WAVESTONE

Audit de sécurité Web & Android COJI 2034

Synthèse managériale

16 Mars 2022

Gauthier VIDAL, Yavuz AKIN, Charles CHREIM, Lucas GEORGET, Ludovic SAHKOUN, Remi FERRER
Cybersécurité & Confiance Numérique

Sommaire

1. Présentation du cadre de la mission

- Contexte : Organisation des Jeux Internationaux de Paris en 2034 –> Création d'un site web et application pour réservation de billets, visionnage en streaming, …
- Dates : 09-03-2022 au 16-03-2022
- Mission : Effectuer des tests d'intrusion sur ces plateformes afin d'identifier les potentielles vulnérabilités et effectuer des recommendations vis-à-vis de ces vulnérabilités.

Types de tests d'intrusion effectués

Boîte noire	Boîte Grise
Attaquant externe sans aucun compte sur les services	Attaquant possédant un compte dans l'application

2. Vulnérabilités de l'application

Les principales vulnérabilités :

- Utilisation du mauvais protocole : HTTP au lieu de HTTPS –> donc les communications ne sont pas encryptés ni authentifiés (VULN_06).
- Mauvaise gestion des logs : Logs qui affichent les identifiants et tokens des utilisateurs (VULN_07,VULN_09, …).

```
03-16 20:24:28.194 20472 20472 D [NetworkService]: SEND POST REQUEST TO : http://15.237.46.156:8456/auth/login
03-16 20:24:28.194 20472 20472 D [NetworkService]: POST REQUEST BODY : {"email":"YOYOYO","password":"12345","remember":true}
03-16 20:24:28.264 20472 26099 D [NetworkService]: GET REPONSE CODE : 400
03-16 20:24:28.264 20472 26099 D [NetworkService]: GET REPONSE CONTENT : {"error":"USER_NOT_FOUND"}
03-16 20:24:45.247 20472 20472 D [NetworkService]: SEND POST REQUEST TO : http://15.237.46.156:8456/auth/login
03-16 20:24:45.248 20472 20472 D [NetworkService]: POST REQUEST BODY : {"email":"123","password":"12345","remember":true}
```


- Accès possible à une ancienne base de données SQL en utilisant la clé symétrique se trouvant dans le code (VULN_10, VULN_11, VULN_12).

```
public class CryptoService {
    private static final String initVector = "R4nd0MInitV3ct0r";
    private static final String key = "Sup3rS3cretK3y$$";
```

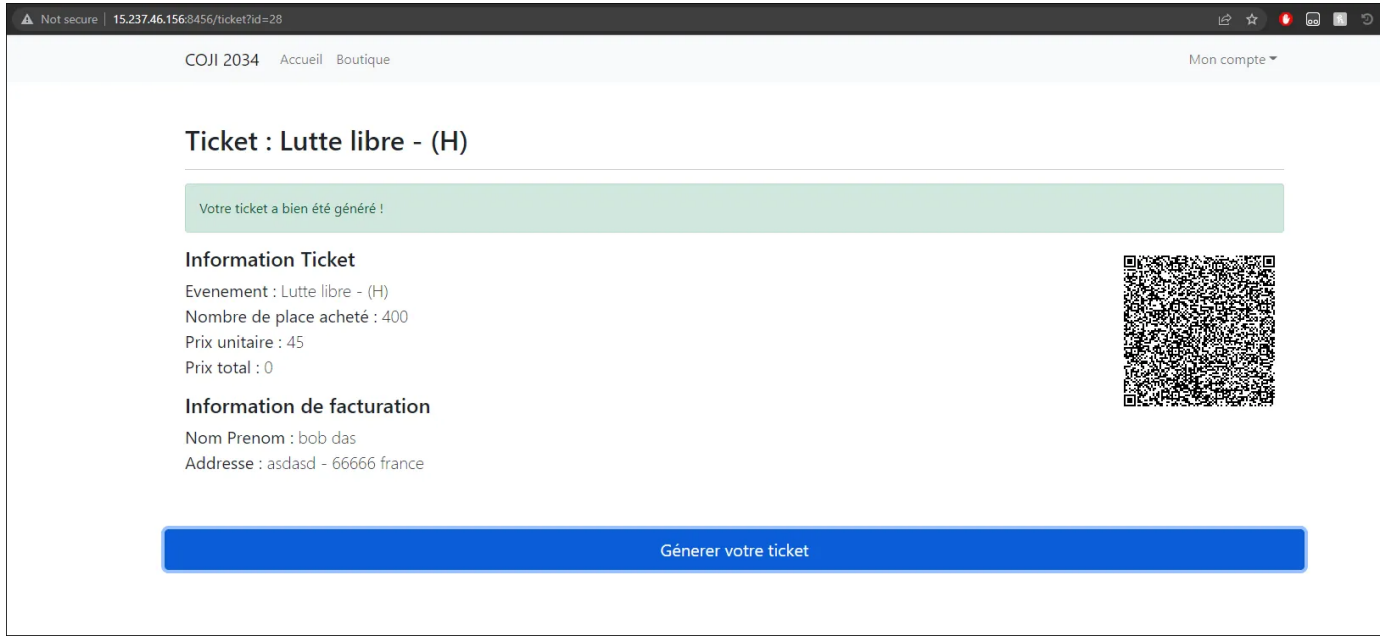
La clé et le vecteur d'initialisation présents en clair dans le code

3. Vulnérabilités du site web

Les principales vulnérabilités :

- La gestion de l'identification et l'authentification peut être fortement renforcée
- Protocole et contremesures à implémenter (HTTPS, XSS, SQL injections, etc...)
- De nombreuses données dans la billeterie sont exposées en clair, et peuvent même être modifiées

Example d'attaque : Achat de 400 tickets gratuitement



4. Conclusion

Afin de respecter la RGPD, le site ainsi que l'application doivent être plus respectueuses de la confidentialité des données des utilisateurs.

Aussi, l'intégrité de ces dernières est très importante pour le bon fonctionnement des plateformes et de la billeterie, sans quoi le schéma économique risque d'en pâtir fortement.

Enfin plusieurs failles pouvant mener à des attaques classiques sont encore présentes, leur correction améliorera en conséquence le niveau de sécurité des systèmes.