

Cégep Limoilou

TP1

Travail présenté à :

Patrick Dubois

Dans le cadre du cours :

420-6B6-LI

Sécurité des applications

Par :

Amir Boulmerka, Lawrence Lefebvre et Antoine Fortier

Date : 2024-04-03

## Introduction :

Sécurité des logs, des journaux et de la gestion des erreurs.

Un log, événement ou journal, est simplement la notification d'un événement d'une importance plus ou moins élevée envoyée par un service, un système, un élément réseau ou une application. Les journaux d’événement permettent en administration systèmes, réseaux et en sécurité de retracer les actions et la vie d'un système. Les logs ont un intérêt et une importance cruciale en informatique, car il s'agit là de savoir ce qu'il s'est passé sur un ensemble d'applications ou systèmes.

## Clientèle cible :

[À qui s’adresse cette présentation? Aussi, est-ce qu’il s’agit d’une clientèle novice ou initiée? Ici, voir plus loin que le contexte de ce travail. Si vous aviez à la présenter dans le cadre d’une conférence, à quel genre de public il serait adapté?]

## Objectifs :

[Quels sont les objectifs de cette présentation? Quelles sont nos intentions en tant que formateur?]

## Contenu général :

[Quels sont les points et sous-points qui seront traités ?].

**Les failles les plus courantes :**

* Les connexions, échecs de connexion ou de transactions sensibles ne sont pas journalisées
* Les alertes ou les erreurs ne font l’objet que de journalisations insuffisantes ou peu claires, s’ils en font l’objet tout court
* Les protocoles d’API et d’application ne sont pas contrôlés pour déceler des activités suspectes
* Les protocoles ne sont stockés qu’en local
* Il n’y a pas de seuil ou un seuil inefficace d’alerte ni de remontée d’information pour y répondre
* Il n’est pas possible d’identifier une attaque en temps réel

**Comment y remédier :**

* Mettez en œuvre un processus de contrôle et journalisez tout ce qui concerne la connexion
* Conservez les données de journalisation suffisamment longtemps
* Sauvegardez les données dans des formats supportés par les gestionnaires de logs
* Faciliter l’accès aux logs en centralisant les journaux afin d’obtenir une vision complète et globale des performances de l’application.
* Utiliser un format de log structuré optimal
* Utiliser des messages de journalisation descriptifs
* Traiter les informations sensibles de manière appropriée

## Références :

[Placer ici l’ensemble des références que vous avez utilisé selon les normes APA. Voir : <https://mondiapason.ca/fichiers/OutilBibliographique/index_APA.php>].

[OWASP Top 10 : les plus grosses failles de sécurité des applications web - Digicomp Blog](https://www.digicomp.ch/blognews/2022/11/29/owasp-top-10-failles-securitaires-applications-web#9)

[Bonnes pratiques de journalisation - CrowdStrike](https://www.crowdstrike.fr/cybersecurity-101/observability/logging-best-practices/)