**Wordpress Footprinting On** [**http://192.168.1.65/**](http://192.168.1.65/)

**Date:- 10th April 2023**

**Submitted by:- Binay Chaudhary**

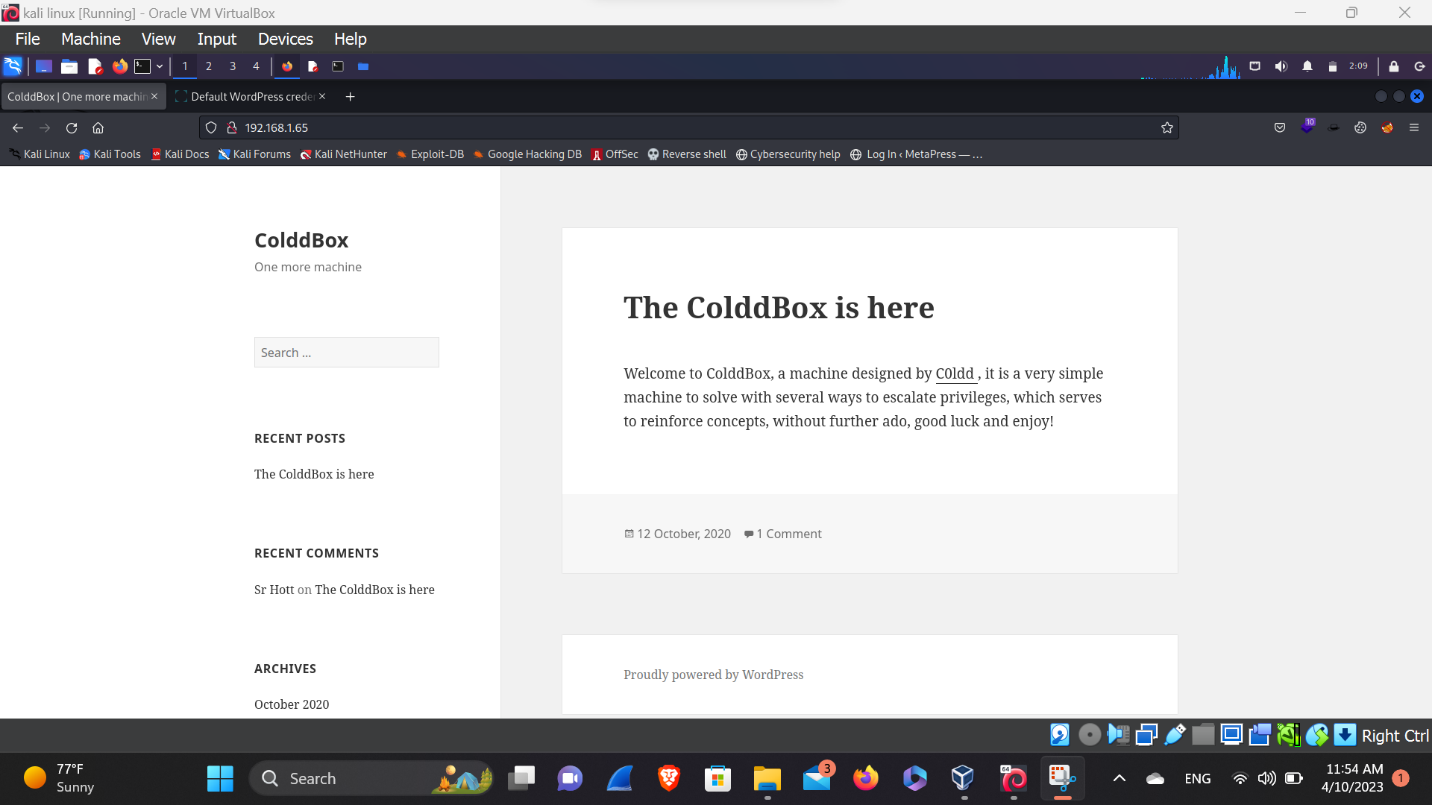
**Submitted to:- Er. Suman Basnet sir**

**Table of Contents page no.**

* **Introduction 3**
* **Wpscan For VP 4**
* **Wpscan for username 5**
* **Wpscan for password 6**
* **Wordpress Login 8**
* **Conclusion 9**

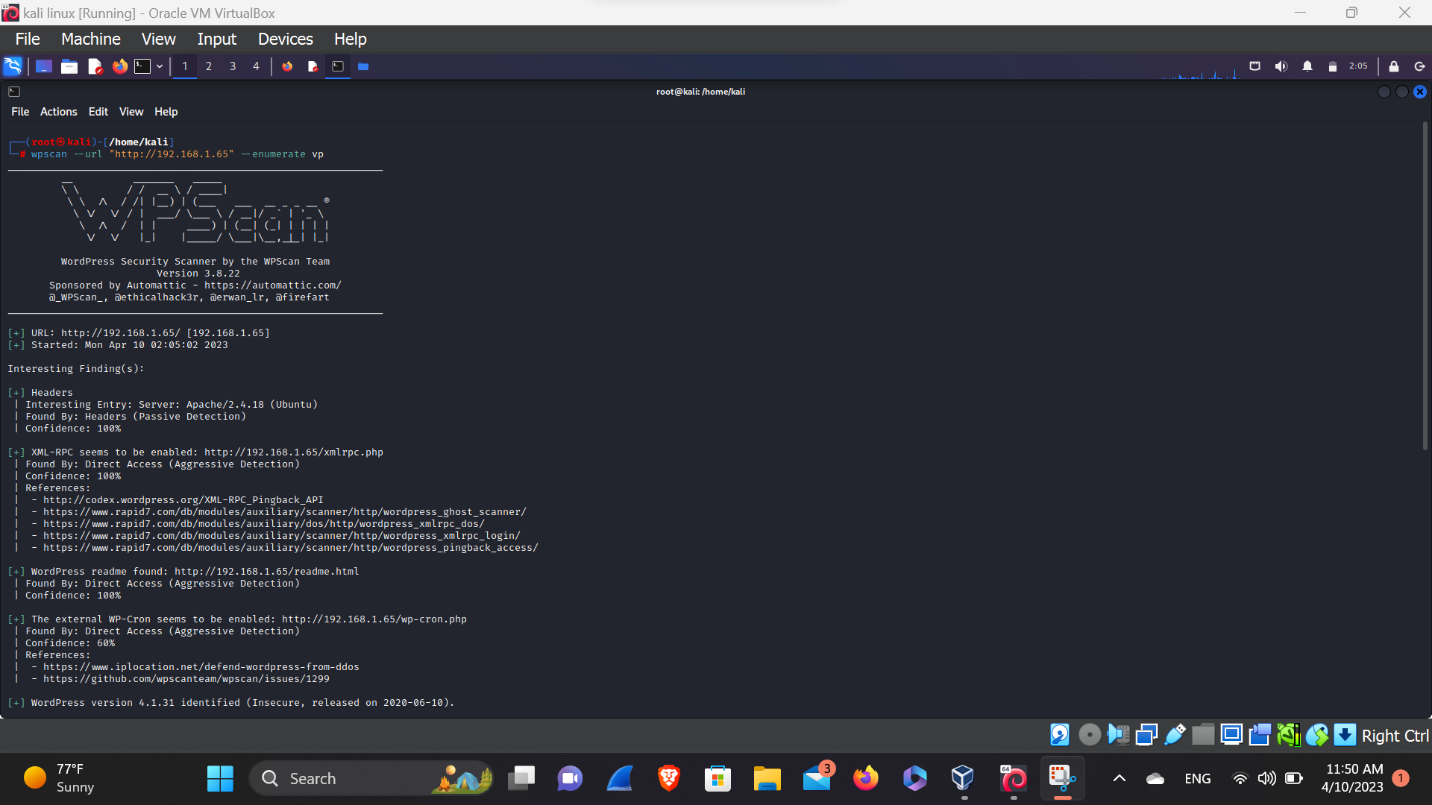
**Introduction**

Here, in this picture we have seen the website of the coldbox, i.e. made up of wordpress.

****

**WPSCAN vp (vulnerable plugin)**

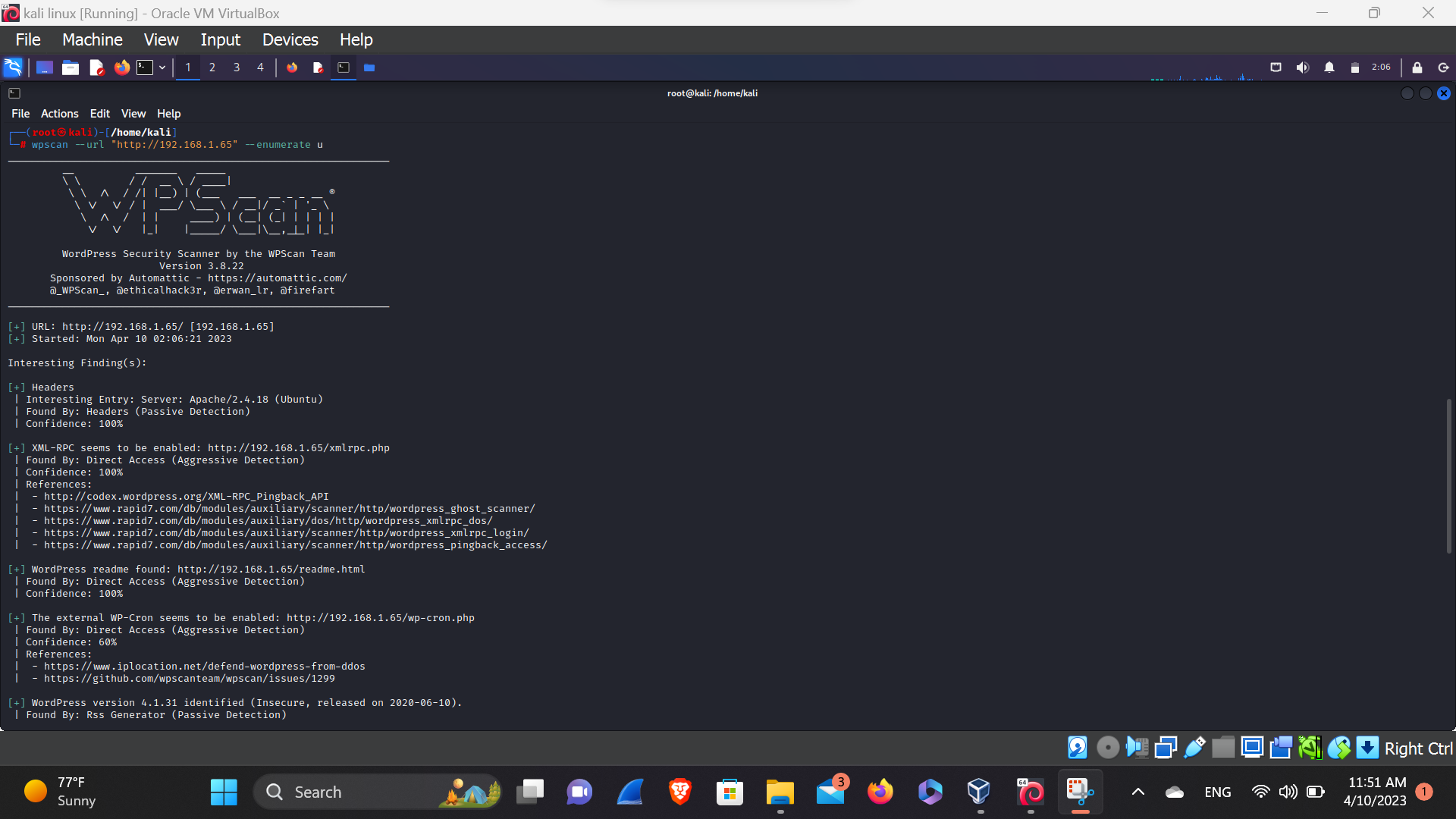
Here, in this picture we’ve search for the vulnerable plugin that can be vulnerable to SQL injection. But in this scan we’ve not found anything but the wordpress version is out of date. So, we need to upgrade the wordpress to the latest version.

****

**Wpscan for username**

Here, in this picture we’ve scan for the username enumeration so, let’s find the username of the login page of the wordpress. After some time we’ve found the 3 username i.e. :-

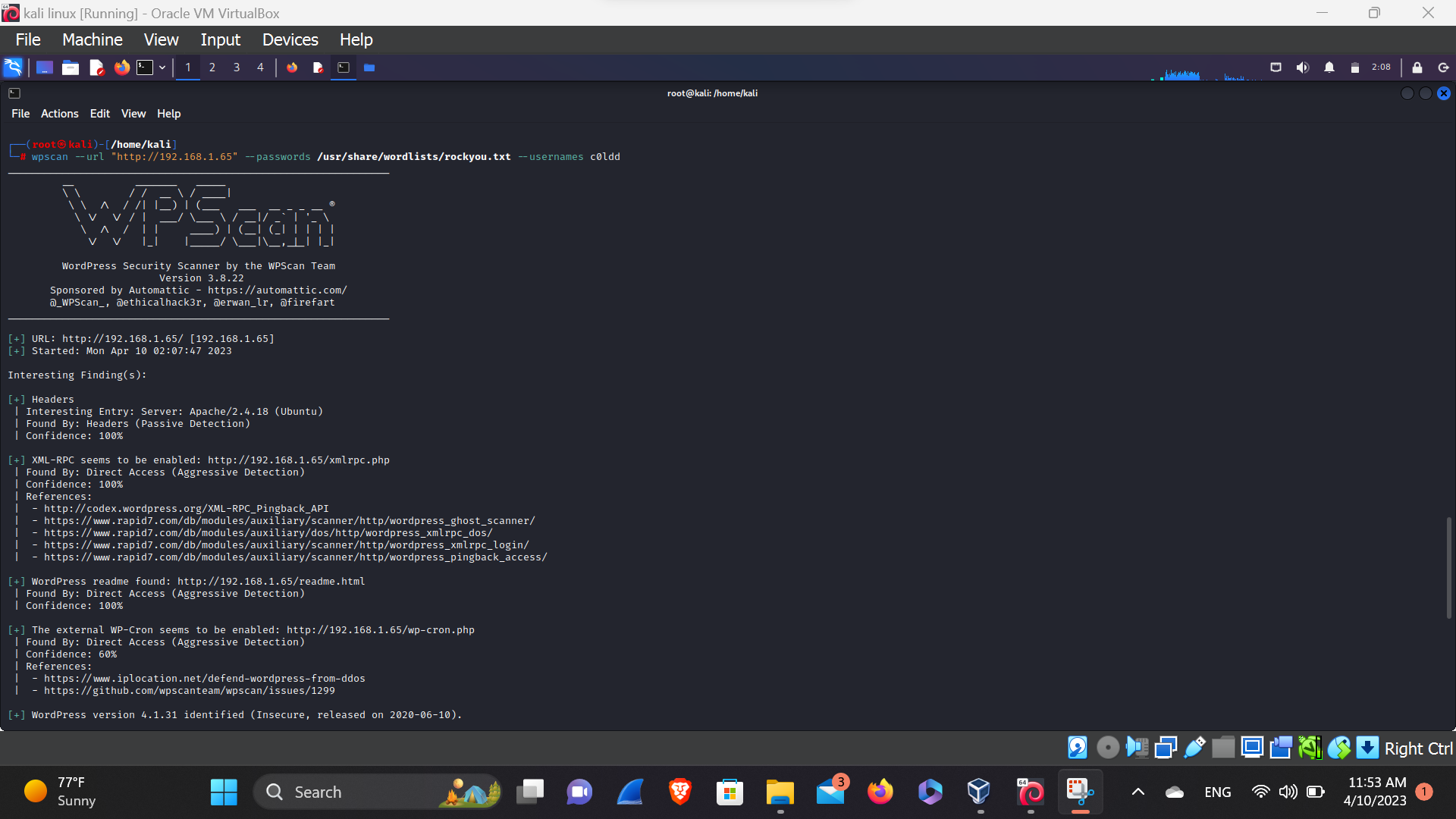
1. Philip
2. c0ldd
3. hugo

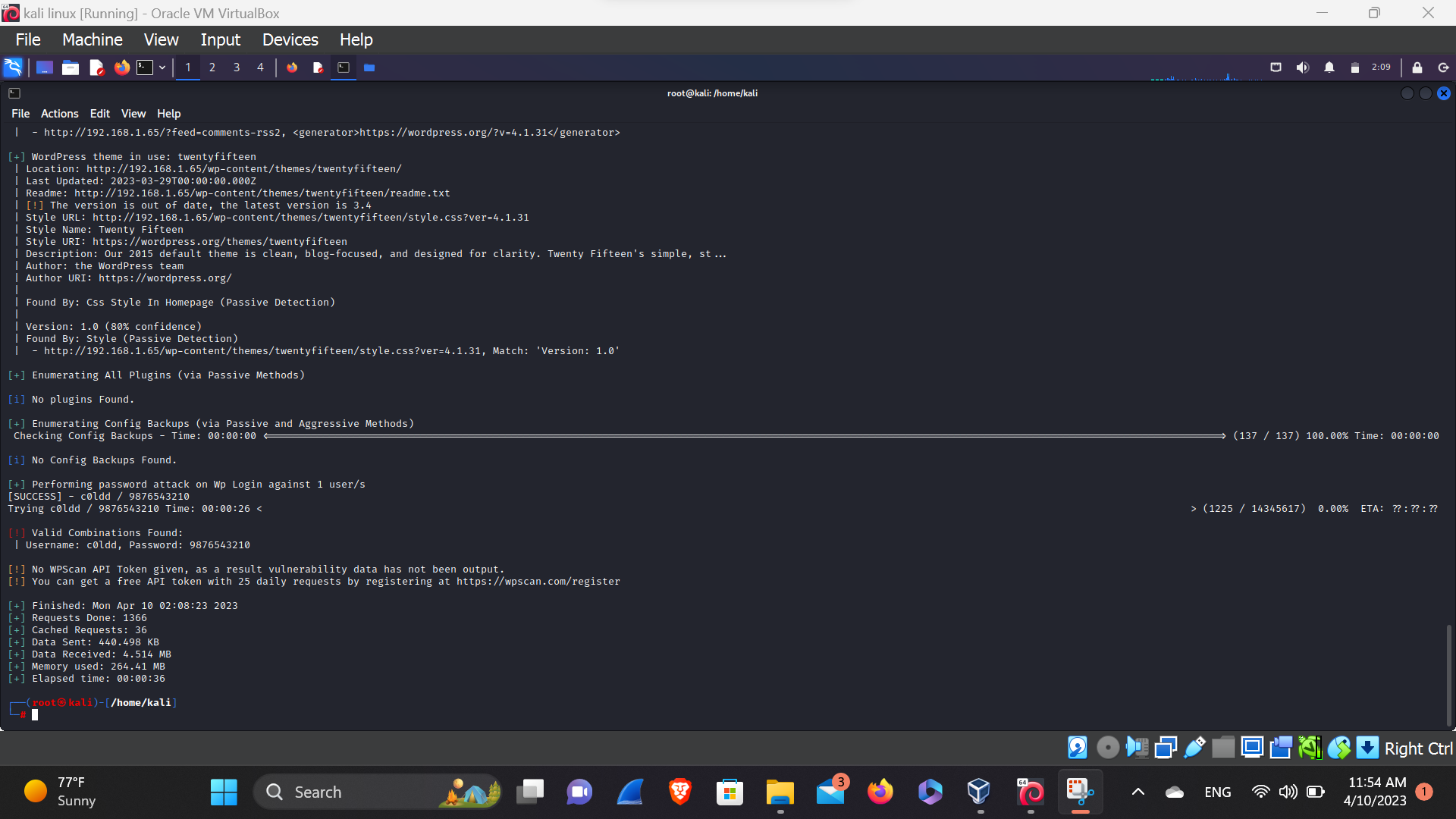


**Wpscan for password**

Here, in this picture we, have bruteforce the weak credentials of the founded username i.e.

1. Philip
2. c0ldd
3. hugo

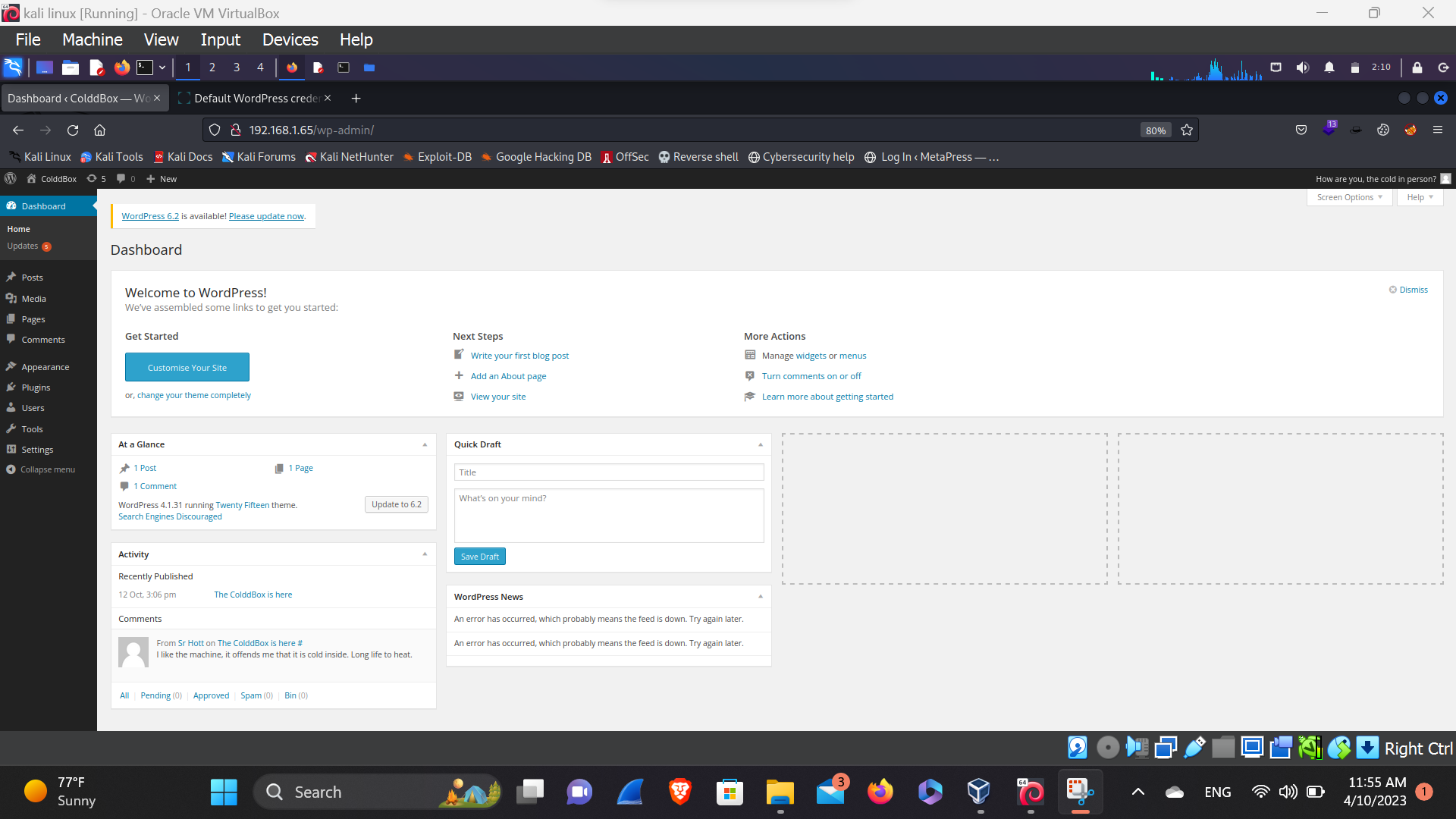
After bruteforcing we’ve found the weak credentials of the username is c0ldd and the is his mobile number.



Her, in this above picture we’ve seen the weak password of the username is 9876543210. So, let’s try to login in the wordpress.

**Wordpress Login**

Here, in this picture we can see the we’ve logged in the c0ldd account with the help of his weak credentials

****That may an attacker can brute force the password and logged in the account.

**Conclusion**

1. To prevent attack in the wordpress Be, sure to update your version and the plugin.
2. Always use strong password that can’t be found through the brute force attack and can’t guessable your password.