TP 1 : Injection SQL et XSS

Introduction à la sécurité Web

Olivier LASNE - olivier@lasne.pro

2020-12-11

Ressources

Pour ce TP, nous allons nous entrainer sur les ressources suivantes :

- La machine virtuelle **OWASP Broken Web Apps**
- La machine virtuelle **Web for pentester I**

Si vous terminez ce TP. Vous pouvez également aller voir les sites suivants :

- https://root-me.org
- https://portswigger.com/web-security

Pour vous aider vous pouvez utiliser le cours, mais aussi :

- SQL :
  - **https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection**
  - **https://portswigger.net/web-security/sql-injection**
- XSS :
  - **https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XSS%20Injection**
  - **https://portswigger.net/web-security/cross-site-scripting**

Introduction

Le but de ce TP va être de vous familiarisez avec l'exploitation des failles d'*injection SQL* et *XSS*.
Ce sont les deux familles de failles les plus improtantes en sécurité Web.

Configuration

La procédure d'**installation de BurpSuite** est décrite dans le document **burp.pdf**. L'importation des machines virtuelles sera faite **au début du TP**.

OWASP Broken Web App

L'adresse IP de la machine est indiquée dans la fenêtre Virtual Box au démarrage.

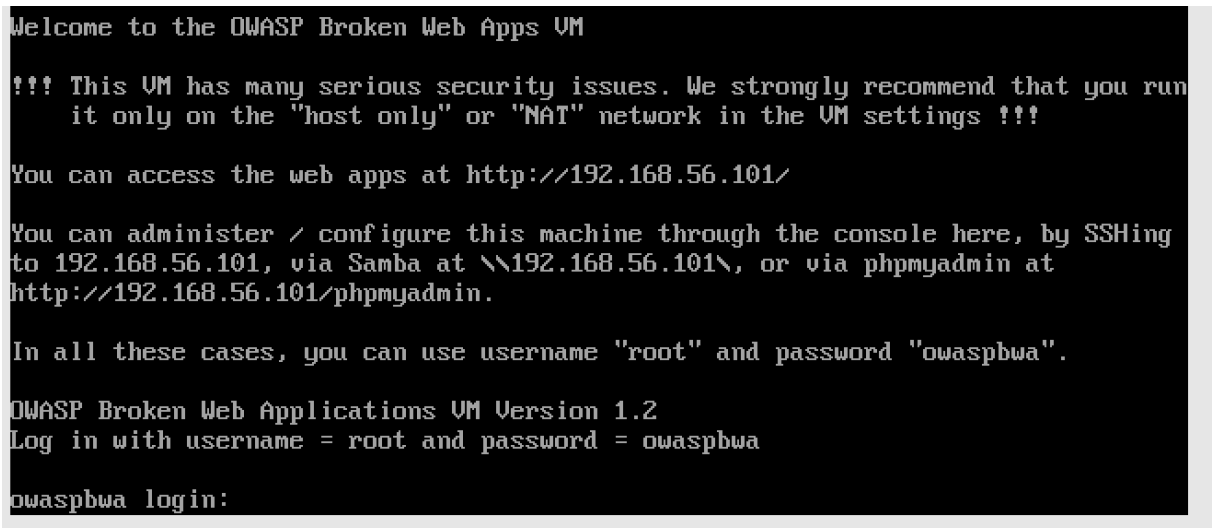

FIG. 1: OWASP Broken Web App boot

Entrez dans votre navigateur l'URL indiquée.
Cette machine propose plusieurs applications. Chosissez **OWASP Bricks**.

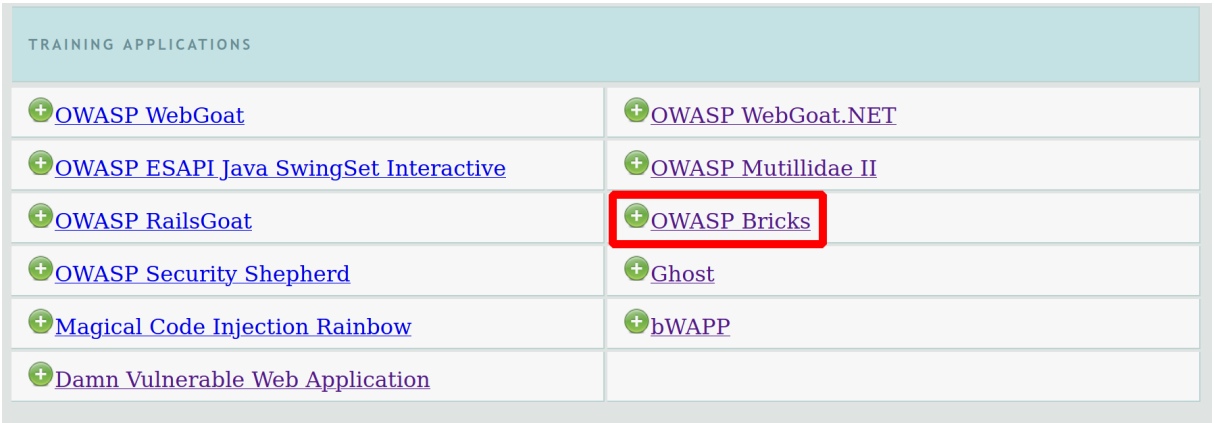

FIG. 2: Les applications vulnérables

Les pages **Login** et **Content** devrait vous permettre de vous familiariser avec ces failles.

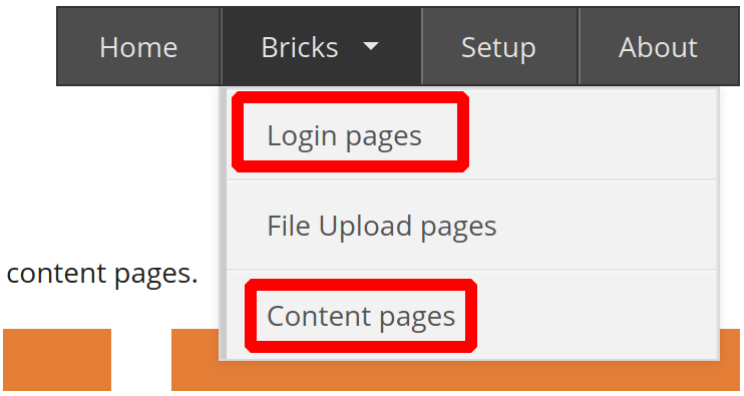

FIG. 3: Pages d'exercices

Dans ces exercises, la requête SQL effectuée par l'application est affichée en dessous. Mais n'oubliez pas de vous familiarisez avec **Burp**. Vous en aurez besoin pour la suite (et certains de ces exercices.)

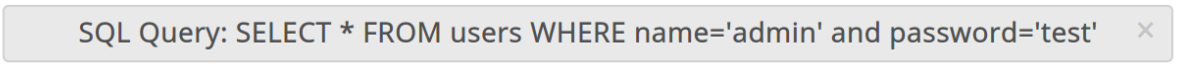

FIG. 4: Requête SQL

Web for pentester

Une fois ces exercises terminés, vous pouvez aller tester ceux de **Web for Pentester**.

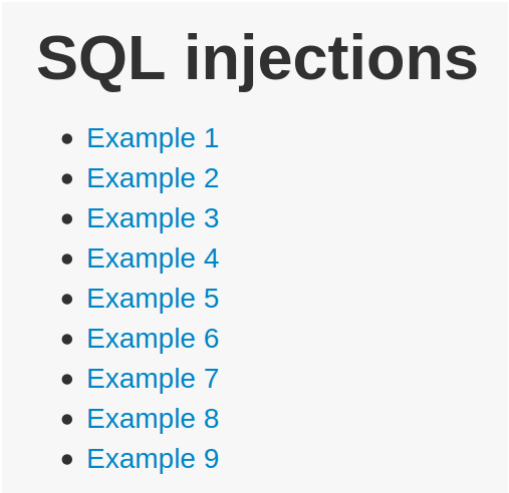

FIG. 5: Exercices SQL

L'ISO dispose de neuf exercices. Certains sont des cas un peu particuliers, et il est donc normal qu'il vous posent problème.

Vous pouvez regader la correction à l'adresse suivante. Mais je vous invite fortement à tester par vous-même avant.
https://www.pentesterlab.com/exercises/web_for_pentester/course

XSS

Vous pouvez vous entrainer sur les exercices de XSS de **web for pentester**.

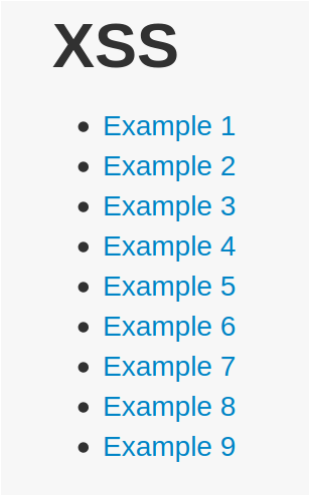

FIG. 6: Web for Pentester XSS

Si je avez terminer, je vous invite à vous essayer aux exercices de PortSwigger **https://portswigger.net/web-security/all-labs#cross-site-scripting** (Correction disponible).
Ou à ceux de root-me **https://root-me.org** (pas de solutions publiques).