Audit de la société Minizon

Contexte

Minizon est une startup de commerce électronique française qui tente de concurrence Amazon. Elle se concentre sur la vente de produits fabriqués en France. Apparue en 2017, les deux fondateurs, Charles et Robert, ont construit cette startup en mettant au centre de leur enjeu la satisfaction rapide des demandes de nouvelles fonctionnalités des utilisateurs. Le site a rapidement pris de l'ampleur et est maintenant simple et intuitif. Après un an d'existence, la société a réussi plusieurs levées de fond dont une de plusieurs dizaines de millions d'euros en juin 2018. Il peut ainsi proposer rapidement ces produits sur le marché français et tenter de combler l'écart face à leurs principaux concurrent, Amazon en tête.

Récemment, l'entreprise a fait face à différentes tentatives de piratage plus ou moins réussies qui ont faits la une des journaux. Les utilisateurs et les investisseurs commencent à s'interroger sur la fiabilité du site. Certains acheteurs commencent à déserter le site. Pour les fondateurs, il est urgent de réagir.

Votre société d'experts en sécurité informatique a été contactée par la société Minizon afin de procéder à un audit de la société.

Prise d'informations

Suite à différents échanges, Minizon vous communique les informations suivantes sur leur organisation:

Environ une dizaine de personnes sont présents dans les fonctions support. Ils sont en charge des aspects financiers et RH de l'entreprise.

Les équipes métier sont constitués du service après-vente (environ dix personnes) et marketing (environ 5 personnes). Le service marketing s'occupe de trouver les fournisseurs, définir les prix et suivre le marché.

Le développement est fait en mode Scrum. Une équipe de 7 personnes est en charge d'apporter de nouvelles fonctionnalités. On y trouve un product owner, quatre développeurs, un testeur et un UX/UI. Toutes les trois semaines, de nouvelles fonctionnalités sont mis en production. Le rythme est soutenu, notamment du fait de la pression des investisseurs, soucieux de voir au plus tôt un retour sur leurs investissements. L'équipe n'a que peu bougé depuis le début du projet. Ils connaissent assez bien le code du projet et sont capables de corriger des anomalies rapidement.

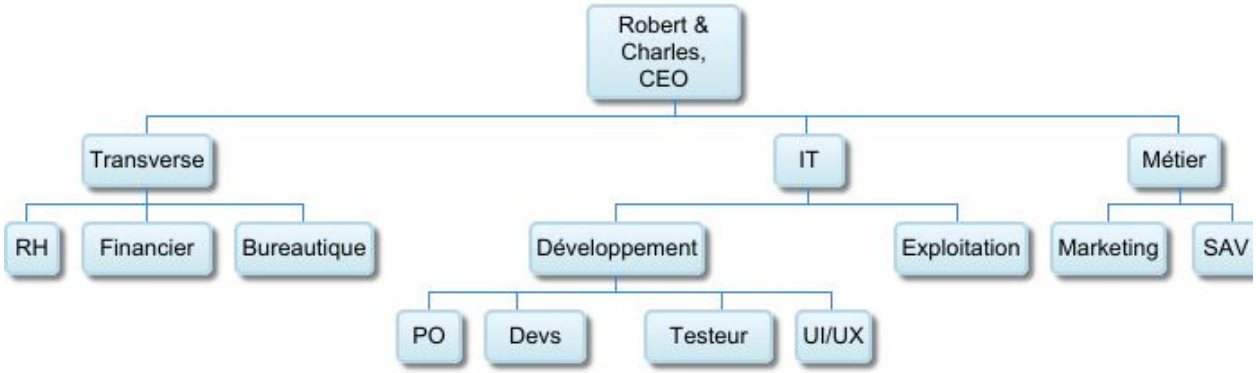
Pour l'exploitation, deux personnes sont en charge de l'installation et le déploiement sur Amazon Web Services. Elles ont en charge la mise à disposition des plateformes, l'infrastructure réseau, l'exploitation au quotidien, …

Au niveau sécurité, les équipes ne sont pas au même niveau.

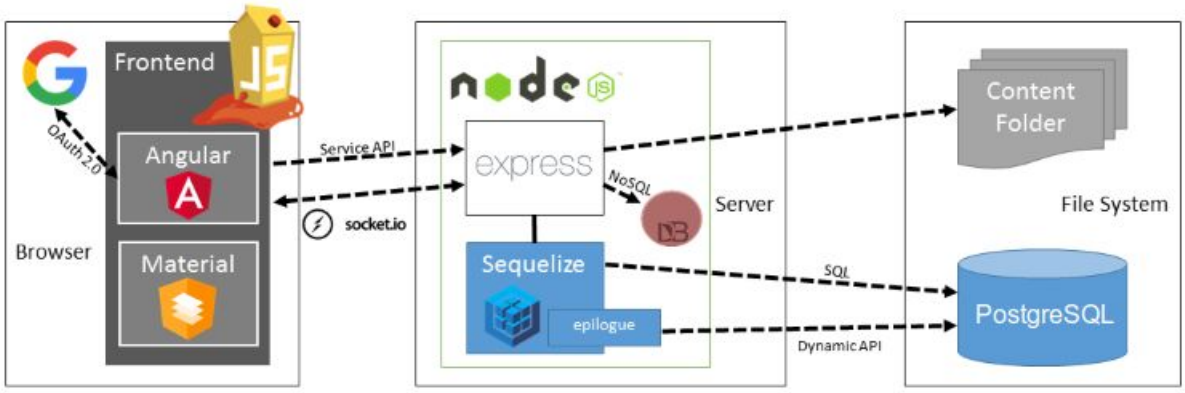
- Côté métier, les équipes considèrent que l'ensemble de la sécurité est à la charge des développeurs.
- Côté équipe de développement, un développeur a un peu d'expérience sur les aspects sécurité. Côté test, rien n'est fait, le testeur étant débordé sur la validation fonctionnelle de l'application.
- Côté exploitation, le personnel est bien formé sur les problématiques de sécurité réseau (VPN, Proxy, NAT, Firewall, VLAN, ….).

Vous avez aussi réussi à obtenir les informations suivantes:

- L'organigramme de la société



- L'architecture globale du système



- Un accès au site de production

  ⇒ **http://ec2-3-86-242-241.compute-1.amazonaws.com:3000/#/**

But de l'audit

Le périmètre de l'audit est le suivant: le site Minizon.

Est exclu du périmètre:

- Les faiblesses de type social engineering (comme le phising)
- Les faiblesses physiques (comme s'introduire dans l'entreprise, forcer une porte en la crochetant, …)
- Les faiblesses réseaux (comme le scan de ports via NMAP par exemple, les attaques de type interception/MiTM, ...)
- Les faiblesses de la plateforme

Pour la société Minizon, votre mission est de proposer des innovations afin rendre l'application sécurisée de manière native. Pour cela, vous devrez:

- Analyser l'organisation et de proposer des solutions pour améliorer la prise en compte de la sécurité à tous les niveaux
- Effectuer une analyse des risques de l'application
- Etudier la surface d'attaque
- Effectuer un audit de l'application (audit boite noire)
- Proposer des solutions pour automatiser la sécurité

Suite à votre audit, vous produirez un rapport d'environ une vingtaine de pages décrivant:

- Votre méthodologie
- Votre approche du problème
- Les failles rencontrées (notamment celles associées aux risques du TOP 10 OWASP) et la démonstration de leurs exploitation
- Les propositions que vous pouvez faire pour cette société en vous basant sur le cours, l'état de l'art ou des idées novatrices
- Un plan d'action pour résoudre les problèmes que vous avez pu imaginer

Le dossier sera noté aussi bien sur le fond que sur la forme. Un dossier contenant trop d'erreurs de fautes de français, illisibles, … sera pénalisé.