UNIVERSITÉ DE SHERBROOKE

Faculté de génie

Département de génie électrique et génie informatique

Rapport

Sécurité web

GEI-772

Présenté à

Guy Lépine

Présenté par

Brian Compagnat – comb2301

Joel Perron-Langlois – perj2324

Sherbrooke – 3 octobre 2018

# Table des matières

[Table des matières 1](#_Toc526264078)

[1 Introduction 1](#_Toc526264079)

[2 Vulnérabilités communes 1](#_Toc526264080)

[2.1 Injection 1](#_Toc526264081)

[2.2 Violation de gestion d’authentification et de session 2](#_Toc526264082)

[2.3 Exposition de données sensibles 2](#_Toc526264083)

[2.4 XML External Entities (XXE) 3](#_Toc526264084)

[2.5 Violation de contrôle d’accès 3](#_Toc526264085)

[2.6 Mauvaise configuration sécurité 3](#_Toc526264086)

[2.7 Cross-site scripting (XSS) 4](#_Toc526264087)

[2.8 Insecure Deserialization 4](#_Toc526264088)

[2.9 Utilisation de composants avec des vulnérabilitées connues 4](#_Toc526264089)

[2.10 Insufficient Logging & Monitoring 5](#_Toc526264090)

[3 Conclusion 5](#_Toc526264091)

# Introduction

# Vulnérabilités communes

## Injection

**Description**

Les attaques par injections peuvent se produire sur toute source de donnée. Une attaque réussi serait lorsque l’utilisateur réussi a envoyé des données non-autorisées à un interpréteur. L’attaque la plus commune serait par exemple l’injection SQL pour laquelle nous pourrions supprimer des données dans la base de données ou bien obtenir plus d’information que ce qui était prévu.

Application SansSoussi

**Mitigations**

## Violation de gestion d’authentification et de session

Description

Cette vulnérabilité consiste à posséder un système d’authentification faible permettant aux malfaiteur d’usurper l’identité d’un autre usager ou même de l’administrateur. Pour ce faire, ils peuvent utiliser des dictionnaires pour faire une attaque par force brute par exemple.

Application SansSoussi

Mitigations

## Exposition de données sensibles

Description

Comme le nom le décrit bien, l’exposition des données sensibles est aussi une vulnérabilité populaire. Une exposition de ses données a souvent lieux lorsque l’information transige, c’est-à-dire, entre le serveur et le client. Un malfaiteur peut alors surveiller le réseau pour voir les informations en clairs ou bien être un *man in the middle* pour se faire passer pour quelqu’un d’autre. Ainsi, l’information des usagers est à risque.

Application SansSoussi

Mitigations

## XML External Entities (XXE)

Description

Pour les applications basées sur les fichier XML, cette vulnérabilité consiste à télécharger des fichiers XML directement sans vérification. Ces fichiers peuvent être malsain et donc mettre en péril la sécurité de l’application.

Application SansSoussi

Mitigations

## Violation de contrôle d’accès

Description

Un viol d’accès a lieu lorsqu’un attaquant consulte des données dont il n’est pas autorisé. Par exemple, un simple utilisateur pourrait avoir accès à des fonctions privilégiés où il pourrait ajouter ou modifier des données applicatives qui sont normalement seulement accessible par les administrateurs de l’application.

Application SansSoussi

Mitigations

## Mauvaise configuration sécurité

Description

Une mauvaise configuration de sécurité est une vulnérabilité très large qui englobe beaucoup de possibilités. Parmi s’est possibilités, nous retrouvons les comptes administrateurs par défaut, les failles de sécurités connu qui n’ont pas été mis à jour, les fichiers ou dossiers non protégés etc.

Application SansSoussi

Mitigations

## Cross-site scripting (XSS)

Description

Cette vulnérabilité consiste à permettre aux malfaiteur d’inclure des scripts client à l’aide d’un entré de texte ou autre sur la plateforme web. Ainsi, le nouveau script faisant maintenant partie de la page web peut désormais accéder aux cookies ou autre information détenue par le navigateur.

Application SansSoussi

Mitigations

## Insecure Deserialization

Description

Cette vulnérabilité consiste à la possibilité de générer du code malsain lors d’une conversion de données sérialisées venant d’un fichier ou d’un paquet réseau en un objet reçu par un client malfaiteur.

Application SansSoussi

Mitigations

## Utilisation de composants avec des vulnérabilitées connues

Description

Cette vulnérabilité consiste à ne pas tenir a jour les différents composant de l’application. Ainsi, lorsqu’une faille de sécurité est détectée sur un de ses composant et rendu publique, les méthodes d’attaques deviennent aussi publiques et très simple d’utilisation.

Application SansSoussi

Mitigations

## Insufficient Logging & Monitoring

Description

Une insuffisance de *logs* et de surveillance permet effectivement aux malfaiteur de tenter plusieurs attaques sans ce faire détecter. C’est pourquoi cette insuffisance consiste à une vulnérabilité importante. Par exemple, le fait de *logger* les tentative d’authentification suivi d’un échec permet de découvrir les attaques par force brute si elles ne sont pas déjà empêchées!

Application SansSoussi

Mitigations

# Conclusion