TP 2 – Web

L’objectif du TP2 – Web est de mettre en œuvre les principales techniques d’attaque permettant d’exploiter des vulnérabilités web. Vous avez deux choix d’architecture :

- Installer un serveur web sur votre Kali Linux. Avantage, vous virtualisez une machine en mois, donc gagnez en performances. https://github.com/ethicalhack3r/DVWA
- Utiliser la VM cible du TP 1 et se rendre à l'adresse http://adresse_ip_machine_cible/dvwa

#Todo 1 : Préparation du lab

Si vous n'utilisez pas la VM du TP 1 :

Depuis votre machine d’attaque, ouvrez votre navigateur et rendez vous sur la page d’accueil de l’application vulnérable (http://IPADDR_CIBLE/DVWA-master).

Dans le menu, cliquez sur le bouton “Setup / Reset DB” et assurez vous que tous les voyants sont au vert. Aidez-vous du Readme.md de la page github.

Sinon :

Vous pouvez vous authentifier avec le compte admin:password.

Le menu est organisé selon les catégories de vulnérabilités les plus courantes. Pour chacune d’elle, il existe différents niveaux de vulnérabilité et différentes méthodes de sécurisation. L’objectif du TP est que vous voyez des techniques d’intrusion d’une complexité croissante.

Dans un premier temps, vous fixerez donc le niveau de difficulté à “Low” dans la page “DVWA Security”.

Outillage

Vous n’utiliserez pas d’outils automatisés pour ce TP. L’ensemble des tests sont donc à faire à la main ou avec l’un des deux proxy applicatif suivant :

- Burp Suite : Il existe deux versions dont une gratuite. Cette version est un peu limitée mais suffisante pour le TP.
- ZAP : Solution Open Source d’OWASP. Moins ergonomique et pratique que Burp, cette solution propose cependant les mêmes fonctionnalités.

Un fois actif, le proxy applicatif se positionne entre le client (votre navigateur) et le serveur, soit un contexte de Man-in-the-Middle. Vous pourrez alors intercepter, modifier et ré-envoyer les requêtes HTTP échangées avec le serveur.

#Todo 2 : Hack it

Pour chaque élément du menu, vous devez parvenir à exploiter le niveau Low, Medium et High. Le niveau Impossible se veut invulnérable (à ce jour).

- Chaque page de challenge comporte les mêmes éléments :
- un ou plusieurs points d'entré que vous devrez exploiter ;
- un ensemble de lien qui proposent des explications sur la vulnérabilité ;
- un bouton "View source" afin de voir le code source de la page (pré-exécution) ;
- un bouton "View help" afin de vous donner un coups de pouce.

L'ensemble de ces éléments devraient vous permettre de progresser à travers les niveaux.