

SR03

Rapport du Devoir 2

GILLET Guillaume

HERKENS Antoine

26/04/2020

Sommaire

[Introduction 3](#_Toc38792620)

[Cahier des charges 3](#_Toc38792621)

[Contenu du rapport 3](#_Toc38792622)

[Bonnes pratiques de sécurité 4](#_Toc38792623)

[Synthèse : sécurité des applications web 5](#_Toc38792624)

[L’authentification à deux facteurs : sécurité élevée, implémentation simple. 5](#_Toc38792625)

[Conclusion 6](#_Toc38792626)

# Introduction

## Cahier des charges

Vous allez mettre en place une petite application web à destination des clients et des employés d'une banque, et implémenter des fonctionnalités basiques que l’on peut trouver dans une telle application. On part du principe que c’est le même site qui est utilisé par les différents profils d’utilisateurs : clients de la banque et employés de la banque. La nécessité de sécuriser cette application est assez évidente et les attaques potentielles faciles à imaginer. Les actions malveillantes ou non autorisées peuvent dans notre cas venir de différentes sources : un pirate complètement extérieur à l’application, un client de la banque, ou même un employé de la banque !

## Contenu du rapport

Dans un premier temps, nous allons aborder la sécurisation de notre application web. Nous verrons quelles failles nous avons sécurisé et comment nous nous y sommes pris. Dans un deuxième temps, nous ferons une synthèse d’une technique de sécurisation actuelle : l’athentification à deux facteurs.

# Bonnes pratiques de sécurité

# Synthèse : sécurité des applications web

## L’authentification à deux facteurs : sécurité élevée, implémentation simple.

L’authentification à 2 facteurs est un moyen simple mais très efficace de sécuriser des applications web, qu’elle soit pour une banque ou un réseau social ou encore une plateforme de jeu vidéo. Ce qui fait la puissance de cette authentification à 2 facteurs (ou A2F) est sa versatilité.

Le principe de fonctionnement est simple, lorsque vous souhaitez vous connecter à votre compte sur le site/l’application web il vous est demandé d’entrer un code unique qui vient d’être généré. Ce code est reçu dans la majorité des cas sur votre smartphone par sms. Dans certains cas vous pouvez aussi le recevoir par mail. Dès lors, il suffit d’entrer le code reçu dans l’application et vous pouvez accéder à vos données en ayant très peu de chance de vous faire pirater votre compte car le pirate n’a pas accès à tous vos appareils comme votre réception de SMS. Il existe un site qui recense tous les sites/applications qui utilisent cette méthode de sécurisation ( https://twofactorauth.org).

Certains sites plus aboutis en terme de sécurité ont amélioré cette méthode (notamment Google et Facebook). Google utilise par exemple le smartphone ou tout autre appareil connecté à votre compte sur lequel une notification est envoyée demandant de valider la connexion du nouvel appareil en indiquant sa localisation est son nom/ip pour assurer de ne pas accepter de connexion mal intentionnées.

Il existe aussi des applications dites « authenticator » qui permettent de générer en continu de nouveaux codes pour chaque compte de chaque application et le renouvellement de code en continu permet d’éviter les attaques par essais infinis (le code change tous les certains laps de temps). Ces applications sont plus sures que des sms car elles sont gérées uniquement sur un terminal et les codes contrairement aux sms ne peuvent pas être interceptés par des pirates. Mais ils imposent une contrainte lors de la perte du terminal qui contient l’application, dans ce cas la personne le retrouvant pourrait si elle parvient, a y accéder et utiliser les codes de l’authenticator et entrer dans vos différents comptes.

Une nouvelle méthode d’authentification à deux est apparue. Elle utilise une clé USB externe qui une fois connectée à votre terminal va directement vous connecter de manière sécurisée à votre compte, mais pour cela il faut que l’application soit certifiée FIDO et accepte l’utilisation de cette clé U2F.

Finalement on remarque que l’authentification à 2 facteurs prend aujourd’hui différentes formes mais reste une norme qui se démocratise de plus en plus en sécurité, simple d’utilisation et d’implémentation. Elle réduit drastiquement les risques de piratage et donc l’accès aux données personnelles. Mais elle reste encore assez peu utilisée dans certains domaines et demande d’être activée manuellement lors du paramétrage des comptes utilisateurs, elle n’est pas obligatoire.

Concernant une application de banque on comprend que l’A2F est très importante. Elle est notamment utilisée lors des achats sur le net ou pour confirmer un virement. Par exemple lorsque vous utilisez votre carte bleue sur un site internet muni de cette technologie, il va vous être demandé un code, code envoyé par sms pour bien confirmer que c’est vous qui effectuez l’achat et que vous ne vous êtes pas fait voleé vos données de cartes bancaire.

Lors d’une fuite de données liée au piratage du serveur gérant l’application web, si les données personnelles de personnes n’ayant pas activé cette option fuitent, les pirates peuvent récupérer toute information compromettante à travers l’application. Ce n’est donc pas une méthode de sécurité suffisante, elle doit être combinée avec d’autres méthodes notamment des chiffrages côté serveur pour éviter le vol des données brutes.

# Conclusion

Pour conclure, nous avons répondu au cahier des charges demandé dans ce devoir. Nous avons effectivement strucuturé l’application comme convenu et sécurisé les failles abordées dans le cours. Avec d’avantage de temps, il serait possible d’ajouter plus de sécurité à notre application, comme nous l’avons vu par exemple avec la possibilité de l’authentification à deux facteurs.