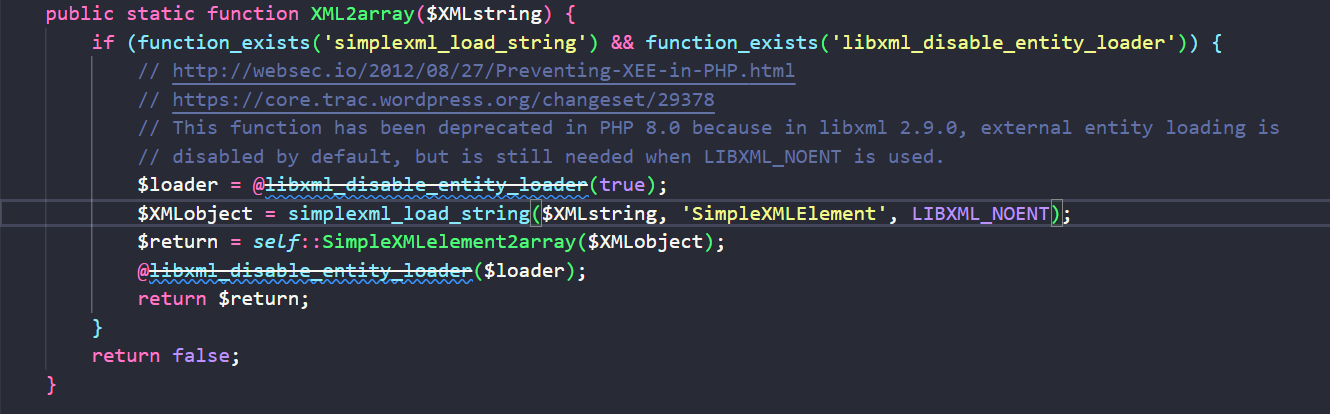
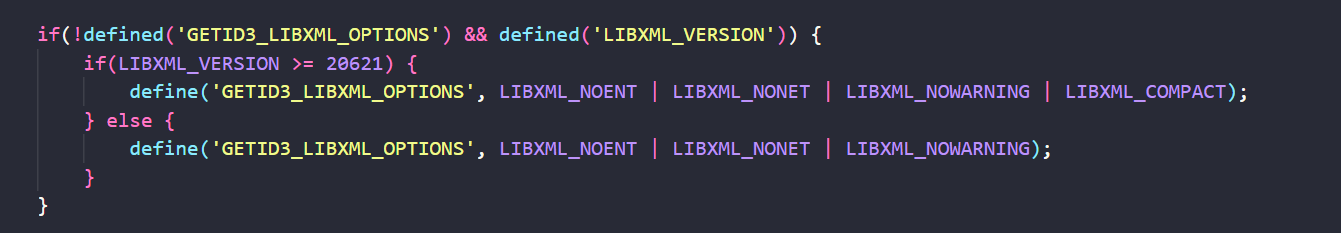
**NGUYỄN ANH PHÁP – phapna01@gmail.com**

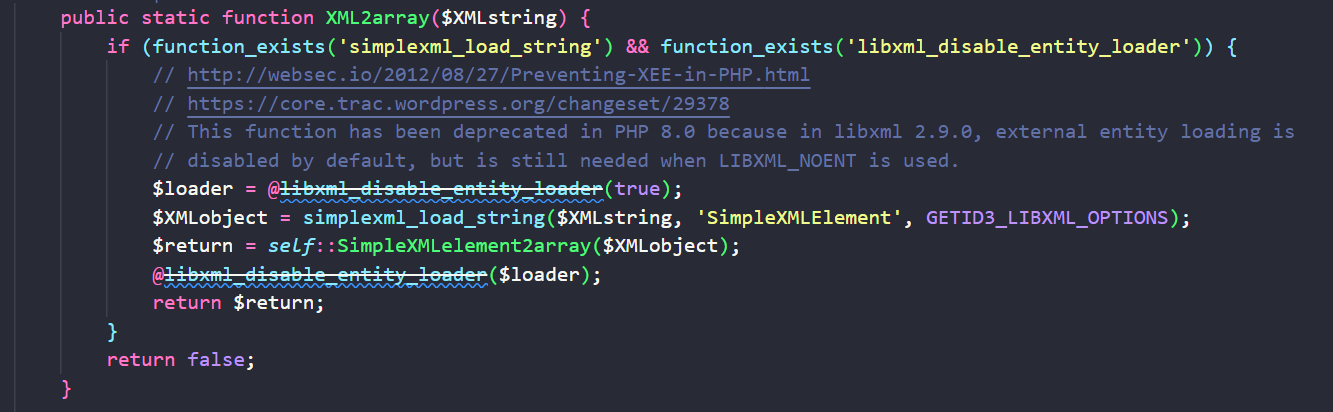
CVE-2021- 29447

1. Nguyên nhân

Lỗ hổng này xảy ra vì WordPress sử dụng thư viện SimpleXML để phân tích tệp XML và xử lý đầu vào độc hại trong tệp XML đó.

+ Trong phiên bản Wordpress 5.7 việc sử dụng LIBXML\_NOENT được sử dụng cho phép các tham chiếu bên trong chuỗi XML. Cho phép tham đến nội dung định nghĩa trước, giúp giảm thiểu việc lặp dữ liệu nhưng dẫn đến việc bị tấn công XXE 

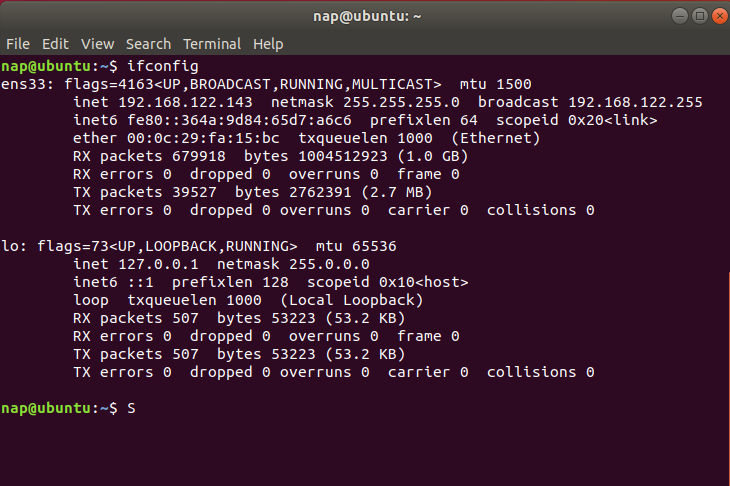
+ Trong phiên bản Wordpress 5.7.1. Đoạn mã dưới đây để xác định các thư viện. Nếu phiên bản LIBXML\_VERSION >= 20621 thì sẽ sử dụng thư viện GETID3 

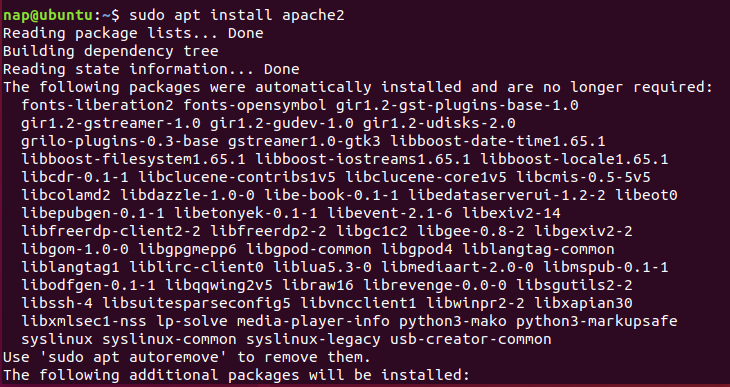
Sử dụng GETID3\_LIBXML\_OPTIONS sẽ tùy chọn cho phép hoặc vô hiệu hóa tính năng cụ thể của libxml. Với các LIBXML\_NOENT sẽ vô hiệu hóa khai thác XXE thông qua ENTITY và DOCTYPE bằng cách không phân giải các tham chiếu đối tượng bên trong XML

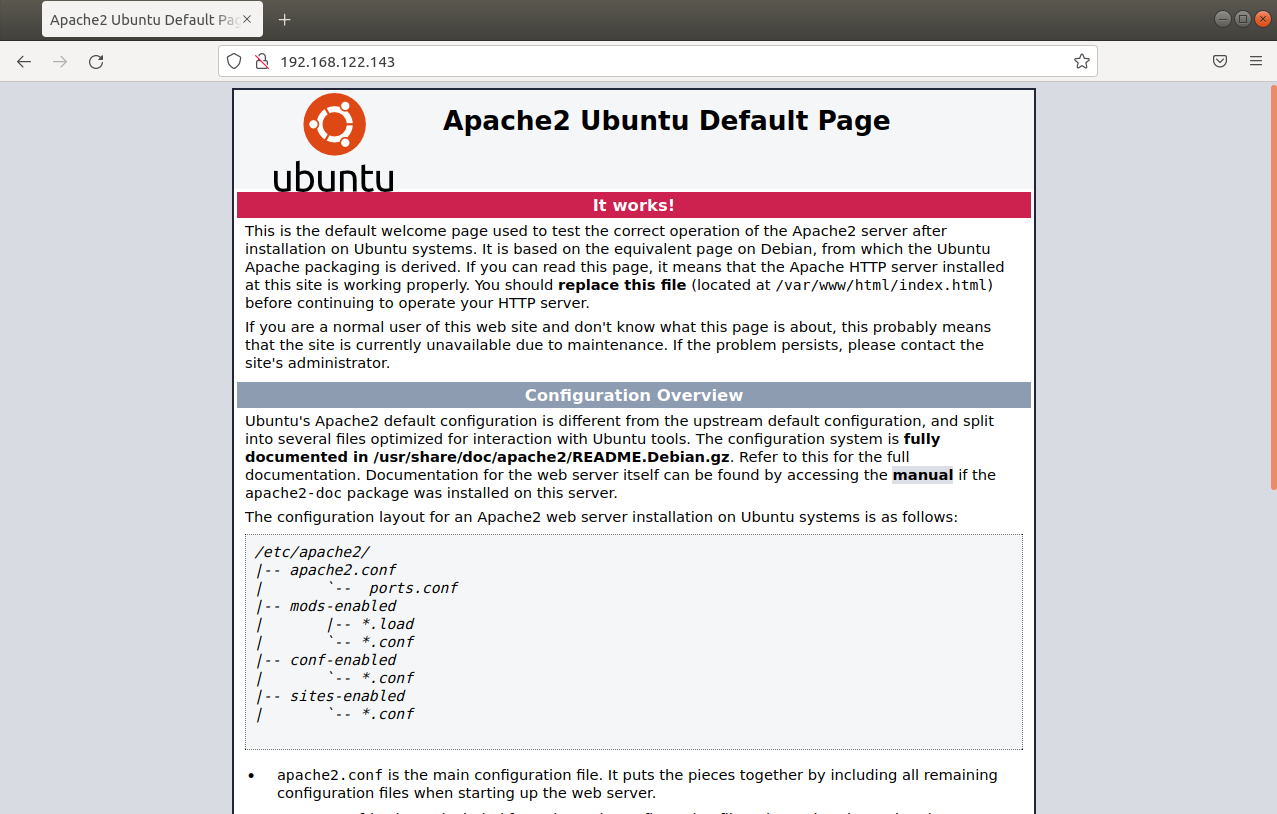
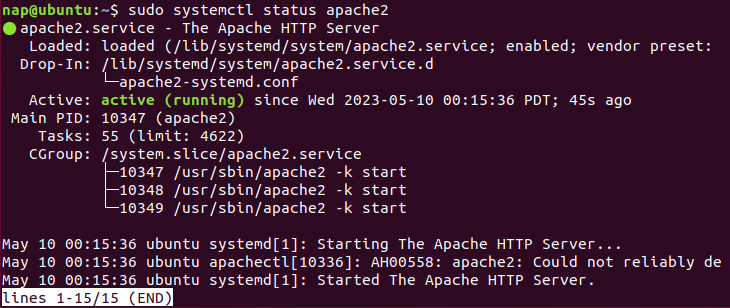
1. Mô tả thực hiện khai thác

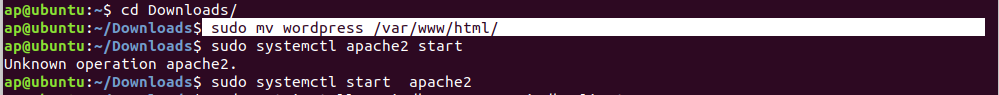
Thực hiện khai thác trên Ubuntu với Wordpress 5.7 và PHP 8.0.\*. Người dùng tạo tệp XML có chứa mã độc và gửi lên máy chủ Wordpress bằng chức năng tải lên tệp trong giao diện Wordpress.

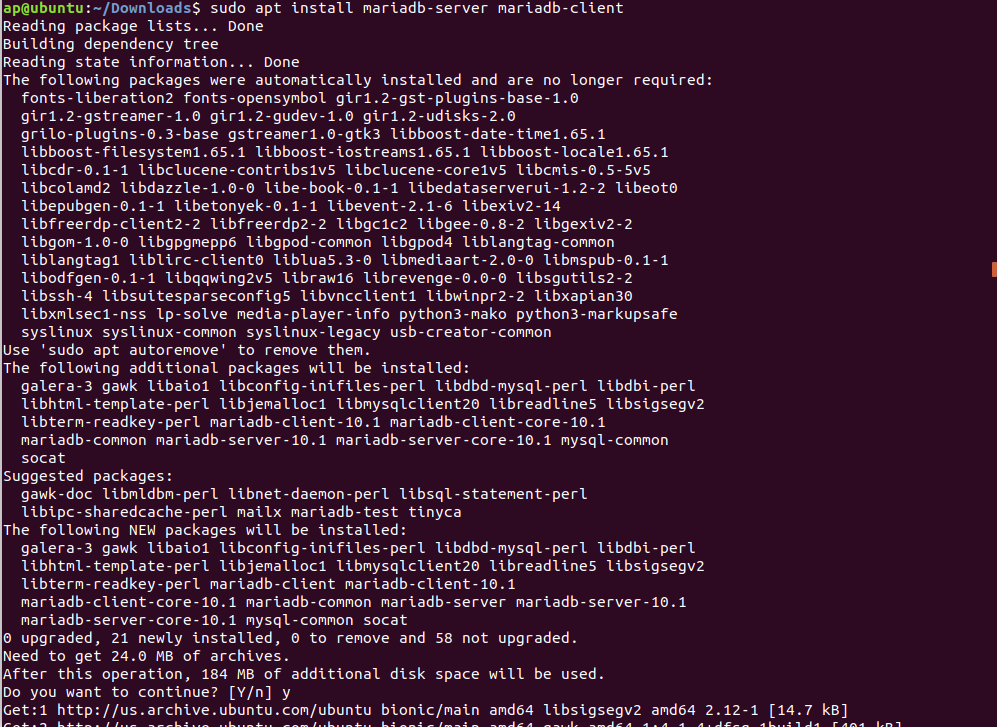
Thực hiện tiến hành Demo

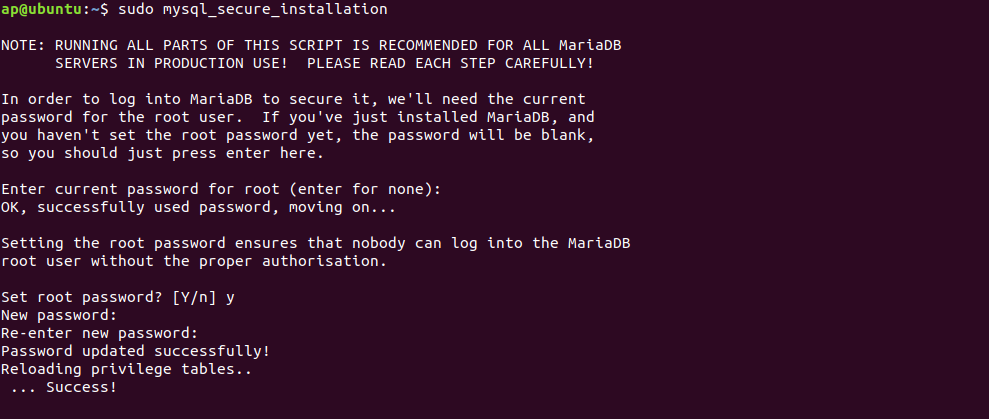
Máy Victim với Ip: 192.168.122.143 

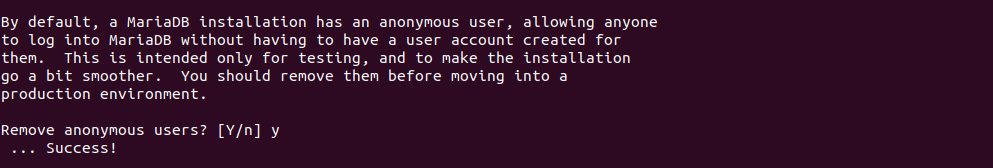
Dowload WebServer Apache2

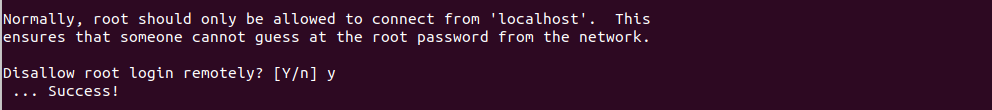
Kiểm tra đăng chạy

Di chuyển thư mục ‘wordpress’ đã được giải nén trong word vào đường dẫn /var/www/html/

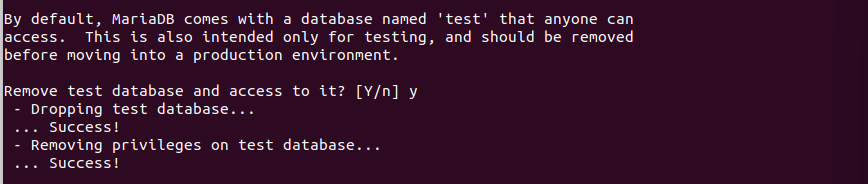
Sử dụng Database Server MariaDB

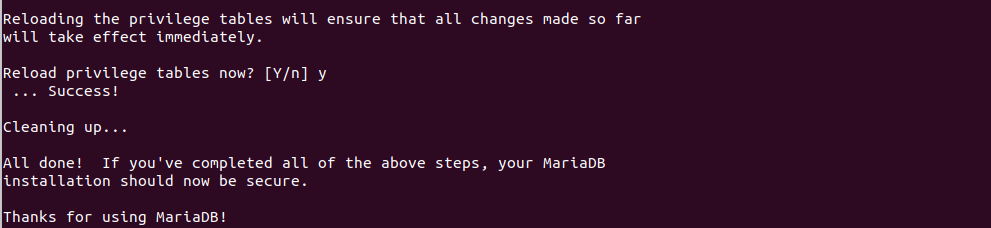
Thiết lập mật khẩu cho tài khoản root 

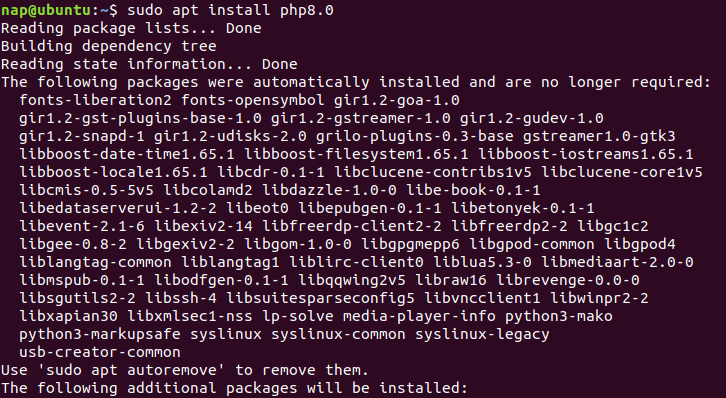
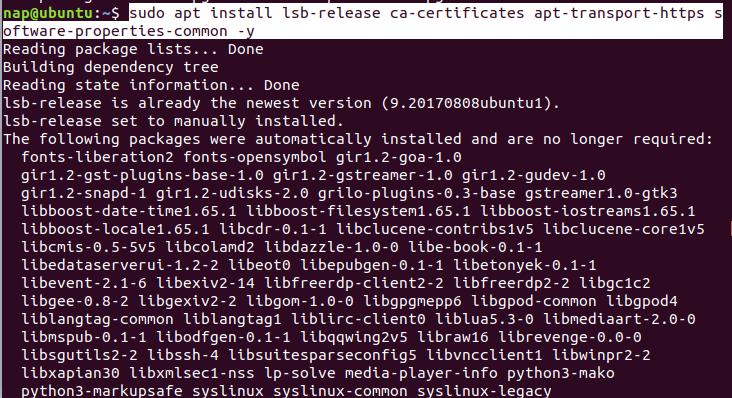
Sẽ được nhắc xóa người dùng ẩn danh

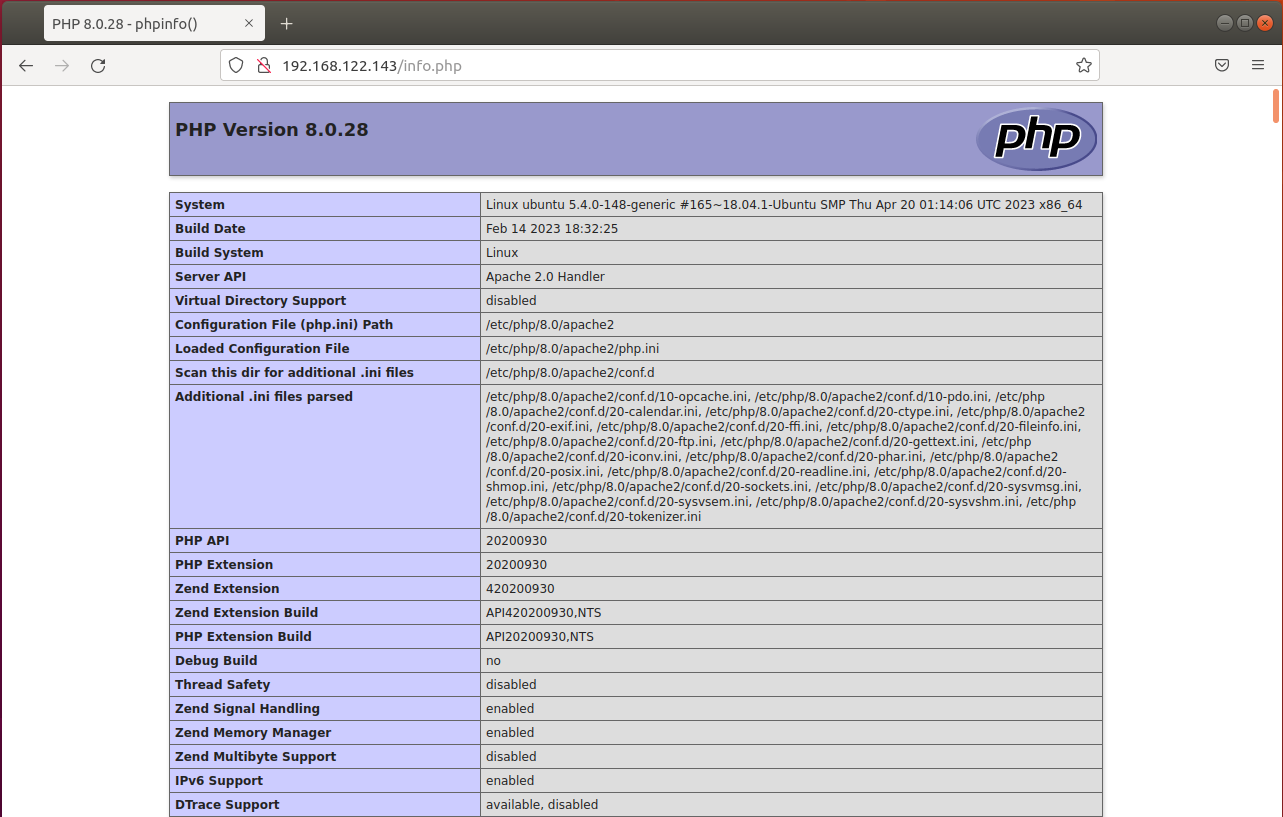
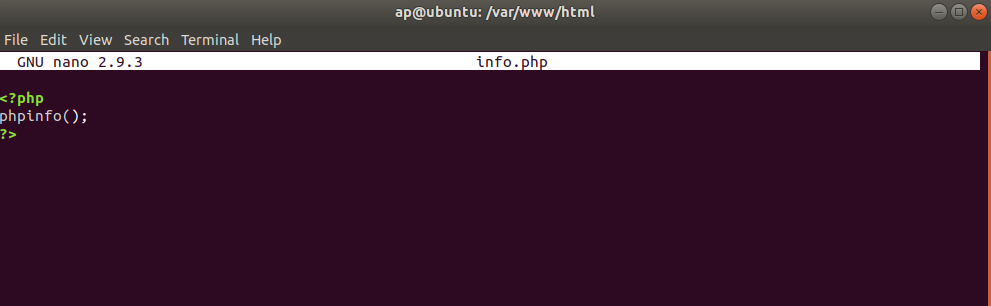
Không cho phép root truy cập database từ xa

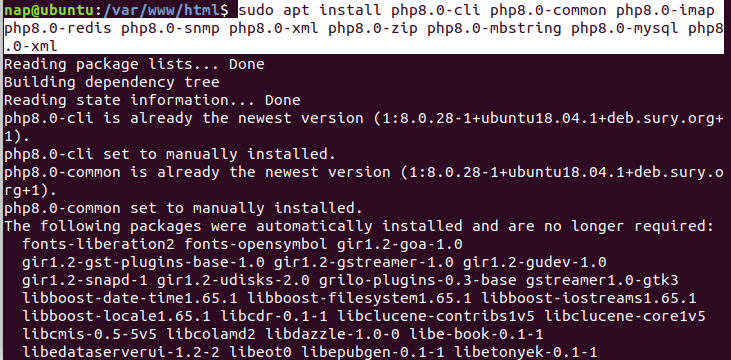
Xóa cơ sở dữ liệu thử nghiệm



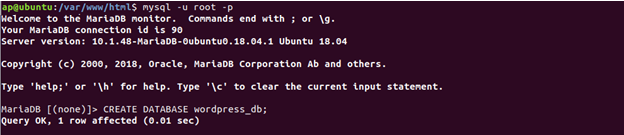
Tải lại cơ sở dữ liệu để thực hiện các thay đổi

Tiếp tục tải PHP 8.0

Tạo 1 tệp info.php để kiểm tra xem PHP

Cài đặt các extension cho PHP

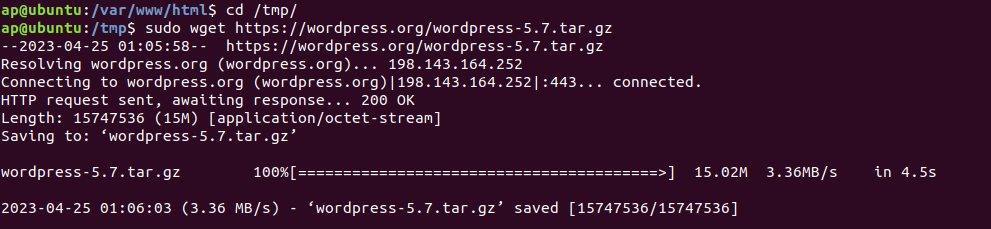
Tạo Database Wordpress

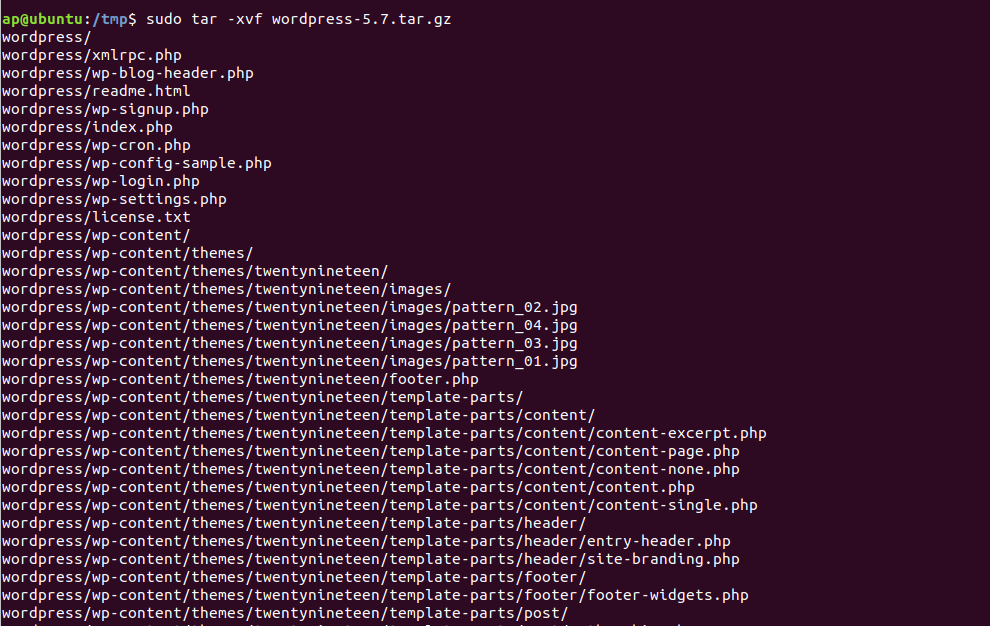
Đăng nhập vào Database MariaDB với quyền root và Tạo database với name: ‘wordpress\_db’

Tạo User ‘wp\_user’ và Password ‘password’

Cấp quyền cho người dùng truy cập cơ sở liệu



Chuyển đến thư mục tmp và tải bản ‘5.7 WordPress’

Giải nén thử mục 

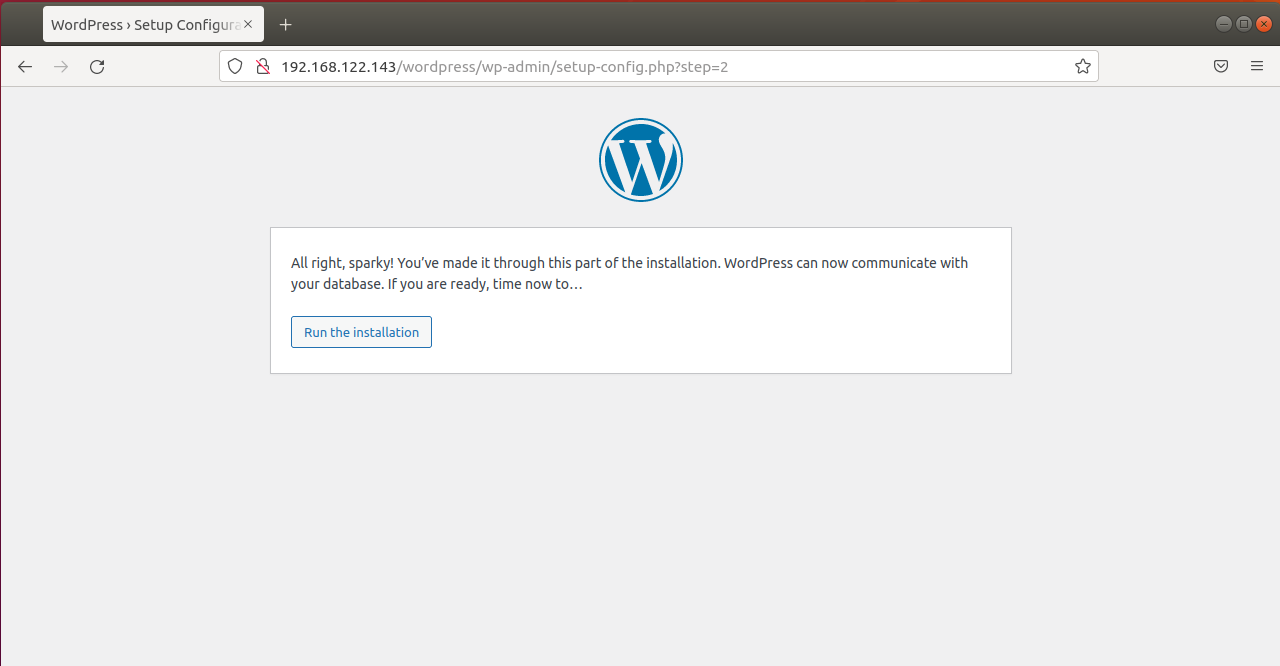
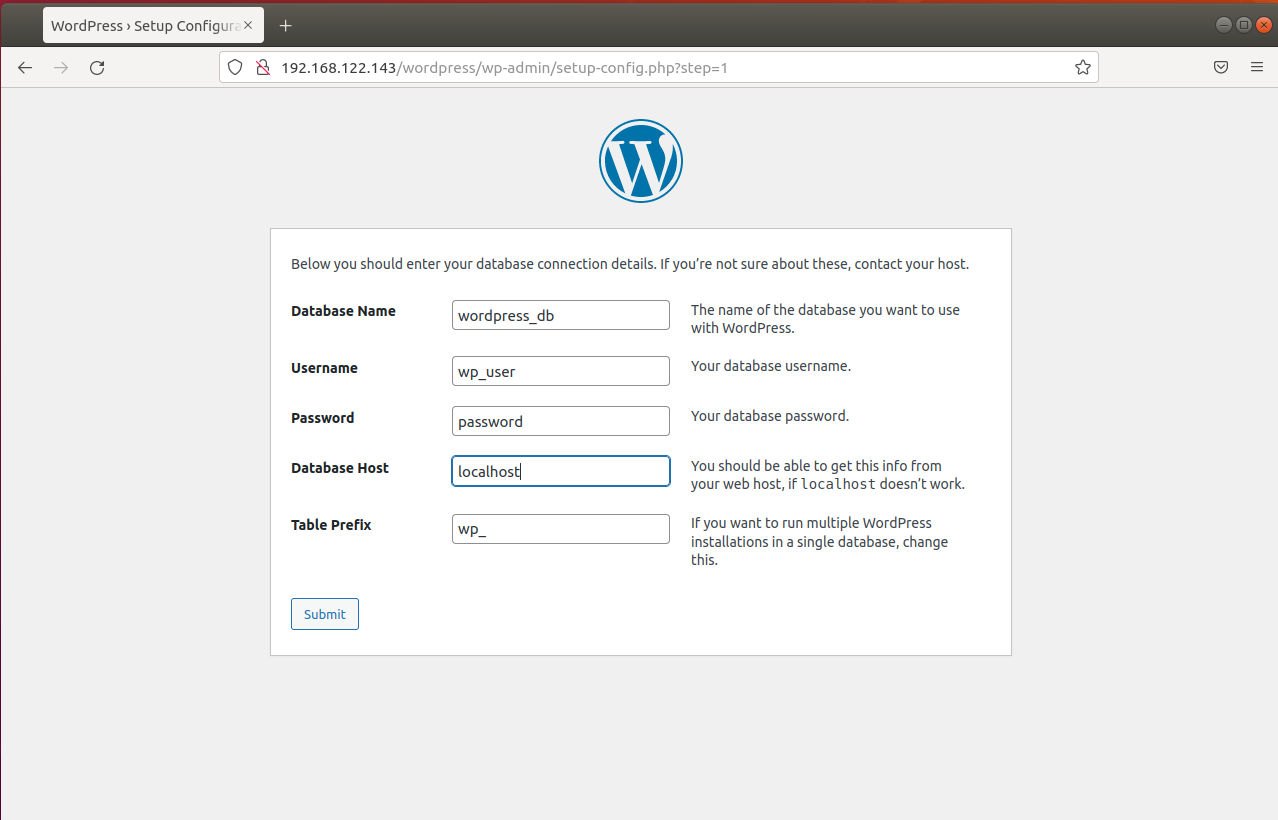
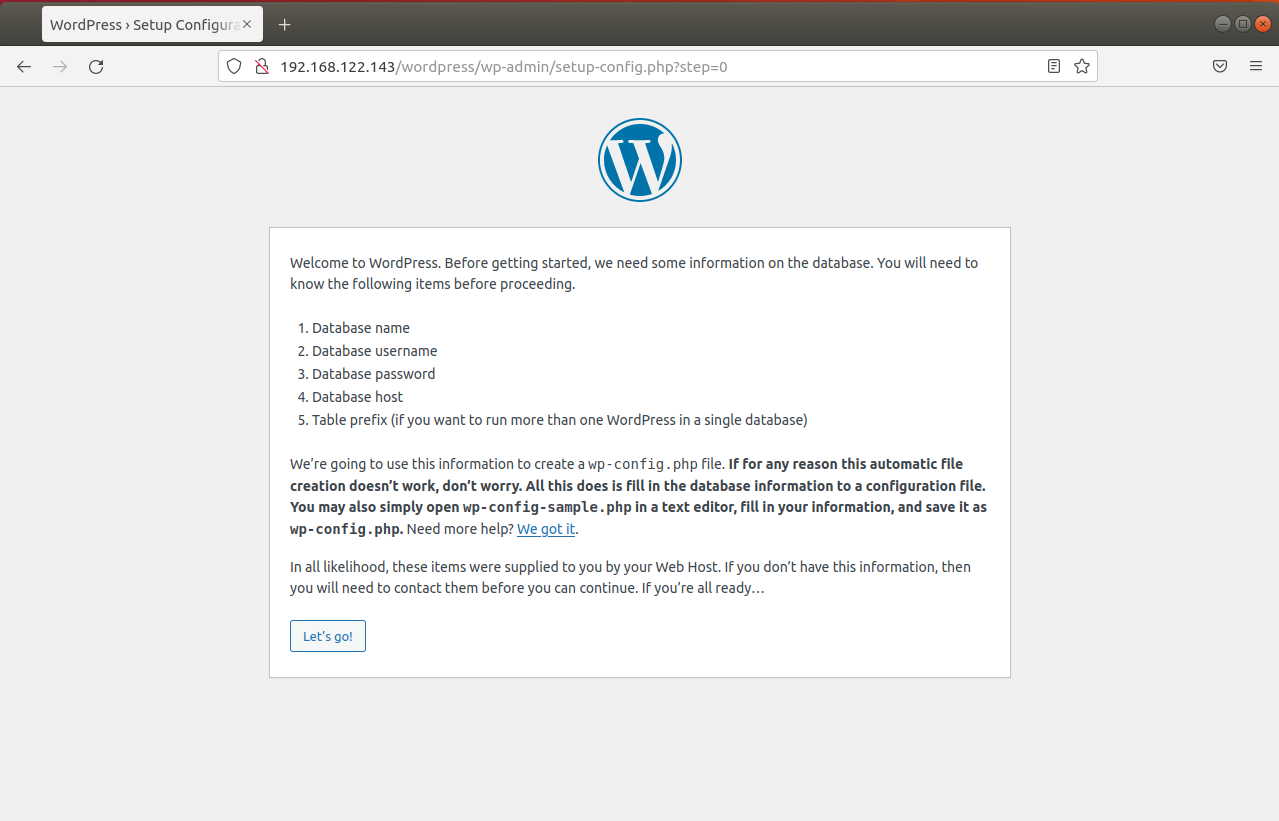
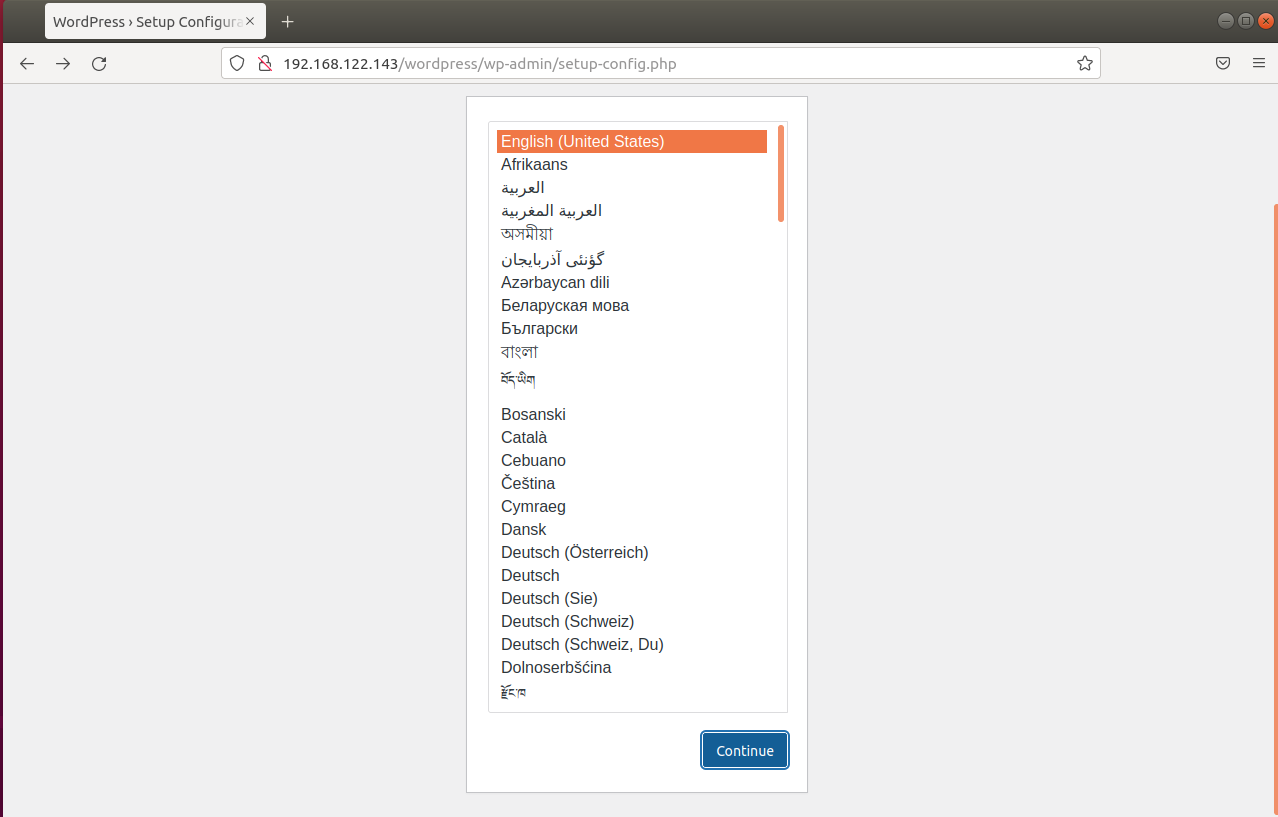
Copy thư mục sang /var/www/html

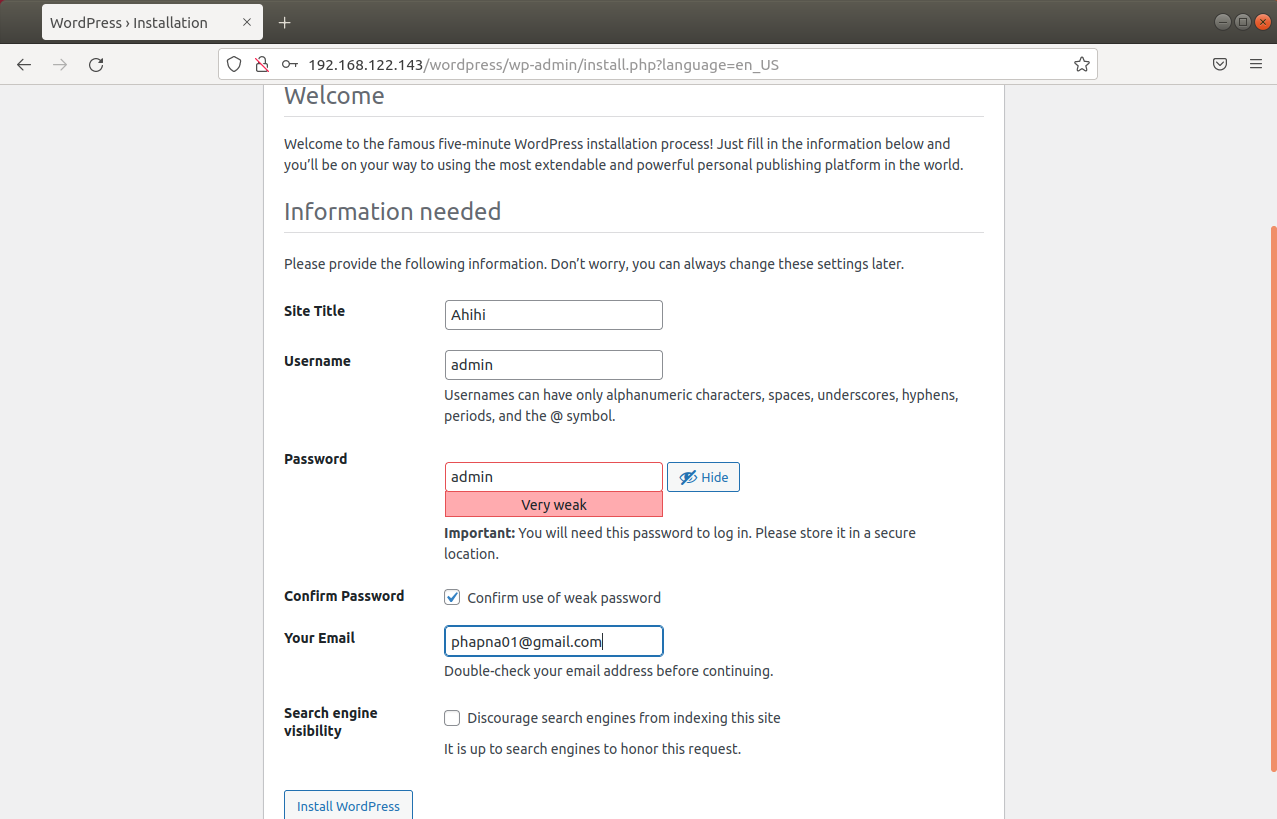
Thay đổi quyền sử hữu của ‘wordpress’ 

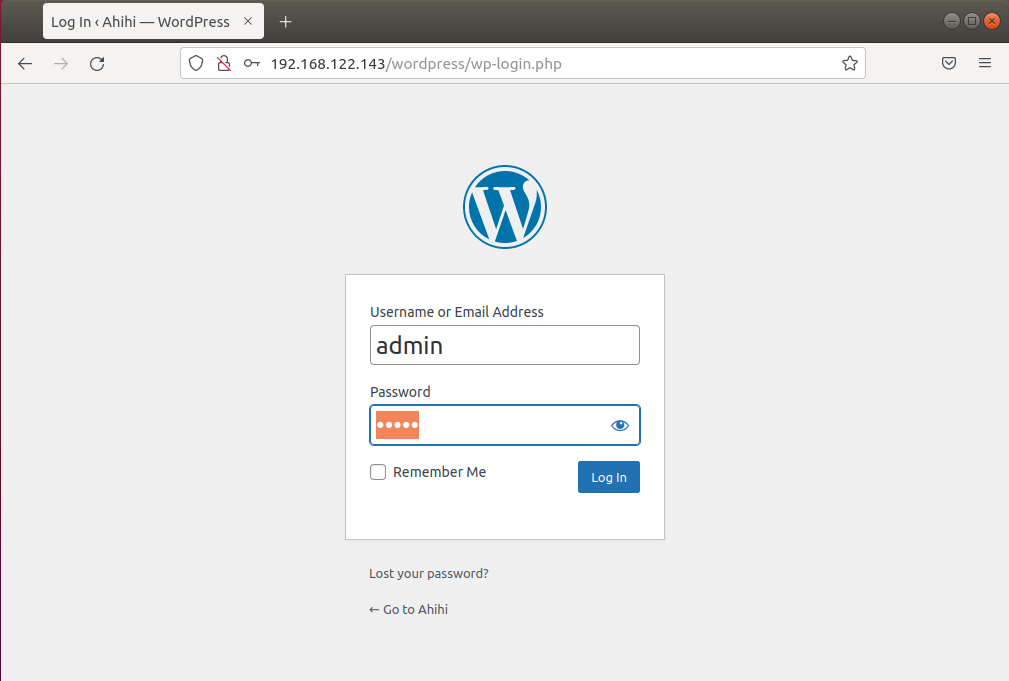
Thay đổi quyền truy cập tệp wordpress

Tạo thư mục uploads để lưu trữ tất cả media được tải lên

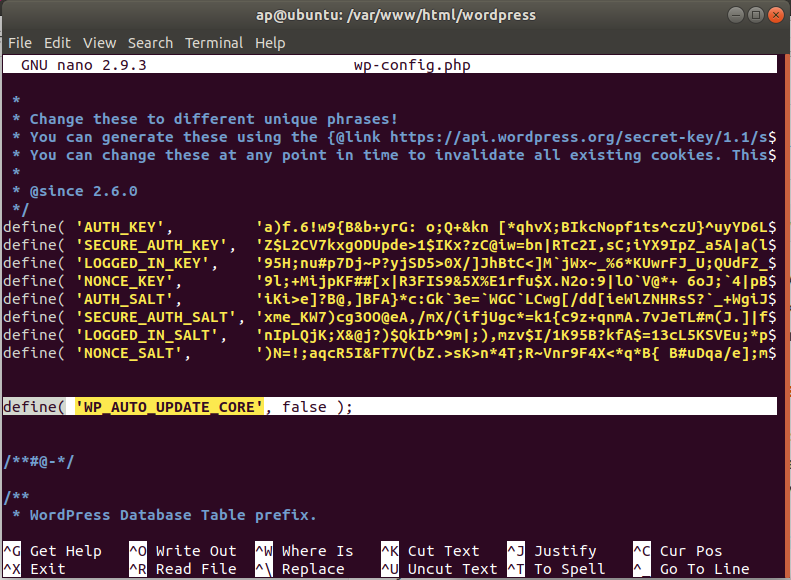
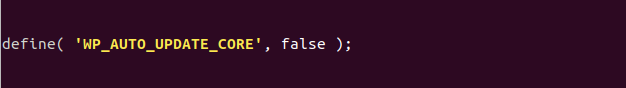


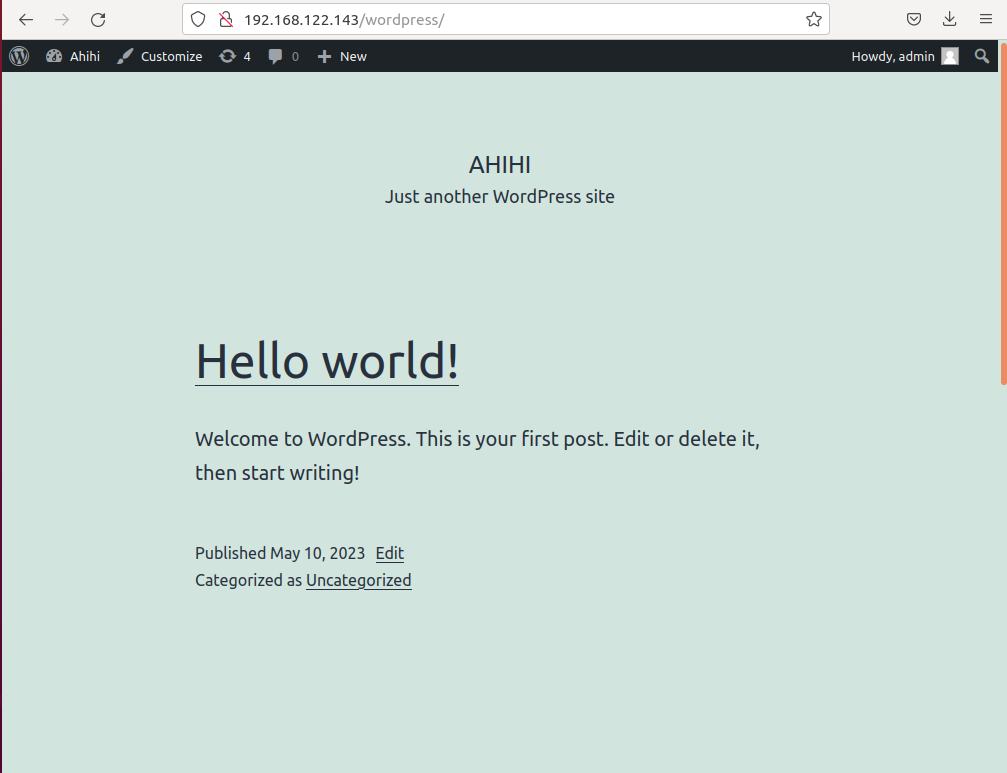
Truy cập wordpress và cài đặt

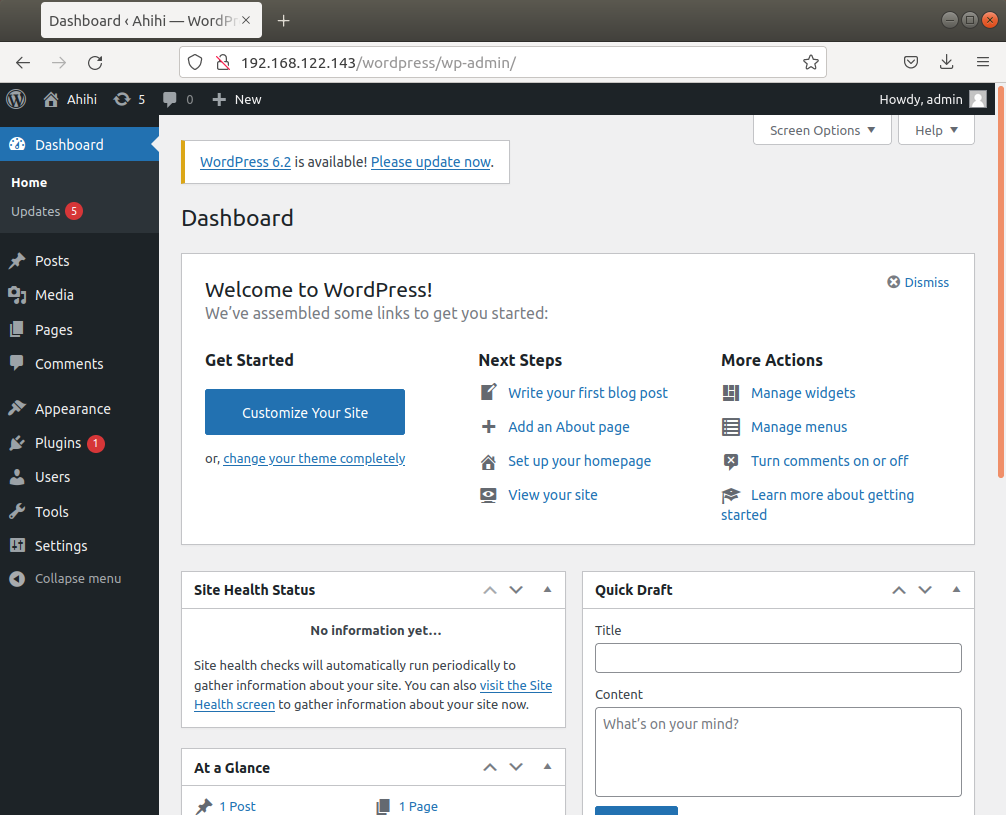
Tạo tài khoản admin

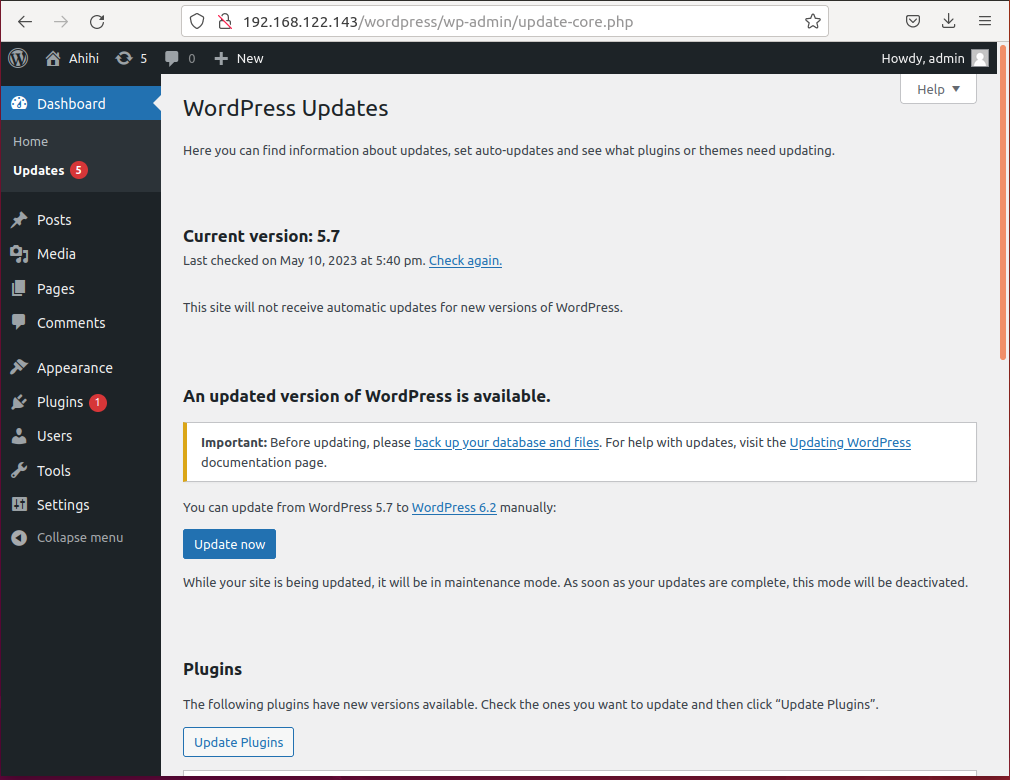
Đăng nhập vào wordpress

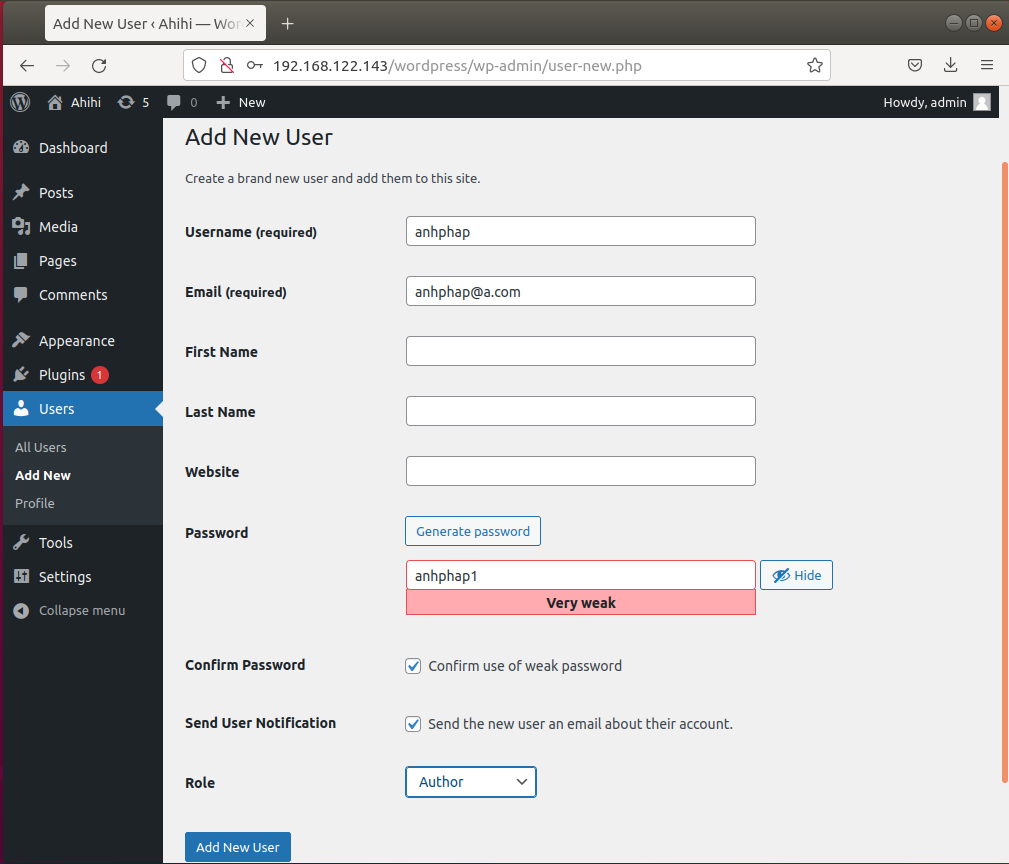
Do Wordpress cho phép tự động cập nhật khi có there is a minor update available. Thêm config vào file wp-config.php để ngăn chặn việc tự động update trên trang web của mình

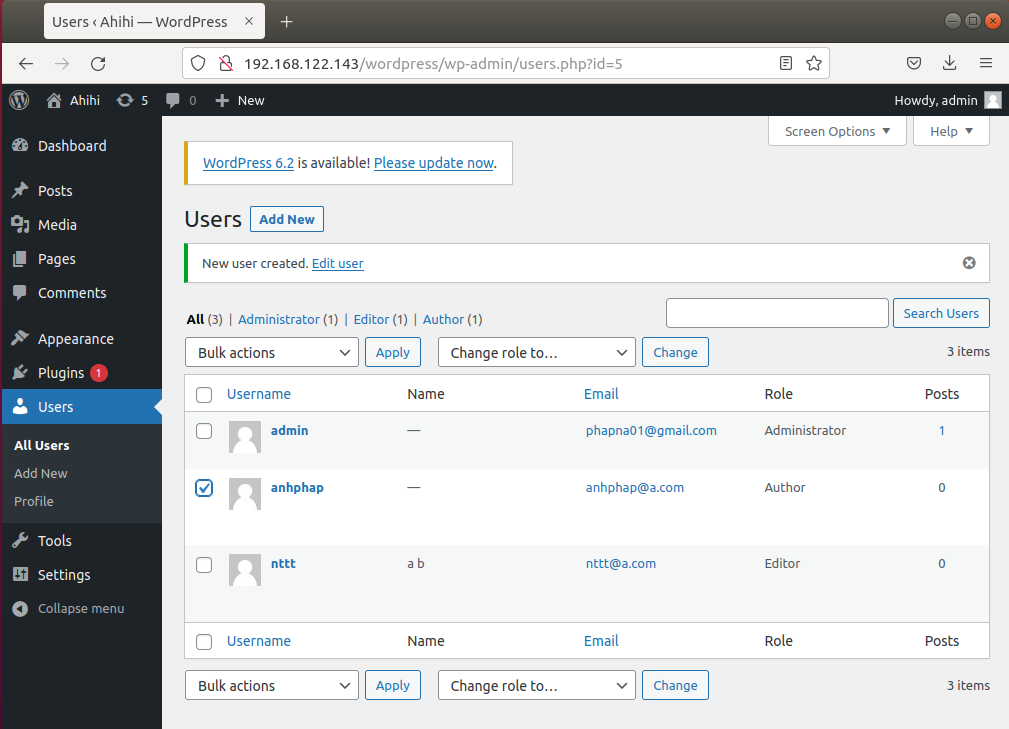


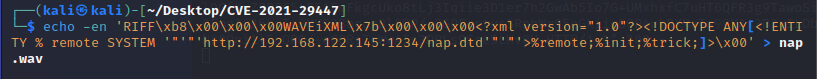
Login thành công với Username: admin và Password: admin 

Giao diện Dashboard trên wordpress

Check Version hiện tại 

Truy cập vào Users và Add New UserAdd user với Role Author để có chức Add Media

Add User thành công

Tạo tệp nap.wav 

+ ‘echo -en’ Hiển thị và kích hoạt sử dụng các ký tự đặc biệt

+ RIFF định dạng tệp âm thanh RIFF

+ \x8\x00\x00\x00\x00: Định dạng khối lượng với 32bit(4byte)

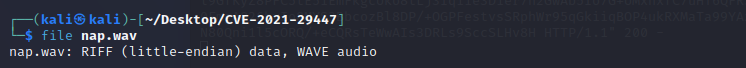
+ WAVE cũng định dạng tệp âm thanh WAV

+ Trong Entity: % remote thực thể tham số (parameter entity) định nghĩa Entity có chứa tham số

+ %remove. %init, %trick (entity reference) được định nghĩa để trỏ đến các parameter entity

+ \x00 kết thức tệp wav

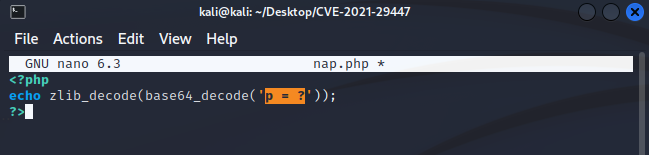
+ > nap.wav: được lưu vào tệp nap.wav

Đọc loại tệp nap.wav 

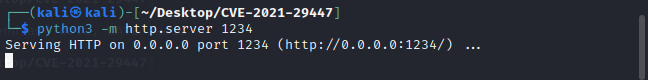
Tạo tệp nap.dtd 

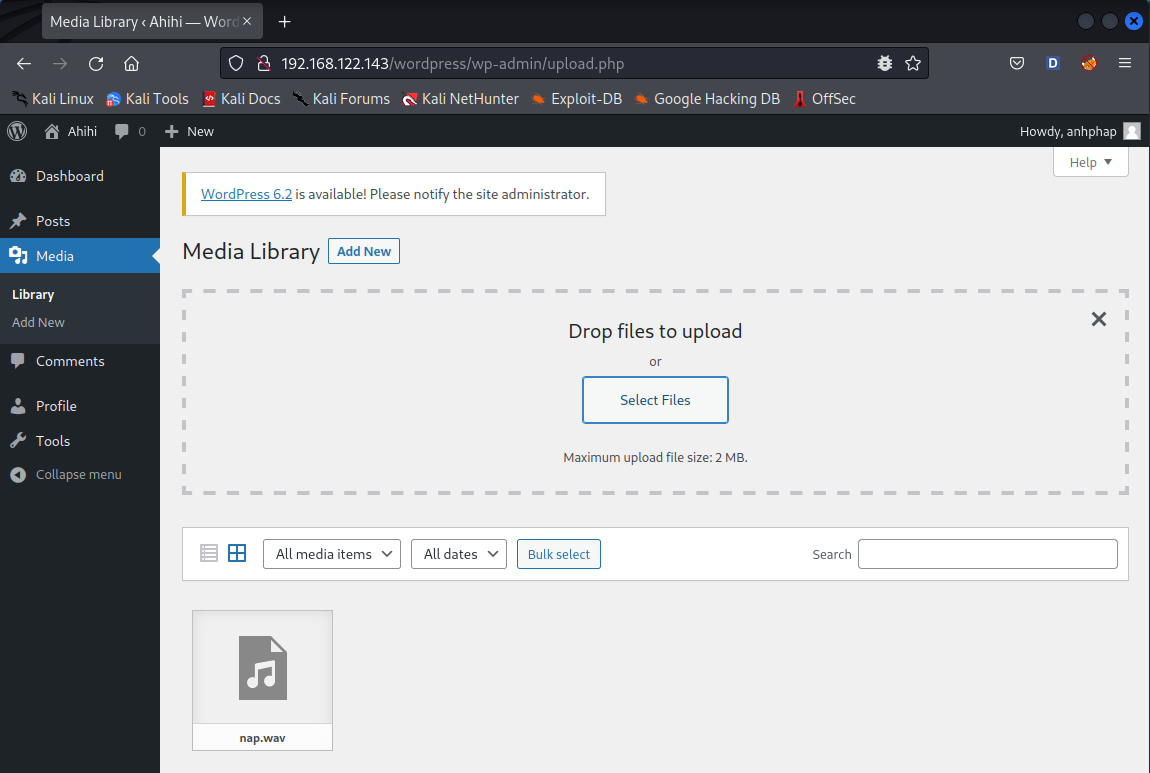
+ Tạo 1 thực thể % file: Để filter các dữ liệu từ thư viên zilb mã hóa thành chuỗi base64 và đường dẫn để đọc và nén dữ liệu

+ Tạo 1 thực thể % init: Trong 1 parameter entity giá trị % sẽ được encode thành ‘&#x25;’ , thực thể trick định nghĩa cho url với tham số p=%file

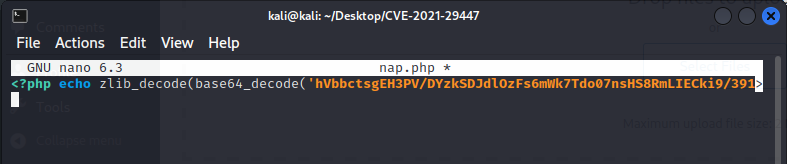
Taọ tệp nap.php

Giá trị p sau khi mã hóa chuỗi 64 sẽ được dán vào “p=?’

Tạo máy chủ http.server với port 1234

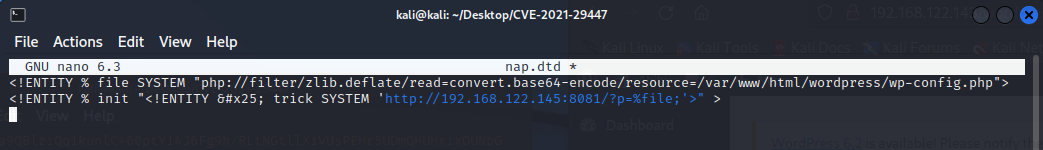
Tải lên tệp nap.wav

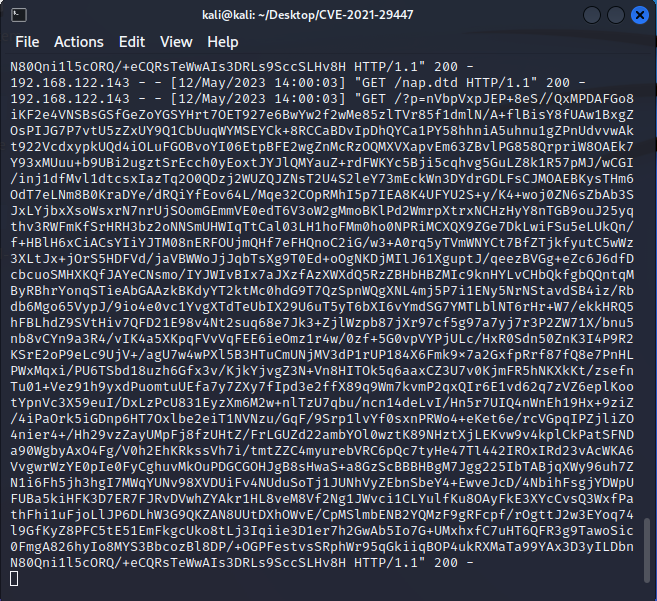
Giá trị p được trả về 

Sao chép giá trị p và chèn vào tệp nap.php

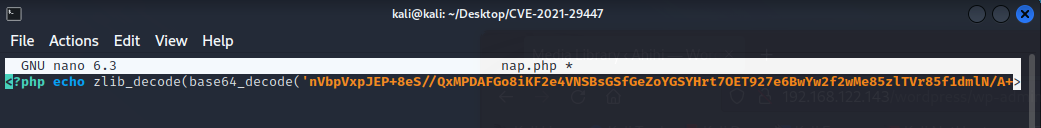
Thực thi bằng câu lệnh ‘php nap.php’Giá trị sau khi chạy tệp php

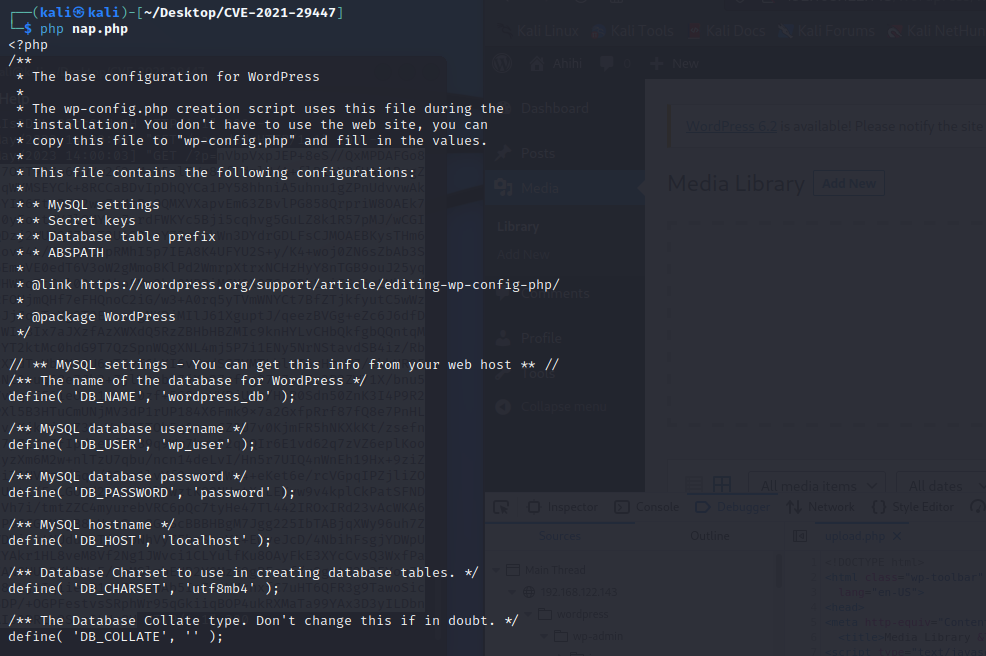
Thay resource để đọc tệp wp-config.php



Sau khi tải lên tệp nap.wav

Giá trị p trả về

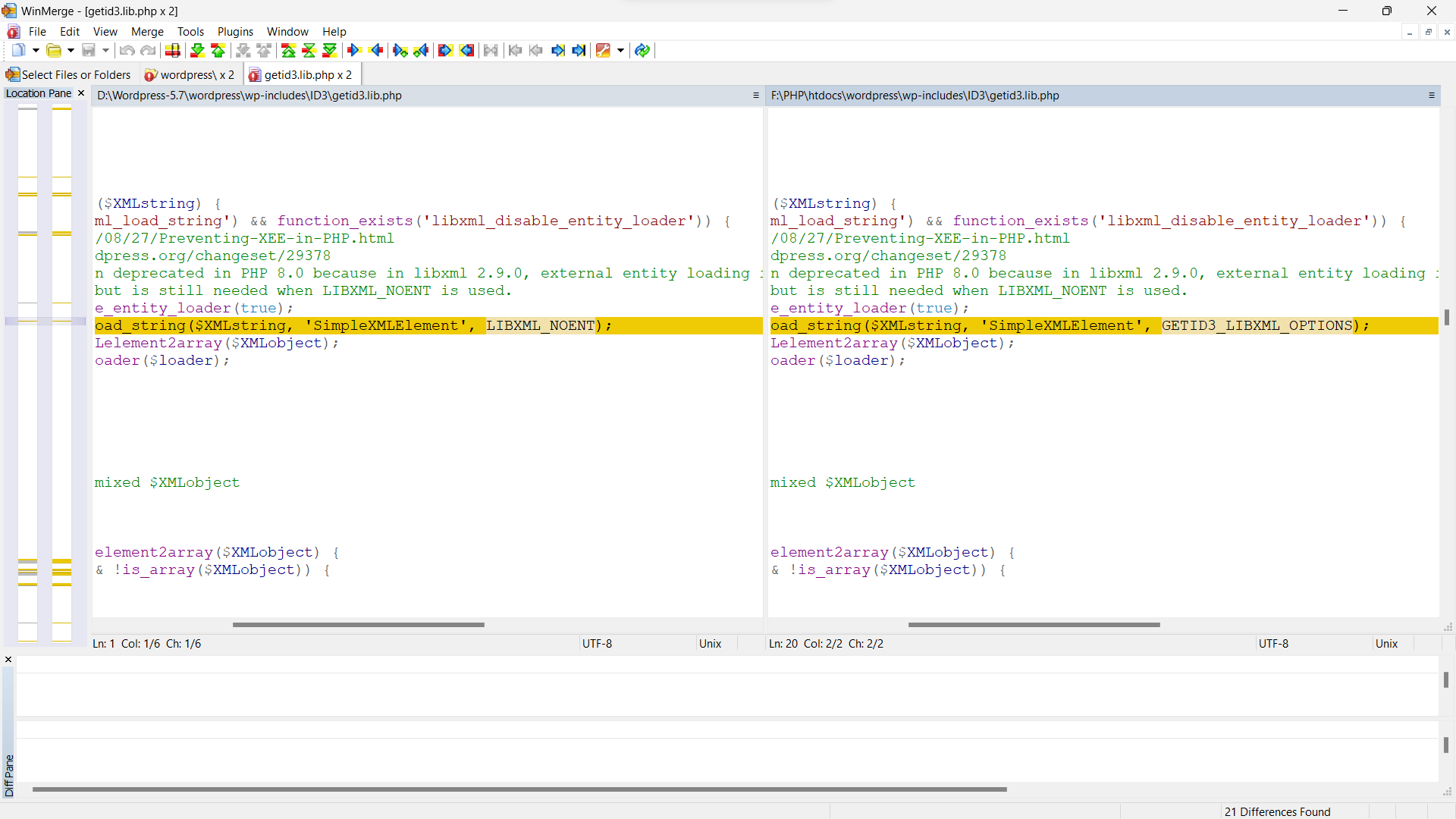
Sao chép giá trị p và dán vào tệp nap.php

Kết quả thu được -> Đọc được file config thành công

Trên máy vật lý: Tải xuống 2 phiên bản wordpress 5.7 và wordpress 5.7.1.

Sử dụng WinMerge để phân lích folder wordpress 5.7 với wordpress 5.7.1

Tải xuống WinMerge để so sanh tập tin của 2 phiên bản wordpress



WordPress 5.7 $XMLobject = simplexml\_load\_string($XMLstring, 'SimpleXMLElement', LIBXML\_NOENT);

WordPress 5.7.1 $XMLobject = simplexml\_load\_string($XMLstring, 'SimpleXMLElement', GETID3\_LIBXML\_OPTIONS);