
WAVEGAME
BY WAVESTONE
Epreuve #1
ÉDITION 2022

CONTEXTE & ENJEUX

CONTEXTE

/ Le Comité d'Organisation des Jeux Internationaux (COJI) a pour mission d'organiser les Grands **Jeux Internationaux de Paris** en **2034**. Il est ainsi en charge de **planifier**, de **coordonner** et **d'assurer le bon déroulement** des jeux, mais également **d'assurer la communication** autour de cet événement sportif.

/ Dans le cadre de l'organisation de cet évènement majeur, le comité va se charger de **la création d'un site web** (décliné également en **application mobile**), permettant aux spectateurs de **réserver leurs billets** en amont de la compétition. Ce service permettra également de **diffuser en streaming** les différentes épreuves sportives **en direct pendant toute la durée de l'évènement**.

/ Les **utilisateurs cibles** d'un tel service représentent une volumétrie importante et variable. L'objectif premier est donc de permettre à des millions d'utilisateurs très dispersés dans le monde de suivre et d'assister aux jeux, grâce à des interfaces ergonomiques et accessibles, tout en assurant un streaming de qualité, une disponibilité continue des services et la sécurité des données des utilisateurs.

NOTRE POSITION

Vous jouerez le rôle de **consultants Wavestone** dépêchés chez le client.

Nous sommes ainsi missionnés par **le COJI** pour travailler en étroite collaboration avec leurs équipes SI et cybersécurité sur la **mise en place du service et sa sécurisation**.

Compte tenu la taille de l'évènement et sa popularité, des **millions d'utilisateurs sont attendus sur le service**. Cela implique d'en tenir compte dans sa conception.

WAVESTONE

Wavestone se propose d'accompagner le COJI afin de répondre à ces enjeux.

WAVEGAME
LE CHALLENGE CYBERSÉCURITÉ BY WAVESTONE

TEST D'INTRUSION WEB & ANDROID

Objectif

- Conduire des tests d'intrusion sur **l'application web et sur l'application mobile.**
- Ce test d'intrusion devra permettre de **formaliser une liste de recommandations détaillées** à prendre en compte afin de permettre à l'application de surmonter la montée en charge et de renforcer la sécurité de l'application et du SI.

Tâches

- Des tests en **boîte noire** (i.e. sans compte sur l'application) et en **boîte grise** (en vous créant des comptes utilisateurs) vous sont demandés.
- Lister les **vulnérabilités découvertes** sur les applications, en spécifiant pour chacune le **domaine d'applicabilité**, les **charges malveillantes utilisées,** etc. ;
- Emettre pour chaque vulnérabilité a minima une **recommandation** visant à la **mitiger**. Chaque recommandation devra être **priorisée** dans le contexte de ce plan d'action et devra permettre aux équipes techniques de corriger la vulnérabilité, y compris sans connaissance avancée des vulnérabilités web.
- Synthétiser vos découvertes dans 1-2 slides permettant **au RSSI** d'avoir une **vision globale des découvertes et des chantiers à mener**.

Livrables

Rapport vulnérabilités

Synthèse managériale