La start-up Tilkee bluffée par les résultats d'un Bug Bounty

Le phénomène est apparu aux Etats-Unis avec des plateformes comme HackerOne, avant que l'Europe et la France en particulier se réveille avec des initiatives comme Bounty Factory, Wavestone ou Yogosha. Chacune à ses spécificités, mais en règle générale, ce type de programme intéresse les grandes entreprises.

Erreur ! Les bug bounty s'adressent aussi aux start-ups. Tilkee est une jeune pousse qui propose un service de suivi des documents commerciaux pour optimiser les opérations de prospection. L'année dernière, Tilkee est entré en contact avec Yogosha ayant l'accélérateur Axeleo en commun. « *Nous sommes très exigeants en matière de sécurité, car nous traitons des données sensibles. Nous avons l'habitude de réaliser des pentests, mais nous voulions aller plus loin* », explique Tim Saumet, co-fondateur et CTO de Tilkee.

Bluffé par la compréhension rapide du fonctionnel

D'où l'idée de lancer un Bug Bounty. « *Avec les équipes de Yogosha, nous avons réalisé les spécifications, le périmètre, la copie de la production, les vulnérabilités autorisées. Le programme a été lancée en janvier 2017* », souligne le dirigeant. Il ajoute, « *nous étions plutôt confiant dans la sécurité de notre service en pensant que ce programme n'apporterait que 2 ou 3 rapports de vulnérabilités* ». La confiance du dirigeant a été ébranlée rapidement, « *en 2 jours, nous avons reçu une avalanche de rapports. Au bout de 3 mois, une vingtaine de chercheurs a délivré une soixantaine de rapports dont 30 étaient très intéressants et 10 constituaient des failles importantes que nous avons corrigées* ».

Tim Saumet avoue avoir été « *bluffé par la capacité à comprendre le fonctionnel de notre solution. Après avoir créé un compte en quelques minutes, certains chercheurs ont réussi des prouesses. Le plus beau restant sans doute la suppression d'un fichier* ». Les meilleurs chercheurs ont été récompensés en fonction de la criticité des failles. Les primes s'étalent de 1000 à 500 euros.

Et pour la suite, le responsable envisage de renouer l'expérience du Bug Bounty, « *nous sommes en phase de développement d'une nouvelle solution plutôt orientée marketing. Elle s'appuie sur le cœur unique de Tilkee où tourne le programme de recherches de bug, donc le périmètre va s'élargir* ». Il envisage une ouverture plus grande de ce programme pour trouver des faiblesses. Enfin, Tim Saument résume en conclusion son intérêt pour le Bug Bounty, « *nous révéler ce qui est invisible* ».

A lire aussi :

Une marketplace du Dark Web lance un bug bounty

Le Bug Bounty de l'US Army trouve une faiblesse du réseau interne

crédit photo © andriano.cz – shutterstock