Dossier 2 : Inclusion de fichiers distants

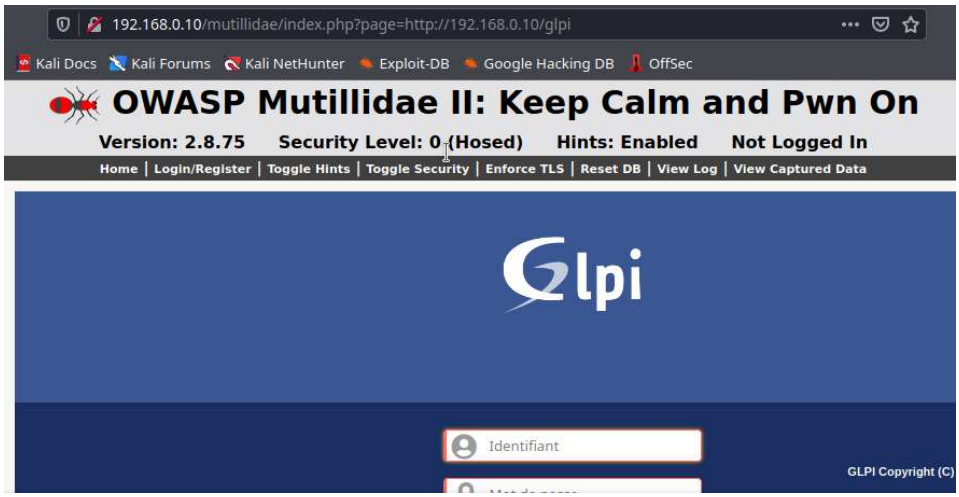
Le fichier qui est affiché ou exécuté est situé sur le serveur web du pirate.

- **Test de vulnérabilité :**

On peut essayer d'afficher la page web de google en indiquant le lien vers cette page dans l'URL. Mutillidae décrit cette procédure dans son application. Pour cela, cliquer sur le lien **Hints and videos**.

Puis cliquer sur **Remote File Inclusion**. Vous pouvez alors tester un accès à la page de google si la maquette de travail dispose d'un accès à internet.

Dans l'exemple ci-dessous, le serveur web qui héberge Mutillidae héberge aussi l'application GLPI.



- **Exploitation de vulnérabilité :**

Un attaquant peut faire référence à l'adresse IP de son serveur pour faire exécuter un code malveillant. Sur Mutillidae, on peut avoir plus de renseignements sur l'exploitation de cette vulnérabilité en suivant le chemin suivant :

OWASP 2017 => A5- Broken Access Control => Insecure Direct Object References => Remote File Inclusion.

Il est possible que le serveur web bloque, par défaut, les fichiers d'inclusion. Il faut donc, pour les besoins de la démonstration, supprimer ce blocage.