



**OS** **OBJECTIF SÉCURITÉ**  
Architecte de la sécurité informatique

Route Cité-Ouest 19, CH-1196 Gland  
+41 22 364 85 70 / [info@objectif-securite.ch](mailto:info@objectif-securite.ch)

# 1. Contexte

CeRFI a développé le guichet pré- et parascolaire **MonPortail** qui donne accès à six applications Web. Afin de s'assurer que l'ensemble de ces applications dédiées à l'accueil préscolaire (crèches) et aux activités parascolaires a été développé selon les bonnes pratiques de sécurité en vigueur, CeRFI SA a souhaité le faire auditer.

Ce document est le rapport exécutif des tests de sécurité effectués par **Objectif Sécurité** sur la plateforme **MonPortail**.

## 2. Conditions de réalisation

L'audit de sécurité a été effectué en septembre 2022 depuis les locaux d'Objectif Sécurité. Les tests ont porté sur la version 1.5.48.13536 de la plateforme **MonPortail** comprenant les six applications suivantes:



MaCantine



MesDevoirs



MesLoisirs



MesSports



MonAccueil



MaCrèche

Un compte de super administrateur sur **MonPortail** a été fourni préalablement à l'audit. Ce compte a pu être utilisé pour créer des nouveaux comptes de représentants légaux et d'employés des différentes structures, comme des cuisiniers, des moniteurs de sports et des surveillants.

## 3. Résumé exécutif

**Les tests menés dans le cadre de cet audit ont permis d'aboutir aux conclusions suivantes:**

### **Bonne configuration du serveur web:**

Aucun problème n'a été découvert par nos scans automatiques du serveur web hébergeant l'application **MonPortail**.

La configuration de ce serveur ainsi que de la couche TLS permettant de chiffrer le trafic HTTP est conforme aux bonnes pratiques de sécurité.

### **Application implémentée selon les meilleures pratiques:**

L'application **MonPortail** est implémentée selon les bonnes pratiques en matière de développement sécurisé. En effet, nous n'avons trouvé dans la version 1.5.48.13536 de l'application aucune vulnérabilité typique selon l'OWASP Top 10, telle que du Cross-Site Scripting ou des injections SQL. De même, nous n'avons pas été en mesure d'accéder à des données protégées d'autres utilisateurs.

**Nous n'avons trouvé aucune faille de type OWASP Top 10 dans cette application.**

