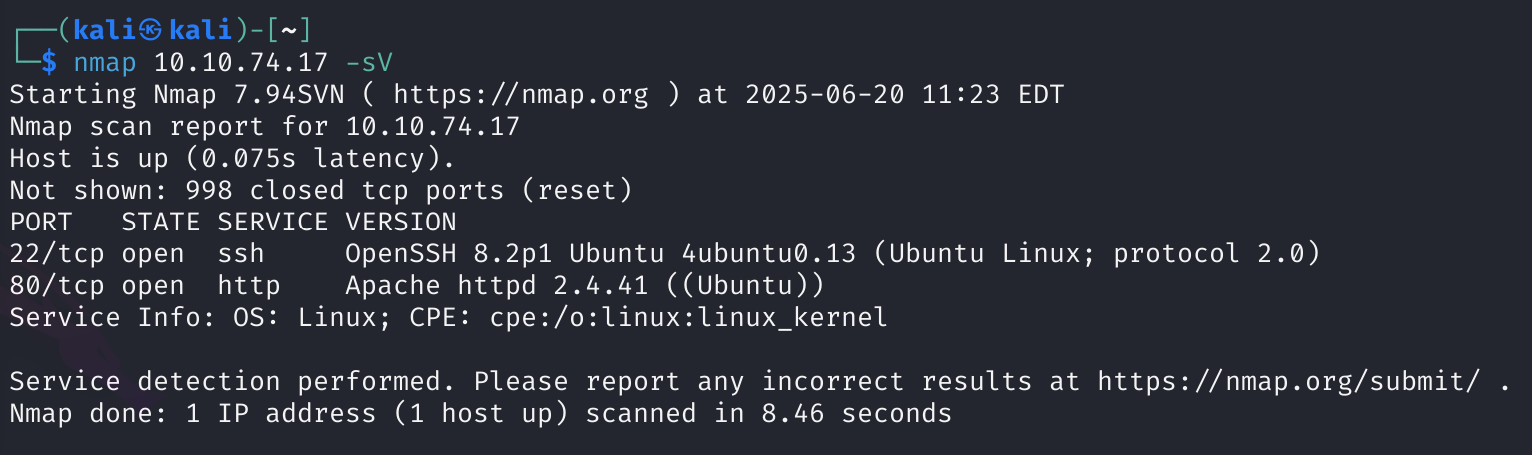
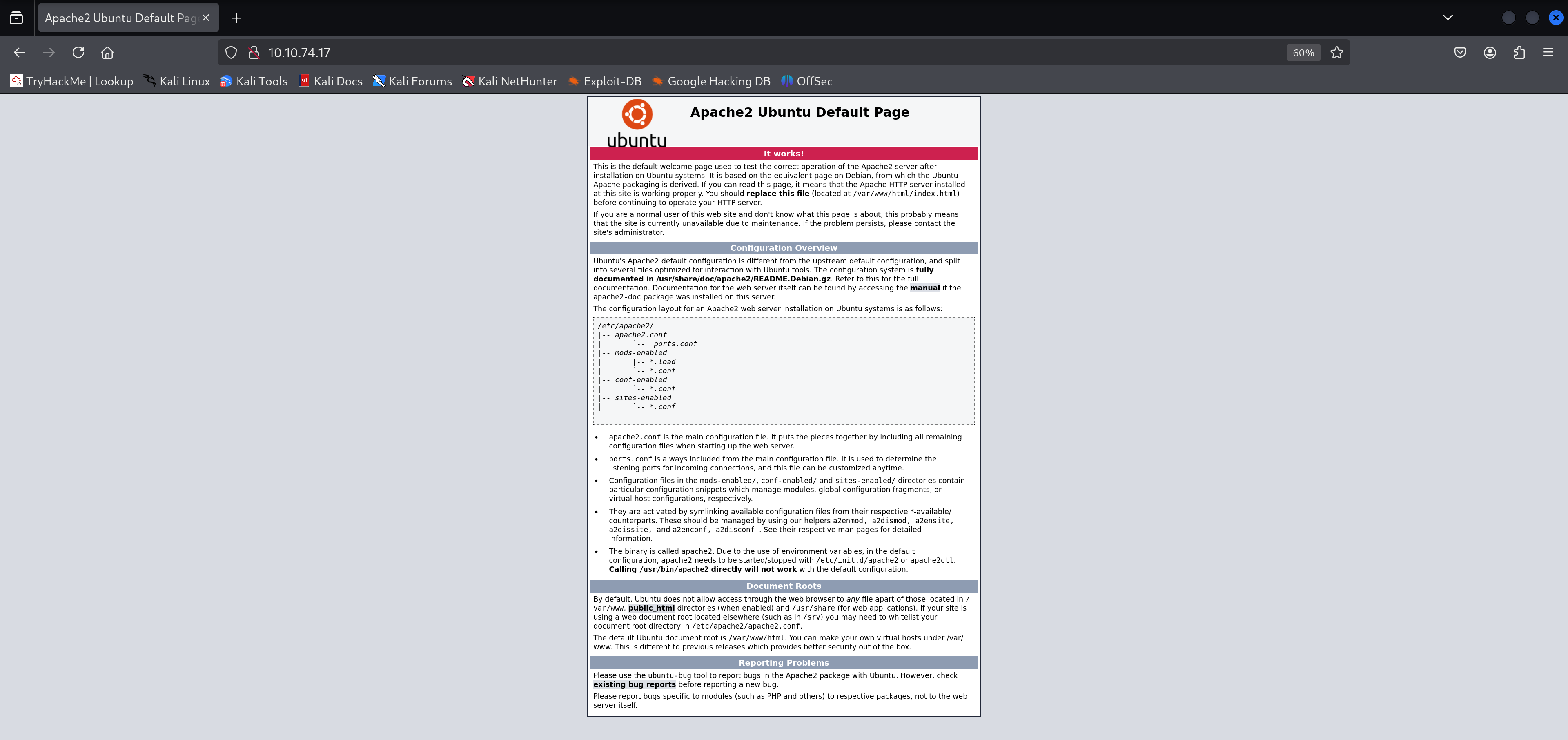
**Dreaming Solution Documentation**

**Written by: Yuval Quina**

1. To begin with, I started by performing a basic Nmap port scanning using this command:

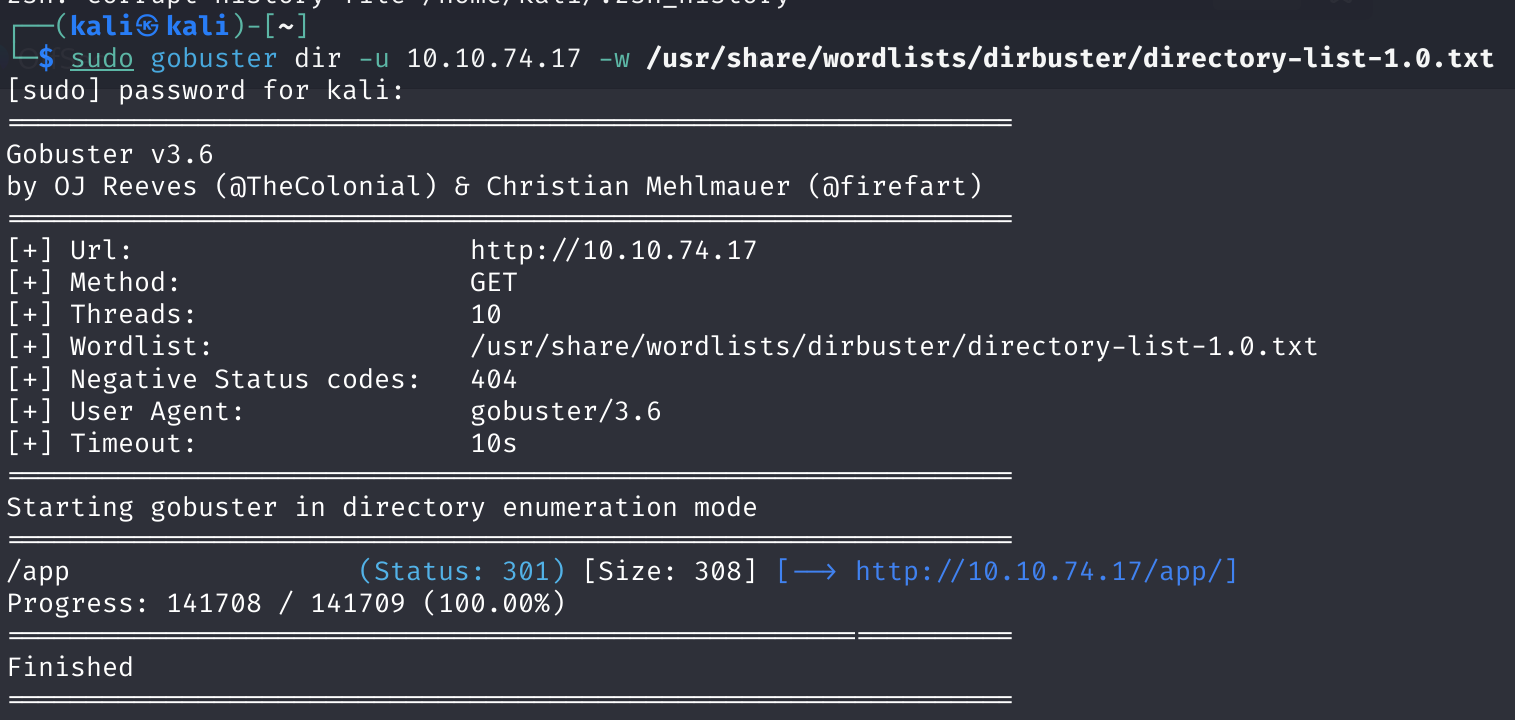


1. So, I opened the website of the machine:

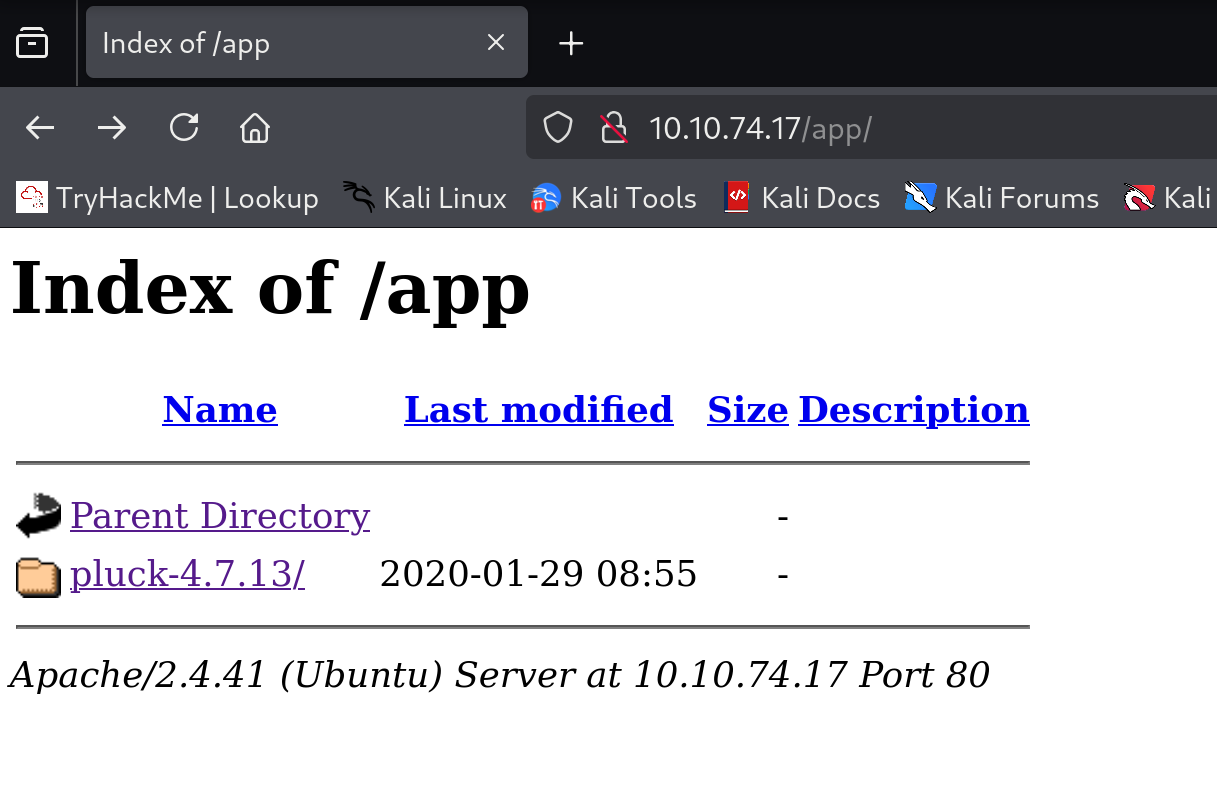


I immediately noticed that this machine running of “Ubuntu” and running “Apache” server.

1. I did a little investigating on this website (such as viewing inspector, trying robots.txt and more) but I found nothing.
2. I chose to perform a directories scan using gobuster and found this directory:



1. So, I opened the directory:



I clicked on the “pluck-4.7.13” directory and it moved me to this page:

תמונה שמכילה טקסט, צילום מסך, תוכנה, תכונות מולטימדיה

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

Now, I started investigating this page.

1. I saw in the inspector that clicking on the “admin” label will move me to a login page:



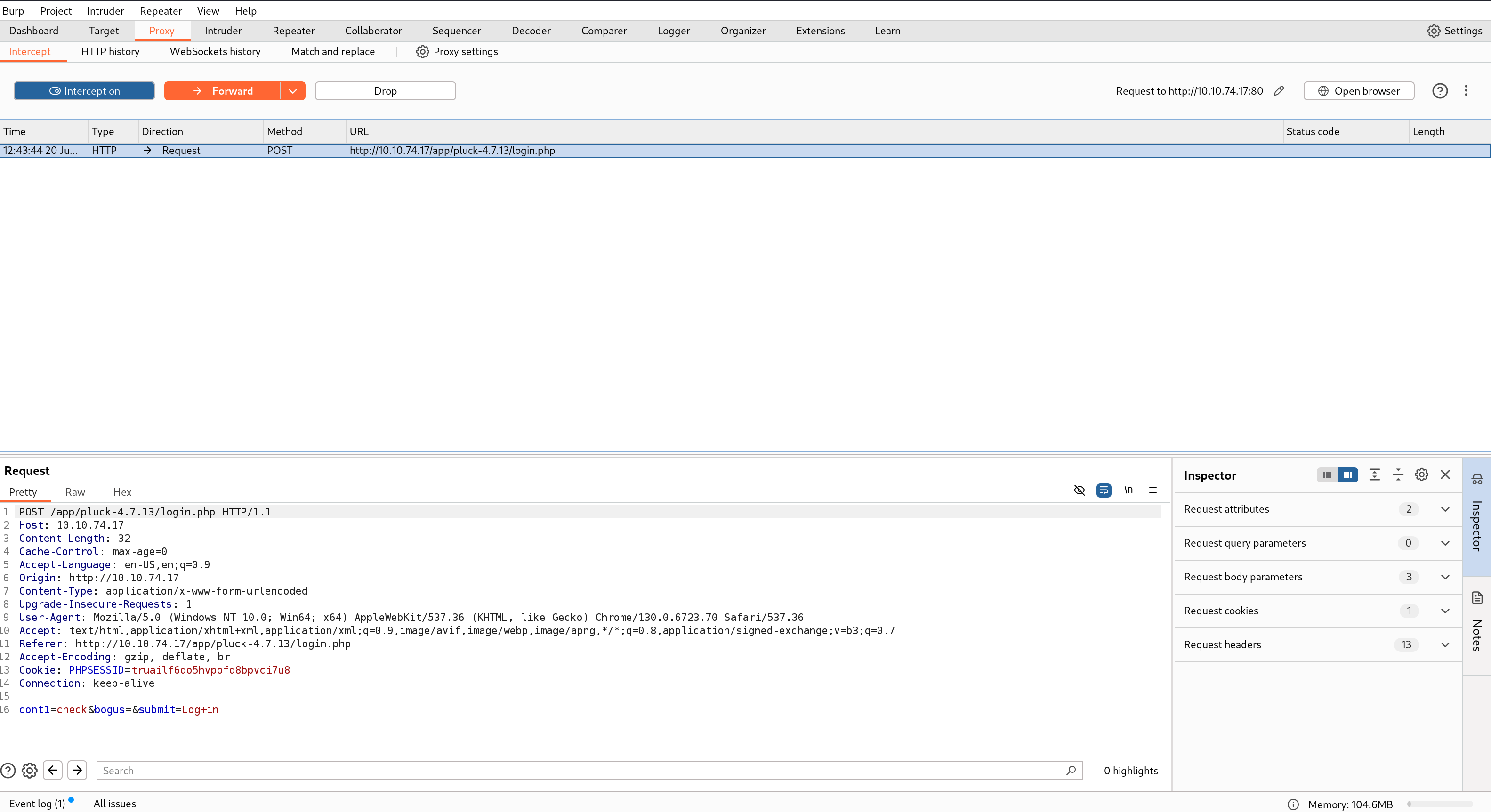
So, of course I clicked on it and this is the login page:

תמונה שמכילה טקסט, צילום מסך, תוכנה, סמל מחשב

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

1. I saw that I needed only password (probably the username is admin) so I used the “burpsuite” tool to bruteforce the right password.

I began with capturing a login packet:



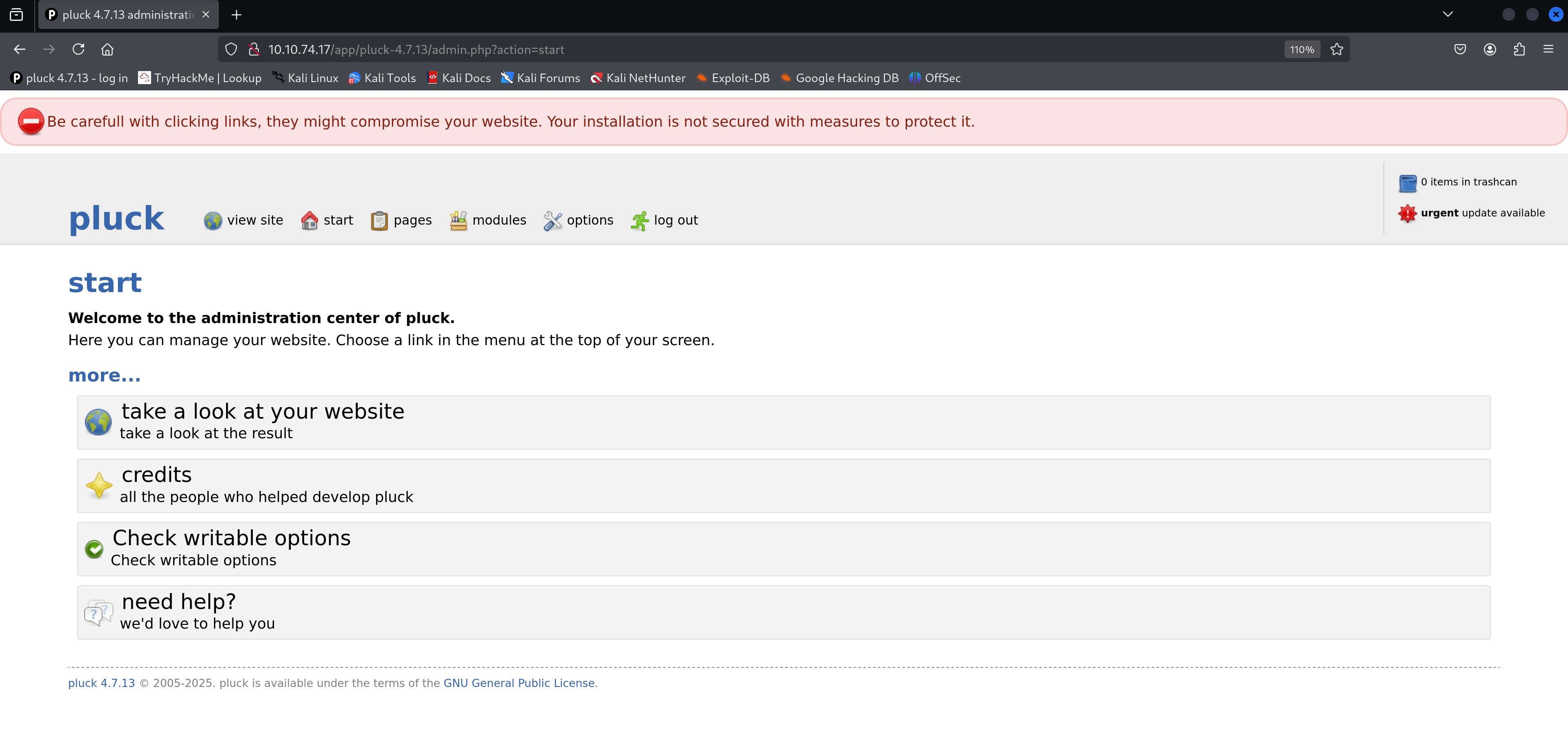
I moved it to the “Repeater”, marked the “contl” header value, select the “/usr/share/wordlists/rockyou.txt” wordlist and runed the bruteforce:

תמונה שמכילה טקסט, צילום מסך, תוכנה, תצוגה

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

I found that the right password is “password”.

1. Now, I just entered it, and this page was loaded:



So, I scrolled through the page and found that I could upload files to the machine.

תמונה שמכילה טקסט, גופן, צילום מסך

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

Therefore, I uploaded this PHP reverse shell file:

תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

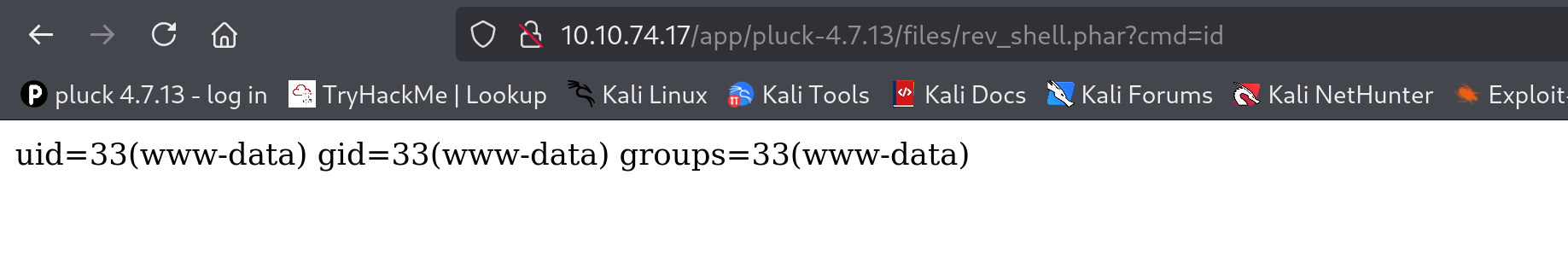
The problem was that when I uploaded this file suddenly the files system transformed it from .php to .txt which makes it inexecutable:



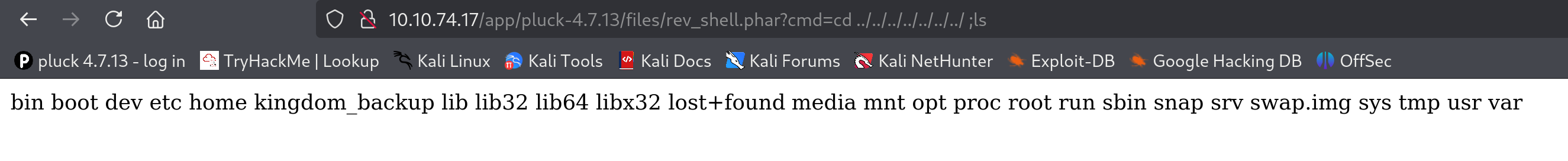
1. This made me think for a moment and after couple of minutes I remembered that there are some alternative executable php formats (like: .phtml and .phar) so I tried both of them I and found that .phar didn’t changed!
2. So, I clicked on the magnifying glass icon (which takes me to the path of the files) and I added the “cmd” header that enable me to run commands over the machine:



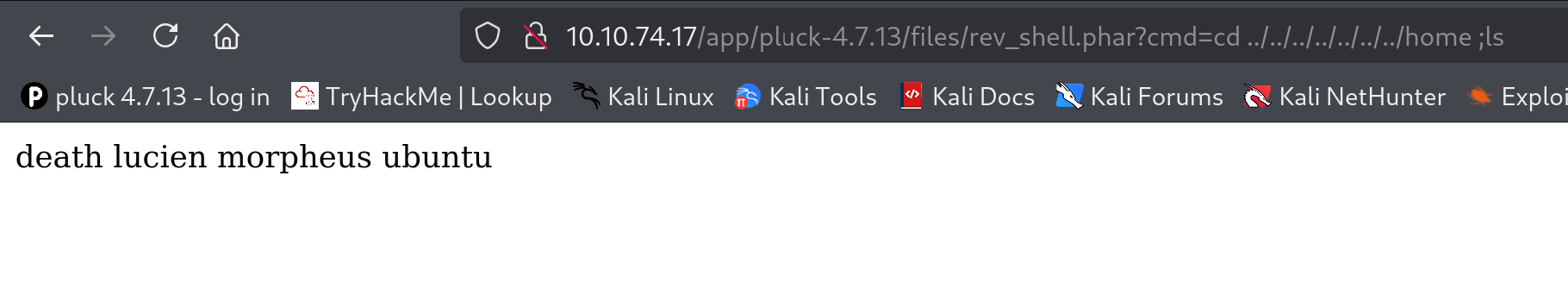
1. After doing all this, I tested it by using the basic “id” command and it worked:



1. Afterwards, I navigated to the root directory:



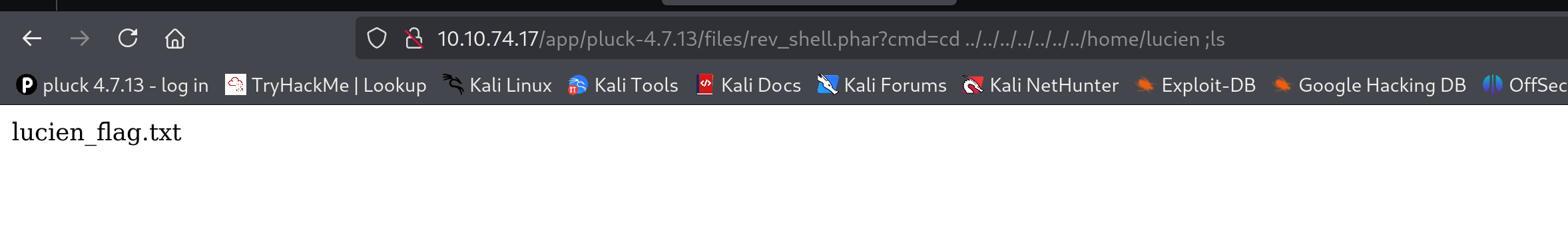
1. After further navigation I found on the home directory the 3 users of the machine that also appears in the flag’s description:



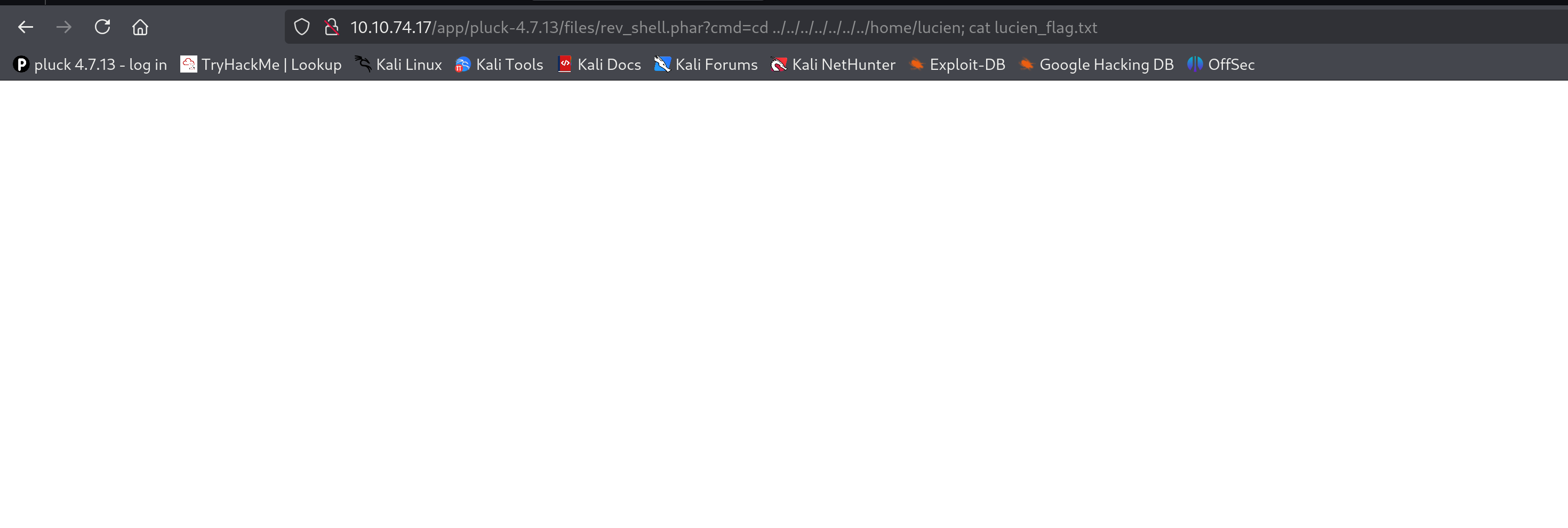
תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

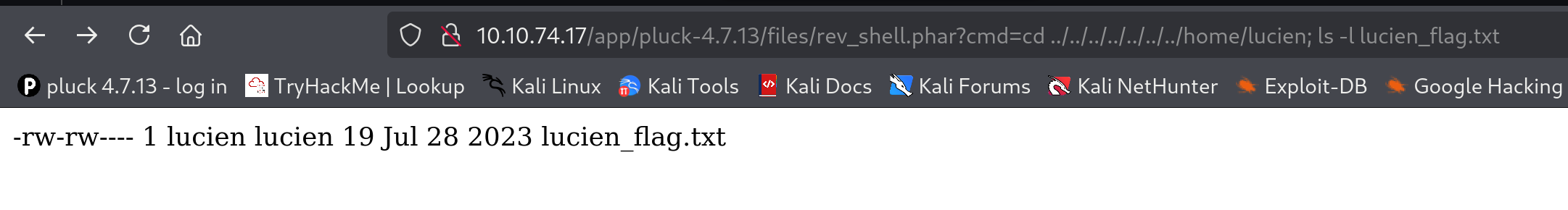
1. The first user that I navigated to was “lucien” and I found in his directory the flag file:



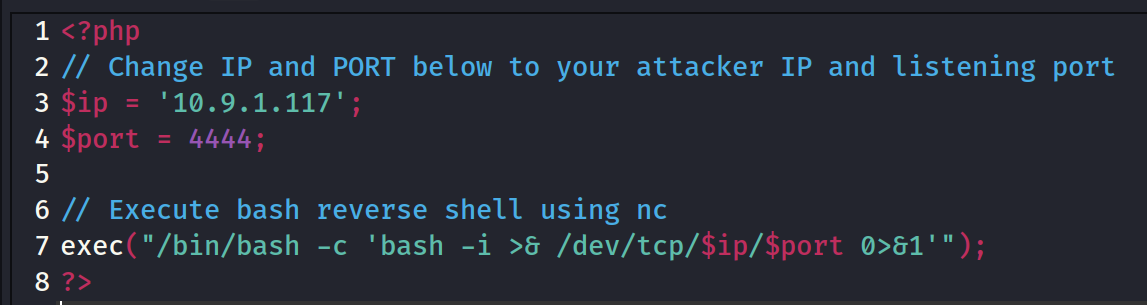
I tried to open it, but it didn’t open:



1. I figured it out that I need to somehow get connected as lucient to access the file content:



1. The problem was that I got a web shell and not a meterpreter so I could not use the shell as usual. Therefore, I chose to first of all change to “netcat” so I will be able to control over the shell more comfortably. I did it by uploading another .phar file that will run the following commands in order to connect to a listener that I’m running on my machine:



תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

תמונה שמכילה טקסט, צילום מסך, תוכנה, תכונות מולטימדיה

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

1. Now, I needed to travel among the files in order to find a clue to how to privilege escalate to the 3 users of this machine:



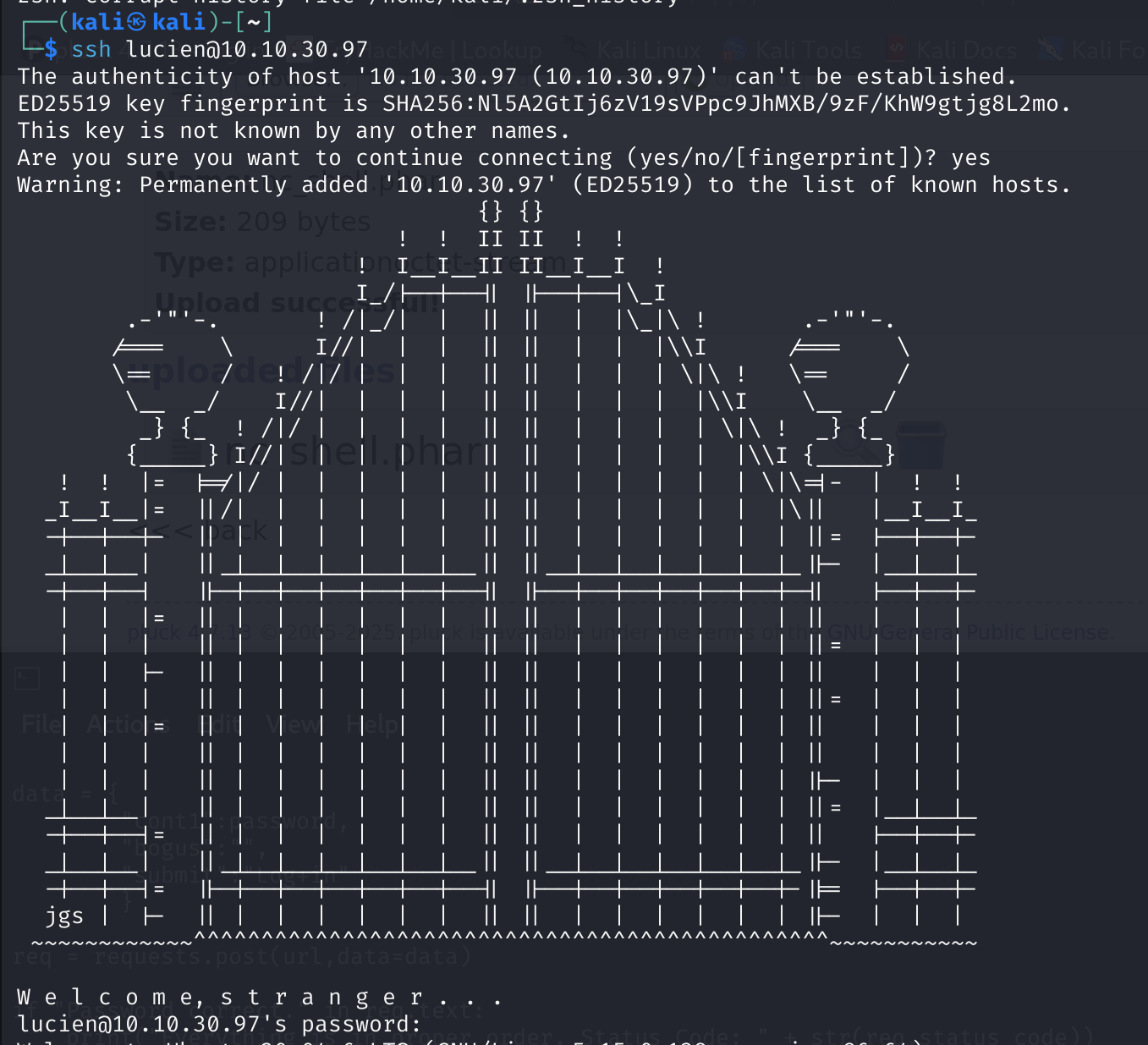
I found in the /opt directory the python file from death’s user directory and another python file.

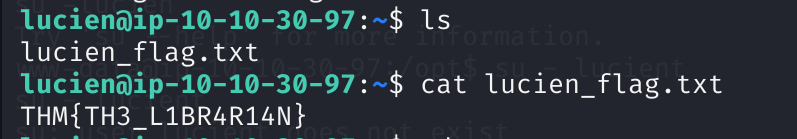
1. I opened the “test.py” file and found the password of the user “lucien”:

תמונה שמכילה טקסט, צילום מסך, גופן

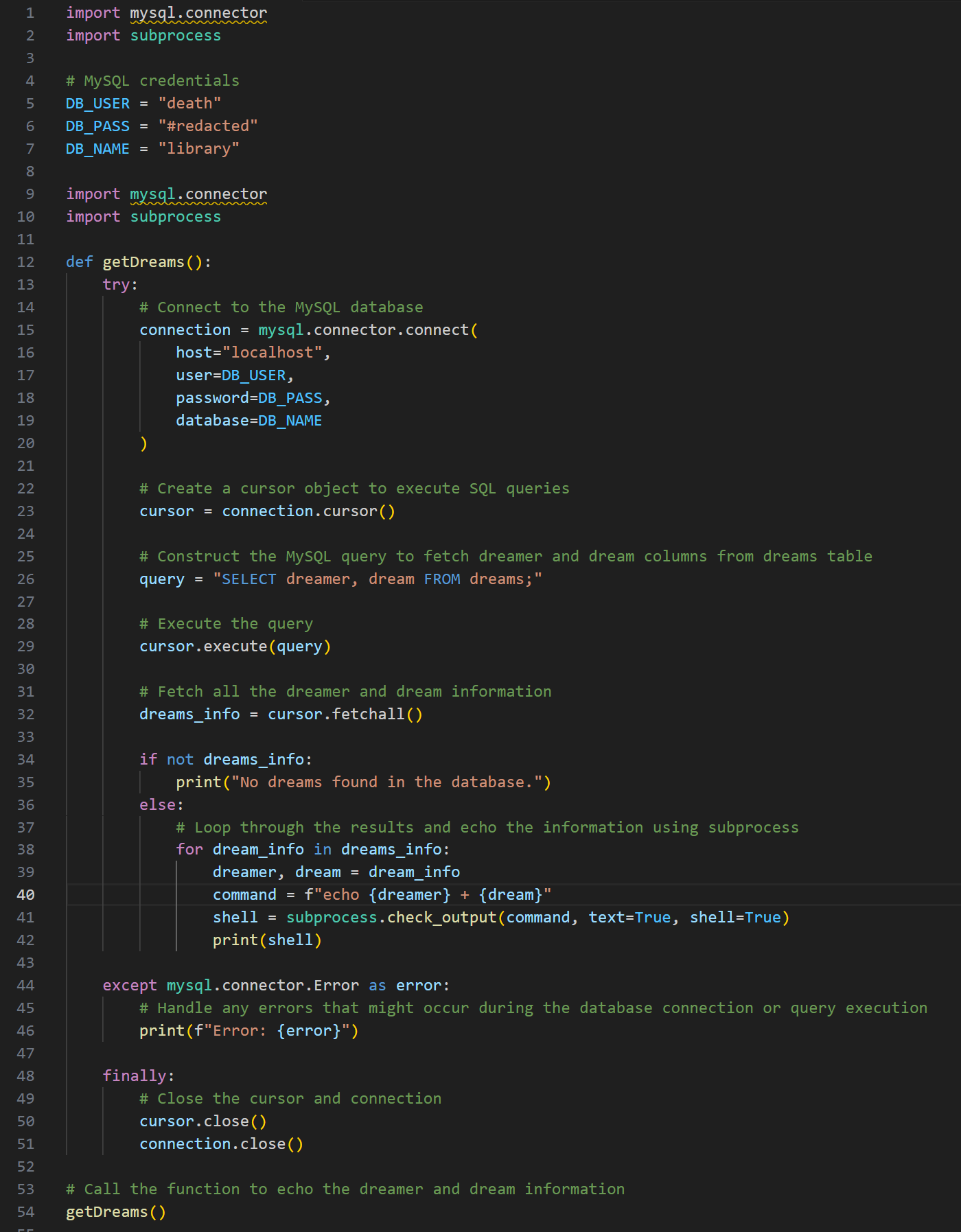
תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

So, I immediately copied it, logged as lucien (using ssh) and opened his flag file:

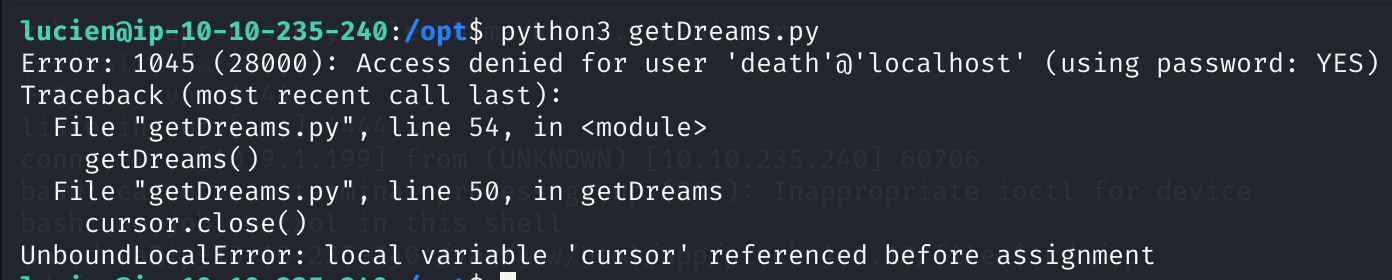




1. Then I opened the “getDreams.py” file and found this script:



After running it on the target machine, I faced this error:

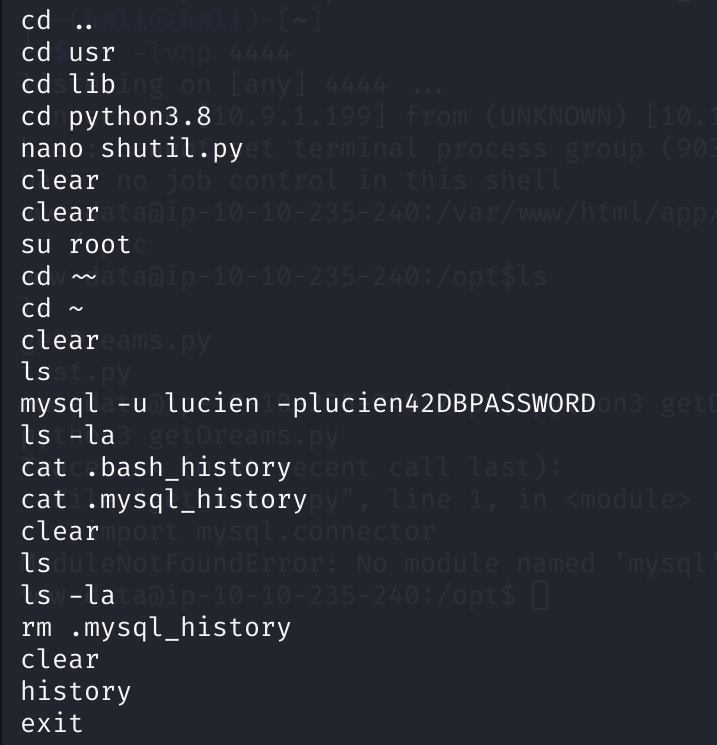


This means that the password of death is probably wrong.

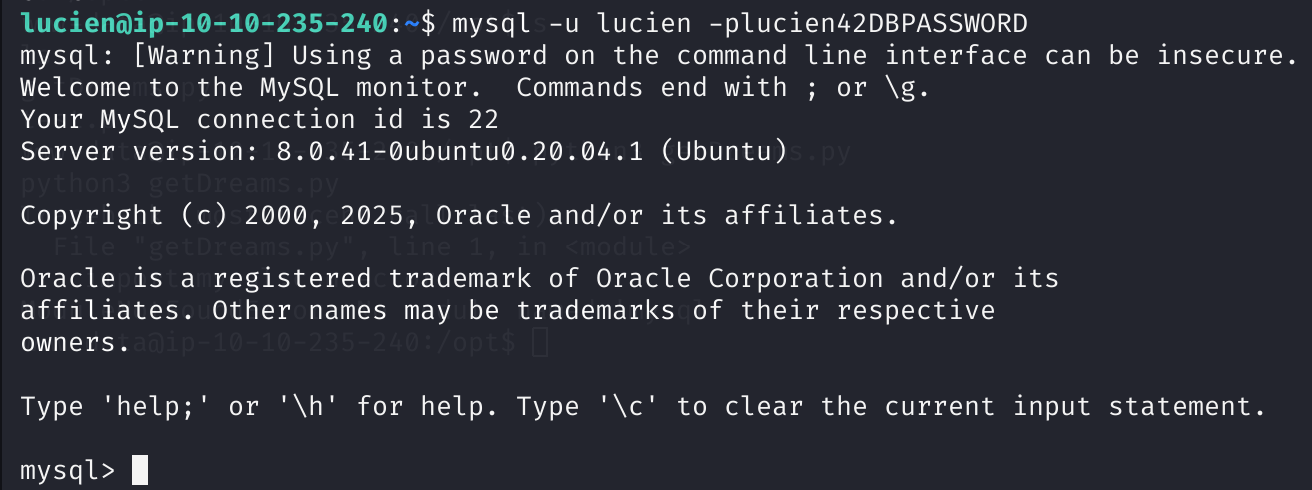
1. I opened the lucien’s “.bash\_history” file:

תמונה שמכילה טקסט, צילום מסך, גופן

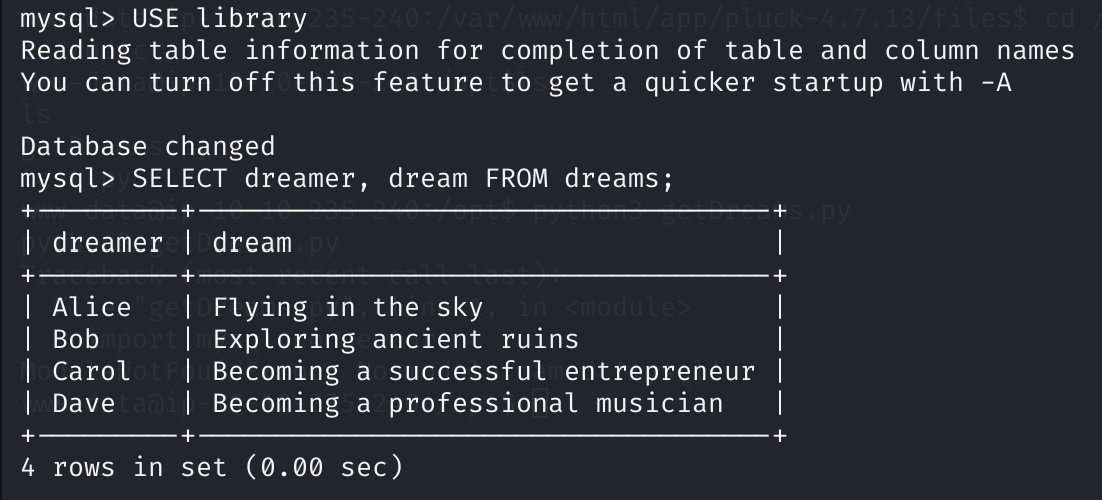
תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.



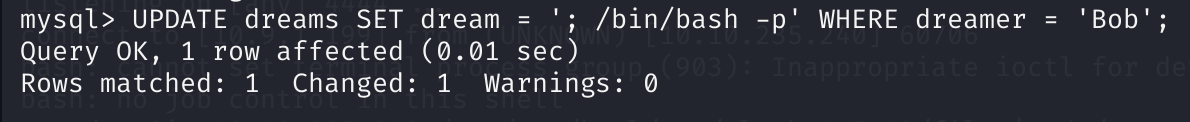
I found here that lucien connected to the mysql database using his credentials. Therefore, I entered the database as lucien:



I accessed the “library” database and entered this mysql command from the getDreams.py file:



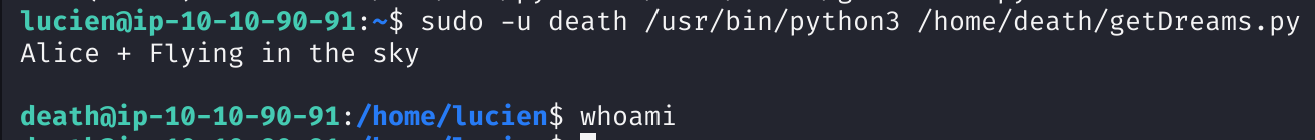
1. I found in the code that the program “echo” the command which makes me able to add another command like echo so the program that run the code as death will be able to give me death’s permissions:



תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

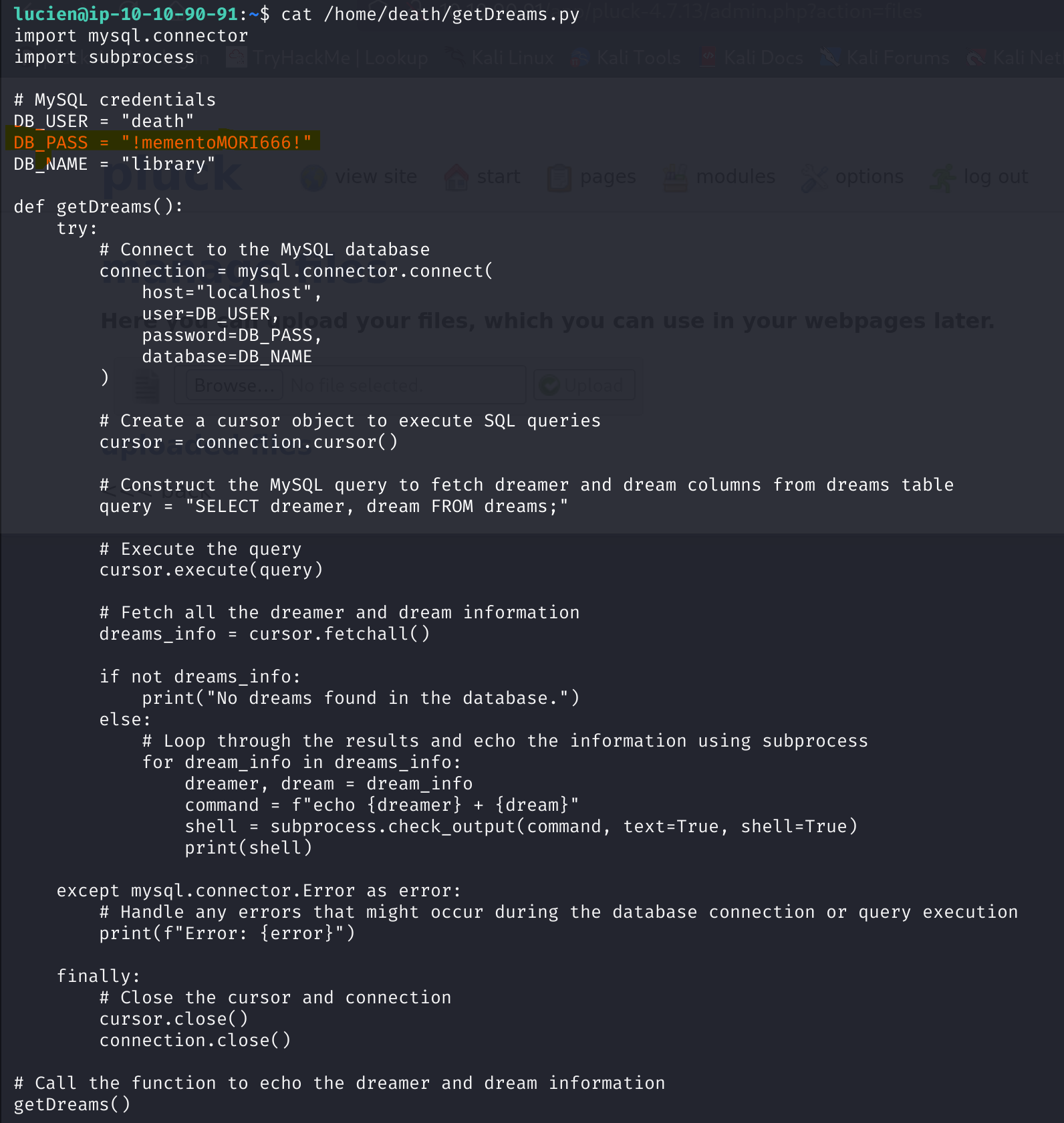
So, when I run the getDreams.py again this is the results:



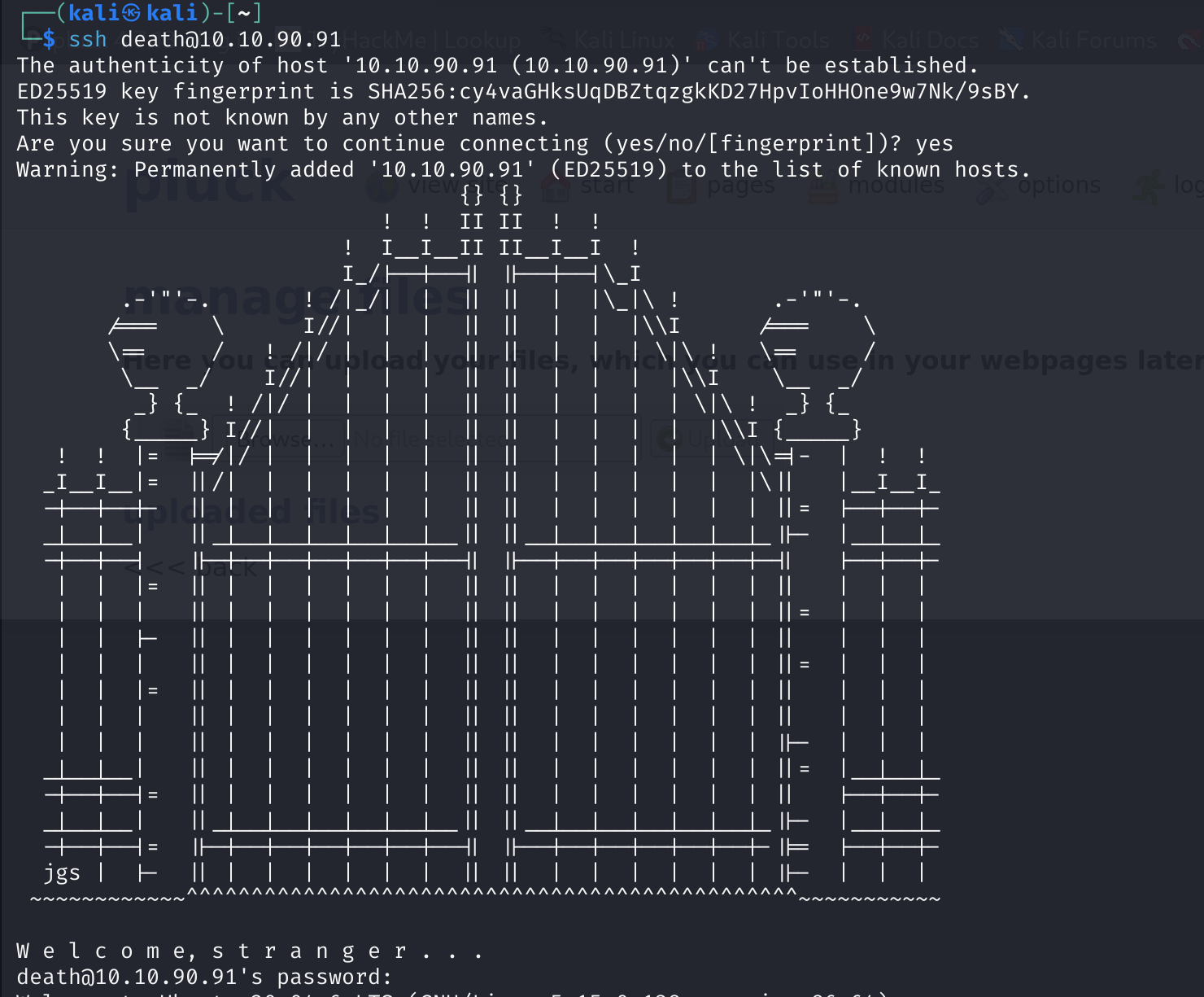
1. The problem is that shell is hard to control and not stable so I changed the permission of “/home/death/getDreams.py” so I will be able to open it via lucien:



1. Now, When I opened it I found death’s password:



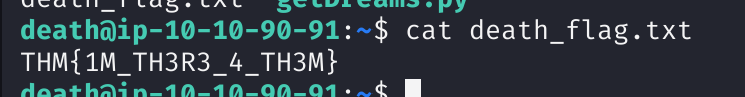
And of course I entered death account via ssh:



תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

Now I just opened the flag file and found the flag:

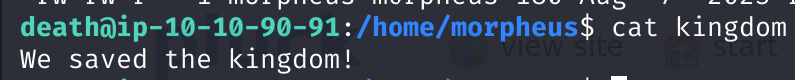


1. After completing this the only thing left was to find Morpheus’ flag.

So, I opened his directory:



I immediately opened the kingdom file:



And restore.py file:

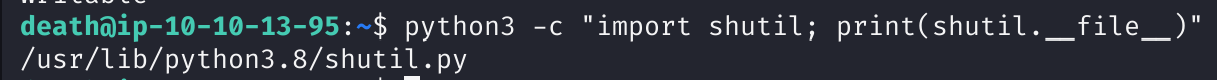
תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

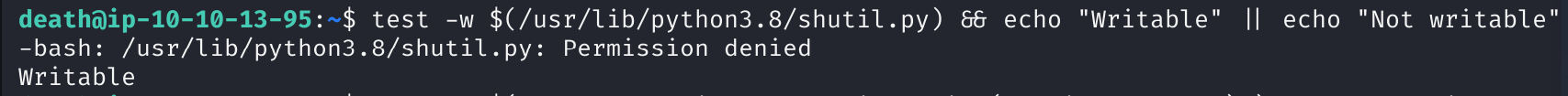
1. I tried to access /kingdom\_backup but I got no permission to do so.

Therefore, I checked if the user death can modify the “shutil” python library so maybe I can change its content to execute other command:

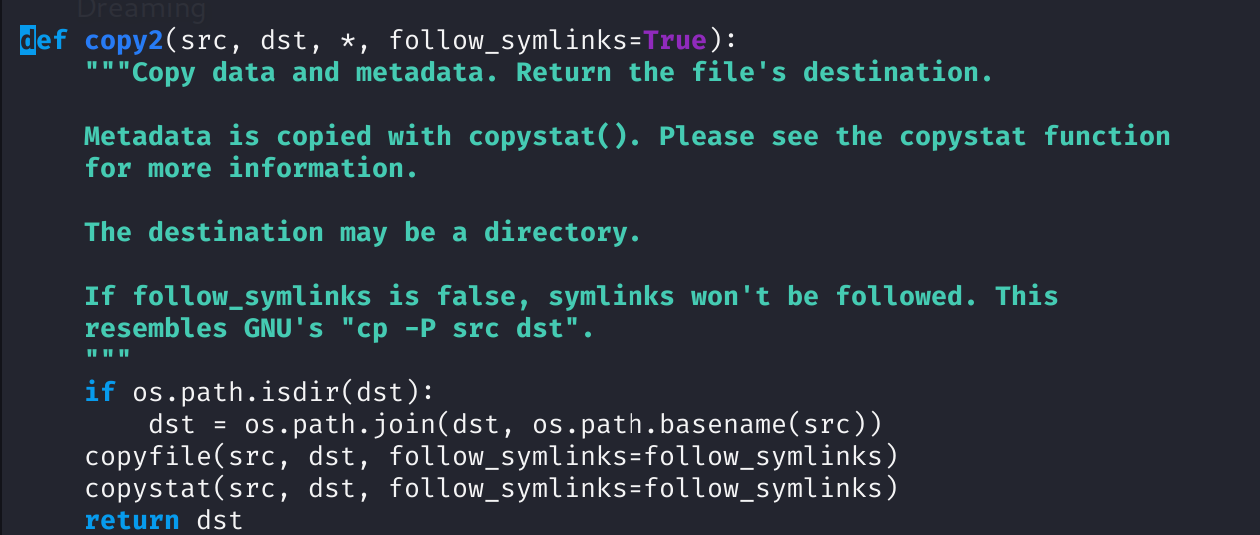
First I located the library path:



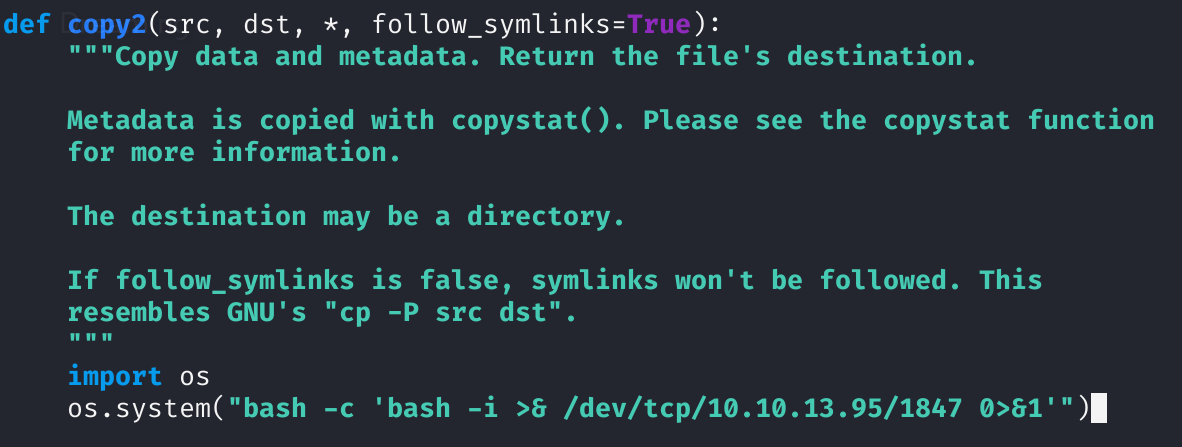
Afterwards, I checked if it’s writeable or not:



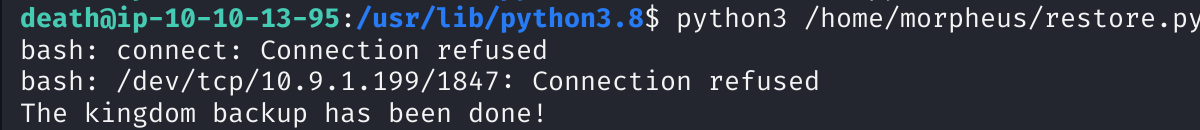
So, I can exploit this library by entering to nano editor and find the used function which named “copy2”:



And edit it so it will start a reverse shell over the machine using the root permissions:



1. Now, I run the py script again (but before I add a netcat listener on my machine):



תמונה שמכילה טקסט, צילום מסך, גופן

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

And I found the last flag:

