Partiel sécurité
ENSEEIHT 3AI 2016-2017

6 décembre 2016

Note Afin de simplifier le sujet du partiel, beaucoup de détails techniques sont ignorés. Si vous faites des suppositions ou hypothèses quant à ce qui existe sur le système cible, *indiquez-les clairement.*

1. Contexte

La société TicketsChic propose des réservations à des spectacles. Elle a deux types de clients :

— des spectateurs, qui souhaitent réserver et acheter des places pour des spectacles, et
— des établissements de spectacle, qui souhaitent mettre en vendre des places pour une ou plusieurs de leurs salles.

TicketsChic joue le rôle d'intermédiaire entre ces deux parties, et facture aux établissements, en fin de mois, une commission sur chaque réservation utilisée. Un ticket non utilisé (« ticket sec ») n'est pas facturé à l'établissement.

Chaque utilisateur dispose d'un compte, de type « établissement » ou « spectateur ».

Les spectateurs peuvent rechercher un spectacle, réserver une ou plusieurs places et régler en ligne. Ces fonctions sont accessible au travers d'une application sur smartphone et du site web. Les informations associées à un utilisateur sont son nom et prénom, ses coordonnées de contact (e-mail et téléphone portable) et l'historique des spectacles pour lesquels il a fait une réservation.

Les comptes « établissement » peuvent créer des spectacles (horaires, photos, prix, description, nombre de places mises à la vente). Ils doivent aussi confirmer les places réservées par les spectateurs. Ce n'est qu'après cette confirmation que les spectateurs reçoivent leur ticket numérique. Les fonctions de gestion des spectacles ne sont accessibles qu'au travers du site Web (pas d'application sur téléphone).

Le ticket numérique est un QR-Code envoyé par courrier électronique au spectateur. Le QR-Code contient le numéro du spectacle, le numéro de la représentation et un numéro de série incrémental. Il suffit de présenter le QR-Code à l'entrée de l'établissement pour valider la place. TicketsChic fournit des lecteurs qui s'interfacent (via le Wifi) avec le

serveur Web de TicketsChic. Le lecteur lit le QR-Code et interroge TicketsChic, en transmettant les informations du QR-Code. Deux URLs sont proposées, selon les cas :

utilisation Si le ticket existe et n'a pas déjà été utilisé, il est marqué comme consommé et le serveur renvoie OK. La facturation de TicketsChic aux salles de spectacle est basée sur cette consommation des tickets. Si le ticket n'existe pas ou s'il a déjà été consommé, le serveur renvoie NOK.

vérification Si le ticket existe, le serveur renvoie OK et les informations associées à la réservation (nom du spectacle, salle, date et heure) qui sont ensuite affichées sur le lecteur. Si le ticket n'existe pas, le serveur renvoie NOK.

Le règlement se fait sur place, à la salle de spectacle.

Un spectateur peut annuler sa réservation (si elle a été confirmée) jusqu'à 12 heures avant le spectacle. Il lui suffit de renvoyer son QR-Code à TicketsChic.

2. Questions

Note

Dans vos réponses, vous **devez justifier** votre avis.

1. Quelles sont les vulnérabilités ou risques que vous identifiez dans le mode de fonctionnement ou les services proposés par TicketsChic ?
2. Comment proposez-vous de limiter/résoudre les trois principaux risques ou vulnérabilités que vous avez identifiés à la question 1 ?
3. Après de nombreux mois de fortes ventes sur trois salles d'un même établissement, TicketsChic observe une augmentation significative du nombre de tickets secs. Cela peut-il indiquer une fraude ? Si oui, de qui (spectateurs ou établissement) et comment ? Comment le vérifier ? Que corriger dans le système de TicketsChic ?
4. Comment un responsable malveillant d'une salle de spectacle pourrait-il nuire à ses concurrents (autres salles) par le biais du système de TicketsChic ?

1) 1) Chiffrer données
2) usurpation identité établissement (site web + API
3) falsification qrCode
4) DDOS du site web

2) 1) SSL
2) Token unique par établissement
3) pas série incrémentale ou facilement modifiable mais token aléatoire uniq.

3) Oui établissement pour éviter commission, taxe directement vérification. Si ça retourne les infos, alors paiement et jamais de validation par l'utilisateur. Vérification : logs de l'utilisation de la vérification. Correction : Vérification = Validation.

4) En essayant de se connecter à leur place et en essayant de valider des tickets au hasard