Лабораторна робота 1

**Назва:** Збір інформації

|  |  |
| --- | --- |
| **Група:** ФІ-92 | |
| **Команда** | **Учасник** |
| Команда №1 | Поночевний Назар |
| Романченко Дмитро |
|  |

**Розробники:**

* Anders Carlsson
* Oleksii Baranovskyi

**Передумови:** Для виконання робіт рекомендується встановити програму віртуалізації для операційних систем, VirtualBox [1] https://www.virtualbox.org/wiki/Downloads, на яку рекомендується встановити дистрибутив Kali Linux [2] https://www.kali.org/get-kali/#kali-virtual-machines – що є Linux дистрибутивом який створено на основі Debian з відкритим вихідним кодом, призначений для вирішення різних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки і комп'ютерна криміналістика.

Встановлена цільова віртуальна машина, для виконання лабораторної роботи.

https://drive.google.com/file/d/1A4OpvQ-zXyZzDBX6igJORCPl6gstmL1E/view?usp=sharing

Зміст

[Завдання 1. Визначення сервісів 1](#_Toc94360897)

[Завдання 2. Перерахування користувачів 5](#_Toc94360898)

## ****Завдання 1. Визначення сервісів****

**Призначення:** зрозуміти, як визначати сервіси на веб-серверах / серверах додатків.

**Після цієї роботи студент має:**

* знати: що таке сканування;
* вміти: аналізувати заголовки HTTP та процес їх генерації.

**Завдання:**

* проаналізувати наданий веб-ресурс на віртуальній машині 192.168.56.2, перевірити його параметри, проаналізувати заголовки, виконати сканування.

**Технічні інструменти для виконання роботи:**

* nmap (утиліта, додаток, програма для сканування)
* Browser Developer Tools (Інструменти розробника браузера)

**Рішення:**

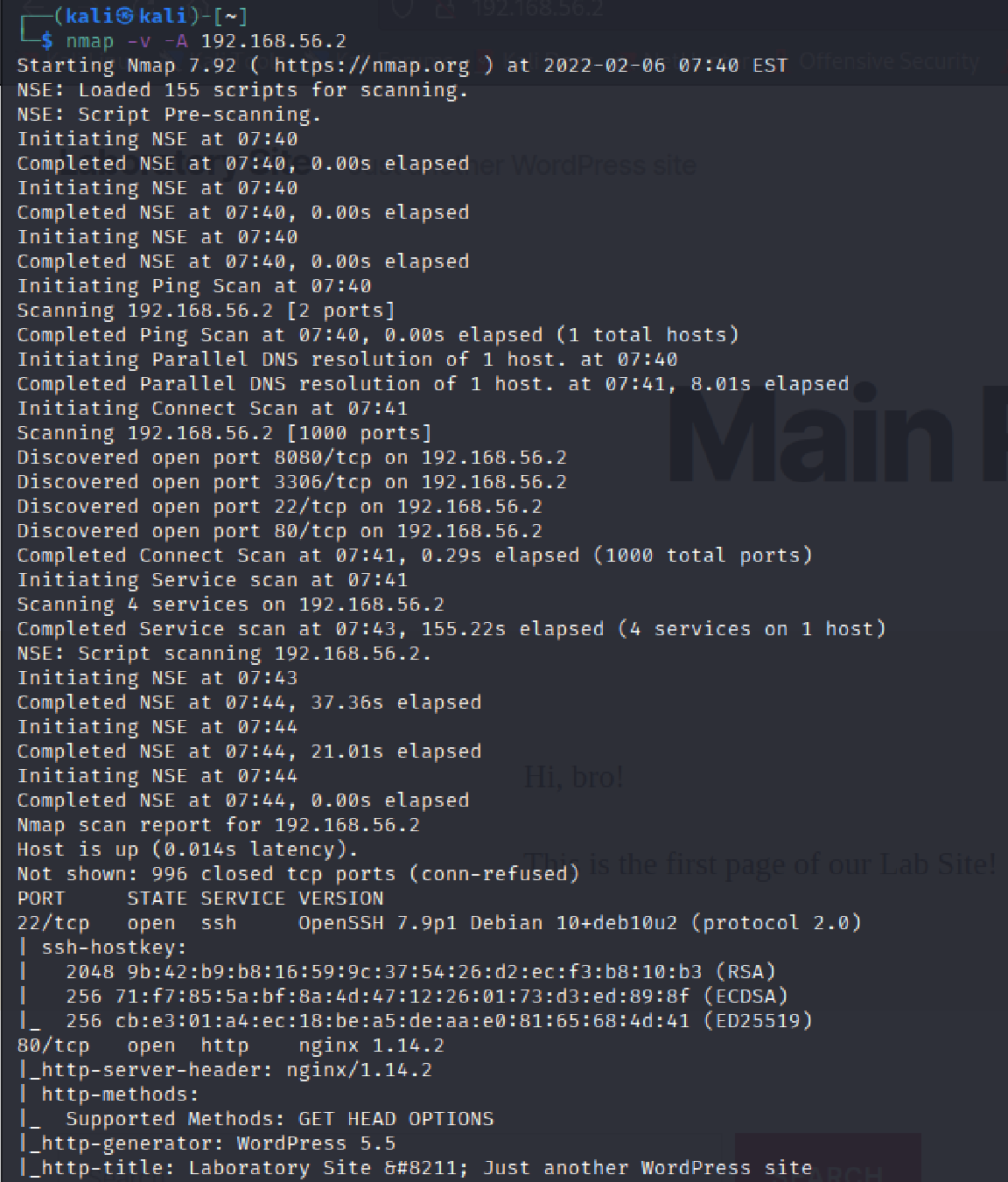
Відкрити сайт у браузері. Проаналізуйте HTTP-параметри для запитів GET/POST. Використати надані інструменти для визначення сервісів.

**ЗАВДАННЯ 1**

Який сервер встановлено? Доведіть це за допомогою знімка екрану.

**Відповідь:**

Встановлено сервер nginx 1.14.2

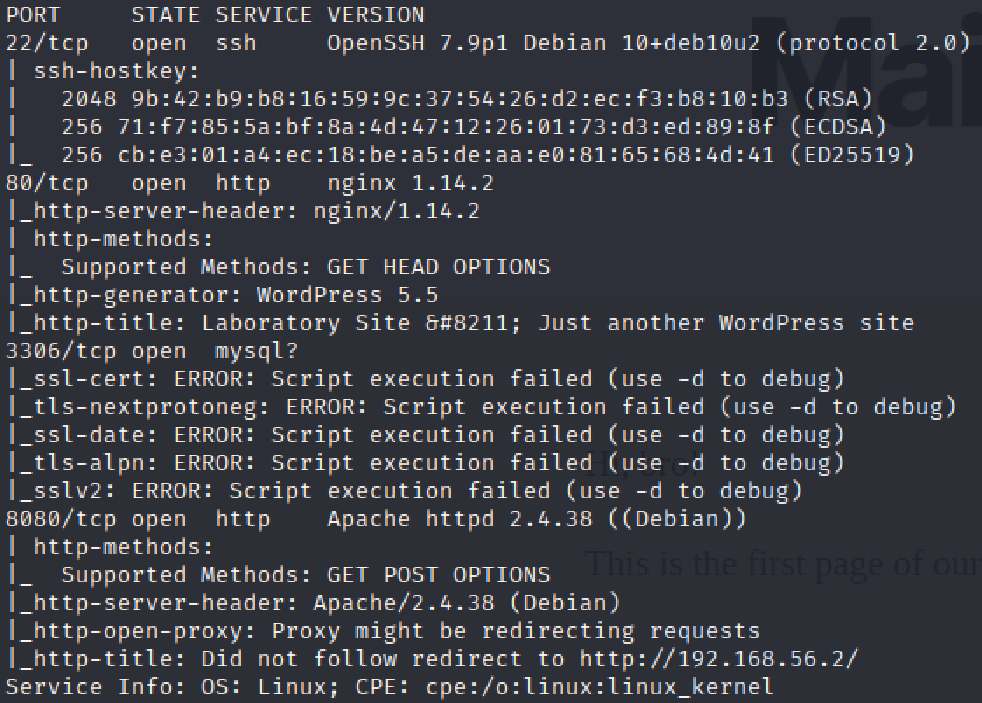


**ЗАВДАННЯ 2**

Які ще служби встановлено? Доведіть це (надайте знімок екрану).

**Відповідь:**

Apache 2.4.38, MySQL і OpenSSH 7.9p1

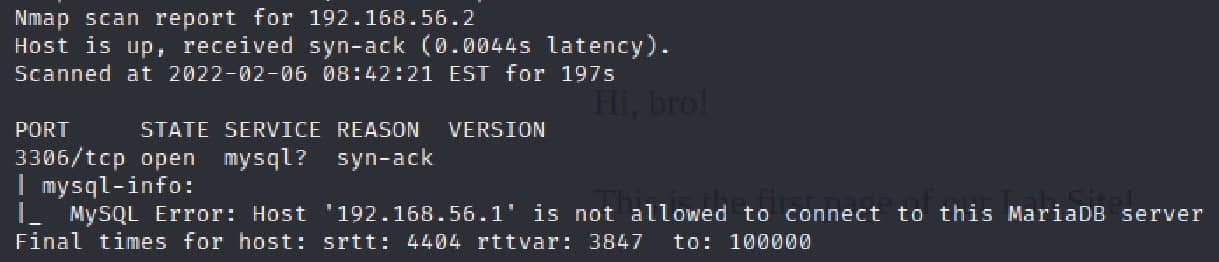


**ЗАВДАННЯ 3**

Яка база даних використовується? Доведіть це (надайте знімок екрану).

**Відповідь:**

Nmap визначив БД як MySQL, проте не визначив версію, тому, напевно, це MariaDB – доволі поширений форк MySQL

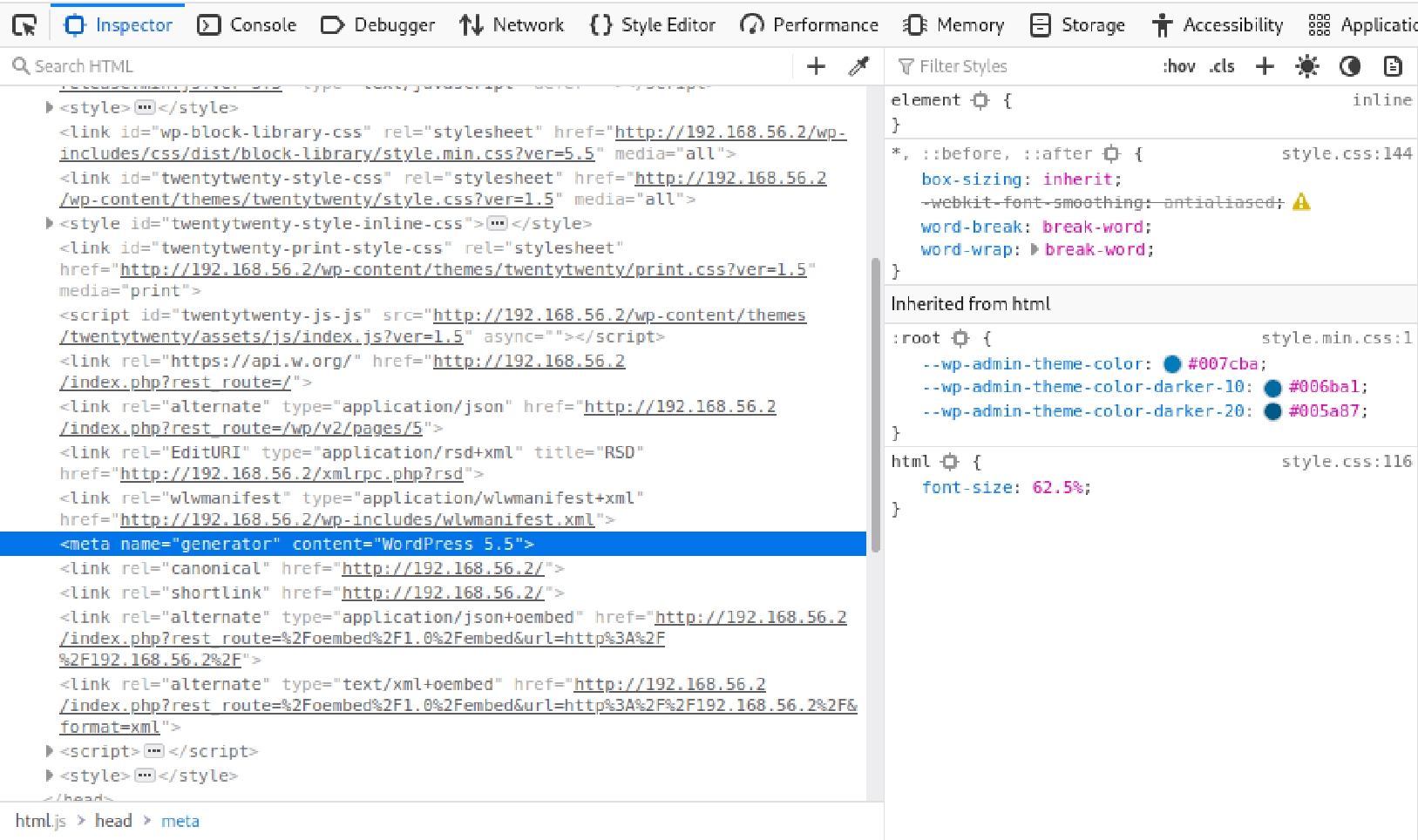


**ЗАВДАННЯ 4**

Яка CMS використовується? Доведіть це (надайте знімок екрану).

**Відповідь:**

WordPress 5.5



## ****Завдання 2. Перерахування користувачів****

**Призначення:** зрозуміти, як виконувати перерахування користувачів

**Після роботи студент повинен**

* знати: що таке перерахування користувачів;
* вміти: виконувати перерахування користувачів;

**Завдання:**

* проаналізувати наданий веб-ресурс на віртуальній машині 192.168.56.2. знайти сторінку входу, виконати перерахування користувачів

**Технічні інструменти для виконання роботи:**

* wfuzz
* THC-hydra
* etc

**Рішення:**

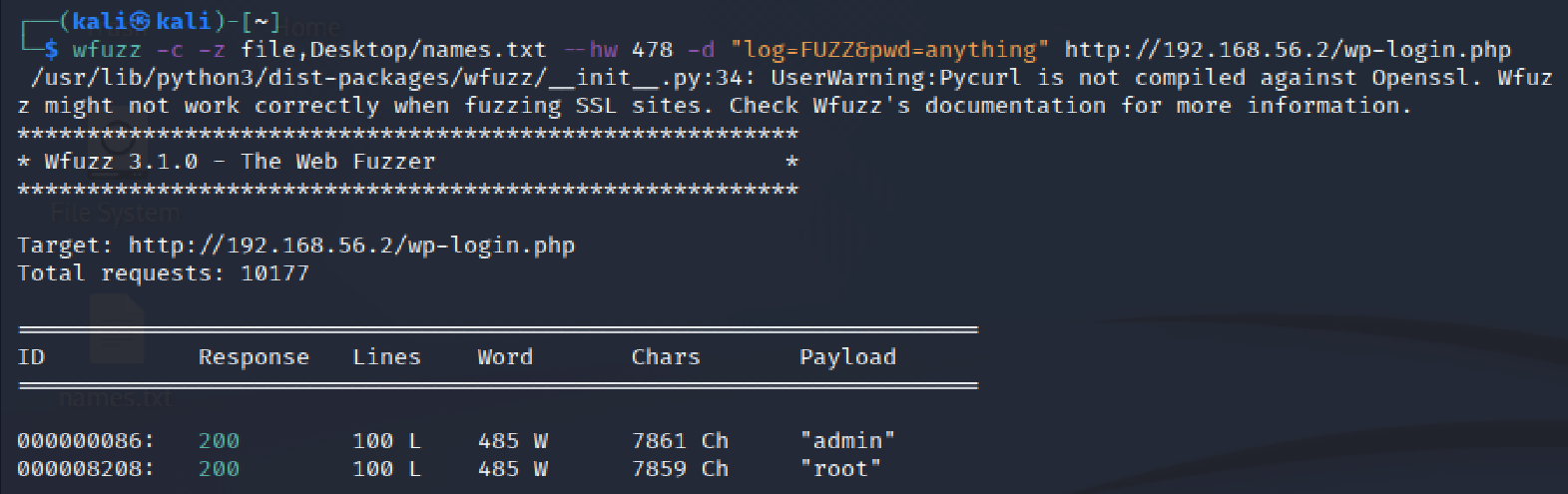
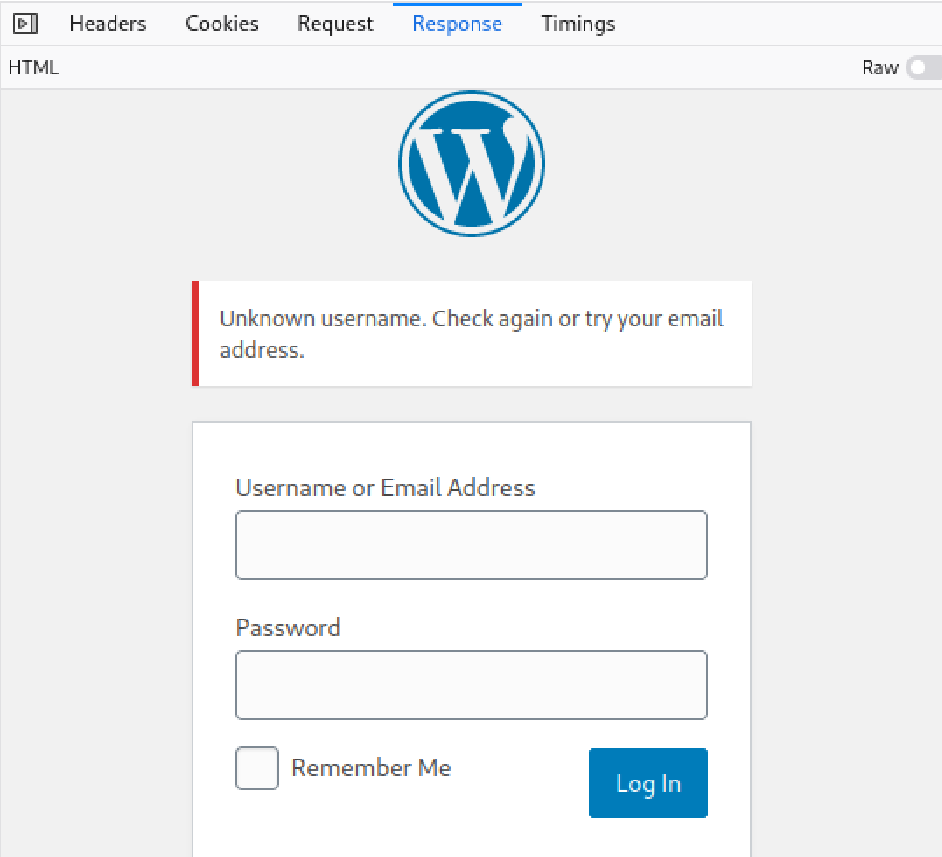
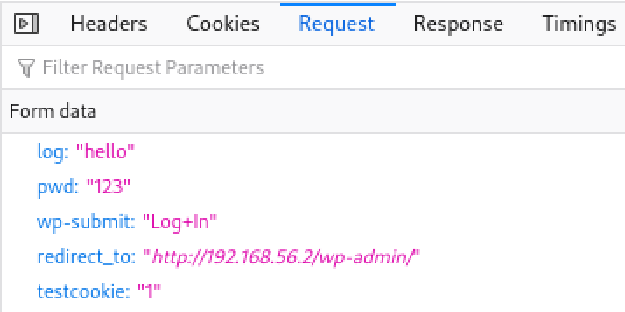
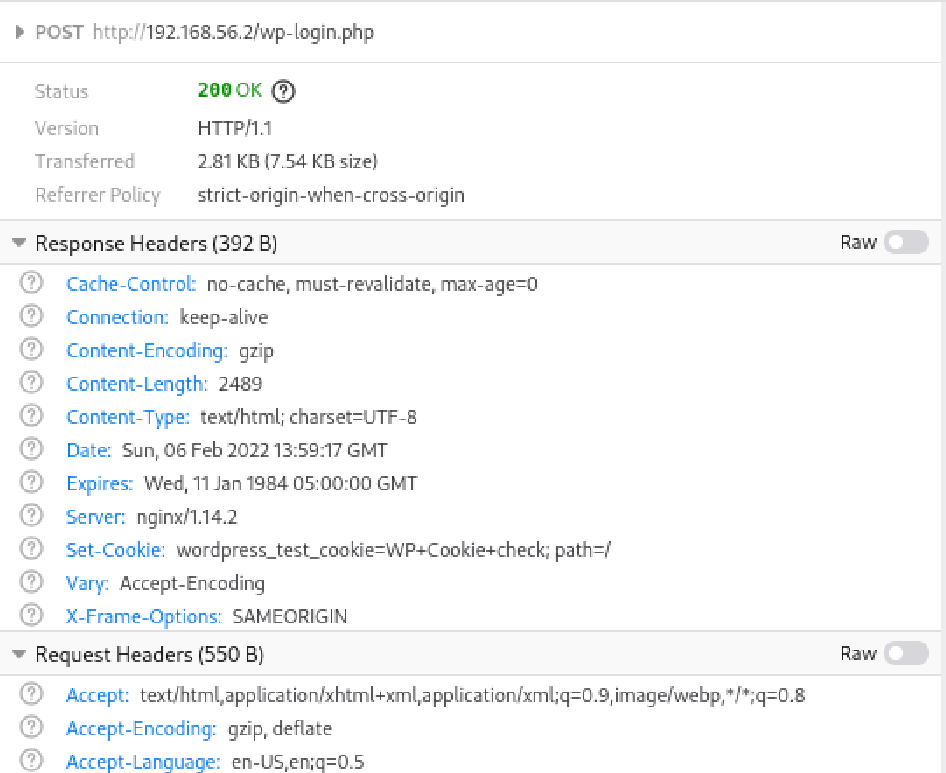
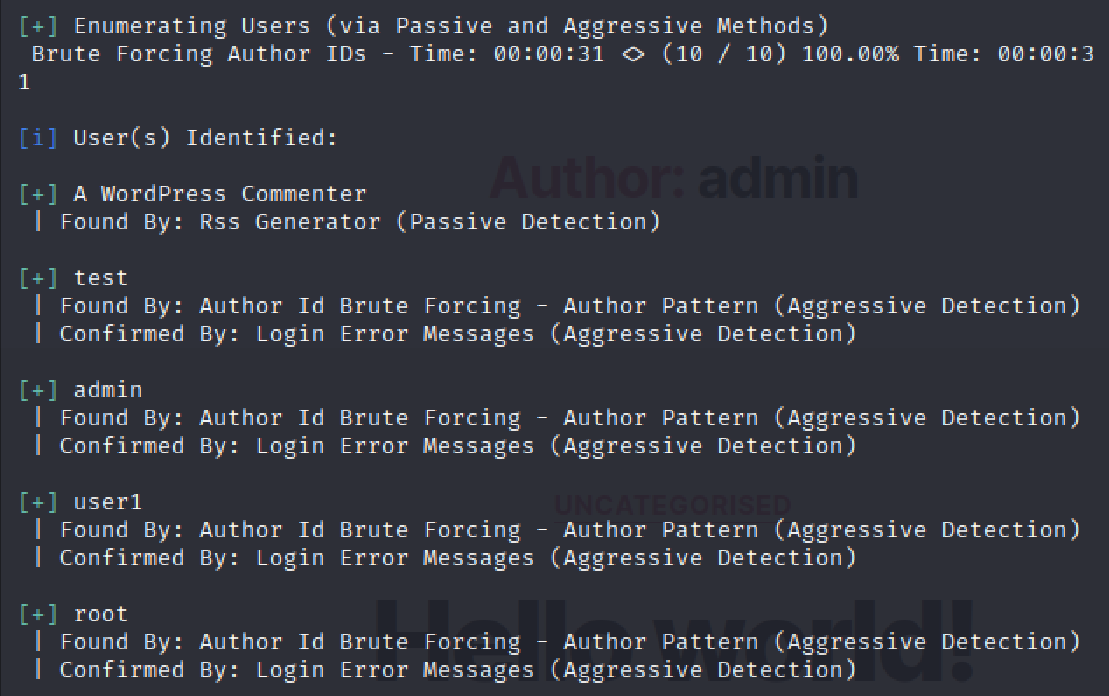
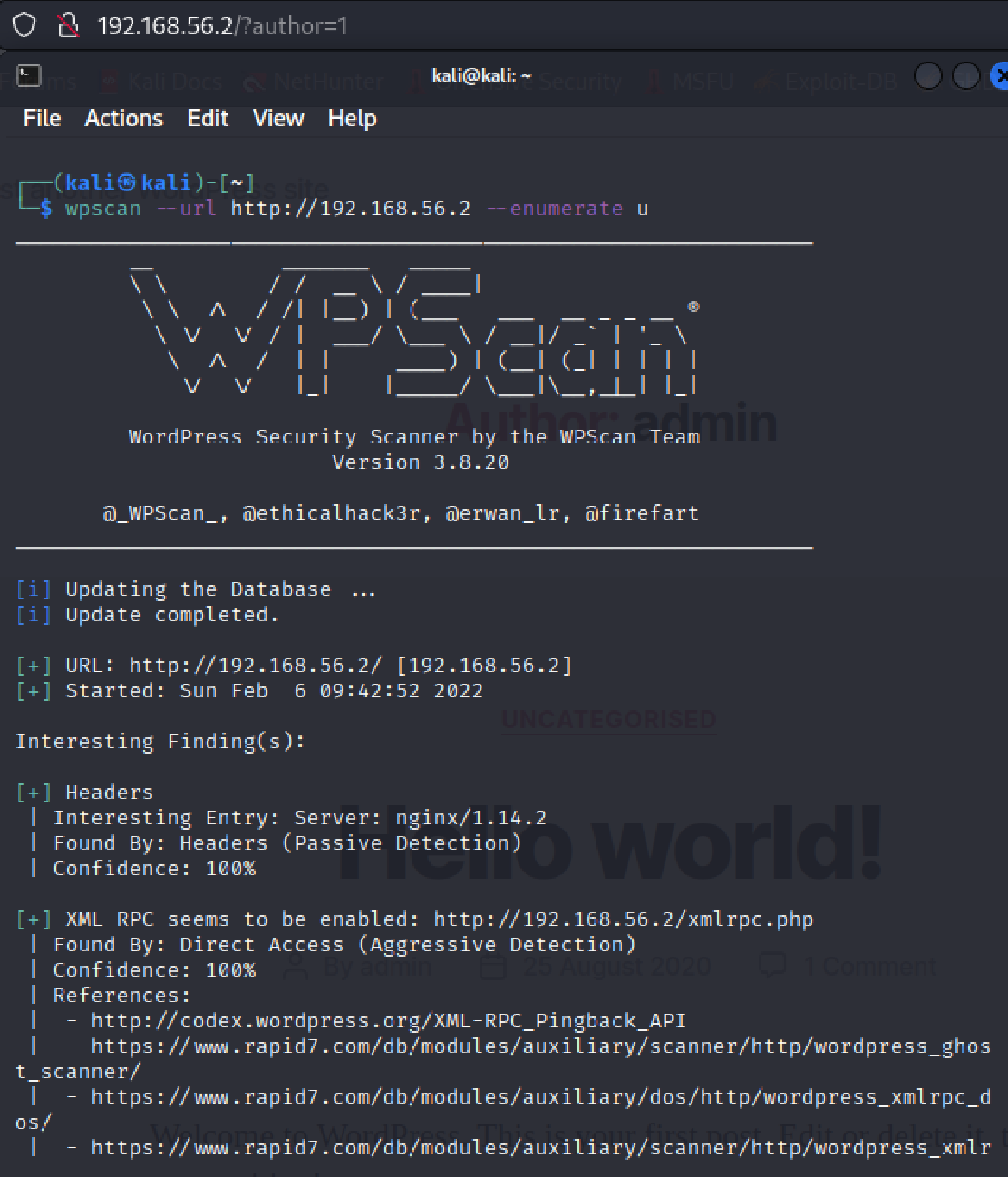
Відкрити сайт у браузері. Проаналізувати HTTP-параметри для запитів GET/POST. Використовуйте надані інструменти для перерахування користувачів.

**ЗАВДАННЯ 1**

Надайте відповідь – для даного веб-ресурсу: які користувачі зареєстровані? Доведіть це (надайте знімок екрану).

**Відповідь:**

admin, root, user1, test



**ЗАВДАННЯ 2**

Чи можлива атака за підбором пароля? Доведіть це (надайте знімок екрану).

**Відповідь:**

Так, бо захисту від brute force атаки (ліміт на кількість невдалих спроб) немає.

