Sécurité - TP
Injections SQL

Virginie Van den Schrieck

5 octobre 2015

L'objectif de ce TP est de permettre aux étudiants de bien comprendre le fonctionnement des attaques par injection SQL en expérimentant par soi-même ces attaques dans un environnement dédié.

Le temps prévu de ce TP est d'environ trois heures, séance comprise, en binôme.

Le TP se base sur le labo PentesterLab *From SQL Injection to Shell*. L'énoncé de ce labo se trouve à l'URL `https://pentesterlab.com/exercises/from_sqli_to_shell/`. Pour la mise en place de l'environnement, il faut télécharger l'image iso de la machine virtuelle, et la booter avec VMWare.

Au niveau de la configuration, il y a lieu d'ajuster le layout du clavier. La distribution utilisée étant une Debian, la commande permettant la reconfiguration est la suivante :

```
sudo dpkg-reconfigure console-data
```

L'énoncé du labo est très détaillé. Vous pouvez sauter la section *Fingerprinting*, puisque nous travaillerons ce sujet ultérieurement. Il vous est par contre demandé de réaliser au minimum les exercices des sections suivantes :

- *Detection of SQL Injection*
- *Exploitation of SQL Injections*

Les curieux ne manqueront pas de réaliser la dernière section, qui reste néanmoins facultative.

Tout au long du TP, il vous est demandé, pour chaque vulnérabilité identifiée et testée, de proposer une contre-mesure permettant de la contrer. Dans le cadre de l'environnement de test utilisé, vous pourriez avoir besoin de consulter les fichiers PHP utilisés par le serveur web. Ceux-ci se trouvent dans le répertoire `/var/www`.

1 Déliverables

Avant le début du prochain cours, vous posterez sur le Campus Virtuel un document PDF d'une page ou deux documentant le travail effectué et proposant des contre-mesures pour corriger les vulnérabilités rencontrées.