Dossier documentaire

Dossier 1 : Inclusion de fichiers locaux

Sur un serveur vulnérable, l'inclusion de fichiers locaux se fait en modifiant directement le contenu d'un paramètre transmis dans l'URL (méthode GET).

Exemple sur l'application Mutillidae :

Dans cet exemple, le paramètre (variable de type GET) se nomme **page** et sa valeur est **home.php**. Il est possible de tester plusieurs combinaisons de fichiers locaux. Plusieurs modes opératoires sont possibles.

- **Modification directe dans l'URL :**

Cette méthode est la plus simple car elle ne nécessite aucun outil.

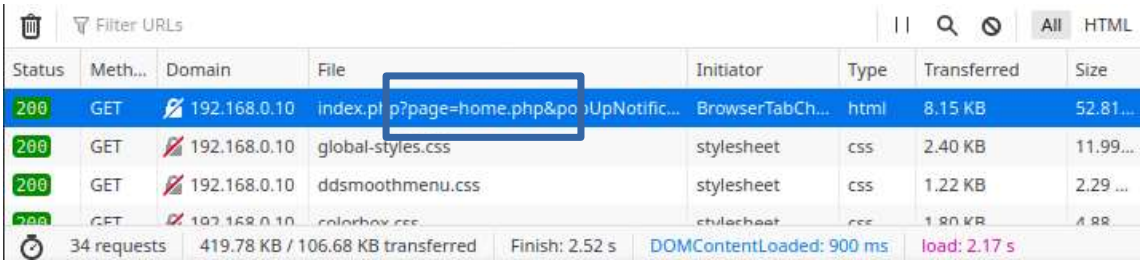
- **Utilisation de l'outil Web Developer de Firefox :**

1. Une fois sur la page d'accueil, cliquer sur **Home**.

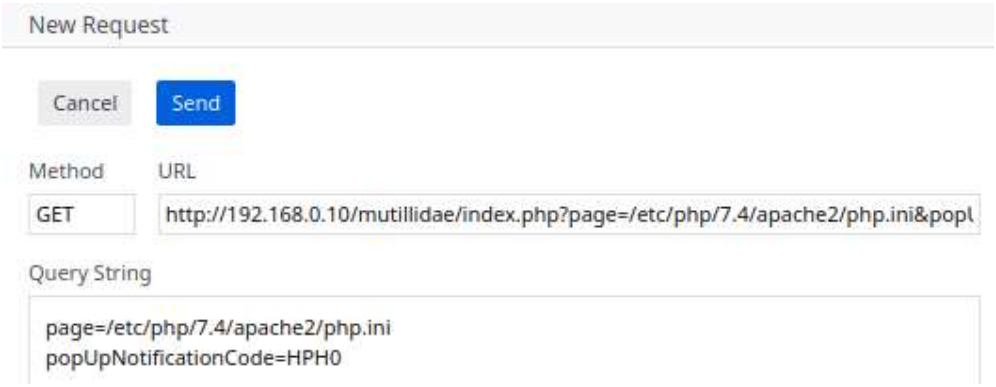
2. Ouvrir l'outil Web Developer de Firefox en suivant le chemin suivant :

   Outils=>Web Developer=> Réseau

3. Rafraîchir la page puis, dans la console du bas, chercher la ligne faisant référence au paramètre nommé page.



4. Faire un clic droit sur cette ligne puis cliquer sur **Modifier et renvoyer**. Il est ensuite possible de modifier la requête via la fenêtre de droite. Dans cet exemple, on teste le contenu du fichier php.ini du serveur (le chemin vers le fichier peut varier selon la version de PHP).



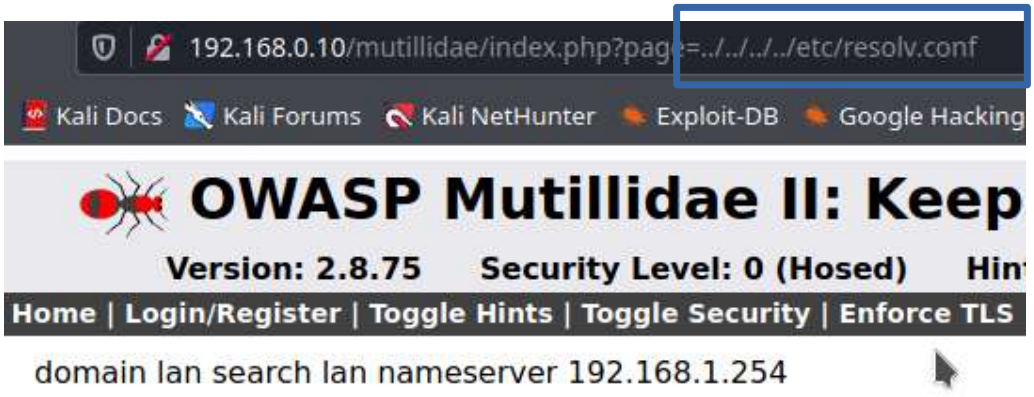
5. Envoyer la requête au serveur en cliquant sur le bouton **Send**.

6. Puis sur la ligne correspondante à cette requête, faire un clic droit puis cliquer sur **Ouvrir dans un nouvel Onglet**.

Le serveur a bien tenté d'exécuter le fichier php.ini. Cette méthode est plus longue mais permet de découvrir l'outil Web Developer de Firefox.

- **Traversement de répertoires :**

Il s'agit d'une variante de la première méthode dans laquelle on utilise un chemin relatif dans l'URL par essais successifs.



Dans un chemin, **..** renvoie vers le répertoire précédent dans l'arborescence.