

# Sécurité des Applications

Octobre 2020 | **Serie 5**

Stéphane Küng

## 1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

### 1.1 Clarification

Dans vos rapports d'exercices, faites attention à bien inclure:

- Captures d'écran de réussite
- Payload utilisés
- Tout code source utilisé pour l'exploitation (ou en annexe)
- Nom des outils utilisé

### 1.2 Doc

Voici quelques ressources permettant de vous aider. Les exercices ont en partie été tirés de ces sites.

- [BufferOverflows](#)
- [Exploitation 1](#)
- [Exploitation 2](#)
- [Exploitation 3](#)
- [Exploitation 4](#)

### 1.3 Conseil

N'hésitez pas à recompiler le code source fournis avec des instructions pouvant vous aider.

## 2 Stack Based Buffer Overflow

### 2.1 BUF1

Le but de ce premier exercice, est d'afficher le **Congratulation** à la suite de l'exploitation d'un buffer overflow.

### 2.2 BUF2

Toujours en exploitant un buffer overflow dans l'application, votre but est de modifier la valeur de la racine carrée par la valeur **10**.

### 2.3 BUF3

Cet exercice est similaire à l'exercice **BUF1**. Sauf qu'ici, une variable **int** vérifiée se situe entre votre buffer et la variable admin. Il vous faudra réécrire la même valeur par dessus.

## 2.4 BUF4

Même chose que **BUF3**, mais avec un tableau de **char** cette fois.

## 2.5 BUF5

Une fonction **secret** se cache dans le binaire, tentez d'y accéder en exploitant un buffer overflow dans la fonction **test**.

## 2.6 BUF6

Pour cet exercice, faite apparaître un **shell** de l'application en exploitant le buffer overflow avec un **shellcode**.