Déploiement application DVWA

Contexte :

Badénio Tech, jeune ESN, votre employeur, a recruté de nouveaux développeurs juniors et souhaite les sensibiliser aux mécanismes de différentes failles de sécurité des applications web afin qu'ils intègrent très tôt les bonnes pratiques de sécurité. Afin de cibler au mieux votre démonstration, vous vous appuyez sur les recommandations et guide de tests proposés par l'OWASP (Open Web Application Security Project, https://owasp.org/)

Présentation de l'application :

Damn Vulnerable Web App (DVWA) est une application Web PHP/MySQL vulnérable. Ses principaux objectifs sont d'aider les professionnels de la sécurité à tester leurs compétences et leurs outils dans un environnement juridique, d'aider les développeurs Web à mieux comprendre les processus de sécurisation des applications Web et d'aider les enseignants/étudiants à enseigner/apprendre la sécurité des applications Web.

Votre tâche :

Afin de répondre à ce besoin, vous préparez des tests d'intrusion sur l'application web vulnérable DVWA que vous devez présenter dans un premier temps via un document puis lors d'un webinaire.

Installer les OS Kali et ubuntu. Installer l'application et préparer la plateforme de tests.
Mettre en évidence et prévenir, sur différents niveaux de sécurité, les failles : injections SQL, injections XXE et XEE, les attaques XSS et CSRF.

Compétences mises en œuvre :

- ➢ Réaliser les tests d'intégration et d'acceptation d'un service
- ➢ Déployer un service

Ubuntu

Ubuntu est un distributeur Linux open source basé sur Debian (système d'exploitation et une distribution de logiciels libres). Le développement de ce système d'exploitation est dirigé par Canonical. Il s'agit d'une société basée au Royaume-Uni qui a été fondée par Mark Shuttleworth.

J'utilise le logiciel **VirtualBox**, c'est un logiciel Open Source proposé par Oracle (SGBD (système de gestion de bases de données) édité par la société du même nom (Oracle Corporation)) permettant la virtualisation de système d'exploitation (OS).

Tout d'abord je me connecte en SSH :

```
dev@mbp-server [18:22:02] [~]
[-> % ssh manorie@192.168.1.111
manorie@192.168.1.111's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-39-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

97 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Apr  9 17:08:57 2022 from 192.168.1.26
```

Sur ma machine virtuelle ubuntu, j'installe la pile logiciel LAMP, acronyme de Linux, Apache, MySQL et PHP. Ensemble, ils constituent un ensemble de logiciels éprouvés pour la création d'applications Web performantes.

```
$ sudo apt update
```

```
$ sudo apt install apache2
```

```
$ sudo apt install mysql-server
```

```
$ sudo apt install php libapache2-mod-php php-mysql
```

Installation DVWA

```
$ cd /var/www/html
```

```
$ sudo apt install git
```

```
$ git clone https://github.com/digininja/DVWA
```

```
manorie@manorie:/var/www/html$ cd DVWA
manorie@manorie:/var/www/html/DVWA$ ls
about.php      dvwa          instructions.php  README.tr.md  tests
CHANGELOG.md   external      login.php         README.zh.md  vulnerabilities
config         favicon.ico   logout.php        robots.txt
COPYING.txt    hackable      phpinfo.php       SECURITY.md
database       ids_log.php   php.ini           security.php
docs           index.php     README.md         setup.php
```

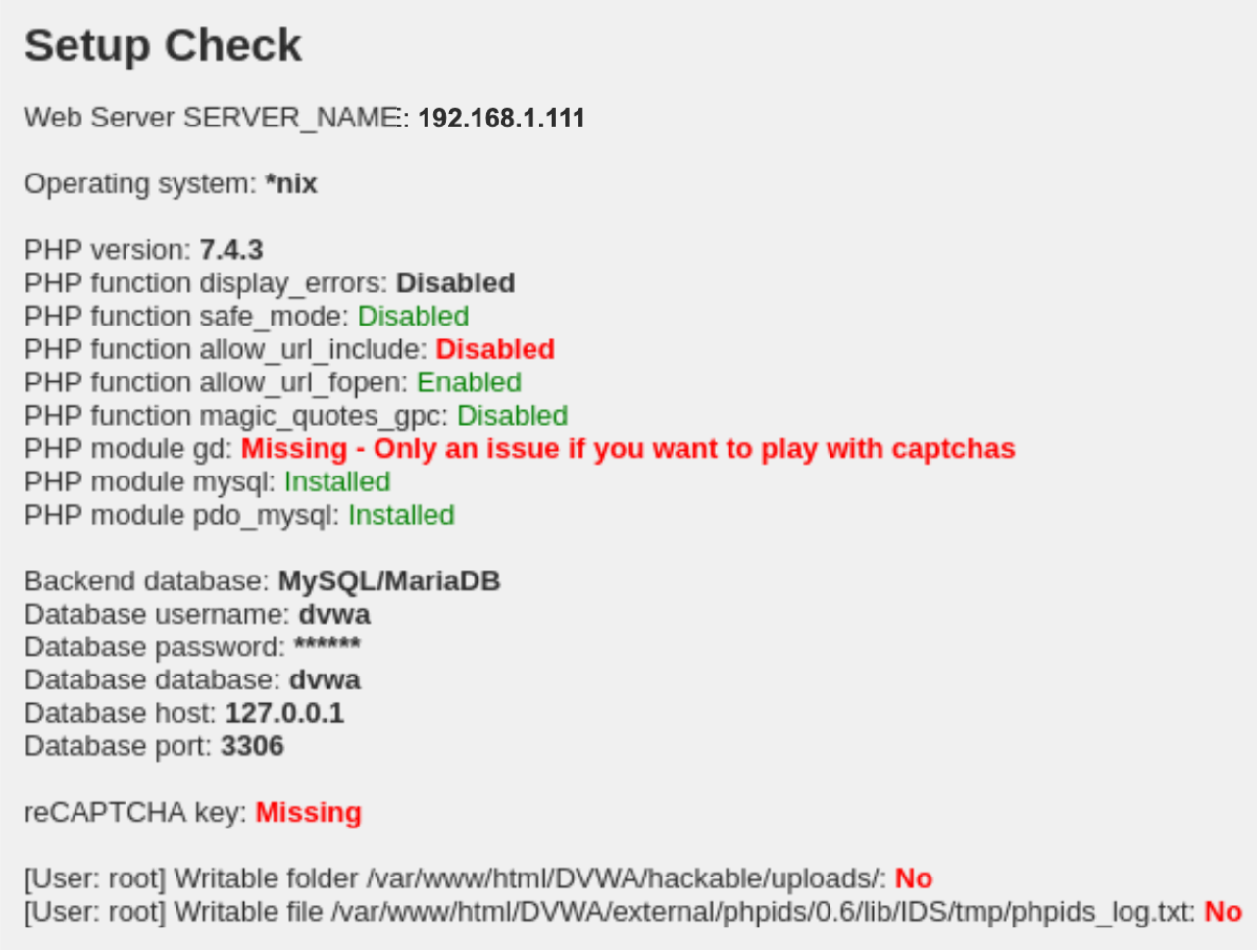
A présent il faut configurer l'application.

```
$ cd /var/www/html/DVWA/config
```

```
$ ll
```

```
$ cp config.inc.php.dist config.inc.php
```

Je lance l'application sur Google.



A présent il faut mettre à jour les droits des fichiers, pour ce faire :

```
manorie@manorie:/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp$ cd
manorie@manorie:~$ sudo su
root@manorie:/home/manorie# apt install git^C
root@manorie:/home/manorie# ^C
root@manorie:/home/manorie# exit
exit
manorie@manorie:~$ cd /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/
manorie@manorie:/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp$ sudo su
root@manorie:/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp# chgrp www-data phpids_log.txt
root@manorie:/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp# chmod g+w phpids_log.txt
root@manorie:/var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp# cd /var/www/html/DVWA/hackable/
root@manorie:/var/www/html/DVWA/hackable# chgrp www-data uploads/
root@manorie:/var/www/html/DVWA/hackable# chmod g+w uploads/
root@manorie:/var/www/html/DVWA/hackable# cd ..
root@manorie:/var/www/html/DVWA# chgrp www-data config/
root@manorie:/var/www/html/DVWA# chmod g+w config/
root@manorie:/var/www/html/DVWA#
```

Setup Check

Web Server SERVER_NAME: **192.168.1.111**

Operating system: ***nix**

PHP version: **7.4.3**
PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: ******
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

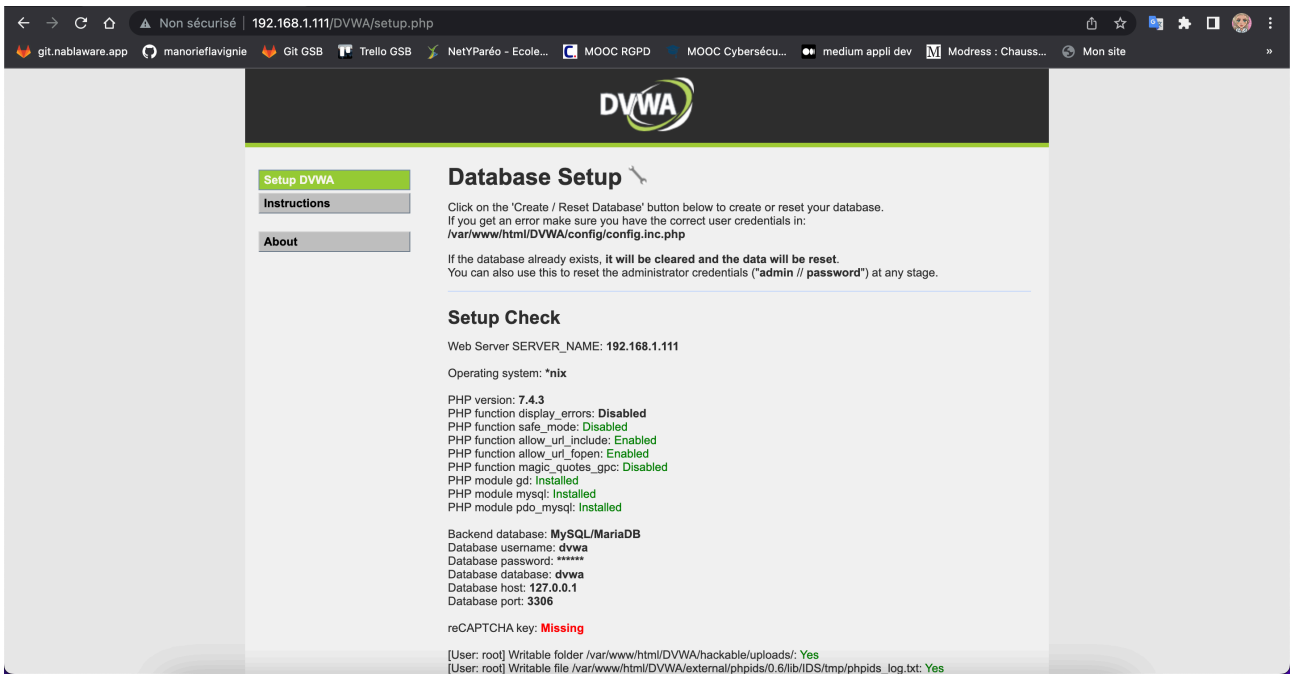
```
$ cd /etc/php/7.4/apache2
```

```
$ nano php.ini
```

```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = Off
```

Devient :

```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On
```



Pour finir il faut configurer la base de données.

```
root@manorie:/etc/php/7.4/apache2# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 881
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

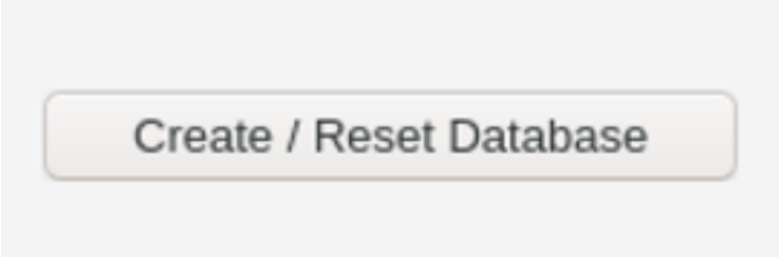
```
mysql> CREATE USER ‘dvwa’@‘localhost’ IDENTIFIED BY ‘p@ssw0rd’;
```

```
mysql> CREATE DATABASE dvwa;
```

```
mysql> GRANT ALL PRIVILEGES ON dvwa.* TO ‘dvwa’@‘localhost’;
```

```
mysql> flush privileges;
```

Puis il faut cliquer sur :



L’installation de l’application DVWA est terminée, pour se connecter : username = admin / password = password.