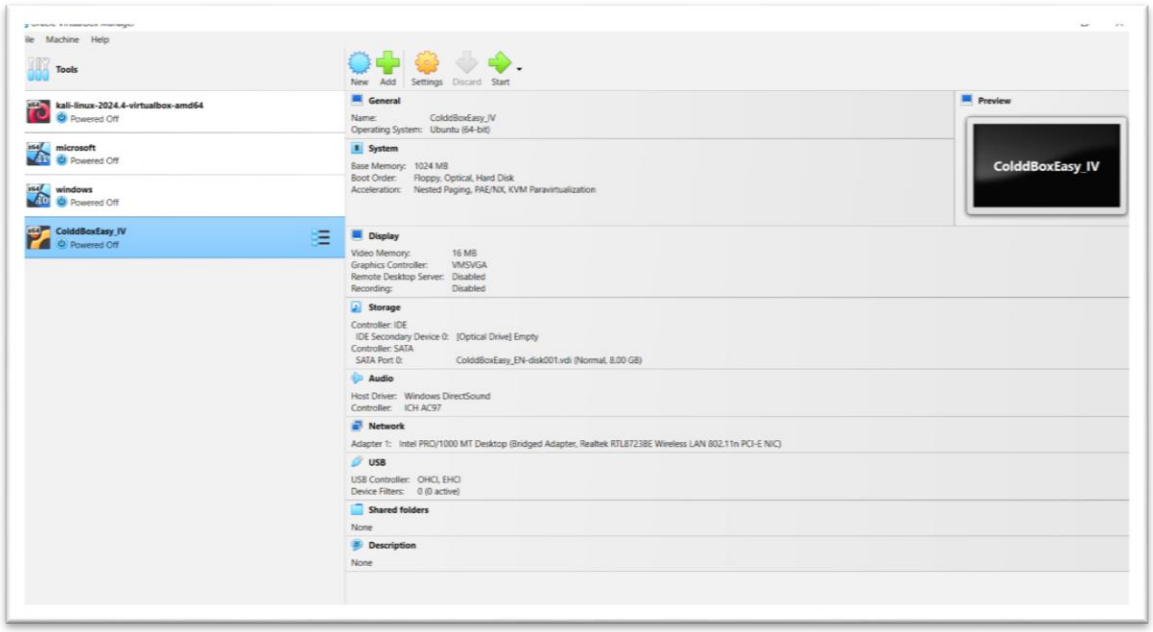
MINOR PROJECT

PENETRATION TESTING ON C0LDDBOX

DONE BY,

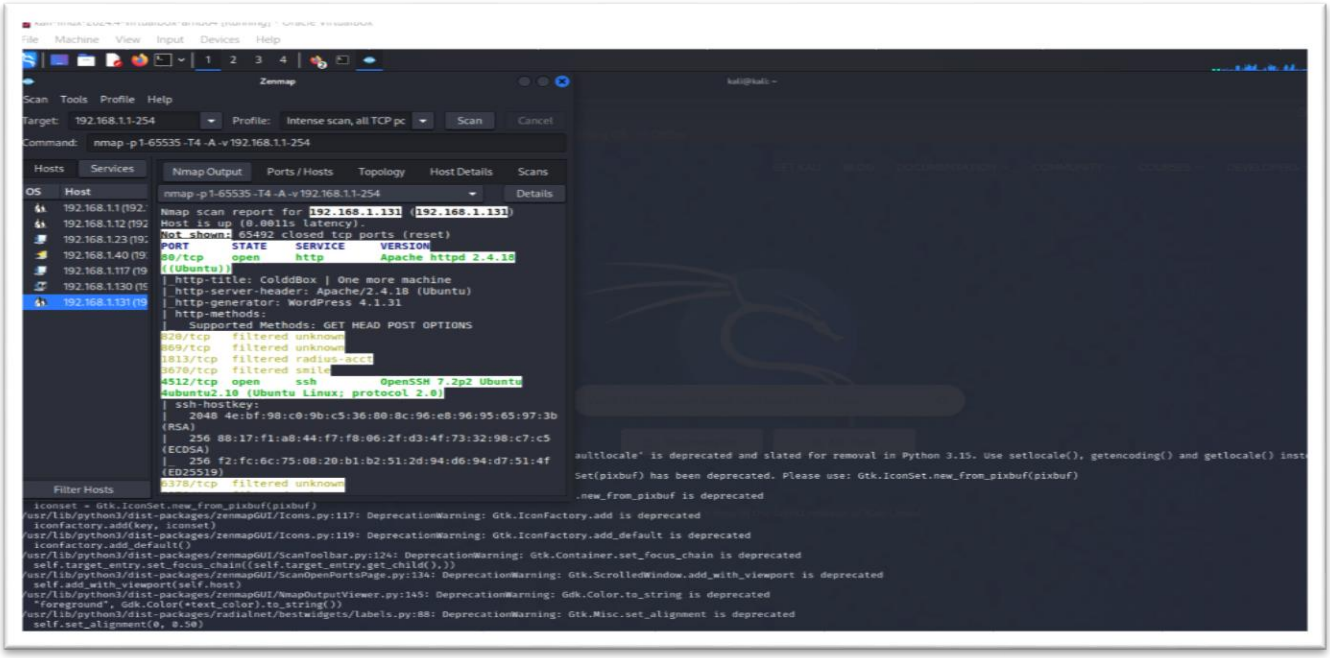
HARIVISHALINI.T

STEP 1: WE NEED TO DOWNLOAD VIRTUAL BOX,KALI LINUX AND COLDDBOX IN OUR SYSTEM

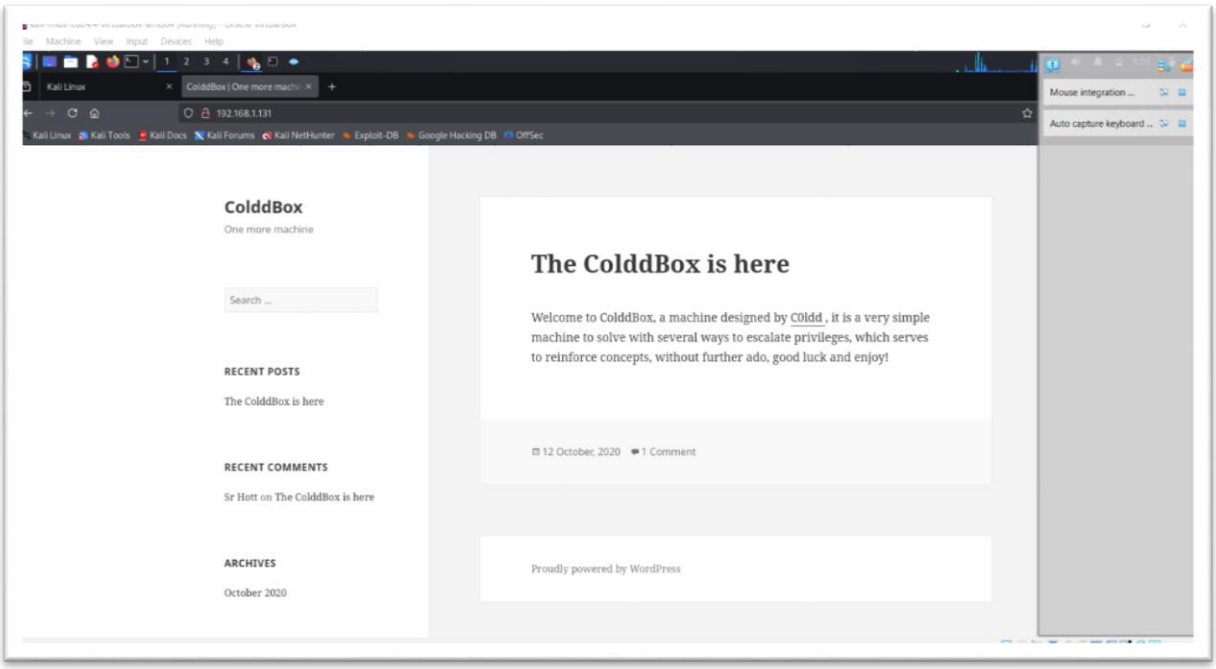


STEP 2:WE NEED TO RUN THE BOTH ON THE VIRTUALBOX,NOW WE NEED TO CHECK THE IP ADDRESS OF THE SYSTEM IN KALI GO TO TERMINAL AND TYPE CONFIG

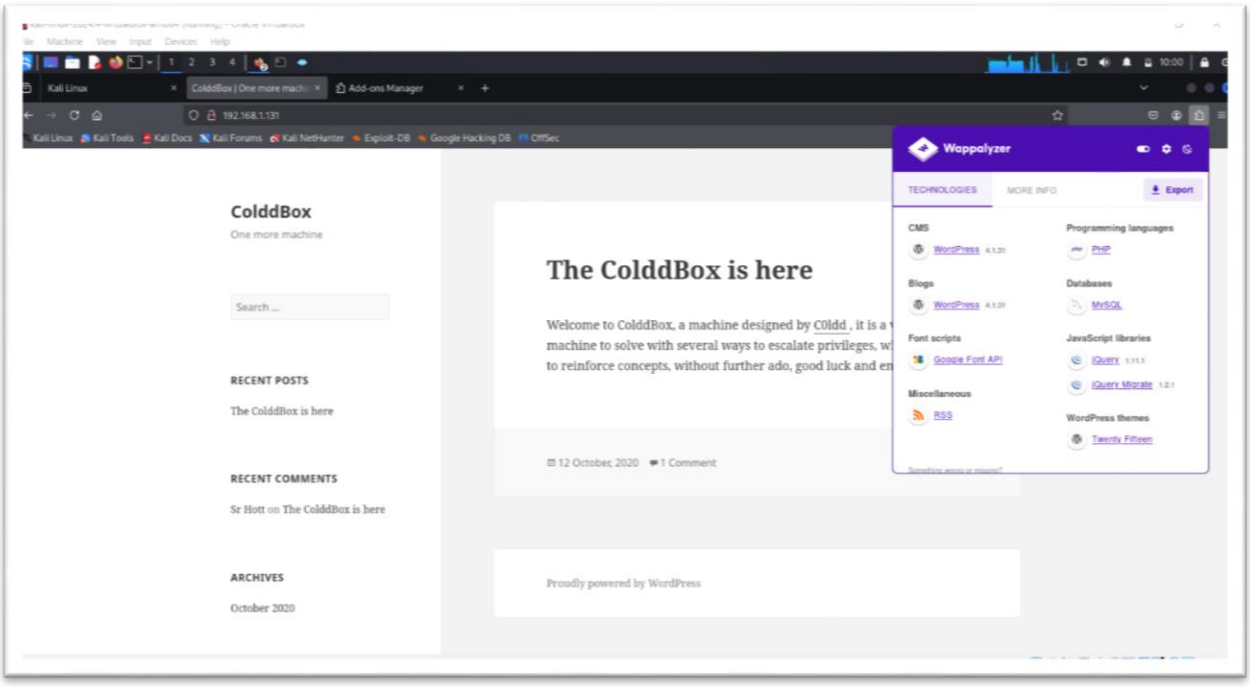
STEP 3:GOTO ZENMAP AND ENTER YOUR IP REPLACING THE LAST ONE NMBER AS 1-254 AND CHANGE PROFILE AS INTENSE SCAN,ALL TCP PORTS AND THEN SCAN



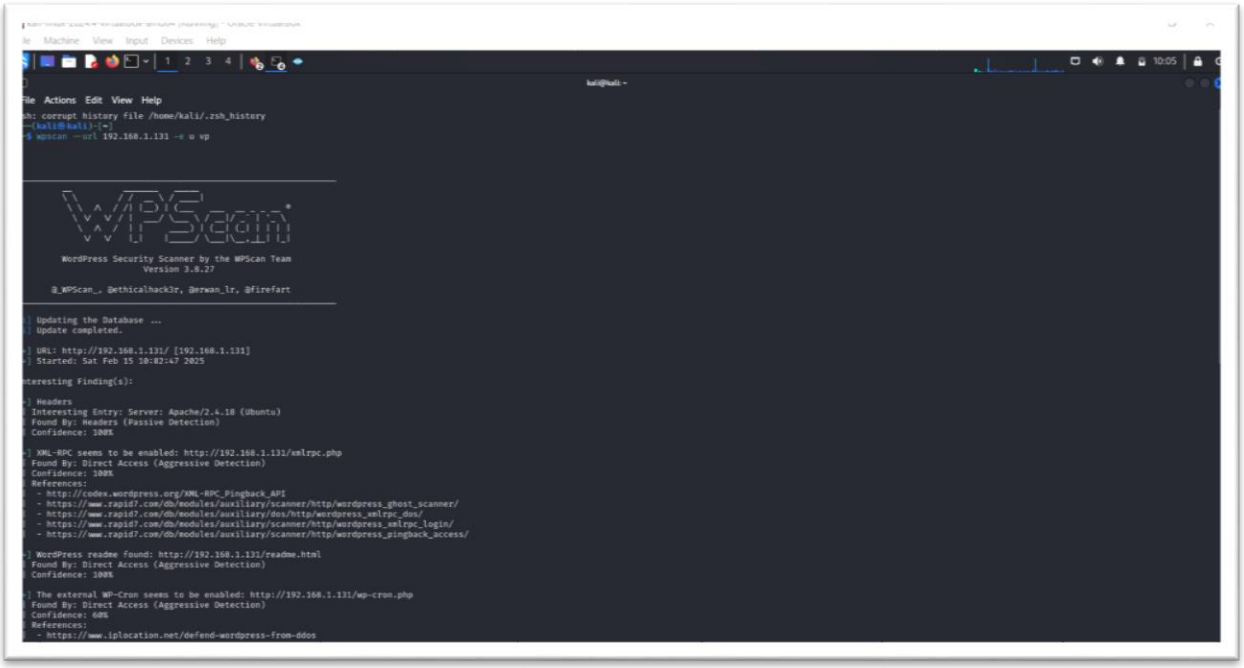
STEP 4:NOW COPY THE URL OF THE COLDDBOX AND PASTE IT IN THE BROWSER



STEP 5:GO TO BROSWER AND DOWNLOAD WAPPALYZE AND UP CORNER THERE IS A PUZZLE PIECE AND WE RUN THE WAPPALYZER IT SHOWS WHAT ARE THE APPLICATIONS ARE PERFORMED IN THAT



STEP 6: NOW WE USE THE WPSCAN FOR THE URL OF COLDDBOX



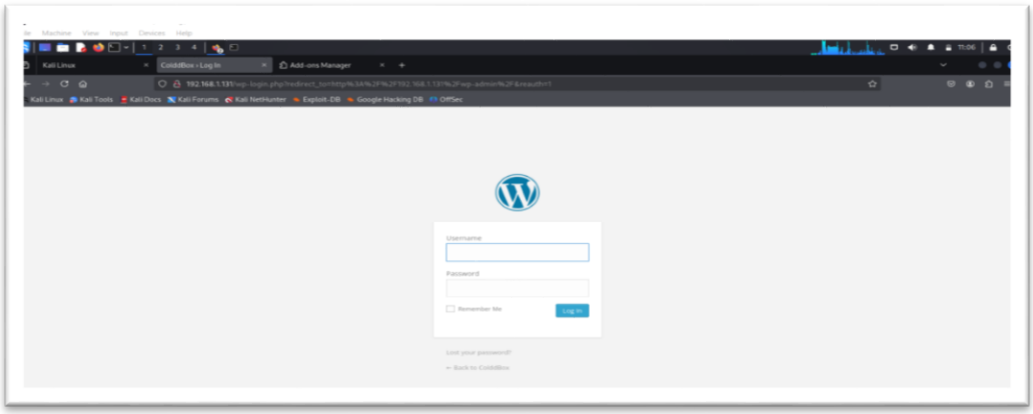
STEP 7:NOW GO TO BROWSER AND DOWNLOAD ROCKYOU.TXT FROM GETHIB .NOW USE THE COMMAND WHICH IS GIVEN BELOW TO GET THE USERNAME AND PASSWORDS

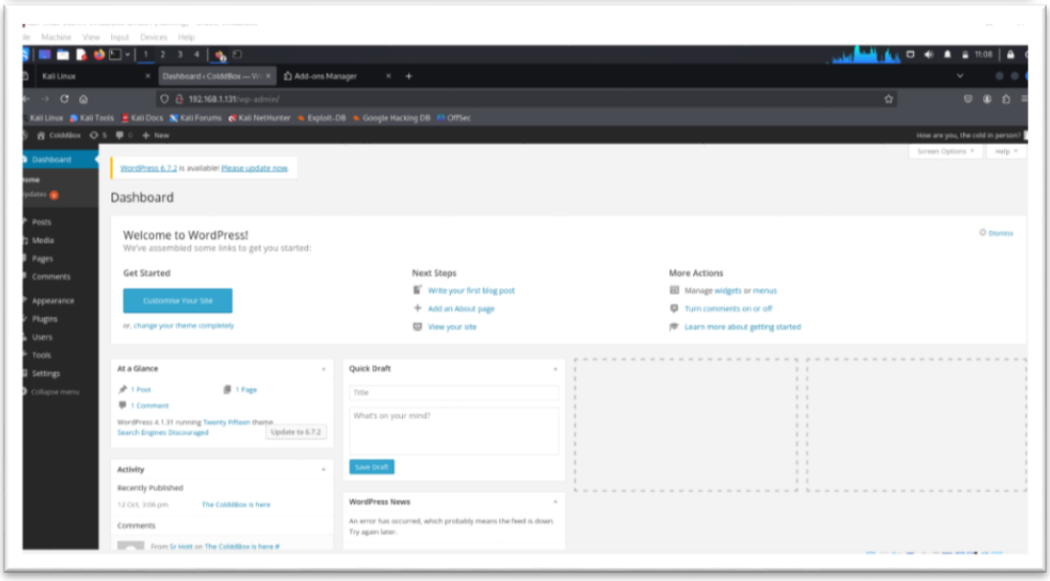
```
┌──(kali㉿kali)-[~]
└─$ wpscan  --url 192.168.1.131 -e u --passwords /home/kali/Downloads/rockyou.txt
```

HERE WE GOT USERNAME=c0ldd

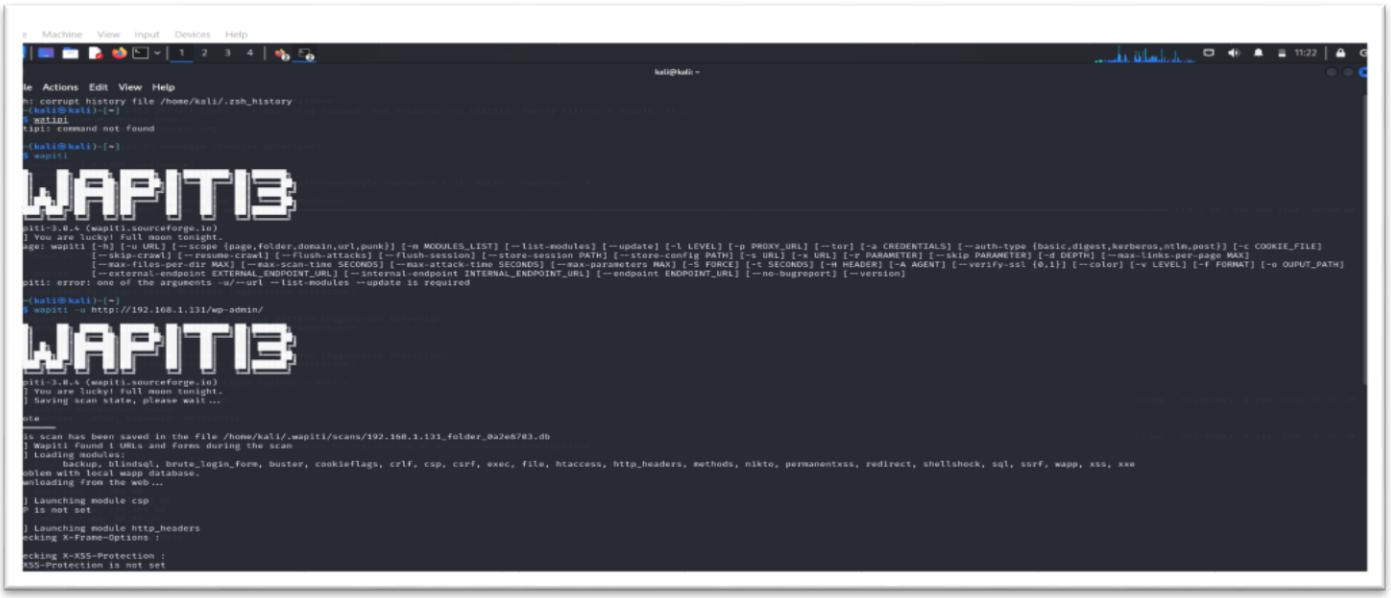
PASSWORD=9876543210

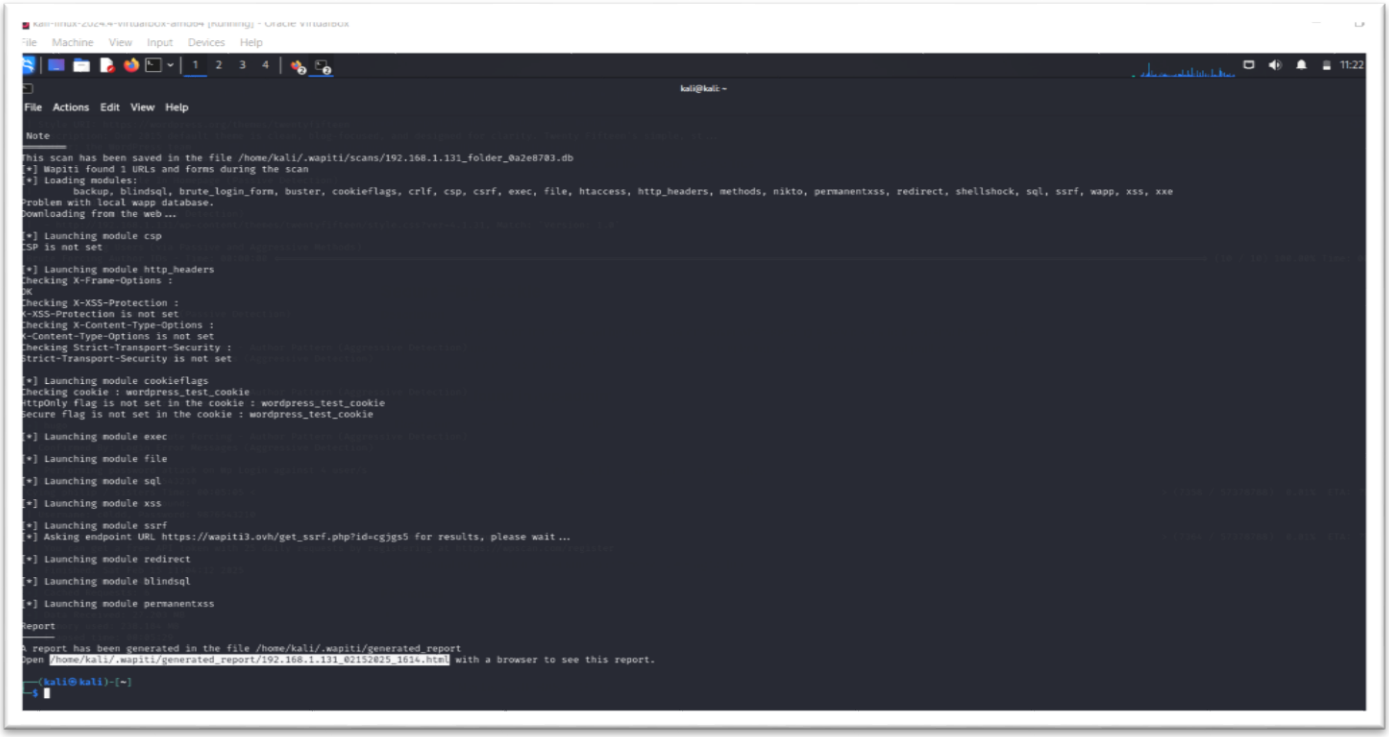
STEP 8:NOW LOGIN TO THE COLDDBOX



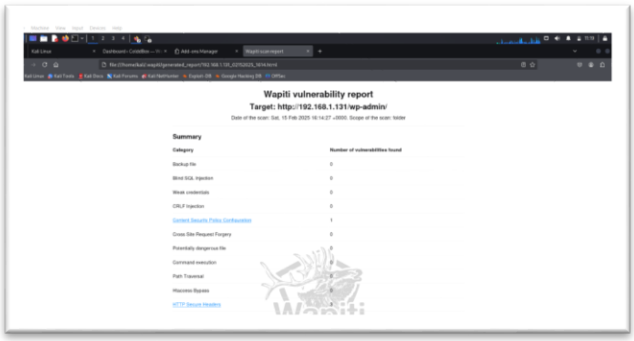


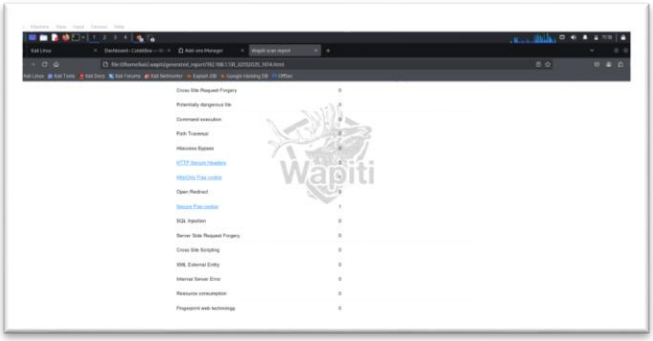
STEP 9:USE WAPITI TO FIND THE VULNERBILITIES PRESENT IN THE COLDDBOX.

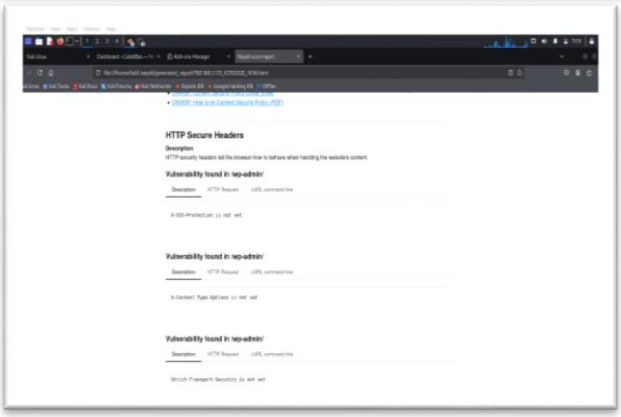


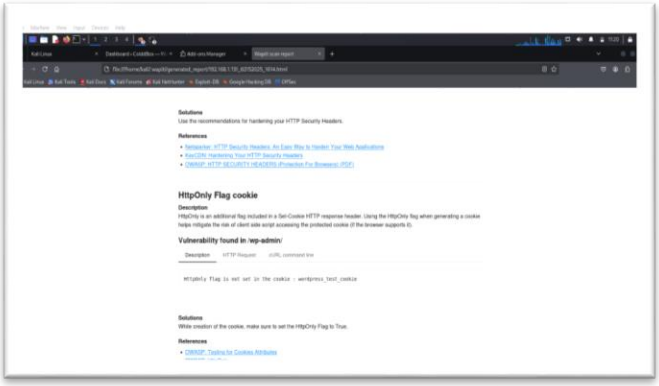


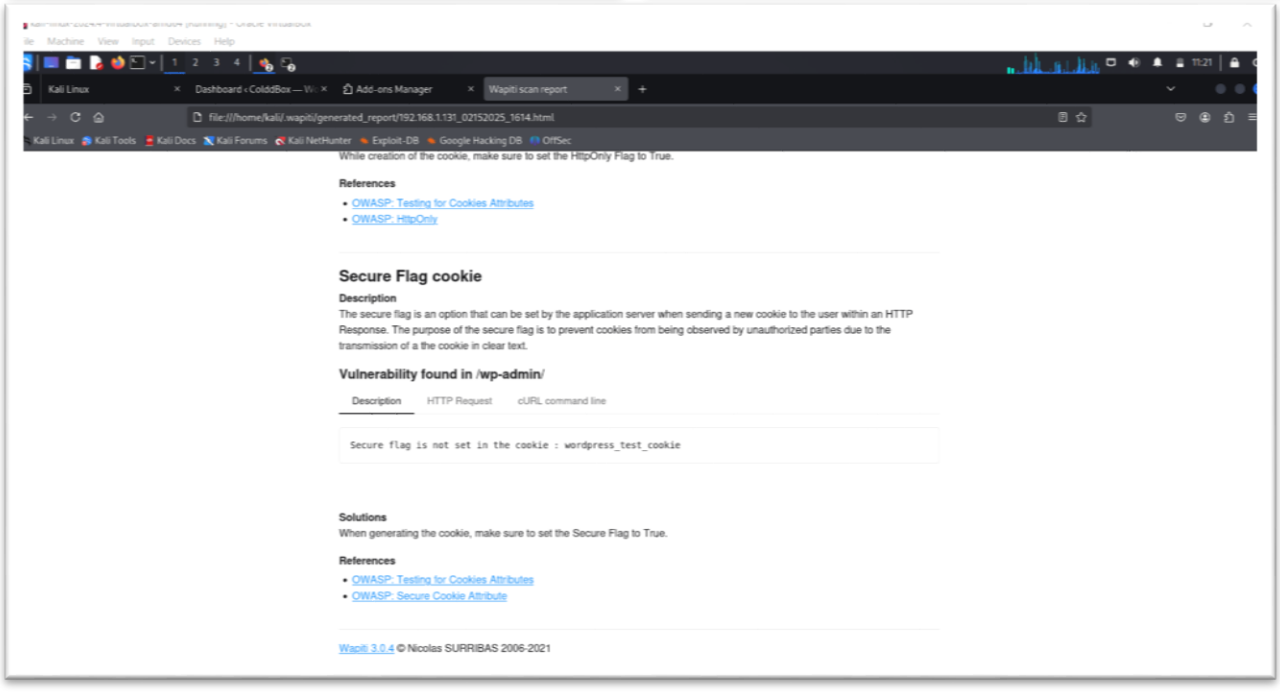
STEP 10:NOW WE CAN VIEW THE SCAN REPORT OF THE VULNERBILITIES AND ITS SOLUTION:











STEP 11: HERE I FOUND ADDITIONAL VULNERABILITIES USING THE WPSCAN ONCE AGAIN

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.1.131/ --enumerate --api-token ZfubsmWU59CHsh4gFYnWpJfZ6WUviqc4QVqiam5KYwY
```

```
] WordPress version 4.1.31 identified (Insecure, released on 2020-06-10).
 Found By: Rss Generator (Passive Detection)
  - http://192.168.1.131/?feed=rss2, <generator>https://wordpress.org/?v=4.1.31</generator>
  - http://192.168.1.131/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.1.31</generator>

 [!] 35 vulnerabilities identified:
```

STEP 12:NOW LETS PERFORM XSS ON THE COLDDBOX

WE GO TO PLUGINS AND EDIT THE HELLO DOLLY

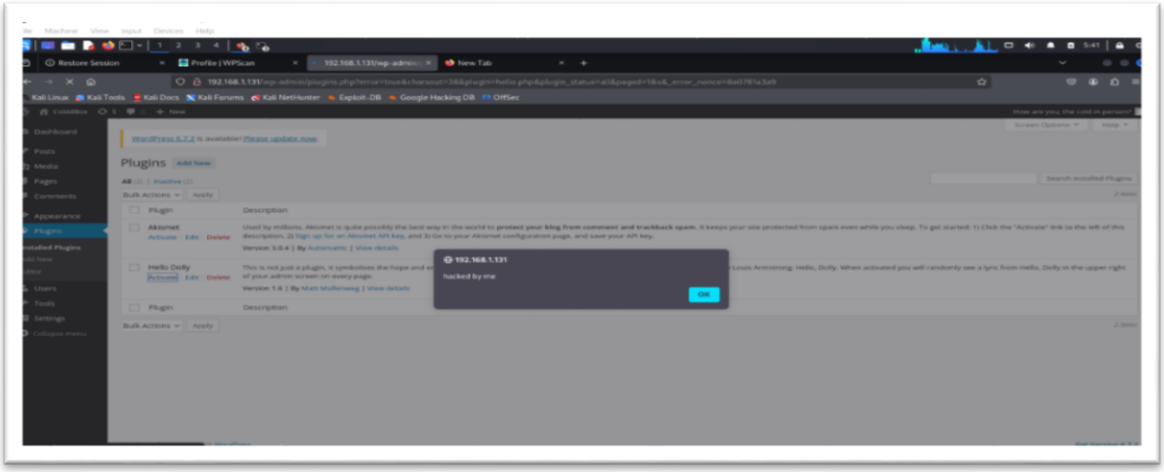
Edit Plugins

Editing **hello.php** (inactive)

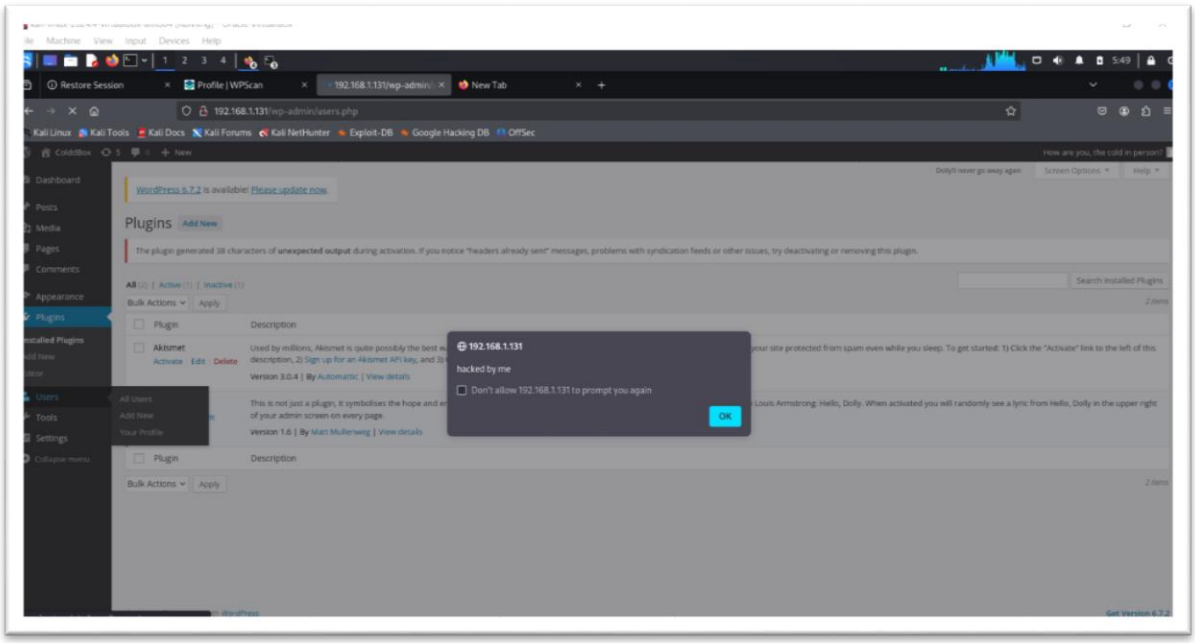
```
        $chosen = hello_dolly_get_lyric();
        echo "<p id='dolly'>$chosen</p>";
}

// Now we set that function up to execute when the admin_notices action is called
add_action( 'admin_notices', 'hello_dolly' );
#**************************************************
echo'<script>alert("hacked by me")</SCRIPT>';
#**************************************************
```

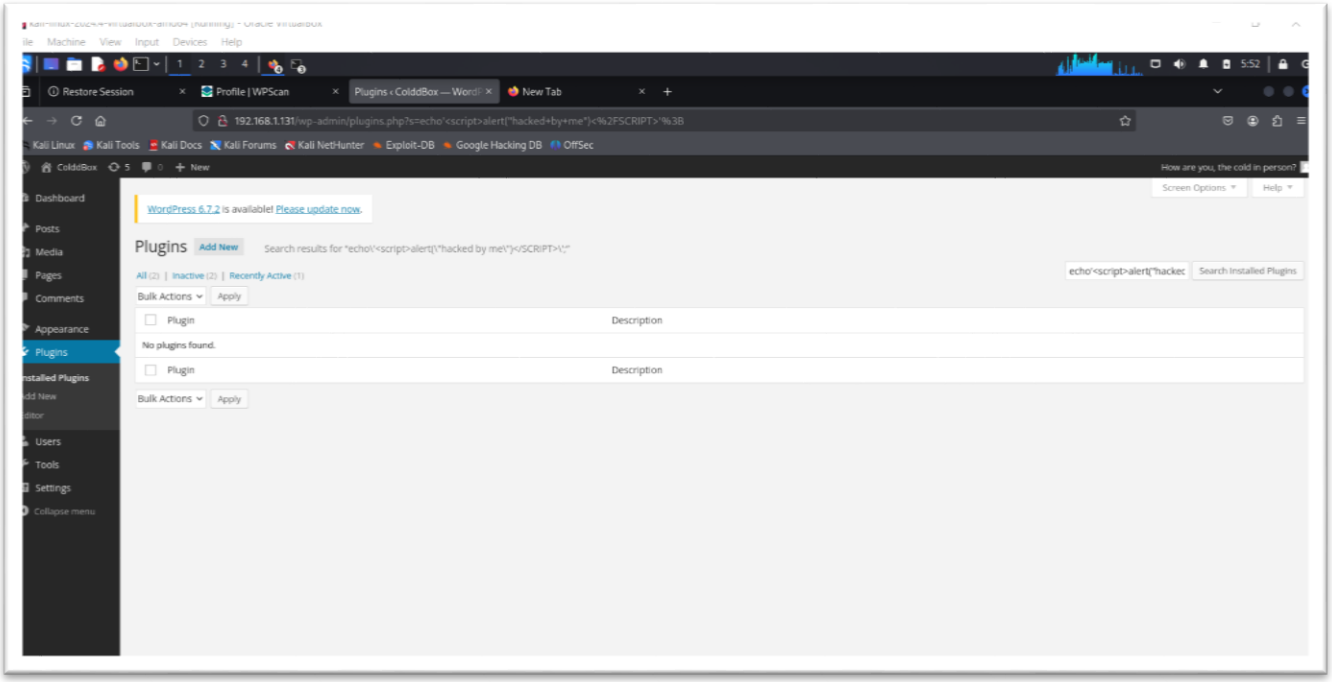
IF WE ACTIVATE IT THE RESULT WILL BE LIKE THIS



IF WE DEACTIVATE IT STOPS, BY KEEPING IT ACTIVATE IF WE GO TO USERS ALSO IT WILL SHOW LIKE THAT SO IT IS A STORED XSS



IF WE TYPE THAT PROGRAM SOMEWHERE IT SHOWS NO ERROR WHICH MEANS IT IS PROTECTED



STEP 13: SQL INJECTION USING THE SQLMAP AND THE URL OF THE COLDBOXX