**Procédure d’utilisation Arachni**

**SOMMAIRE**

1 Objet du document 3

2 Arachni 3

2.1 Connexion à Arachni 3

2.2 Utilisation 3

2.2.1 Création du Profile 3

2.2.2 Création et lancement du Scan 7

2.2.3 Résultat du Scan 8

# Objet du document

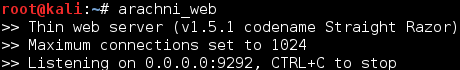
Ce document présente la procédure d’utilisation de l’outil **Arachni**.

# Arachni

## Connexion à Arachni

Arachni se présente sous forme d’interface web.

1. Pour lancer Arachni, taper dans un terminal la commande ***arachni\_web*** et ensuite, tout en gardant le terminal d’ouvert, se connecter à l’adresse **http://localhost:9292**. L'identifiant de connexion par défaut est :  
   username : admin@admin.admin   
   password : administrator

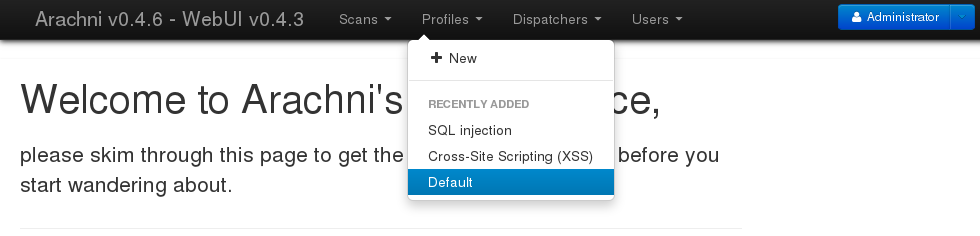


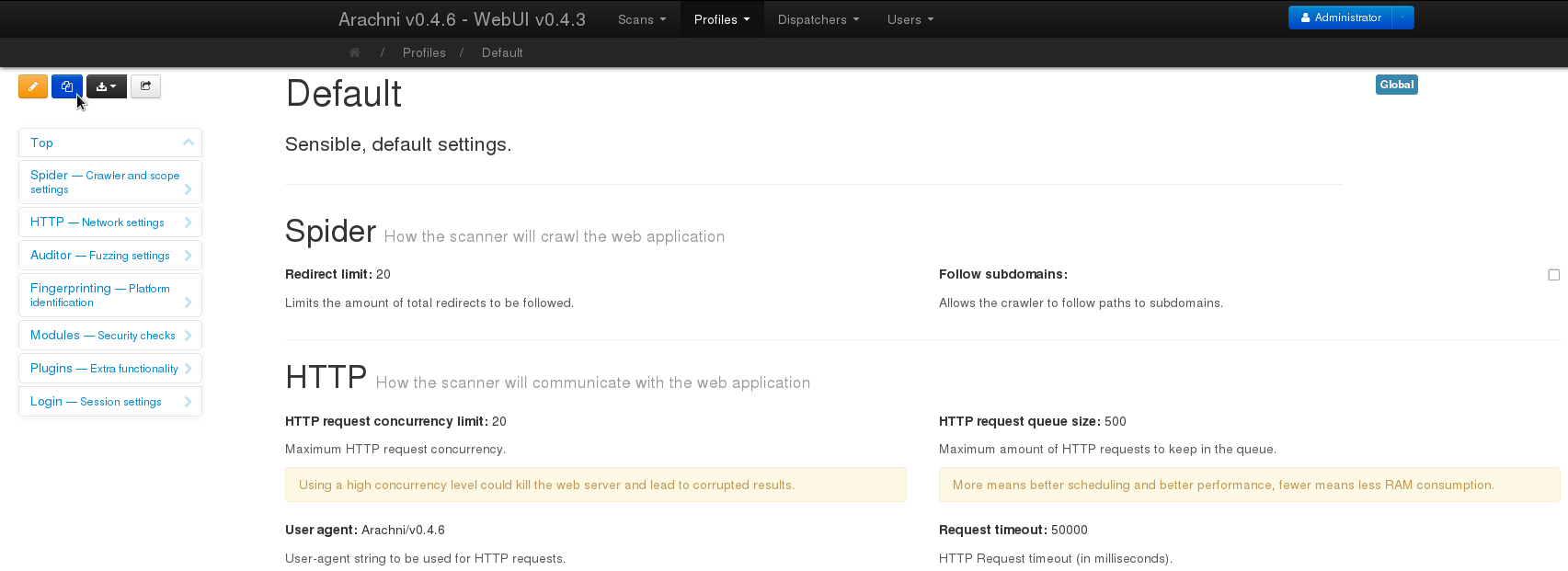
## Utilisation

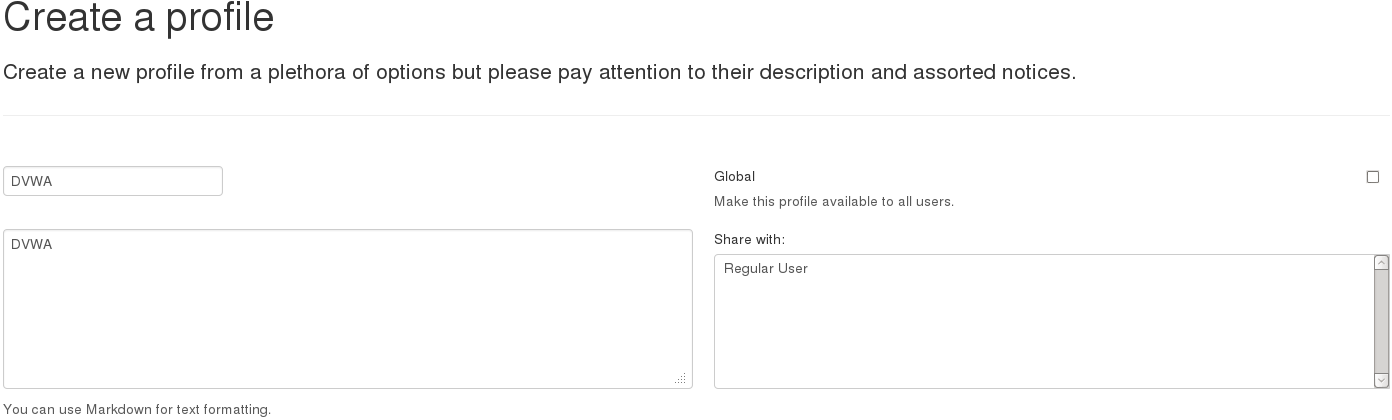
### Création du Profile

La première étape pour effectuer un scan de vulnérabilité est de créer un Profile. Ceci correspond à configurer le scan et les plugins qui seront utilisés.

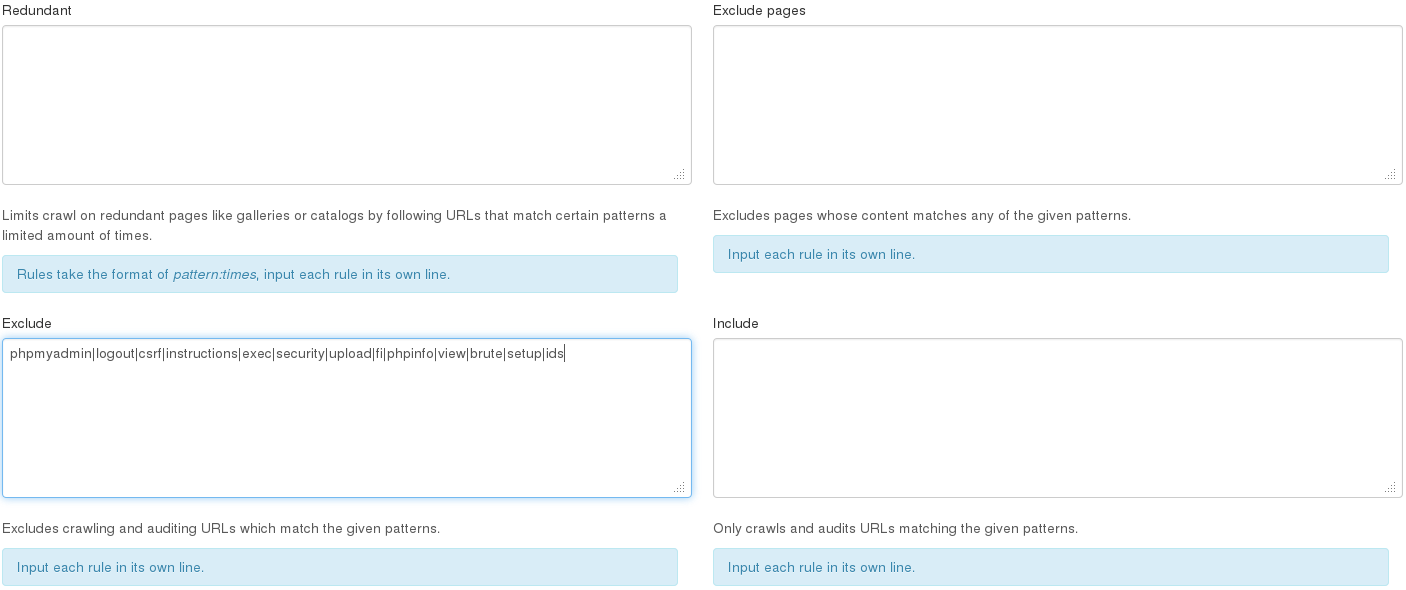
1. La création d'un nouveau profil va s'effectuer à partir d'un profile existant.  
   Pour commencer, se positionner sur le lien **Profile,** situé en haut de la fenêtre, et cliquer sur le modèle **Default**.   
   Cliquer ensuite du l’**icône bleu,** située en haut à gauche de la fenêtre, pour créer un nouveau profile à partir du profile **Default**.   
   Donner un **Nom** et une **Description** au nouveau profile, dans notre cas **DVWA**.



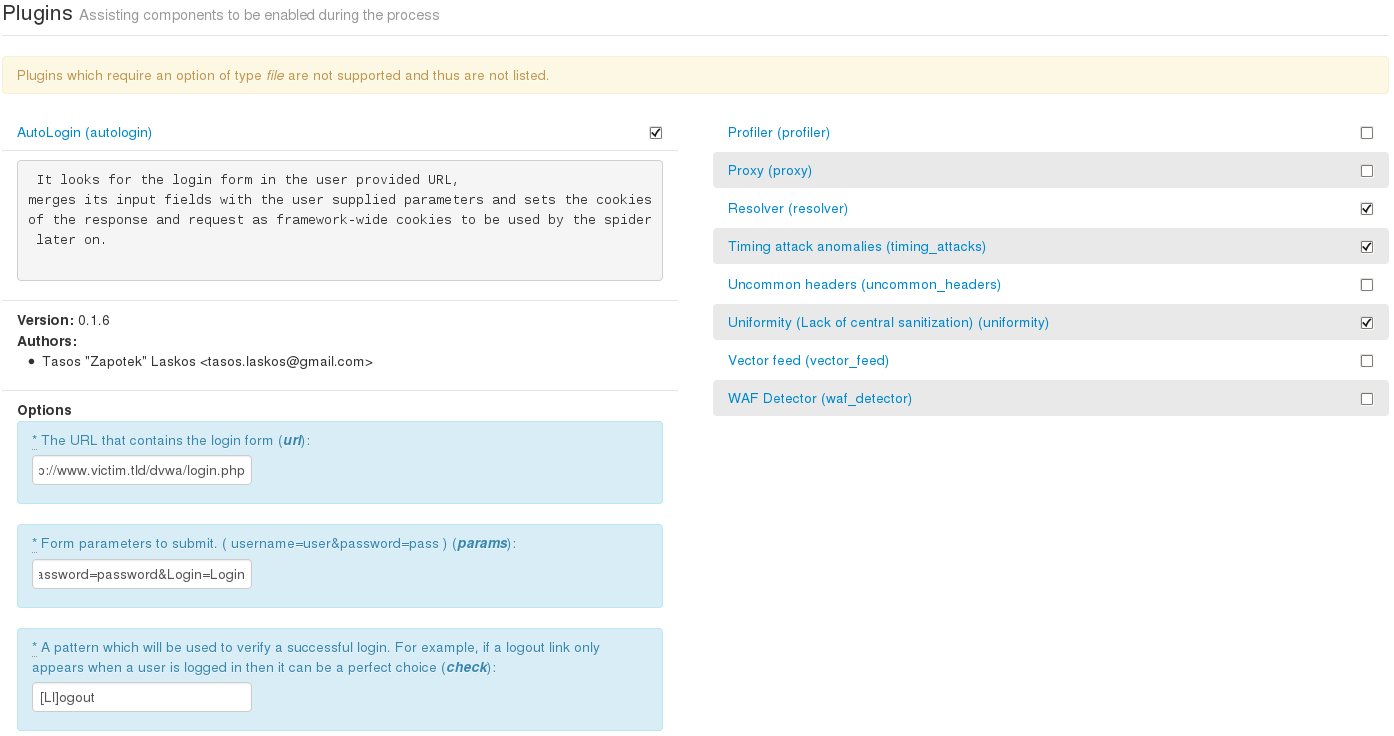




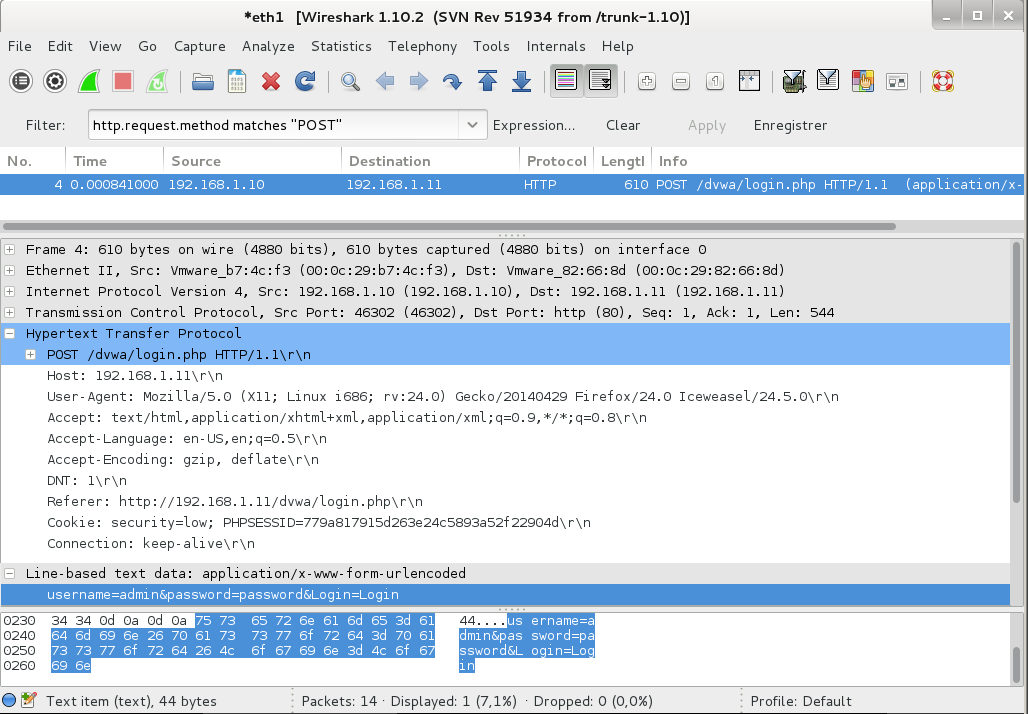
1. Dans le cas d’une application web demandant une authentification, il faut configurer Arachni. Cette étape est donc facultative. Une fois les configurations terminées, cliquer sur le bouton **Create Profile,** situé en bas de la page, pour sauvegarder le nouveau profile.   
   Insérer dans la case **Exclude** les pages devant être exclues du scan. En particulier il faut exclure la page de logout afin qu’Arachni ne se déconnecte pas de l’application en scannant la page de déconnexion.



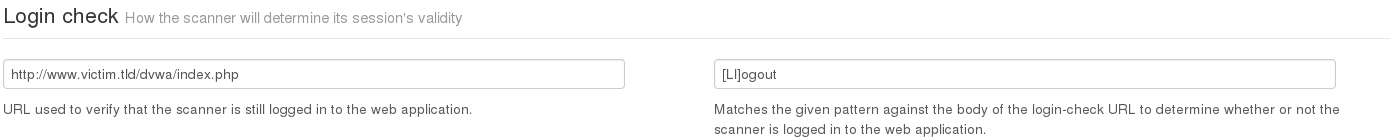
* 1. Il faut configurer le plugin **AutoLogin** pour qu’Arachni puisse s’authentifier sur l’application. Cocher donc la case correspondante au plugin et insérer les paramètres suivants :   
     - L’URL où se trouve le formulaire de connexion : **http://www.victim.tld/dvwa/login.php**  
     - La string de connexion permettant la soumission du formulaire (cf. 2.1.1 pour voir comment récupérer cette string) : **username=admin&password=password&Login=Login**  
     - La string permettant de vérifier qu’Arachni a bien réussi à s’authentifier. Il faut choisir une string qui est commune à toutes les pages : **[Ll]ogout**



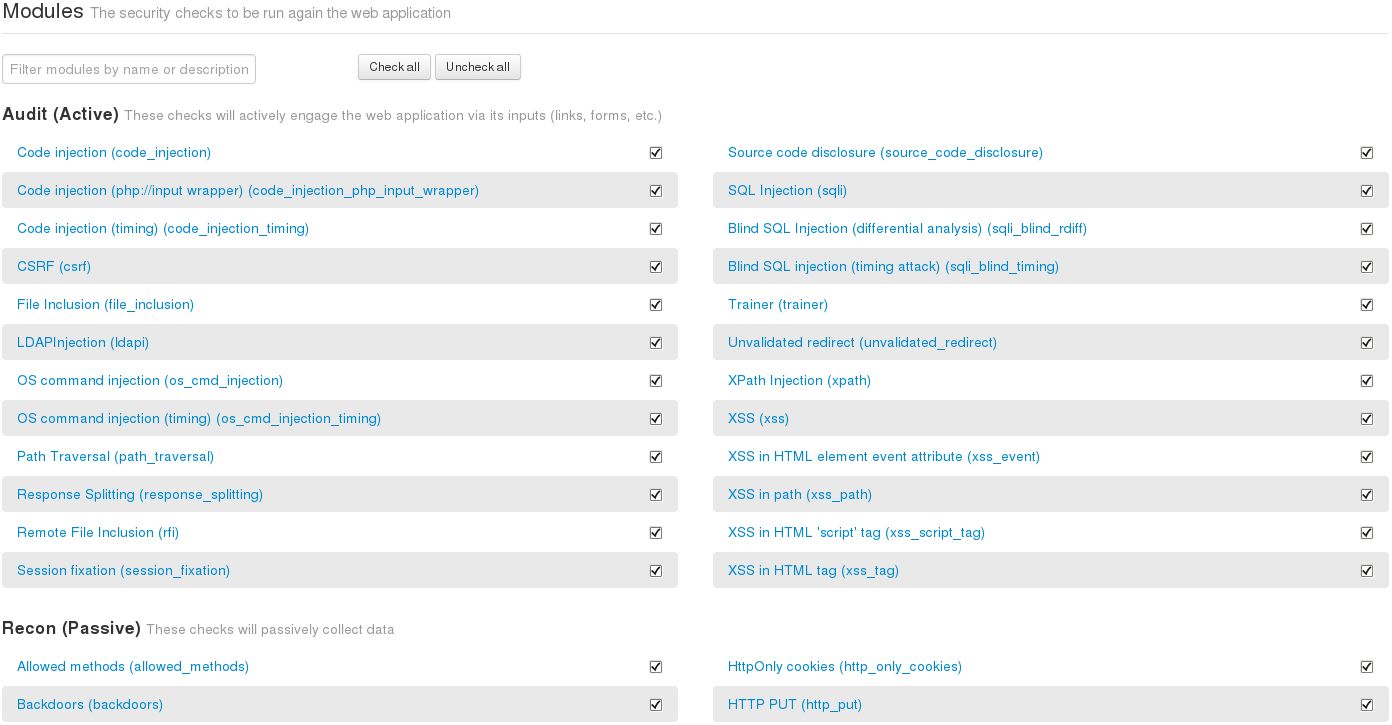
* + 1. Pour récupérer les informations de soumission du formulaire, effectuer l’opération d’authentification en capturant au même moment les paquets avec Wireskark. Utiliser le filtre **http.request.method matches "POST"** dans Wireshark pour récupérer le paquet qui nous intéresse.



* 1. Configurer le **Login check**, avec l’URL qui s’affiche une fois l’authentification réussi : **http://www.victim.tld/dvwa/index.php** et une string contenue dans cette page : **[Ll]ogut**



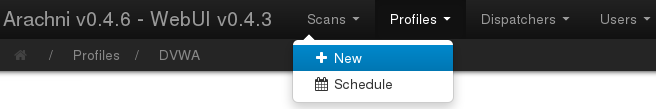
1. On peut maintenant choisir les **Modules** (Plugins) qu’on souhaite activer lors de l’exécution du scan. Une option qui peut être intéressante de coucher est **Fuzz methods**, qui scan les éléments aussi bien avec des requêtes GET que des requetés POST. Attention, cette option double le temps du scan.



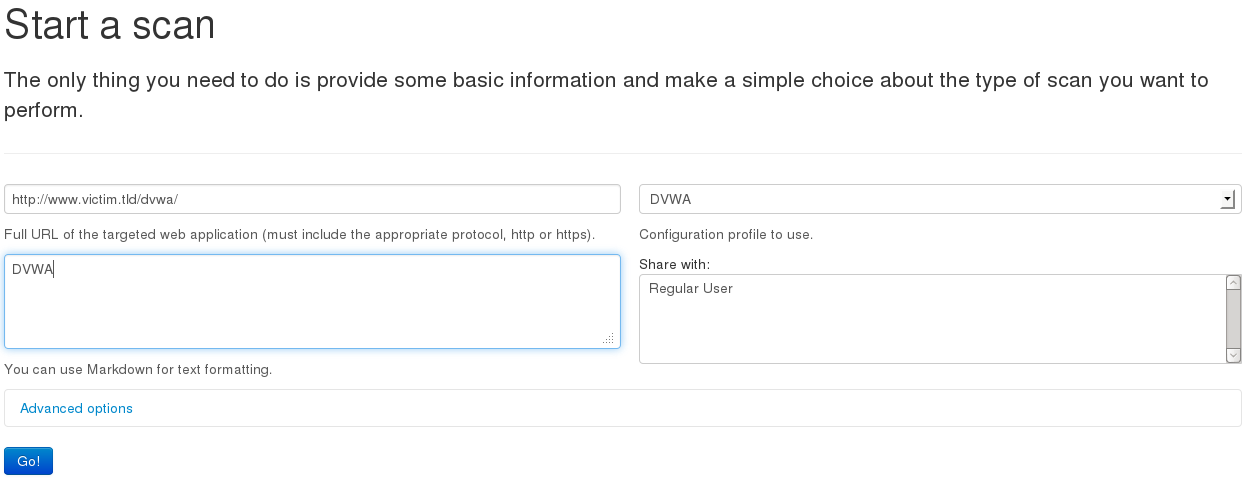
### Création et lancement du Scan

Maintenant que le nouveau Profile est crée, il est possible de créer un Scan.

1. Pour créer un nouveau Scan, se positionner sur le lien **Scans** et cliquer sur **New**.

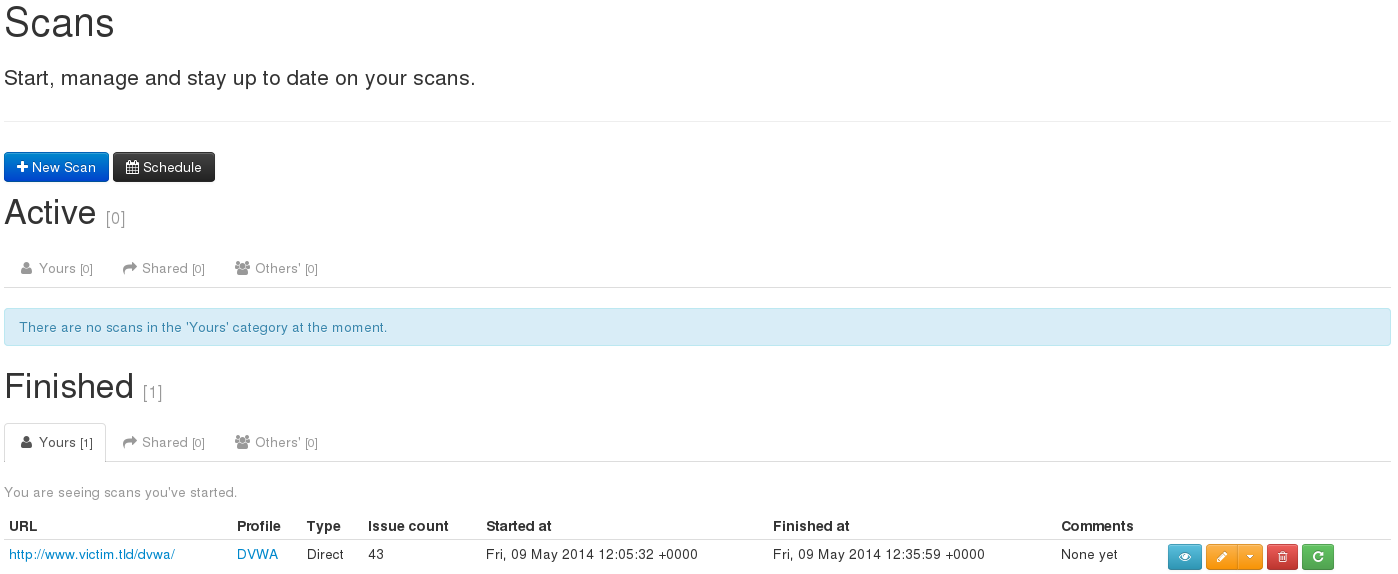


1. Spécifier l’URL du site à analyser, dans notre cas **http://www.victim.tld/dvwa/**. Choisir le Profile souhaité. Donner une description.  
   Pour lancer le scan, cliquer sur le bouton **Go !**.   
   **Attention**: ne pas oublier de mettre le dernier « / » à la fin de l’URL à scanner.



### Résultat du Scan

1. Une fois le scan terminé, l’interface d’Arachni vous en informe.  
   Pour visualiser les détails, cliquer sur le bouton bleu en forme d’œil en correspondance du scan (dans notre cas le scan se nomme DVWA).



1. La fenêtre suivante donne un aperçu du résultat. Nous pouvons, par exemple, constater plusieurs URL vulnérables à XSS et à l’injection SQL.

