PLOUZENNEC Eliaz

TP : Exploitation faille port 80

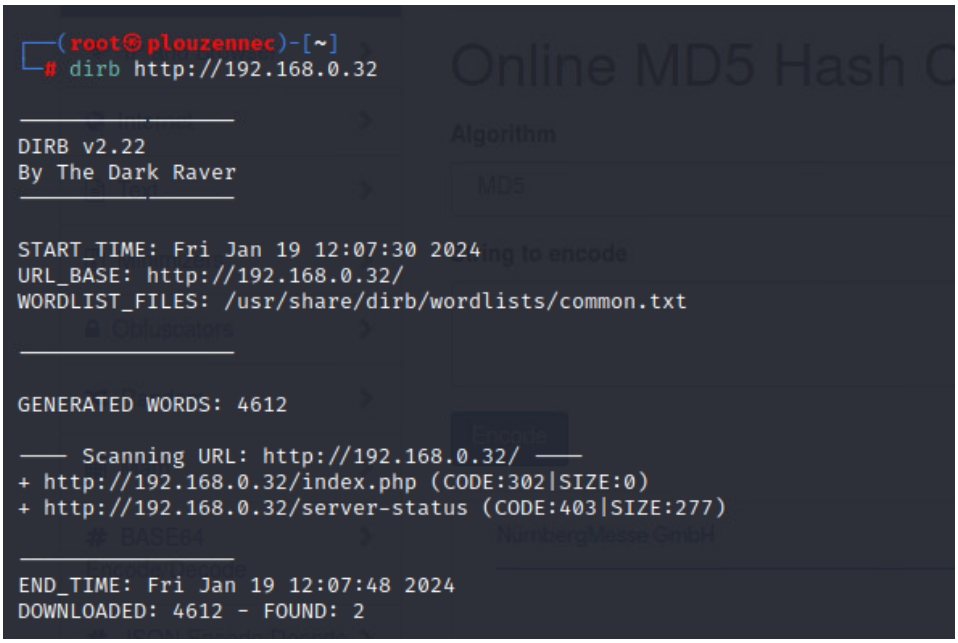
19/01/23

Contenu

Introduction :

Trouver les fichier de l'adresse ip :

Ici l'adresse ip est 192.168.0.32, on utilise la commande dirb pour trouver ces fichier.



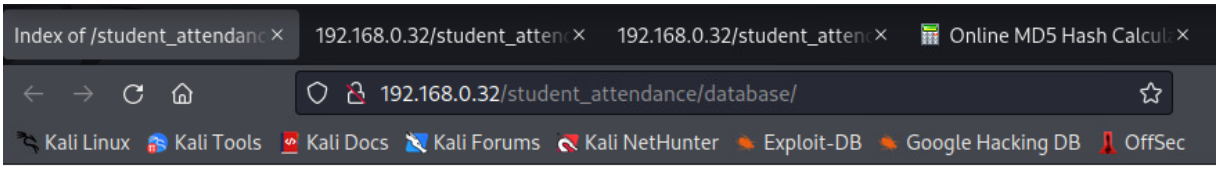
Le fichier index se traduit ici par student_attendance/login.php

On entre donc cette commande avec –w, et on observe que student_attendance/database est lisible

```
┌──(root㉿plouzennec)-[~]
└─# dirb http://192.168.0.32/student_attendance -w

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 19 12:14:54 2024
URL_BASE: http://192.168.0.32/student_attendance/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.32/student_attendance/ ----
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/
==> DIRECTORY: http://192.168.0.32/student_attendance/database/
+ http://192.168.0.32/student_attendance/index.php (CODE:302|SIZE:14619)

---- Entering directory: http://192.168.0.32/student_attendance/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/css/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/js/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/uploads/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/vendor/

---- Entering directory: http://192.168.0.32/student_attendance/database/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.

---- Scanning URL: http://192.168.0.32/student_attendance/ ----
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/
==> DIRECTORY: http://192.168.0.32/student_attendance/database/
+ http://192.168.0.32/student_attendance/index.php (CODE:302|SIZE:14619)

---- Entering directory: http://192.168.0.32/student_attendance/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/css/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/js/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/uploads/
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/vendor/

---- Entering directory: http://192.168.0.32/student_attendance/database/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.32/student_attendance/assets/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
==> DIRECTORY: http://192.168.0.32/student_attendance/assets/vendor/jquery/

---- Entering directory: http://192.168.0.32/student_attendance/assets/vendor/jquery/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Jan 19 12:17:15 2024
DOWNLOADED: 36896 - FOUND: 1
```

Ouverture du fichier database :

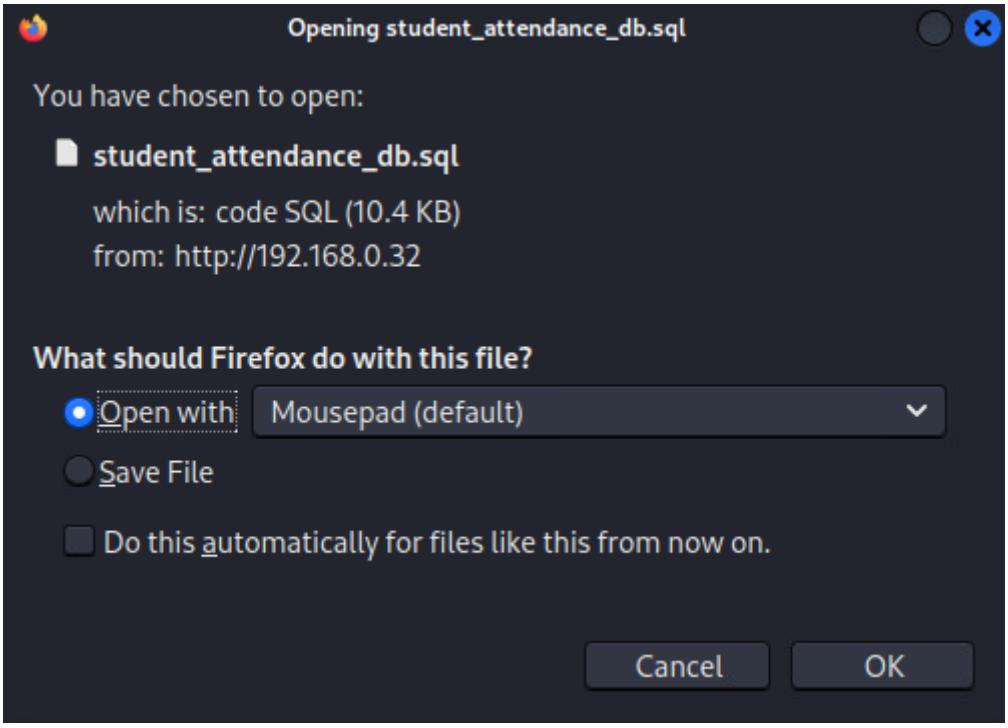
On entre l'url correspondant



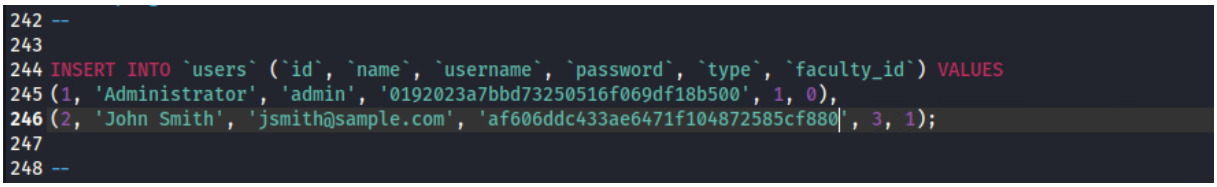
Index of /student_attendance/database

Name	Last modified	Size	Description
Parent Directory		-	
student_attendance_db.sql	2020-10-28 23:00	10K	

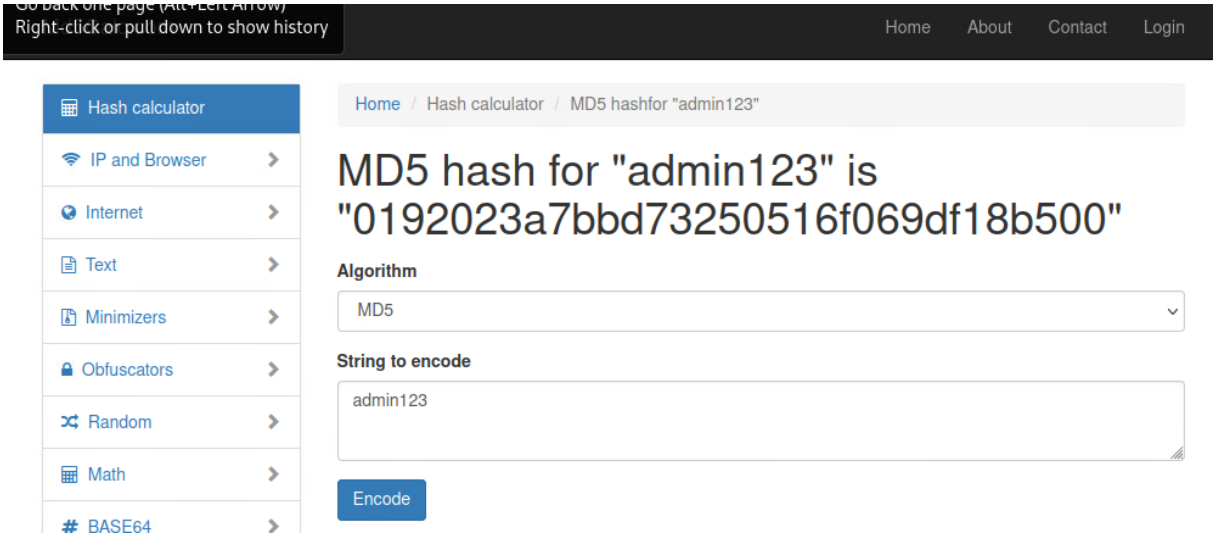
Apache/2.4.38 (Debian) Server at 192.168.0.32 Port 80



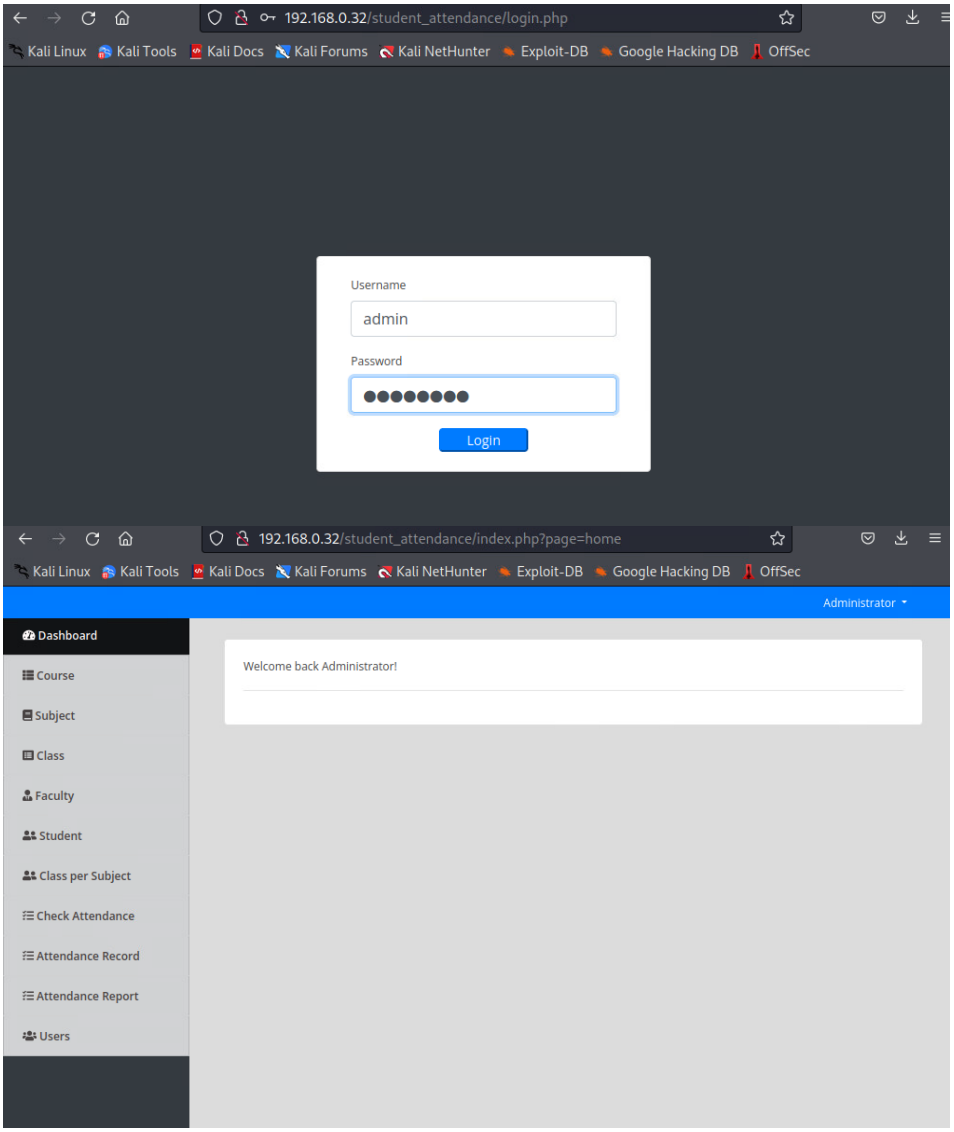
Ce qui nous permet d'ouvrir le fichier sql



On trouve la ligne relative au login et mot de passe, ici on admin et le mot de passe correspondant, qui celui-ci est codé en MD5.



Ce qui donne admin, on peut le rentrer et acceder au site.


192.168.0.32/student_attendance/login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Username
admin
Password
Login
192.168.0.32/student_attendance/index.php?page=home
Administrator
Dashboard
Course
Subject
Class
Faculty
Student
Class per Subject
Check Attendance
Attendance Record
Attendance Report
Users
Welcome back Administrator!