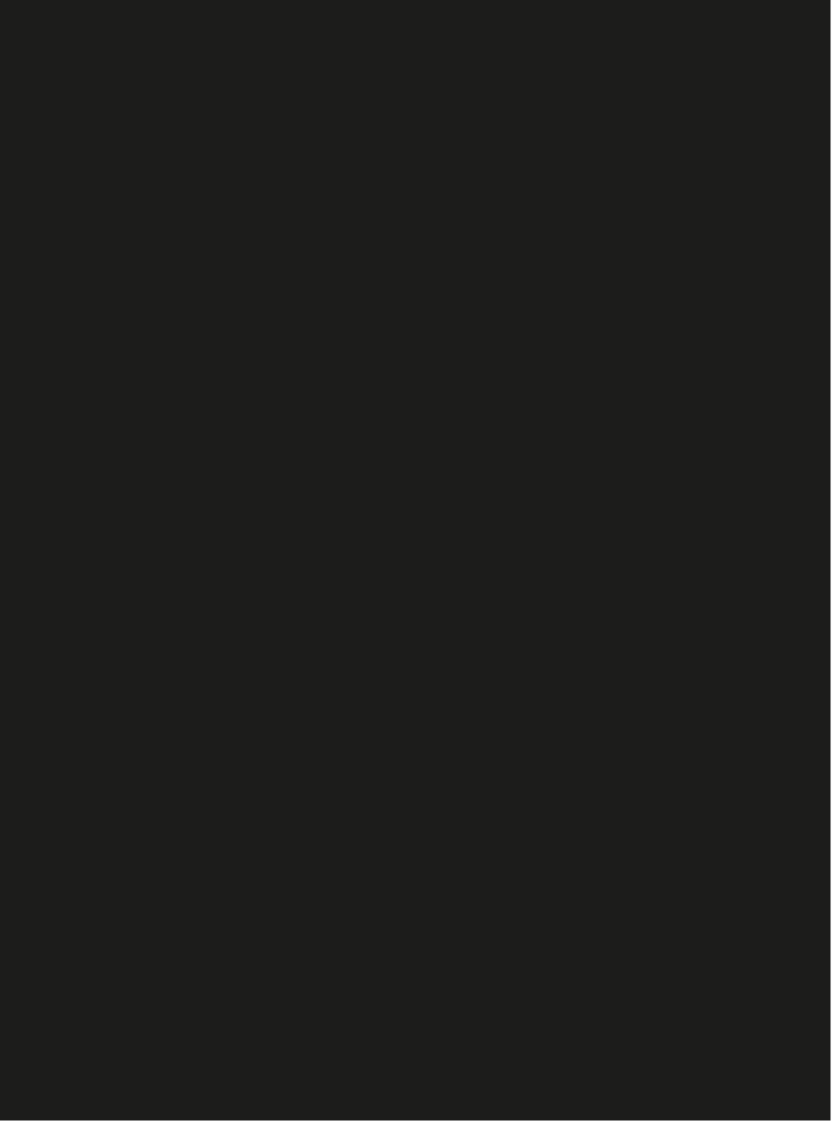
**WRITE-UP   
**

****

Login – Vodka Hacky’nov Aix En Provence

Artur Poetsch 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 ……………………………………………………………………………………………………………………………..

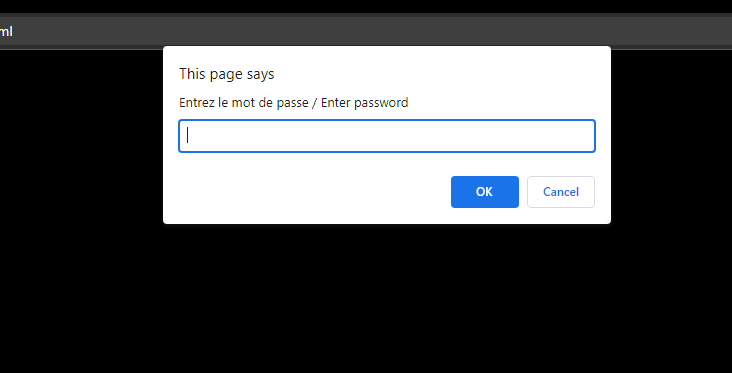
Partie 2 : Sources …………………………………………………………………………………………………………………………………………………………

Partie 3 : Résolution …………………………………………………………………………………………………………………………………………………….

​**​**

Partie 1 : Présentation du challenge

Nom du challenge : Vodka.



Difficulté :Une image contenant enveloppe, carte de visite

Description générée automatiquementUne image contenant stationnaire, enveloppe

Description générée automatiquement Une image contenant stationnaire, enveloppe

Description générée automatiquementUne image contenant stationnaire, enveloppe

Description générée automatiquementUne image contenant stationnaire, enveloppe

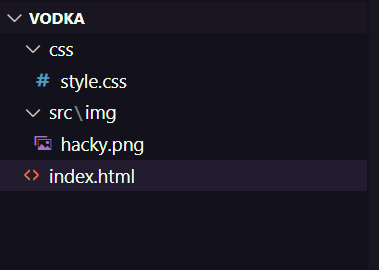
Description générée automatiquement Domaine : Web

Auteur : Artur Poetsch

Description : On arrive sur une alerte nous demandant de rentrer un mot de passe afin de pouvoir nous connecter.

Partie 2 : Sources

Dans le challenge, nous retrouvont les fichiers suivants :

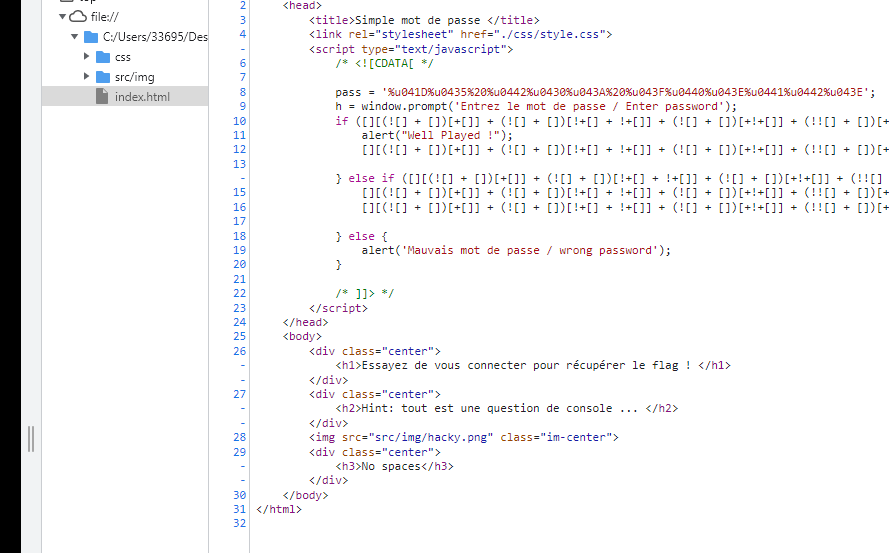


Pour retrouver les fichiers ainsi que le challenge, rendez vous sur le répo du challenge !

Partie 3 : Résolution

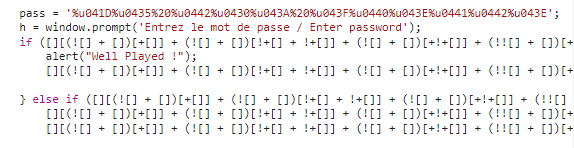
Une fois l’alerte enlevée, nous arrivons sur cette page :



La logique veut que nous inspections la page afin de trouver des informations additionnelles.

Une image contenant flèche

Description générée automatiquement

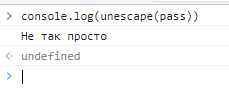


Et en cherchant bien on trouve la variable pass qui contient le flag encodé.

Vu que nous partons d’une injection JS classique, j’ai voulu corser le challenge en rendant la partie script illisible.

En javascript, pour décoder une chaine en héxadécimal, on utilise la fonction unescape(flag). On se rend donc dans la console pour taper « console.log(unescape(pass)) »

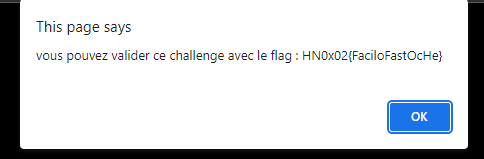
Ce qui nous donne ce résultat :

On récupère ici une chaine de charactères en russe.

Et non, ce n’est pas le flag.

Une fois la phrase traduite, on récupère : « Pas si facile ».

Il suffit ensuite de recharger la page puis de rentrer la phrase SANS espaces (comme le dis l’indice dans le code ) en tant que mot de passe.

Une fois la phrase rentrée, on a désormais accès au flag.

Flag : HN0x02{FaciloFastOcHe}

C’etais bien fastoche !! 😉