Avec Sleepy Puppy, Netflix traque les failles XSS inter-applications

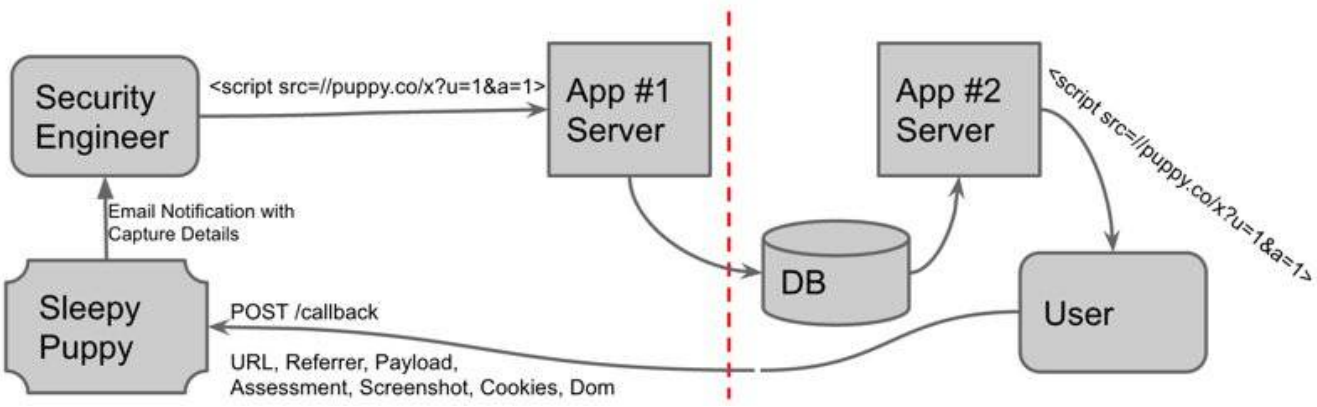
Décidément Netflix est un réservoir à projet Open Source dans le domaine de la sécurité. Pour garantir une expérience utilisateur 100% sécurisée et protéger en même temps son infrastructure IT, le spécialiste de VOD multiplie les initiatives dans ce domaine. De FIDO (orchestration de la sécurité) à Simian Army (sécurité et résilience d'AWS) en passant par le triptyque Scubmlr, Worflowable et Sketchy (anti DDoS), c'est au tour de Sleepy Puppy de se découvrir.

Il s'agit d'un outil de test qui donne aux développeurs et aux administrateurs les capacités de traquer les failles de cross-scripting (XSS) y compris sur des applications tierces. Fruit de deux ingénieurs de Netflix, Scott Behrens et Patrick Kelley, Sleepy Puppy envoie des charges pour diagnostiquer la propagation de la vulnérabilité à travers les applications. Une initiative bienvenue car en général les outils d'audit gratuit réalise leur test en local. Or dans ce cas, les tests sont réalisés sur des applications tierces qui s'appuient sur l'application locale, via des API ou des modules internes qui partagent les bases de données. Les administrateurs peuvent ainsi suivre la propagation XSS au sein du système IT.

Un tableau de bord très complet

Les scripts XSS de tests (cf schéma ci-dessous), nommé PuppyScripts, accordent aux développeurs le soin de suivre en profondeur certains détails, comme l'URL où la faille a été exécutée, le domaine de la page contenant la charge, le User Agent du navigateur, les cookies locaux, information sur les headers référents et même une capture d'écran de l'application où la charge est exécutée. Si cette faille nécessite du temps pour accomplir ses effets et se propager, Sleepy Puppy dispose d'un système de notification par mail. L'outil de test fonctionne par ailleurs sur les applications « containerisées » sous Docker.

A noter que le code source de cet outil est disponible sur Git Hub.



A lire aussi :

Netflix sera bientôt à 100% Cloud

Des pots de vin de fournisseurs IT à la DSI de Netflix ?