Défi n°2 : autre exploitation d'une vulnérabilité SSRF

L'objectif de ce défi est d'exploiter la vulnérabilité SSRF afin de découvrir une autre interface d'administration présente sur un serveur disposant d'une adresse IP différente. Pour cela, BurpSuite est utilisé afin de scanner une plage d'adresses IP (192.168.0.X) de manière automatisée (mode sniper) en exploitant les informations renvoyées par le serveur lors de chaque tentative. L'objectif est à nouveau de supprimer l'utilisateur Carlos sur l'instance de serveur découverte.

Le lien permettant d'accéder au défi est le suivant :

portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

Travail à faire :

Travaux préparatoires

Q1. Suivre le cheminement indiqué dans le dossier documentaire afin d'accéder au labo du défi n°2. Le labo s'intitule « Basic SSRF against another backend system ».

Q2. Activer le proxy BurpSuite (Intercept is on), puis sélectionner un produit et afficher la quantité en stock. Pour cela, il faudra cliquer plusieurs fois sur Forward jusqu'à l'affichage du code de la page contenant le paramètre stokApi.

Q3. Envoyer la page de code source contenant le paramètre stockApi vers le répéteur de Burp.

Q4. Utiliser la fonctionnalité de décodage d'URL de Burp afin que l'URL contenant le paramètre stockApi soit affiché plus clairement.

Réalisation du défi

L'objectif est de découvrir si d'autres instances de serveur sont à l'écoute et hébergent des pages d'administration. Pour cela, on va utiliser le mode sniper de Burp afin de scanner une plage d'adresses IP.

Q5. Depuis l'onglet répéteur, modifier l'URL encodé par la valeur suivante :

http://192.168.0.1:8080

Puis tester manuellement plusieurs envois de requêtes en modifiant le 4ème octet de l'adresse IP. Cela correspond à des tentatives manuelles de découverte d'autres instances de serveur.

Ensuite, faire un clic droit n'importe où sur la requête puis cliquer sur *Send to Intruder*. Puis cliquer sur l'onglet Positions.

Q6. Sélectionner le 4ème octet de l'adresse IP (le reste restant fixe), puis cliquer sur *Add* afin d'indiquer à Burp la variable à tester.

Q7. Toujours dans le menu *Intruder*, cliquer sur l'onglet *Payload*, puis dans le type de payload, choisir l'option *Numbers*. Dans *Payload settings*, configurer une itération partant de 1 à 255. Enfin, lancer l'attaque en cliquant sur *Start attack*.

Q8. Dans la fenêtre de résultat du scan, trier les résultats en fonction du code de status de l'erreur renvoyée afin de détecter une instance valable. Puis, supprimer l'utilisateur Carlos sur cette instance.