



**HACKY'
NOV**

WRITE-UP

Challenge - Web

Alexandre Rocchi

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 : Ctfast



Domaine : Web

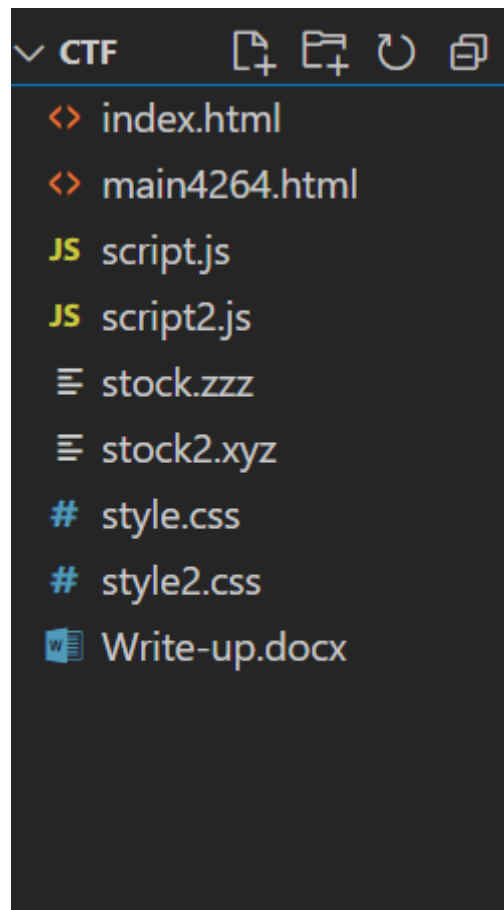
Difficulté :

Auteur : Alexandre Rocchi

Description : Si vous êtes bon en calcul mental et que vous avez une bonne souris, ce challenge n'aura aucun secret pour vous ! Le rendu du flag se fera de la sorte : HN0x02{FLAG} FLAG étant le flag que vous obtiendrait durant ce challenge.

Partie 2 : Sources

Le challenge comporte les fichiers suivants :



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

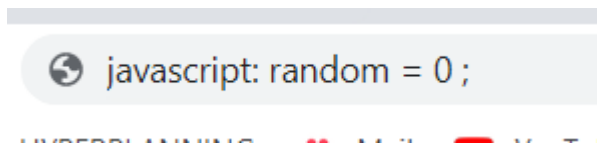
Partie 3 : Résolution

Sur la 1^{ère} page vous arrivez et on vous donne le code !

Malheureusement pour vous le code change en permanence et à moins d'anticiper les calculs ce qui peut s'avérer très long vous aller devoir utiliser JS.

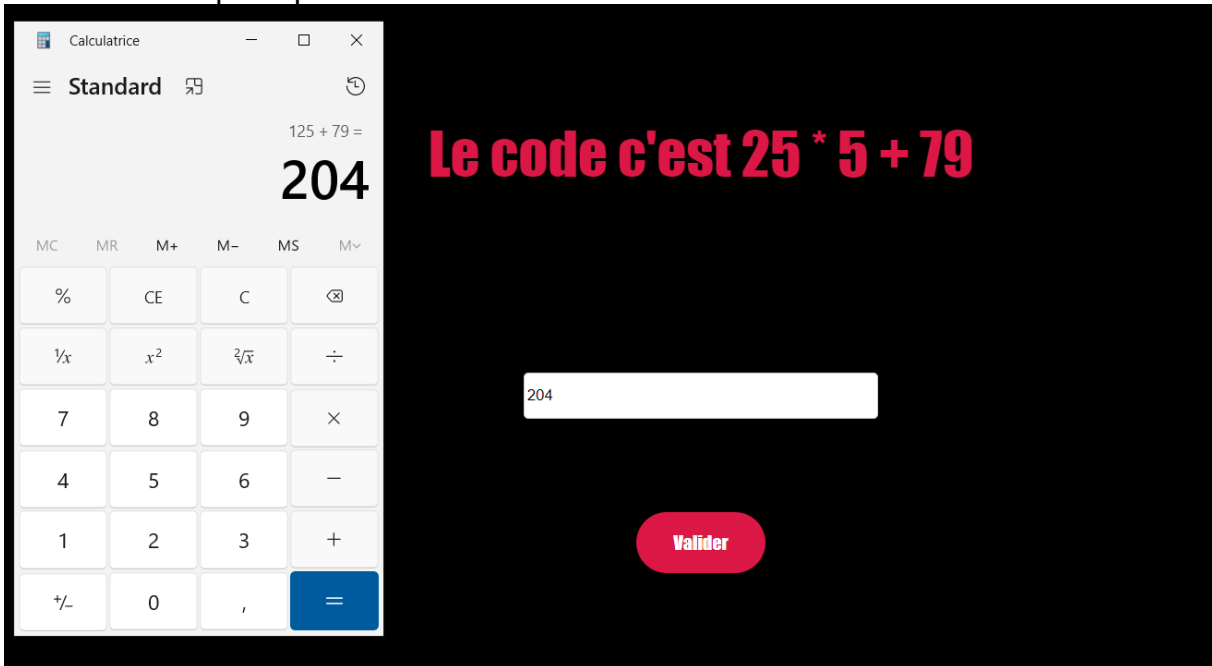
```
index.html  script2.js x
1
2 // Vous pouvez résoudre le CTF en utilisant uniquement le code ci-c
3
4 let duration = Math.floor(Math.random() * 3);
5 let multiplication = Math.floor(Math.random() * (5)) + 5
6 let addition = Math.floor(Math.random() * (5)) + 25;
7 let random = Math.floor(Math.random() * (5)) + 2;
8 function startTimer() {
9     setInterval(function () {
10         duration = duration + random;
11         addition = addition + random * 2;
12         document.getElementById("time").innerHTML = "Le code c'est " +
13     }, 1000);
14 }
15
```

En regardant dans le script JS relié à notre page on peut voir qu'une variable nommée « random » change les calculs en permanence.



Il suffit donc de lui donner la valeur 0 grâce à l'injection par URL suivante : « javascript: random = 0 ; ».

Il nous restera plus qu'à faire le calcul sur calculatrice et de rentrer le code.



Une fois le code rentré nous voilà à la seconde étape où par chance le flag est déjà affiché sur la page ! Bien évidemment ce flag ne va pas se laisser faire et fera tout pour vous empêcher de le toucher.

