Réalisation de Brute Force de Mot de Passe avec Burp Suite

Realisé par : Wissem karous
2 GT 2

Configuration de Burp Comme Proxy pour DVWA :

1. Vérification du Fonctionnement de Burp avec DVWA

- On ouvre Burp et on accède à l'onglet Proxy pour s'assurer que l'option Intercept est activée.

2. Configuration du Navigateur pour DVWA :

- On a changé les paramètres proxy du navigateur pour DVWA.
- Dans Firefox (sur Kali), on accède aux Préférences, dans Avancé, puis onglet Réseau, et enfin Paramètres.
- Sélection de la configuration manuelle du proxy.
- On tape 127.0.0.1 comme adresse pour le proxy HTTP, et 8080 comme port.
- On a coché la case "Utiliser ce serveur proxy pour tous les protocoles".
- On enregistre les paramètres.

3. Vérification de la Configuration avec DVWA

- On a assuré que le trafic HTTP/S de DVWA passe à travers Burp.
- Le tab Proxy dans Burp devrait devenir orange lors de la visite de DVWA.

Brute Force sur la Page de Connexion DVWA :

4. Activation de l'Interception dans Burp pour DVWA

- On a assuré que l'interception dans Burp est activée.

5. Préparation des Listes d'Utilisateur et de Mot de Passe pour DVWA

- On utilise des listes d'utilisateurs/mots de passe existantes ou on prépare notre liste.
- On a chargé une liste d'utilisateurs et une liste de mots de passe dans Burp.

6. Lancement de l'Attaque Brute Force sur DVWA

- On s'est connecté à DVWA et on a accédé à la page de connexion.
- On a capturé la requête dans Burp, puis envoyé à Intruder.
- Dans l'onglet Intruder, Positions, on a choisi Cluster bomb comme type d'attaque.
- On a sélectionné les positions pour les paramètres d'utilisateur et de mot de passe de DVWA.
- On a chargé les listes d'utilisateurs et de mots de passe dans les Payloads.
- Et on lance l'attaque en cliquant sur Start attack.

7. Analyse des Réponses de DVWA :

- On vérifie les réponses pour détecter des anomalies.
- On a identifié les réponses qui indiquent une correspondance réussie.

8. Finalisation de l'Attaque sur DVWA

- On a utilisé les informations découvertes pour accéder à l'interface d'administration de DVWA.