App Carrefour Martinique - découverte d'une faille de sécurité

19.09.2019

Guillem Lefait
guillem@hey.com
Schoelcher, Martinique

Vue d'ensemble

Le code barre généré pour identifier le porteur d'une carte n'est pas sécurisé puisqu'il s'agit d'un ID composé d'un préfixe ("**310972**") et d'un nombre que l'on devine être un ID séquentiel (exemple avec mon compte personnel : "**00000000008942**") formaté sur 14 chiffres.

Dès lors que le code barre utilise un identifiant dont la nomenclature est connue et facilement interprétable, il devient trivial de pouvoir forger le code barre d'un tiers avec deux conséquences immédiates :

1. Pouvoir utiliser la cagnotte d'un tiers
2. Obtenir la civilité, le nom et le prénom de la personne auquel appartient ce code

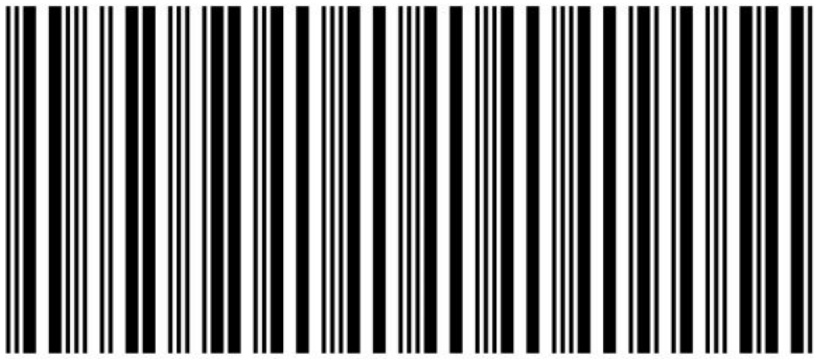
Analyse

Client Carrefour Martinique (principalement Carrefour Cluny), j'ai découvert le 14 septembre, l'application Carrefour Martinique. De part mon activité professionnel (Chief Data Officer chez Holimetrix) et mes activités connexes (intérêts pour la sécurité et la blockchain), j'ai été intéressé par le fonctionnement de l'application.

J'ai dans un premier temps découvert un fonctionnement inadéquat sur l'acceptation des "conditions d'utilisation" qui semble dépendante de l'acceptation de l'*utilisation des données collectées pour m'adresser des offres ciblées*.

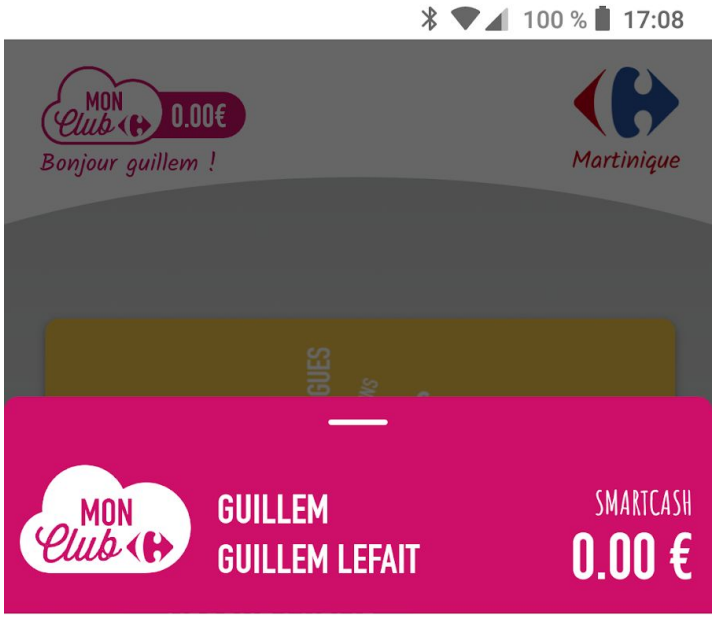
Ne sachant à qui m'adresser, j'ai directement envoyé un tweet au CTO d'Infobam pour lui en faire part (cf : https://twitter.com/guillem_lefait/status/1172964711060713473)

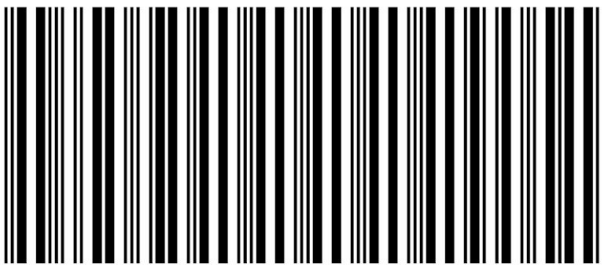
Dans un second temps, après m'être inscrit, j'ai voulu voir à quoi correspondait l'identifiant du code barre lié à mon compte (voir ci-dessous).

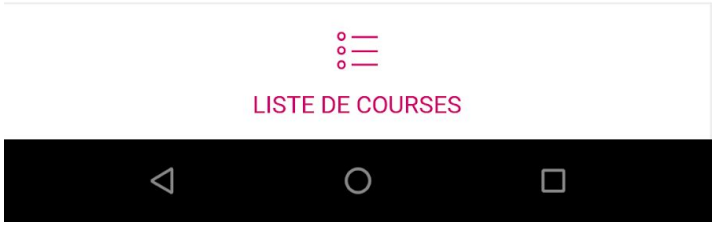


Il s'agit donc d'un code barre IFT.

En utilisant un service de lecture de code-barre (exemple : https://www.onlinebarcodereader.com/), je me suis rendu compte que ce code-barre correspondait à un identifiant qui semblait très peu aléatoire : 31097200000000008942.







Ne voulant pas rendre cette découverte publique mais n'ayant de contact chez infobam, j'ai donc contacté le CTO d'Infobam sur LinkedIn, puis lui ai décrit ma découverte lundi 16 septembre.

Etant client Carrefour Cluny, je me suis rendu dans le magasin de Cluny pour y faire mes courses et j'ai fait scanner mon code barre personnel lors du passage en caisse.

De là, en dehors de l'information du montant de la "cagnotte" disponible, on se rends compte qu'une information sur la civilité, le nom et le prénom du client associé au code-barre est disponible.

Attaque

Aléatoire

Un utilisateur malveillant (*UM*) peut générer un code barre "potentiel". Mon ID étant 8942, des valeurs "candidates" seraient donc des valeurs inférieures à 8942.

UM peut donc :

1. créer un code barre à partir d'un ID, trivial avec un système d'API ou de site en ligne (exemple : https://www.scandit.com/barcode-generator/)
2. intégrer le code barre à une image de l'application (capture d'écran) pour faire croire que le code barre vient de l'application alors qu'il ne s'agit que d'une image statique
3. passer à la caisse en espérant avoir trouvé une cagnotte non vide.

Dans le même temps, *UM* récupère le nom et le prénom du client.

Ciblé

UM ramasse/collecte des tickets de caisses à la sortie du magasin/sur le parking. Après avoir trouvé le code barre d'un client qui contient une cagnotte dont le montant l'intéresse (puisque celui-ci est 'affiché sur le ticket de caisse), il génère le code barre et réalise la même opération que précédemment.

Améliorations possibles

Limiter les données communiquées

Il ne semble pas indispensable d'afficher autant d'informations sur les tickets de caisse, seul le montant de la cagnotte pourrait être conservé et les informations suivantes supprimées :

1. Civilité
2. Prénom
3. Nom
4. Numéro de client
5. Numéro de code barre

Générer un identifiant robuste

Le choix d'un ID séquentiel n'est pas le bon. Si le format IFT doit être conservé ainsi que le préfixe, la solution la plus simple serait de générer un nombre réellement aléatoire sur 14 chiffres : on obtiendrait alors un nombre de possibilités supérieur à mille milliards, ce qui rends la découverte d'un ID existant réel peu probable dans des conditions normales (sous-réserve que la vérification de l'existence d'un ID nécessite un passage en caisse).

S'agissant d'une application, l'ajout d'une option "changer d'ID" pourrait permettre à un utilisateur d'invalider un ID qui aurait pu être identifié par un tiers.

Ce changement devrait être effectué automatiquement sur les utilisateurs existants pour leur offrir une sécurité minimale.

Suites

Comme indiqué sur LinkedIn, je suis disposé à collaborer avec vous si vous le jugez pertinent.