

Mission Installation Mutillidae

DABO ELIJAH

30/05/24

COMPTE RENDU

1er Étape : Mutillidae

Premièrement je me suis connecté à la clé SSH avec :
ssh eljhdb@ssh-eljhdb.awlaysdata.net

Puis je me positionne dans le bon dossier grâce à la commande cd /home/eljhdb/www/ et je clone le dépôt Mutillidae depuis GitHub avec la commande : git clone <https://github.com/webpwnized/mutillidae.git>

```
eljhdb@ssh1:~$ cd /home/eljhdb/
eljhdb@ssh1:~$ cd /home/eljhdb/www/
eljhdb@ssh1:~/www$ git clone https://github.com/webpwnized/mutillidae.git
Cloning into 'mutillidae'...
remote: Enumerating objects: 5025, done.
remote: Counting objects: 100% (1357/1357), done.
remote: Compressing objects: 100% (501/501), done.
Receiving objects: 30% (1508/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 31% (1558/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 32% (1608/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 33% (1659/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 34% (1709/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 35% (1759/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 36% (1809/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 37% (1860/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 38% (1910/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 39% (1960/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 40% (2010/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 41% (2061/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 42% (2111/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 43% (2161/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 44% (2211/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 45% (2261/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 46% (2311/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 47% (2361/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 48% (2411/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 49% (2461/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 50% (2511/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 51% (2561/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 52% (2611/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 53% (2661/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 54% (2711/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 55% (2761/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 56% (2811/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 57% (2861/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 58% (2911/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 59% (2961/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 60% (3011/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 61% (3061/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 62% (3111/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 63% (3161/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 64% (3211/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 65% (3261/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 66% (3311/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 67% (3361/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 68% (3411/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 69% (3461/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 70% (3511/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 71% (3561/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 72% (3611/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 73% (3661/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 74% (3711/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 75% (3761/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 76% (3811/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 77% (3861/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 78% (3911/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 79% (3961/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 80% (4011/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 81% (4061/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 82% (4111/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 83% (4161/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 84% (4211/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 85% (4261/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 86% (4311/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 87% (4361/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 88% (4411/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 89% (4461/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 90% (4511/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 91% (4561/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 92% (4611/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 93% (4661/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 94% (4711/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 95% (4761/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 96% (4811/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 97% (4861/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 98% (4911/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 99% (4961/5025), 3.46 MiB | 6.92 MiB/s  Receiving objects: 100% (5025/5025), 3.46 MiB | 6.92 MiB/s  done.
```

Après avoir récupéré le code de l'application à partir de GitHub, je déplace tout le contenu du dossier src (/www/mutillidae/src) dans fichier mutillidae grâce à la commande : mv src/* .

```
Windows PowerShell
X eljhdb@MSI: ~
X + v
X - [ ] X

eljhdb@ssh1:~/www/mutillidae$ mv src/* .
eljhdb@ssh1:~/www/mutillidae$ ls -la
total 604
drwxrwxr-x 17 eljhdb eljhdb 4096 May 30 11:36 .
drwxr-xr-x 3 eljhdb eljhdb 54 May 30 10:23 ..
-rwxrwxr-x 1 eljhdb eljhdb 12571 May 30 10:23 add-to-your-blog.php
drwxrwxr-x 2 eljhdb eljhdb 53 May 30 10:23 ajax
```

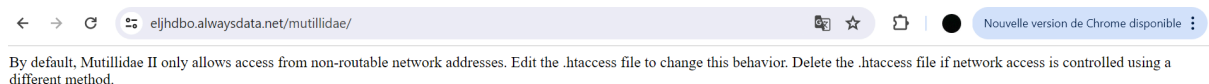
Après avoir déplacé tous les fichiers et dossiers vers mutillidae, je me rend vers l'URL : <https://eljhdbo.alwaysdata.net/mutillidae> pour voir le nouveau dossier qui à été créé, et je suis tombé sur une **erreur**.



Le “Forbidden” veut dire que l'**erreur** vient du dossier src et plus précisément du fichier restant .htaccess qui se trouve pas dans mutillidae. Je vais donc le déplacer manuellement avec la commande : `mv ~/www/mutillidae/src/.htaccess ~/www/mutillidae/`

```
eljhdbo@ssh1:~/www/mutillidae/src$ ls -la
total 8
drwxrwxr-x  2 eljhdbo eljhdbo   23 Jun 13 10:11 .
drwxrwxr-x 17 eljhdbo eljhdbo 4096 May 30 11:36 ..
-rwxrwxr-x  1 eljhdbo eljhdbo   690 May 30 10:23 .htaccess
eljhdbo@ssh1:~/www/mutillidae/src$ mv ~/www/mutillidae/src/.htaccess ~/www/mutillidae/
eljhdbo@ssh1:~/www/mutillidae/src$ ls -la
total 4
drwxrwxr-x  2 eljhdbo eljhdbo    6 Jun 13 10:19 .
drwxrwxr-x 17 eljhdbo eljhdbo 4096 Jun 13 10:19 ..
eljhdbo@ssh1:~/www/mutillidae/src$
```

Puis le en repartant sur l'URL, je trouve :



Maintenant, pour ouvrir l'accès des clients extérieur et installer l'application, on va renommer le fichier d'OWASP : .htaccess en no.htaccess dans le Terminal.

```
eljhdbo@ssh1:~/www/mutillidae$ mv .htaccess no.htaccess
```

Après l'avoir renommer une nouvelle **erreur** apparaît :

Warning: fsockopen(): Unable to connect to 127.0.0.1:3306 (Connection refused) in /home/eljhdbo/www/mutillidae/database-offline.php on line 59

Warning: fsockopen(): Unable to connect to 127.0.0.1:389 (Connection refused) in /home/eljhdbo/www/mutillidae/database-offline.php on line 105

The database server at 127.0.0.1 appears to be offline.

1. [Click here](#) to attempt to setup the database. Sometimes this works.
2. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
3. Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.inc
4. A [video is available](#) to help reset MySQL root password
5. Check the error message below for more hints
6. If you think this message is a false-positive, you can opt-out of these warnings below

Database Diagnostics Information

Database Error message: Failed to connect to MySQL database. Connection refused

Database host: 127.0.0.1
Database port: 3306
Database username: root
Database password: mutillidae
Database name: mutillidae

IP resolved from database hostname: 127.0.0.1

Ping database results:

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

Pour compléter correctement le fichier de configuration, je prépare une base de données MySQL dans le terminal avec un utilisateur attitré qui a tout les ayant droit.

```
eljhdbo@ssh1:~/www/mutillidae$ cd includes/  
eljhdbo@ssh1:~/www/mutillidae/includes$ cat database-config.inc  
<?php  
define('DB_HOST', '127.0.0.1');  
define('DB_USERNAME', 'root');  
define('DB_PASSWORD', 'mutillidae');  
define('DB_NAME', 'mutillidae');  
define('DB_PORT', 3306);  
?>  
eljhdbo@ssh1:~/www/mutillidae/includes$
```




Puis je retourne dans l'interface Alwaysdata dans le menu MySQL pour y créer une nouvelle base de données : eljhdbo_mutillidae
Ensuite j'ajoute un nouvel utilisateur : eljhdbo_mutilli avec comme mot de passe : mutillipwd et je n'oublie pas de lui donner tout les droits.

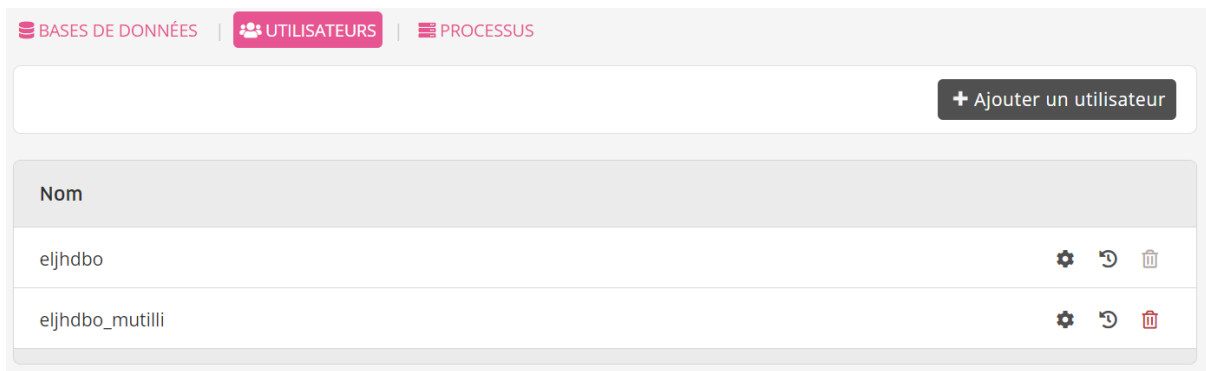
BASES DE DONNÉES | **UTILISATEURS** | **PROCESSUS**

+ Ajouter une base de données

Nom

eljhdbo_mutillidae



Après avoir créer la base de données sur Alwaysdata, je repart sur le Terminal pour mettre à jour le database-config.inc avec la commande nano

```
eljhdbo@ssh1:~/www/mutillidae/includes$ nano database-config.inc
eljhdbo@ssh1:~/www/mutillidae/includes$
```

```
GNU nano 3.2 database-config.inc
?php
define('DB_HOST', 'mysql-eljhdbo.alwaysdata.net');
define('DB_USERNAME', 'eljhdbo_mutilli');
define('DB_PASSWORD', 'mutillipwd');
define('DB_NAME', 'eljhdbo_mutillidae');
define('DB_PORT', 3306);
?>
```

[Read 7 lines (Converted from DOS format)]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-6 Copy Text

Une fois cette étape terminée et en ayant rechargé la page de l'application je tombe sur la même page **erreur**.

Warning: fsockopen(): Unable to connect to 127.0.0.1:389 (Connection refused) in /home/eljhdbowww/mutillidae/database-offline.php on line 105

The database server at mysql-eljhdbowww.alwaysdata.net appears to be offline.

1. [Click here](#) to attempt to setup the database. Sometimes this works.
2. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
3. Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.inc
4. A [video is available](#) to help reset MySQL root password
5. Check the error message below for more hints
6. If you think this message is a false-positive, you can opt-out of these warnings below

Database Diagnostics Information

Database Error message: Failed to connect to MySQL database. Access denied for user 'eljhdbowww'@'%' to database 'eljhdbowww_mutillidae'

Database host: mysql-eljhdbowww.alwaysdata.net
Database port: 3306
Database username: eljhdbowww
Database password: SetM9925
Database name: eljhdbowww_mutillidae

IP resolved from database hostname: 185.31.41.44

Ping database results:

PING mysql-eljhdbowww.alwaysdata.net(mysql25.paris1.alwaysdata.com (2a00:b6e0:1:100:25::1)) 56 data bytes
64 bytes from mysql25.paris1.alwaysdata.com (2a00:b6e0:1:100:25::1): icmp_seq=1 ttl=64 time=0.213 ms

Pour rendre l'application opérationnelle, il suffit de cliquer sur le [Click here](#) de la ligne 1 et renommer le fichier no.htaccess en .htaccess pour rebloquer l'application web. Mais lorsque je clique dessus, une nouvelle page d'**erreurs** s'affiche.

Setting up the database...

If you see no error messages, it should be done.

[Continue back to the frontpage.](#)

HTML 5 Local and Session Storage cleared unless error popped-up already.

Attempting to connect to MySQL server on host mysql-eljhdbowww.alwaysdata.net with user name eljhdbowww

Connected to MySQL server at mysql-eljhdbowww.alwaysdata.net as eljhdbowww

Preparing to drop database eljhdbowww_mutillidae

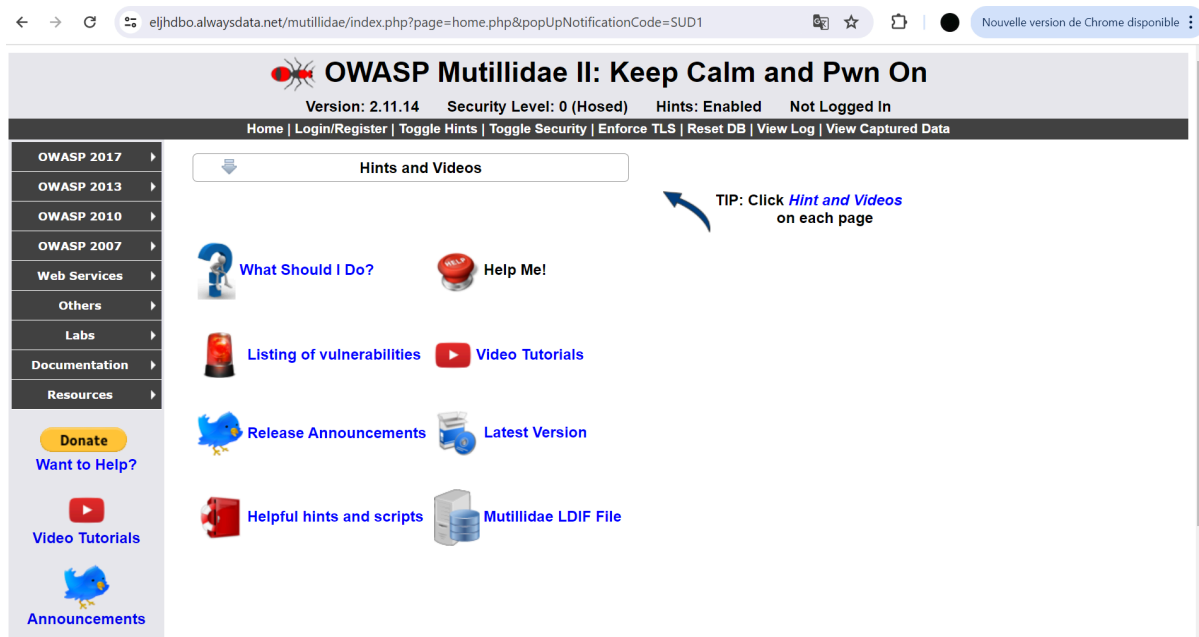
Error was reported while attempting to drop database eljhdbowww_mutillidae

MySQL sometimes throws errors attempting to drop databases. Here is error in case the error is serious.

Error Message

Failure is always an option	
Line	238
Code	0
File	/home/eljhdbowww/mutillidae/classes/MySQLHandler.php
Message	/home/eljhdbowww/mutillidae/classes/MySQLHandler.php on line 238: Access denied for user 'eljhdbowww'@'%' to database 'eljhdbowww_mutillidae' Query: DROP DATABASE IF EXISTS eljhdbowww_mutillidae (1044) [mysqli_sql_exception]
Trace	#0 /home/eljhdbowww/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery('DROP DATABASE I...') #1 /home/eljhdbowww/mutillidae/set-up-database.php(67): MySQLHandler->executeQuery('DROP DATABASE I...') #2 {main}
Diagnostic Information	DROP DATABASE IF EXISTS eljhdbowww_mutillidae

Pour régler cette erreur, j'ai dû aller dans le Terminal et renommer une nouvelle fois le .htaccess en no.htaccess pour que sa m'affiche finalement la bonne page.



2er Étape : BurpSuite

Pour installer BurpSuite, plus exactement l'édition "Community" il faut se rendre sur le site PortSwigger avec l'URL :

<https://portswigger.net/burp/communitydownload>

Entrer son adresse mail puis télécharger l'application.

Une fois tout correctement installé, je me retrouve sur cette page d'accueil (screenshot ci-dessous) et prêt à démarrer la mission OWASP_Mission1.

