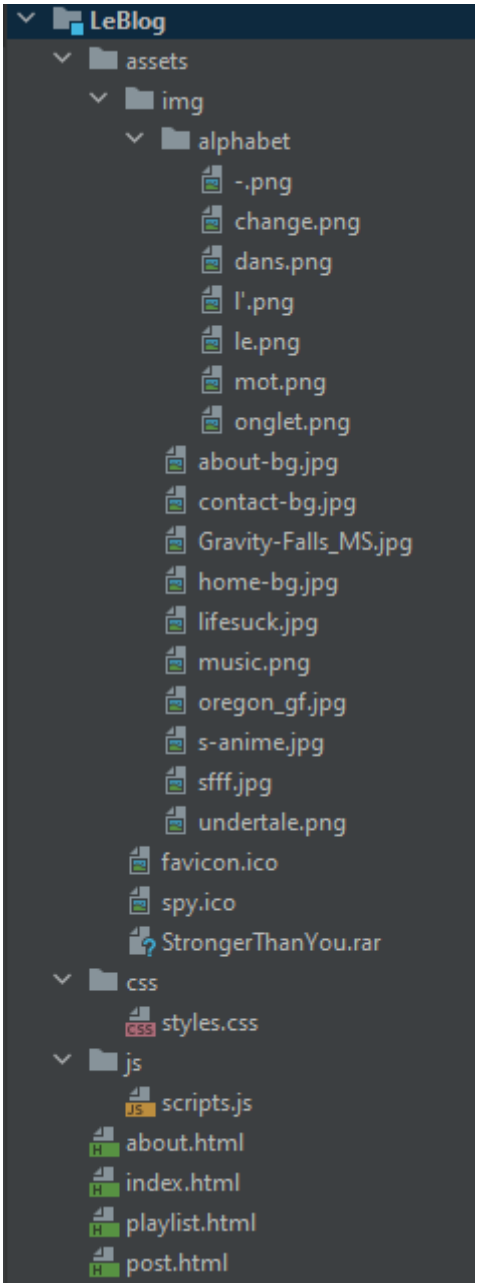
Étant friands d'enquête, vous décidez d'aller sur son site web et de voir si des informations pour la retrouver n'y serait pas caché ? Peut-être trouverez-vous la ville où elle était la dernière fois qu'on l'a vu…

Le site web est un blog, ou la personne disparu raconte certains moments de sa vie personnelle.

ATTENTION : Le flag que vous trouverez sera à remettre en forme HN0x02{flag_trouvé}

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

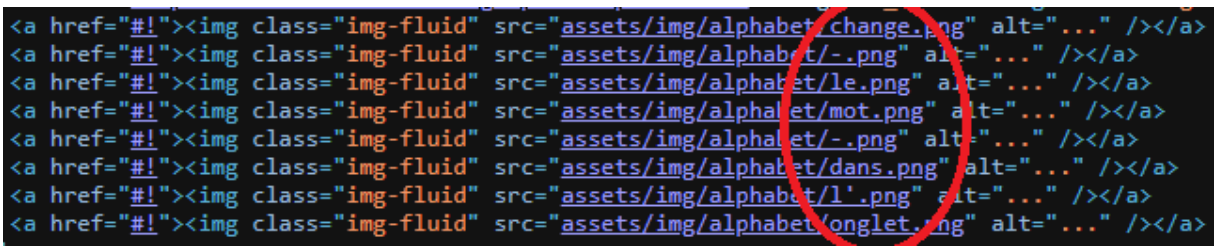
1ère étape :

Sur le blog, on peut observer un article nommé « La découverte d'une série animé ». Grâce à cet article, on va pouvoir commencer à enquêter.

L'image suivante, présente sur l'article, amène sur un site web (https://what3words.com/) qui donne une localisation sur maps avec la combinaison de 3 mots précis. Ce site sera utile plus tard dans le challenge (à l'étage 3).

À la fin de l'article, il y a une série de caractère, qui corresponde à l'alphabet de Gravity Falls (https://www.dcode.fr/gravity-falls-auteur). En déchiffrant ces caractères ont obtient le mot « playlist ».

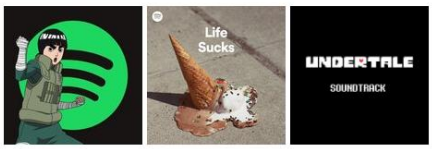
Ensuite, lorsqu'on regarde le code source de la page html, on peut voir un message caché avec les différents noms des caractères de l'alphabet Gravity Falls, qui donne « change le mot dans l'onglet ».



Ce qui amène à vouloir trouver une page html « caché » que l'on trouve grâce au mot « playlist » trouvé précédemment.

Donc dans le lien html de la page, on remplace « post » par « playlist » et la page cachée apparaît.

Un peu tout style de musique que j'écoute



2ème étape :

Une fois sur cette nouvelle page, on peut observer 3 images de playlists.

La 1ère image, amène sur une playlist avec des musiques concernant des animés.

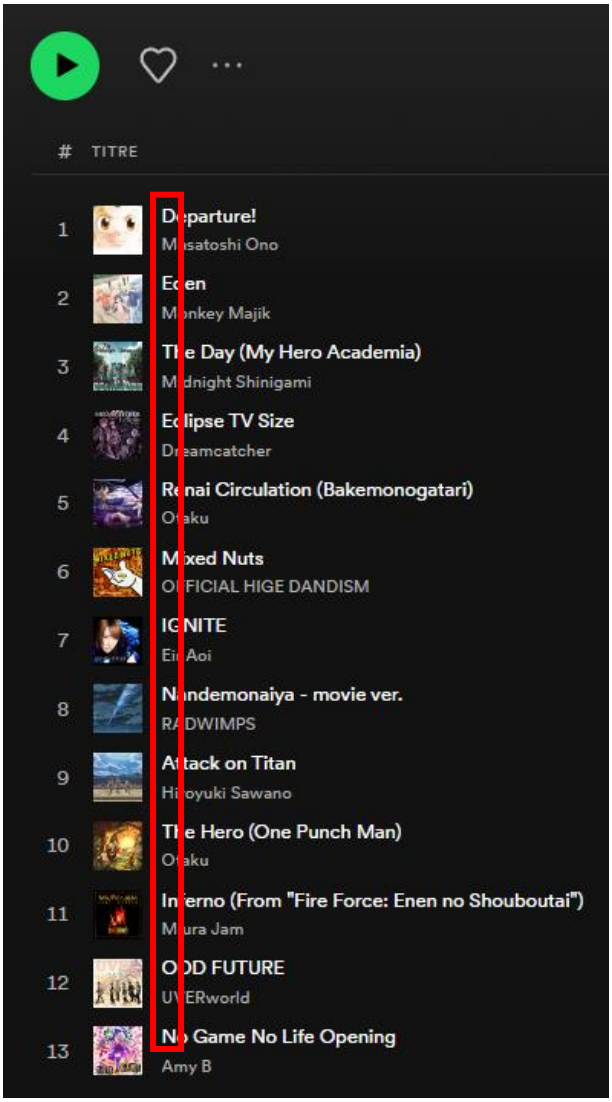
La 2ème image, amène vers une playlist qui ne sera pas utile.

Et la 3ème image permet de télécharger un fichier .rar, nommé « StrongerThanYou.rar ».

Le fichier .rar ne peut pas être ouvert sans mot de passe. Il faut donc trouver le mot de passe.

Celui si est en fait trouvable à travers la 1ère playlist contenant des musiques d'animés.

La playlist ressemble à ceci :

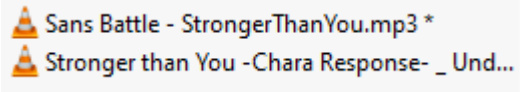


Il faut réussir à trouver un mot caché à travers ces musiques. Et si on prend la 1ère lettre de chaque musique on obtient le mot « DETERMINATION », qui est le mot de passe de notre fichier .rar.

3ème étape :

On peut maintenant ouvrir le fichier « StrongerThanYou.rar » grâce au mot de passe trouvé.

Ce fichier contient 2 musiques.



Dans la musique « Sans Battle – StrongerThanYou.mp3 » est caché une série de 3 mots à travers la chanson. Il faut donc l'écouter, se rendre à 42 secondes et on peut entendre les mots suivants :

- Wins
- Good
- Jobs

Et si on se souvient bien, lors de la 1ère étape on nous a donné un lien qui donne une localisation maps à l'aide de 3 mots.

https://what3words.com/wins.good.jobs

Cette localisation nous permet de trouver la ville « Lancaster », qui est la conclusion du challenge.

Flag : HN0x02{Lancaster}