

Détecteur automatisé de vulnérabilités CSRF

L'ensemble du programme a été développé en Python version 2.6.1.

Il contient quatre fichiers :

- *main.py* : module principal
- *HTTP_request.py* : module gérant toutes les requêtes HTTP
- *handle_html.py* : module s'occupant du traitement du langage HTML
- *comparison_method.py* : module implémentant l'ensemble des fonctions de comparaisons nécessaires à la bonne exécution du programme.

Le détecteur de vulnérabilités CSRF peut être utilisé suivant deux modes :

- Statique avec la commande :

python main.py URL Cookie

Dans ce mode là, seul l'url URL est testée. Deux requêtes HTML sans cookie et deux avec cookie sont transmises à l'url. Pour chaque requête, le code HTML est parsé dans un arbre. La méthode rdiff est appliquée aux deux arbres créé à partir du code retourné suite aux requêtes sans cookie et de même pour les requêtes avec cookie.

Finalement les formulaires sont extraits et seul les formulaires apparaissant uniquement dans l'arbre correspondant à la session authentifiée sont imprimés sur la sortie standard.

- Récuratif avec la commande :

python main.py -R URL Cookie

Dans ce mode une première étape est effectuée pour extraire tous les liens interne du site en question. Par la suite la méthode statique expliquée précédemment est appliquée à chacun de ces liens.