Burp Suite

Burp Suite, aussi appelé Burp, est un **logiciel d'audit de sécurité** développé par **PortSwigger** pour les plateformes, sites et applications web. Grâce à lui, les professionnels de la sécurité internet (**les pentesteurs ou pentesters**) peuvent découvrir les vulnérabilités d'un site web afin de pouvoir les résoudre et sécuriser les informations et données. Vous pouvez télécharger et déployer Burp Suite sur les plateformes sous Windows, Mac et Linux. Par défaut **Burp Suite est livré avec quatre modules de base** qui sont indispensables à l'audit de sécurité : **proxy HTTP, intruder, scanner de vulnérabilité et répéteur HTTP**. D'autres modules peuvent ensuite être installés selon vos besoins via le catalogue d'extensions. Notez que **Burp Suite est codé en Java**, il vous faudra donc installer Java avant de pouvoir vous en servir. **Le module HTTP est un proxy d'interception** qui étudie les requêtes émises par l'utilisateur et qui transitent entre celui-ci et **les applications HTTP.** Cet outil dispose de deux fonctions, une fonction passive qui ne fait qu'établir un historique des requêtes et une fonction active qui peut bloquer les requêtes, pour les modifier si besoin avant de les débloquer. **L'intruder est un outil d'intrusion va vous permettre de simuler, ou de réaliser, des attaques de type attaque par force brute (ou brute force) d'URL**, de formulaire de connexion, de répertoire, de paramètre HTTP POST ou GET, mais aussi des injections SQL, etc. Grâce à l'intruder vous allez donc pouvoir créer des requêtes HTTP pour attaquer votre application web ou votre site et voir comment il réagit. Bien entendu, **l'intruder permet d'automatiser les**

actions d’attaque. Grâce au **scanner de vulnérabilité,** vous pourrez automatiser certains de vos tests sur les requêtes. Pour cela vous devez sélectionner la requête à analyser, Burp va ensuite la charger avec des **payloads** malveillants pour voir comment le serveur réagit.**Le répéteur HTTP (repeater en anglais) est l’outil complémentaire du proxy HTTP**. En effet, c’est lui qui vous permet de modifier puis de renvoyer les requêtes bloquées par le proxy dans un premier temps. Vous pouvez modifier chaque requête individuellement avant de la renvoyer vers le serveur. Le repeater permet de tester les failles logiques.