**Procédure d’utilisation W3AF**

**SOMMAIRE**

1 Objet du document 3

2 W3AF 3

2.1 Utilisation 3

# Objet du document

Ce document présente la procédure d’utilisation de l’outil **W3AF**.

# W3AF

## Utilisation

W3AF est disponible en mode graphique (w3af\_gui) et en mode console (w3af\_console).

La fenêtre principale de w3af\_gui se divise en 3 parties :

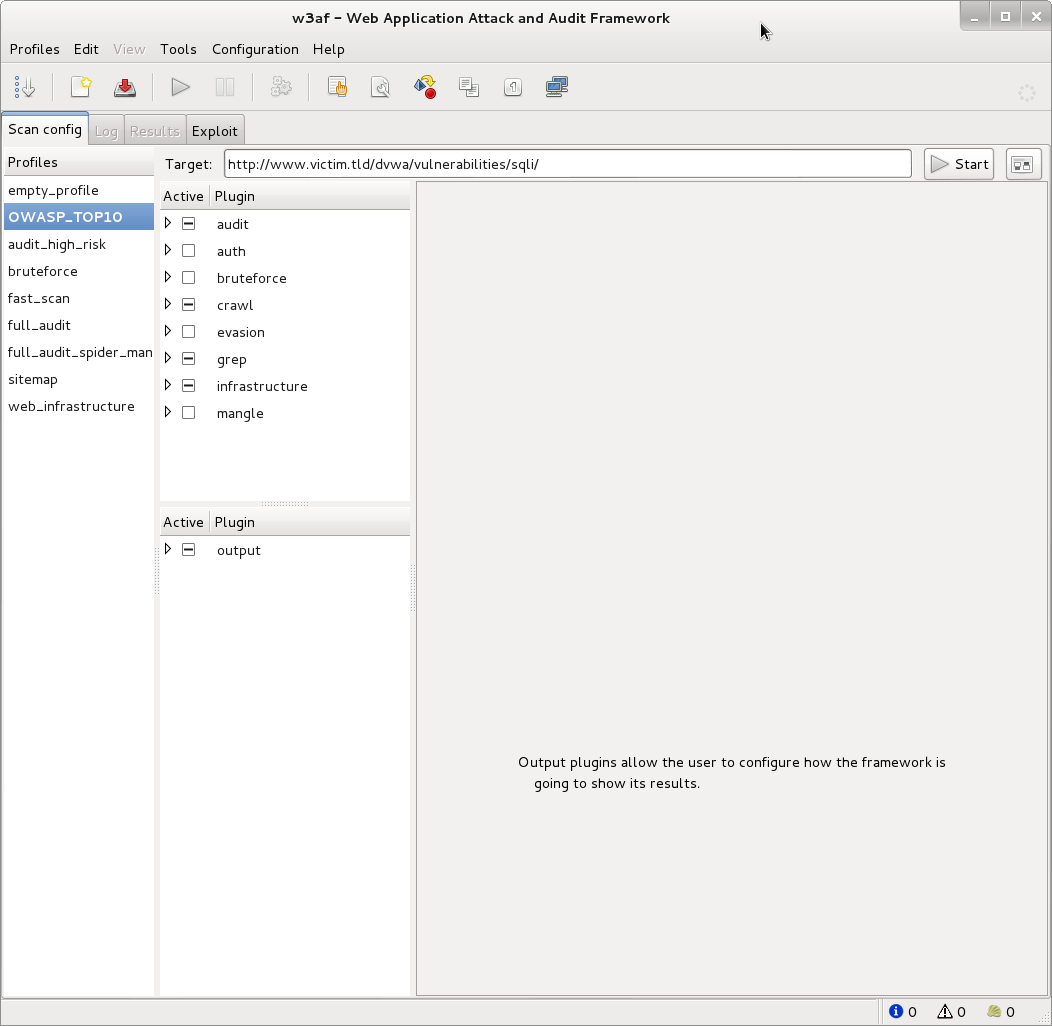
* partie de gauche, intitulée *Profiles*, propose des profils prédéfinis qui effectuent des scans préconfigurés sur la cible. La description de chaque profil apparait dans la partie droite après la sélection du profil ;
* les Plugins sont des tests spécifiques que w3af doit réaliser sur la cible. Par exemple, le profil *OWASP\_TOP10* explique que w3af va scanner la cible à la recherche des dix plus importantes failles de sécurité web (telles qu’identifiées par l'OWASP) ;
* la partie droite change selon ce que l’on a sélectionné. Elle apporte généralement une description de l’élément sélectionné, qu’il soit un profile, une famille de plugins ou un plugin spécifique. Dans certains cas, lors de la sélection d’un plugin, si ce dernier permet d’apporter des configurations, c’est dans cette partie qu’on pourra effectuer le paramétrage.

Chaque profil a des plugins d’activés. Le profil *Empty\_profile* est vide et permet de personnaliser le scan en choisissant les plugins à activer.

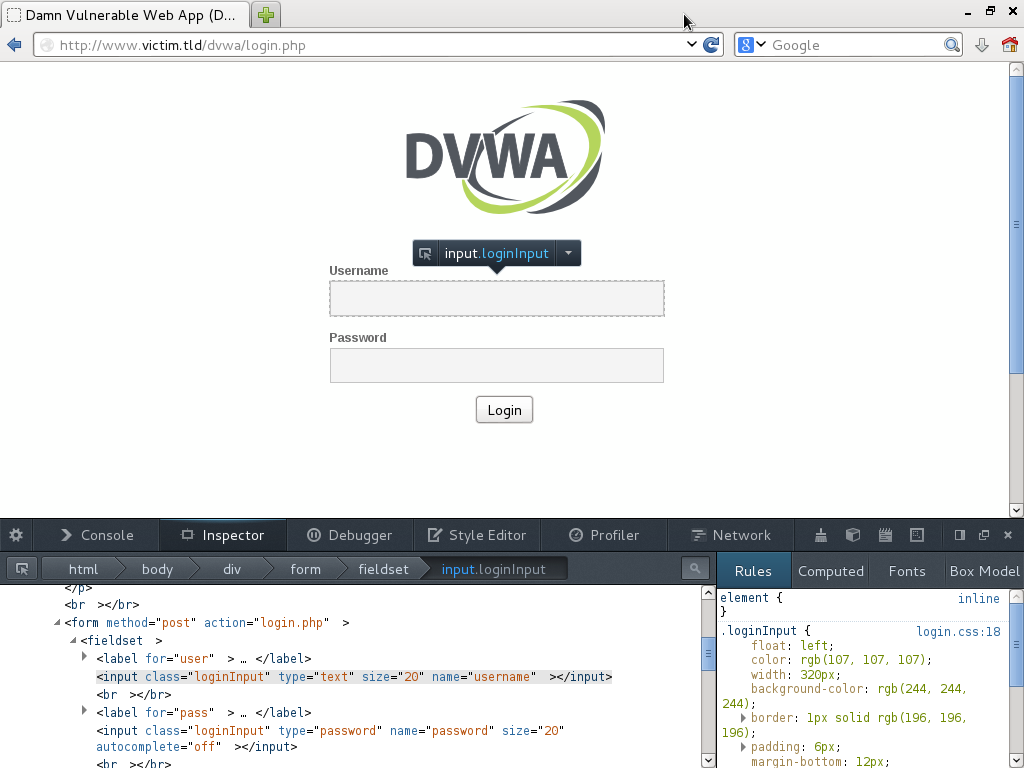
1. Pour lancer W3AF en mode graphique, taper dans un terminal la commande **w3af\_gui**.

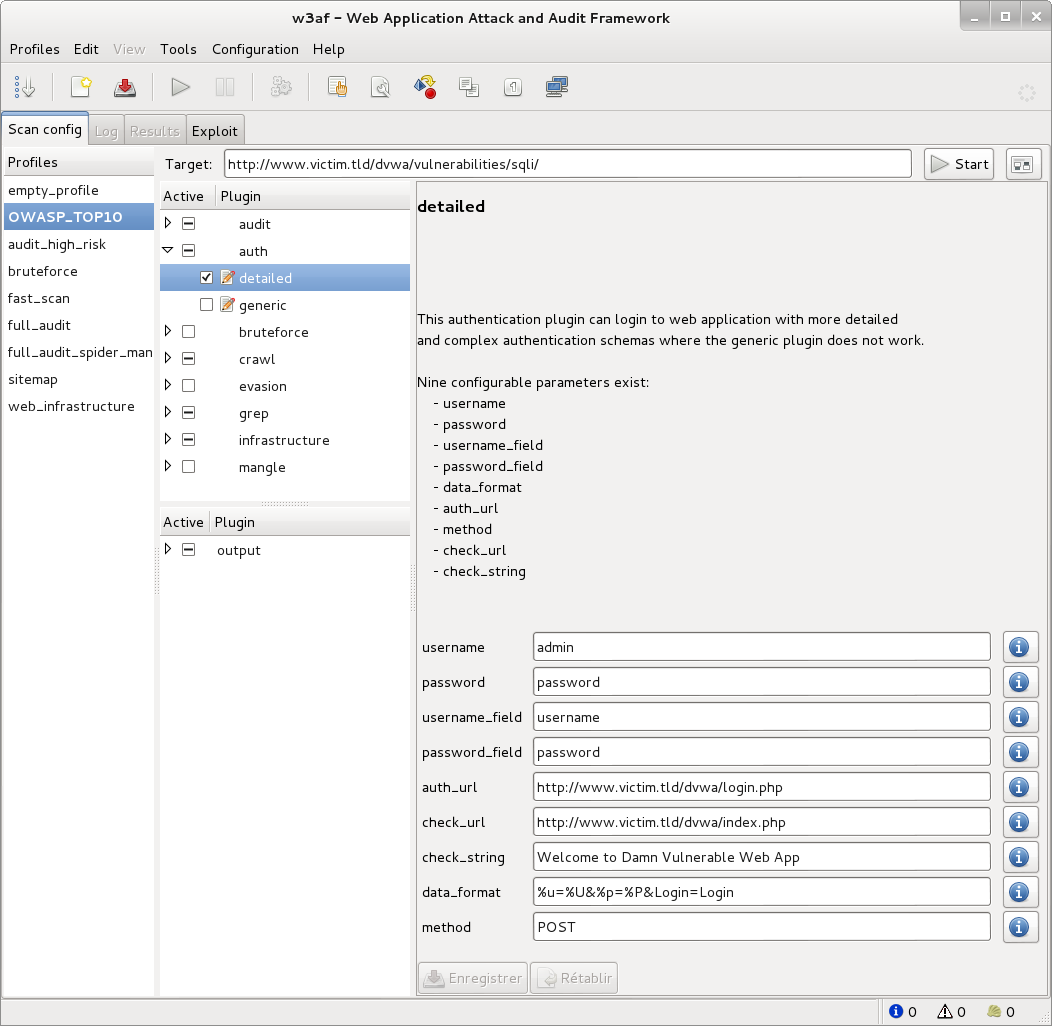
01

1. Commencer par sélectionner le profil approprié, par exemple **OWASP\_TOP10**.  
   Choisir le format d’export du résultat au travers du plugin **output**. Par défaut w3af affiche uniquement le résultat dans sa console et il n’y a pas de possibilité d’exporter le résultat successivement.  
   Ensuite saisir l’adresse IP ou l’URL de la cible dans le champ **Target**.

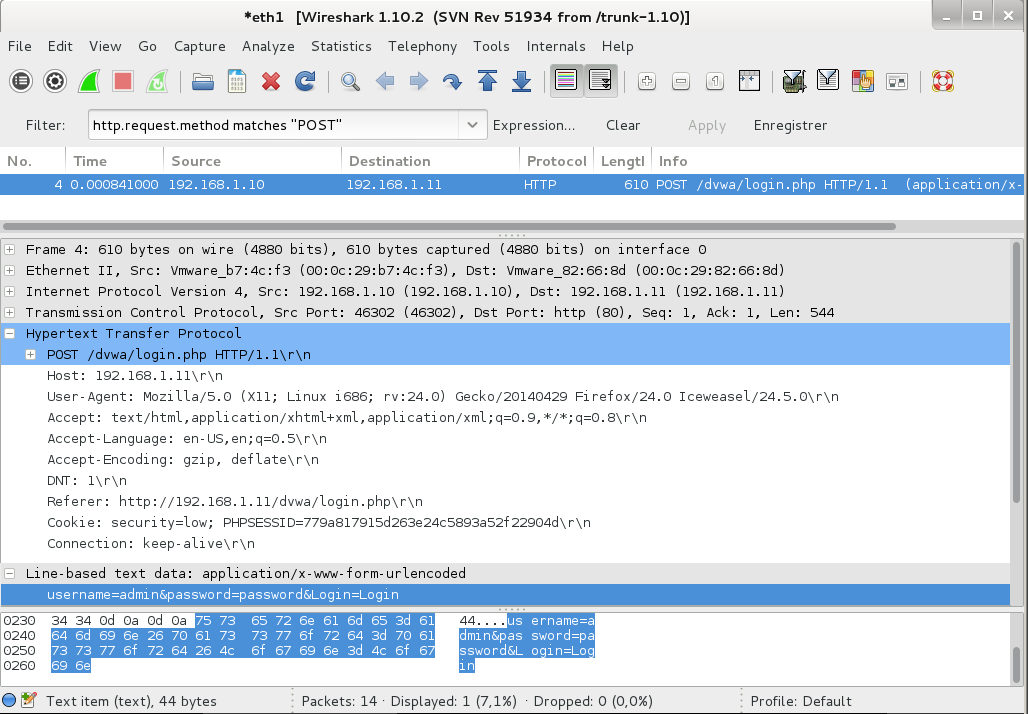


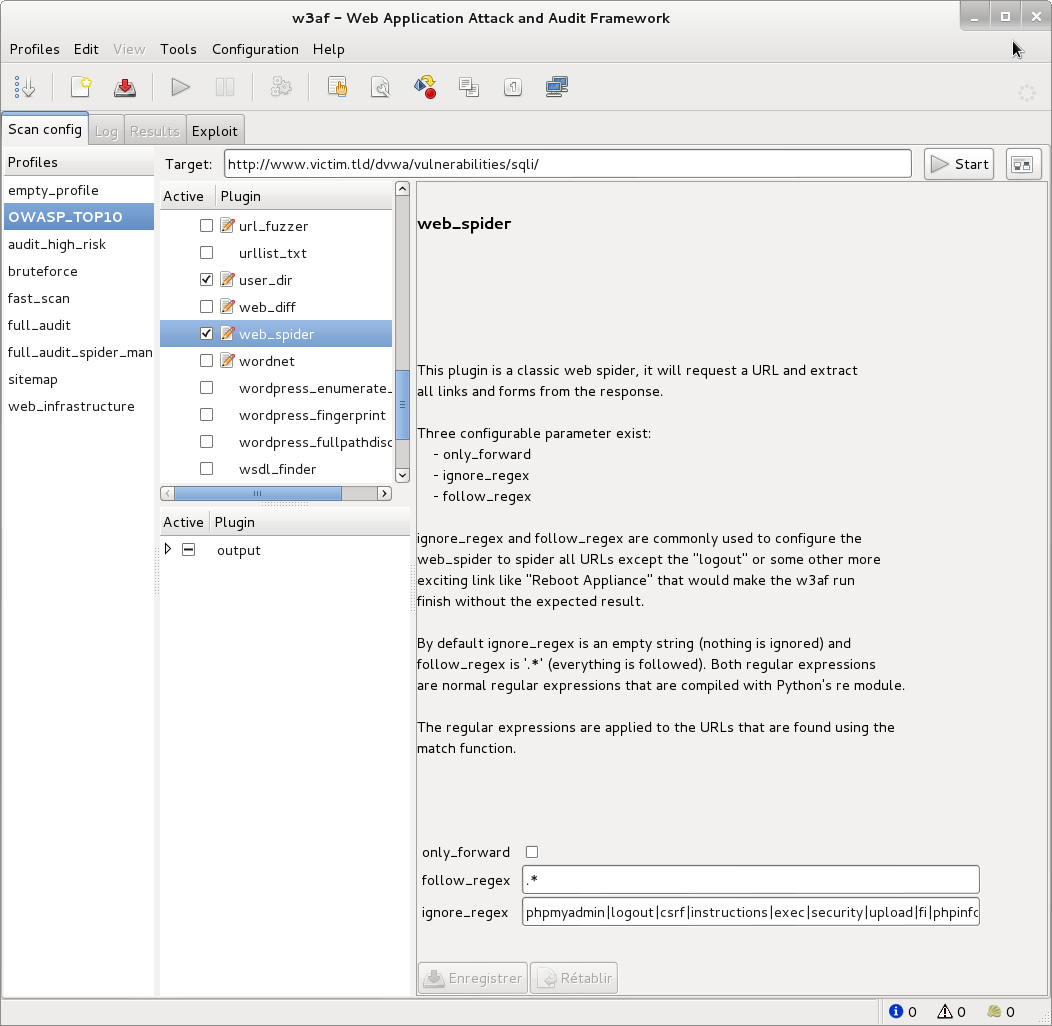
1. Il se peut qu’il faille exécuter un scan sur une application demandant un login. Cette étape est donc facultative. Pour que w3af puisse s’authentifier auprès de l’application web, il faut configurer le module **auth** et le plugin **web\_spider** pour éviter que w3af exécute la page de *logout*, car dans ce cas, w3af se déconnectera du site et ne pourra pas continuer l’analyse des pages. La valeur de **username\_field** et de **password\_field** correspond à l’attribut **name** du champ **username** et **password** du formulaire. Pour récupérer le champ **data\_format** du plugin **auth**, cf. 3.1.  
   Cliquer sur le bouton **Start** pour démarrer le scan.



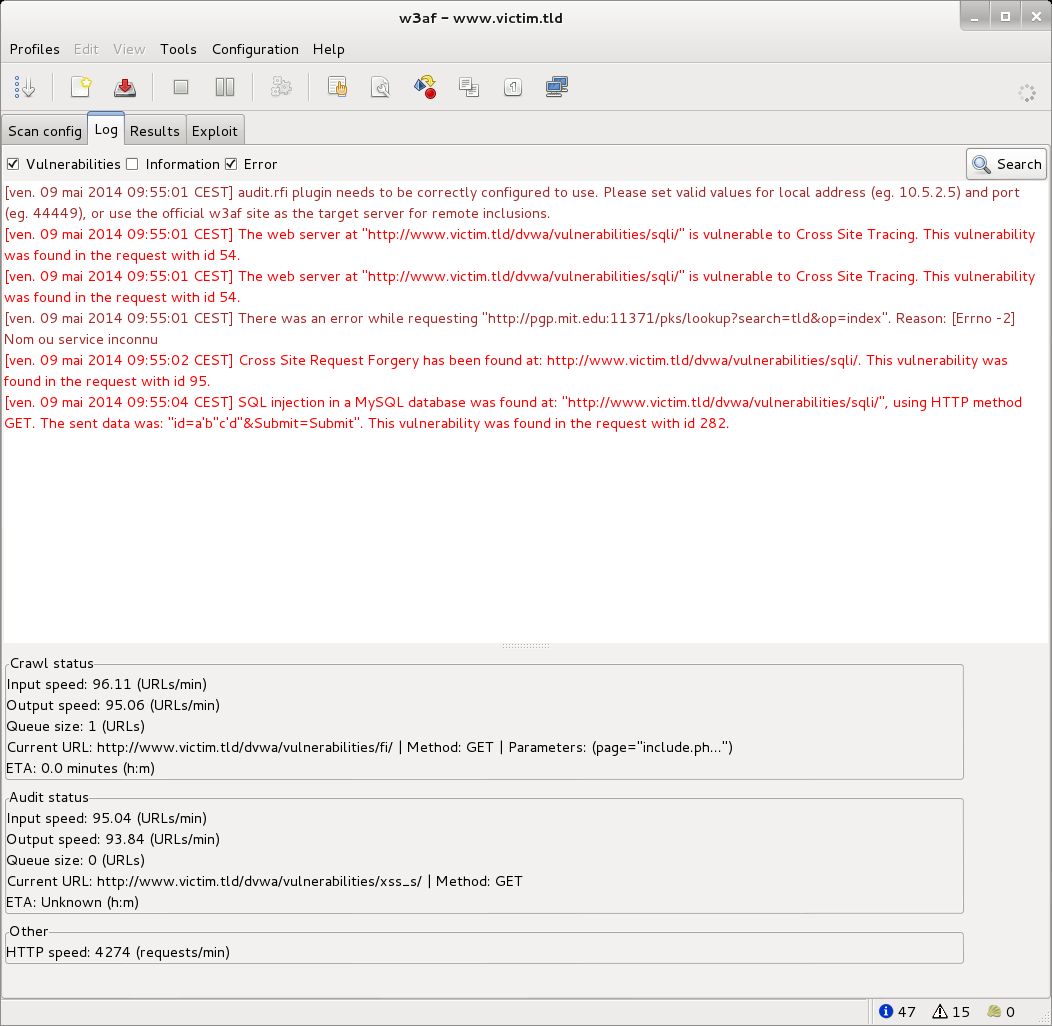


* 1. Pour récupérer les informations de soumission du formulaire, effectuer l’opération d’authentification en capturant au même moment les paquets avec Wireskark. Utiliser le filtre **http.request.method matches "POST"** dans Wireshark pour récupérer le paquet qui nous intéresse.





1. Lorsque le scan est terminé, les onglets **Log**, **Results** et **Exploit** deviennent accessibles et nous pouvons étudier les découvertes en les ouvrants. Dans l’onglet **Log**, décocher les cases **Information** afin de commencer par se focaliser sur les problèmes plus importants.



1. Dans l’onglet **Results**, nouspouvons constater que w3af a détecté une possible injection SQL sur une des pages du site.

