



**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 :** HackOrDie



**Domaine :** Web

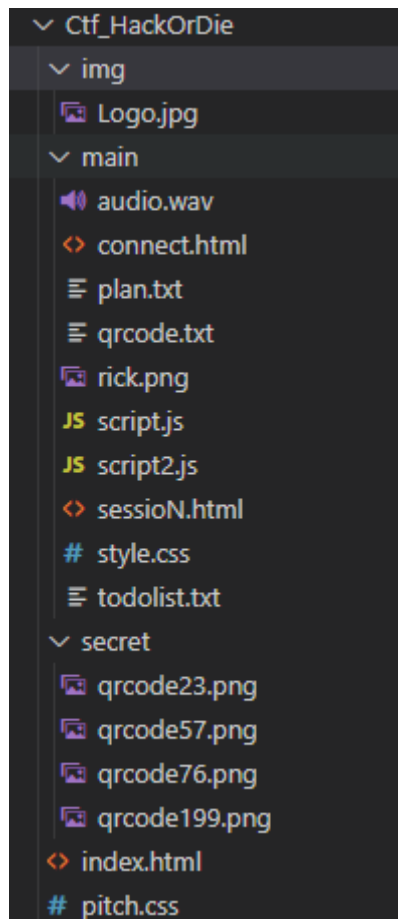
**Difficulté :**

**Auteur :** Alexandre Rocchi

**Description :** Vous avez une mission, retrouver le code pour stopper la bombe. Ce code sera sous forme de QR code et dissimulé dans les défis qui vous attendent. Ce challenge est accessible à tous les niveaux car il demande plus de logique que de compétence informatique.

### Partie 2 : Sources

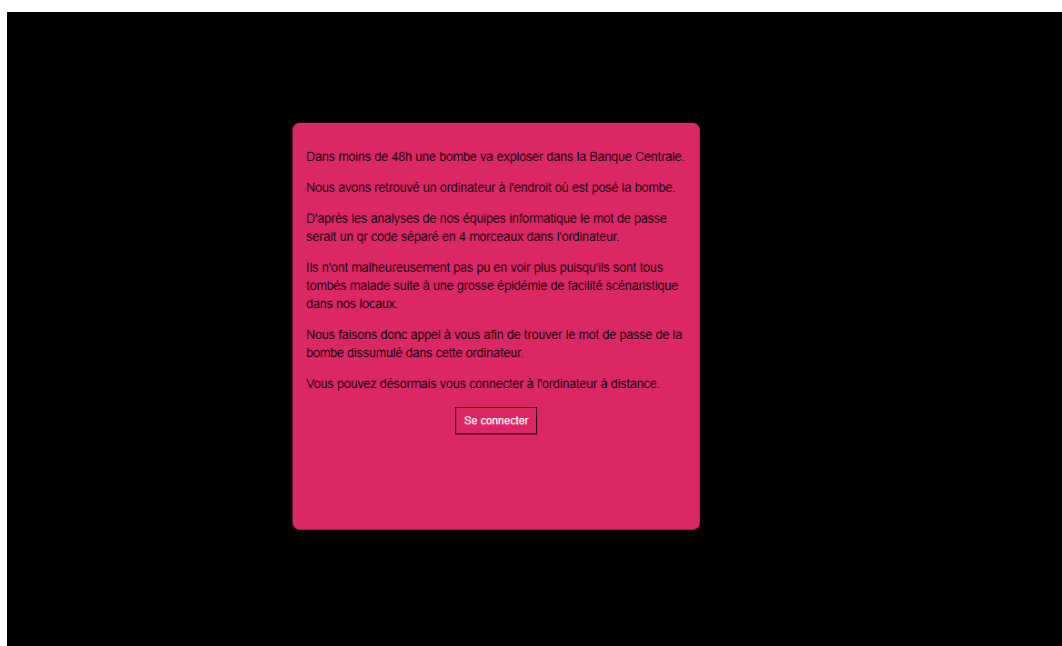
Le challenge comporte les fichiers suivants :



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

## Partie 3 : Résolution

Vous allez arriver tout d'abord sur une page vous expliquant pourquoi votre mission.



On pourra trouver sur cette page dans le code source html le code suivant : BCRENUGOOA

```
><div id="bloc-note"><div></div>
<p class="hidden">BCRENUGOOA</p>
```

Sur la page suivante, on nous demande d'entrer un mot de passe.

```
Veillez entrer votre mot de passe
connexion@localhost:/$
```

Le mot de passe est l'anagramme de BCRENUGOOA soit BONCOURAGE

```
Veillez entrer votre mot de passe
connexion@localhost:/$ BONCOURAGE
Connexion en cours...
connexion@localhost:/$
```

Vous arrivez maintenant sur la troisième page, la page où les parties du QR code sont cachées.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$
```

## 1 ère Partie :

La première partie est très simple à trouver puisqu'il suffit de se balader dans les dossiers jusqu'à trouver un fichier qrcode.txt qui contient un des mots de passe des QR codes.

```
jhondoe@localhost:/$ ls
Audio
Plan
Private
Todo
jhondoe@localhost:/$ cd Plan/
jhondoe@localhost:Plan$ ls
plan.txt
QR
jhondoe@localhost:Plan$ cd QR
jhondoe@localhost:Plan/QR$ ls
qrcode.txt
jhondoe@localhost:Plan/QR$ cat qrcode.txt
Mot de passes QrCode : 1 : Cenestqueledebut 2 : ? 3 : ? 4 : ?
jhondoe@localhost:Plan/QR$
```

On va maintenant récupérer la 1<sup>ère</sup> partie du QR code grâce à la commande dl.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ dl CeneStqueledebut
Téléchargement du QrCode en cours...
jhondoe@localhost:/$
```

Image :



## 2<sup>ème</sup> Partie :

La deuxième partie est contenue dans l'audio morse du fichier Audio.






```
jhondoe@localhost:/$ ls
Audio
Plan
Private
Todo
jhondoe@localhost:/$ cd Audio
jhondoe@localhost:/Audio$ ls
audio.wav
jhondoe@localhost:/Audio$ get audio.wav
Téléchargement du fichier en cours...
jhondoe@localhost:/Audio$
```

Il nous suffit donc de le décoder afin d'obtenir le mot de passe.

Alphabet to decode into  
Latin

All these alphabets can be sent in Morse using standard timing. The "Latin" alphabet is e.g. "ABC" (and includes accented characters and prosigns).

Use the microphone:      Or analyse an audio file containing Morse code:

Listen    Stop    Upload    Play    Stop 

Filename: "audio.wav"

LEMOTDEPASSEC39ESTPLINKPLINKPLONK

On obtient donc : LEMOTDEPASSEC39ESTPLINKPLINKPLONK

On peut maintenant récupérer la deuxième partie du QR code.

```
jhondoe@localhost:/$ d1 LEMOTDEPASSEC39ESTPLINKPLINKPLONK
Téléchargement du QrCode en cours...
jhondoe@localhost:/$
```

Image :



### 3 ème Partie :

La troisième partie se trouve dans le dossier Private.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ cd Private
jhondoe@localhost:/Private$ ls
password.txt
jhondoe@localhost:/Private$
```

Le password.txt n'est pas accessible par cat ou get comme les autres txt.

Il faudra donc utiliser la commande john.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ cd Private
jhondoe@localhost:/Private$ ls
password.txt
jhondoe@localhost:/Private$ john password.txt
Analyse du fichier en cours...
Un nouveau dossier a été débloqué dans le dossier Private
jhondoe@localhost:/Private$
```

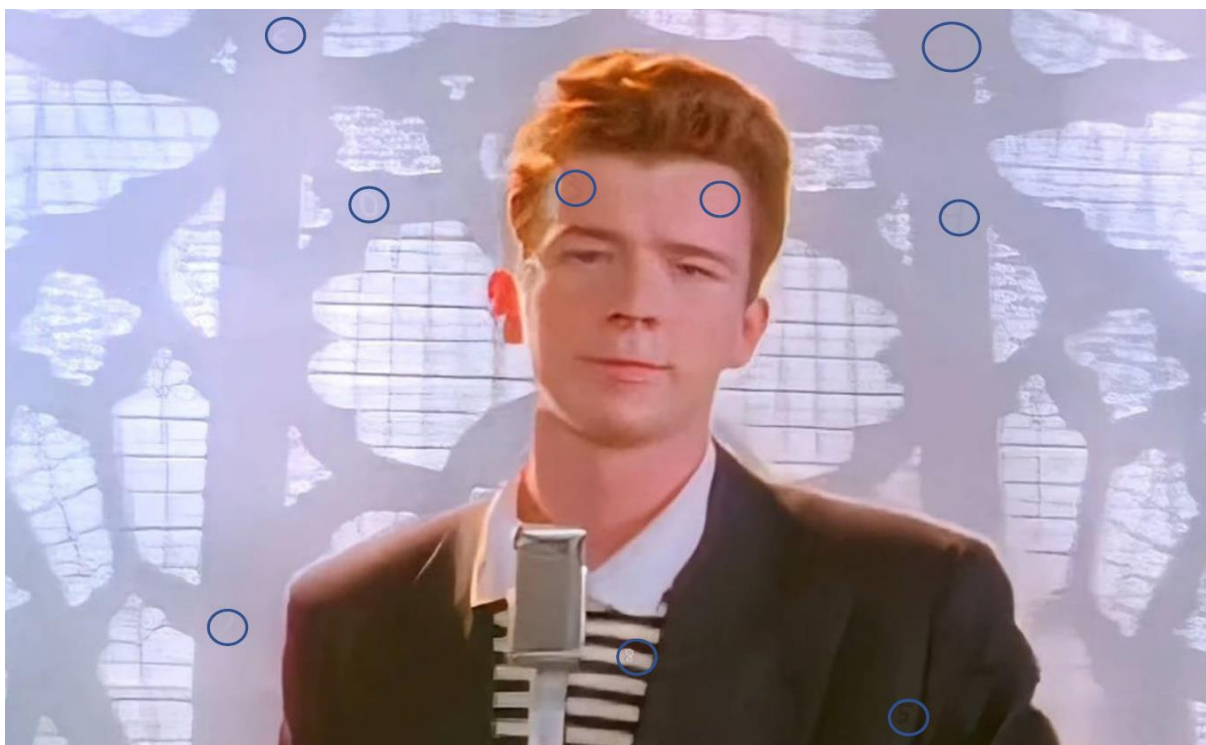
Nous avons maintenant accès au dossier Hidden qui contient l'image rick.png qu'il faut télécharger.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ cd Private
jhondoe@localhost:/Private$ cd Hidden/
jhondoe@localhost:/Private/Hidden$ ls
rick.png
jhondoe@localhost:/Private/Hidden$ get rick.png
Téléchargement du fichier en cours...
jhondoe@localhost:/Private/Hidden$
```

Le principe sera alors de trouver les nombres cachés sur l'image.



Solution ( des outils de stéganographies peuvent être utilisés afin de se faciliter la tâche.) :



On trouvera donc le nombre 690334285 qu'on rentrera pour obtenir la troisième partie du QR code.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ dl 690334285
Téléchargement du QrCode en cours...
jhondoe@localhost:/$
```

Image :

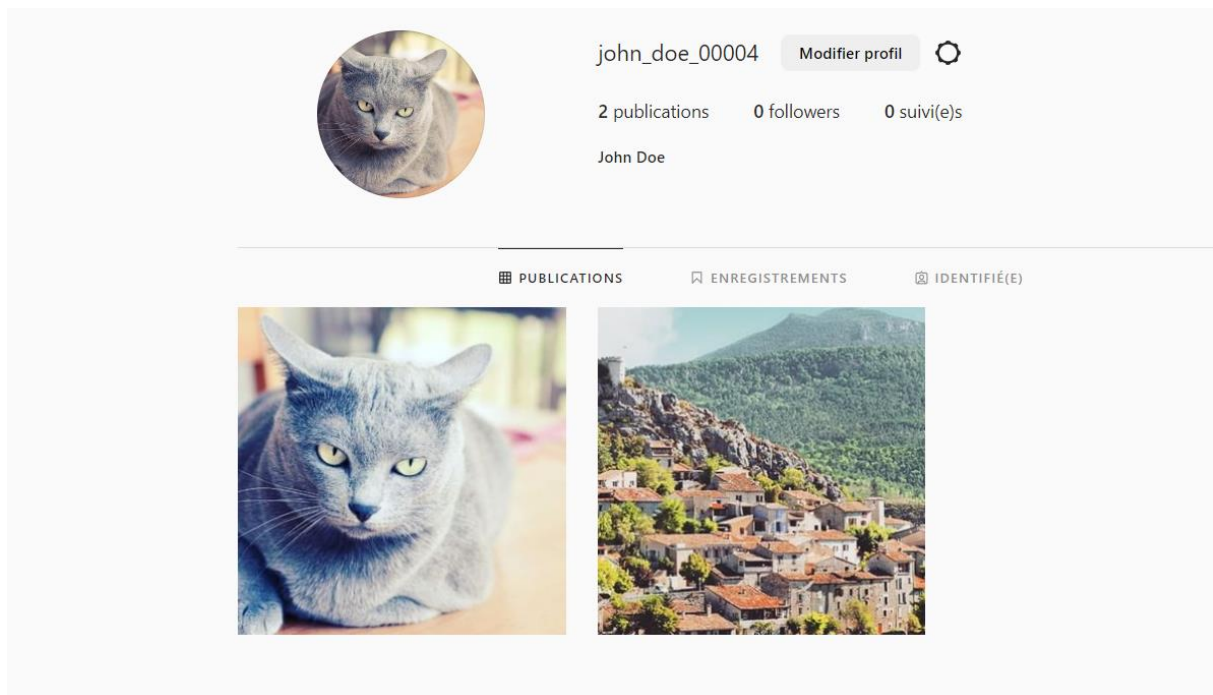


## 4 ème Partie :

Pour la dernière partie du QR Code il faut aller dans le dossier Todo afin d'y trouver un texte.

```
Bienvenue dans votre session de travail
jhondoe@localhost:/$ cd Todo
jhondoe@localhost:/Todo$ ls
todolist.txt
jhondoe@localhost:/Todo$ cat todolist.txt
Mettre à jour instagram : john_doe_00004
jhondoe@localhost:/Todo$
```

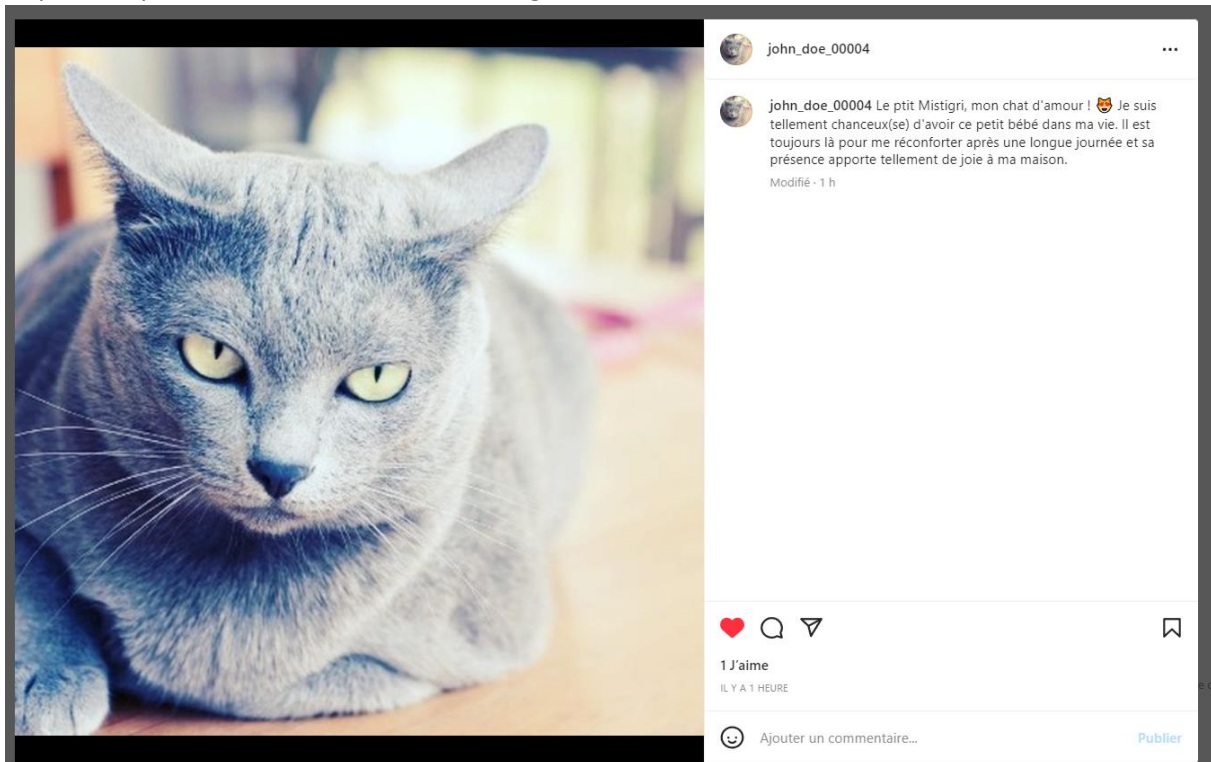
Il faudra alors se rendre sur Instagram : [https://www.instagram.com/john\\_doe\\_00004/](https://www.instagram.com/john_doe_00004/)



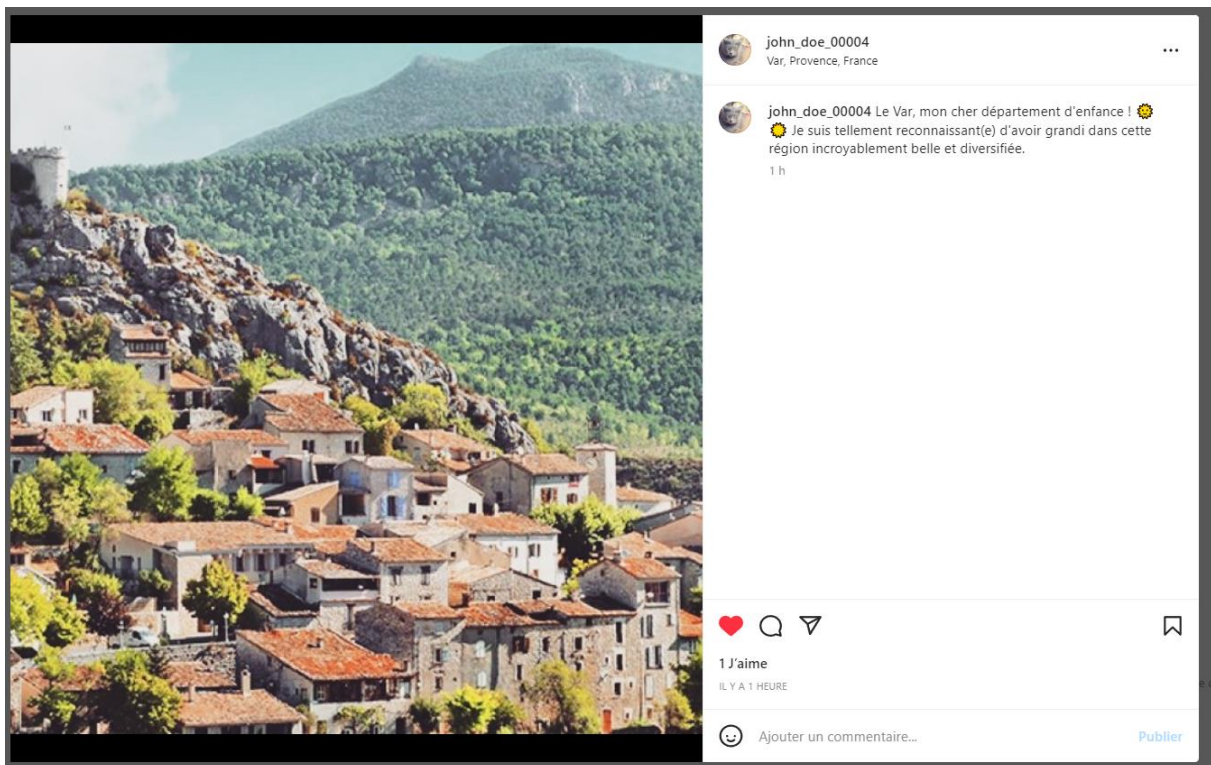


Il faudra donc analyser les deux post Instagram afin de trouver le mot de passe.

Le premier poste nous donnera le mot Mistigri.



Le second nous parlera du Var dont le numéro de département est 83.



Les informations récoltées nous donnent donc le mot de passe : Mistigri83

On peut donc enfin télécharger le dernier morceau du QR code.

```
jhondoe@localhost:/Audio$ dl Mistigri83  
Téléchargement du QRcode en cours...  
jhondoe@localhost:/Audio$
```

Image :



Il ne nous reste plus qu'à réassembler le QR code avec par exemple : [https://pinetools.com/merge-images?utm\\_source=bdmtools&utm\\_medium=siteweb&utm\\_campaign=pinetools-merge-images](https://pinetools.com/merge-images?utm_source=bdmtools&utm_medium=siteweb&utm_campaign=pinetools-merge-images)

On obtient alors le flag du challenge :



**FLAG : HN0x02{GGPRENDSTONFLAG!}**