

---

# **TP 1 : Injection SQL et XSS**

Introduction à la sécurité Web

Olivier LASNE - [olivier@lasne.pro](mailto:olivier@lasne.pro)

2020-12-11

## Ressources

Pour ce TP, nous allons nous entraîner 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 familiariser avec l'exploitation des failles d'*injection SQL* et *XSS*.  
Ce sont les deux familles de failles les plus importantes 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.

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.56.101/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Samba at \\192.168.56.101\, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

FIG. 1: OWASP Broken Web App boot

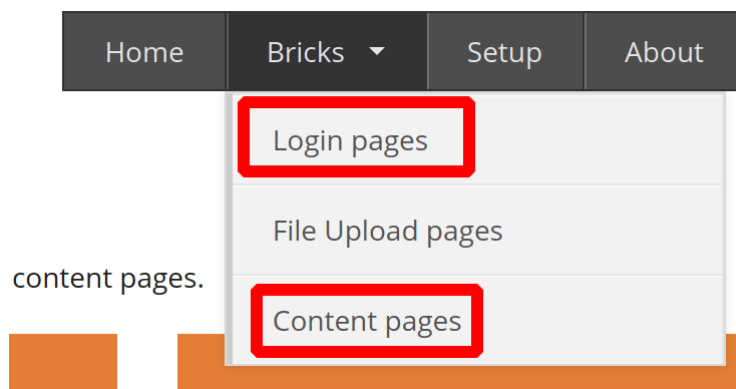
Entrez dans votre navigateur l'URL indiquée.

Cette machine propose plusieurs applications. Choisissez **OWASP Bricks**.

TRAINING APPLICATIONS	
<a href="#">+ OWASP WebGoat</a>	<a href="#">+ OWASP WebGoat.NET</a>
<a href="#">+ OWASP ESAPI Java SwingSet Interactive</a>	<a href="#">+ OWASP Mutillidae II</a>
<a href="#">+ OWASP RailsGoat</a>	<a href="#">+ OWASP Bricks</a>
<a href="#">+ OWASP Security Shepherd</a>	<a href="#">+ Ghost</a>
<a href="#">+ Magical Code Injection Rainbow</a>	<a href="#">+ bWAPP</a>
<a href="#">+ Damn Vulnerable Web Application</a>	

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 exercices, 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.)

```
SQL Query: SELECT * FROM users WHERE name='admin' and password='test' ×
```

**FIG. 4:** Requête SQL

## Web for pentester

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

## SQL injections

- [Example 1](#)
- [Example 2](#)
- [Example 3](#)
- [Example 4](#)
- [Example 5](#)
- [Example 6](#)
- [Example 7](#)
- [Example 8](#)
- [Example 9](#)

**FIG. 5:** Exercices SQL

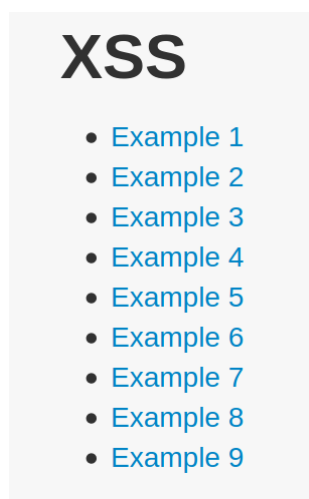
L'ISO dispose de neuf exercices. Certains sont des cas un peu particuliers, et il est donc normal qu'il vous posent problème.

Vous pouvez regarder 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](https://www.pentesterlab.com/exercises/web_for_pentester/course)**

## XSS

Vous pouvez vous entraîner 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).