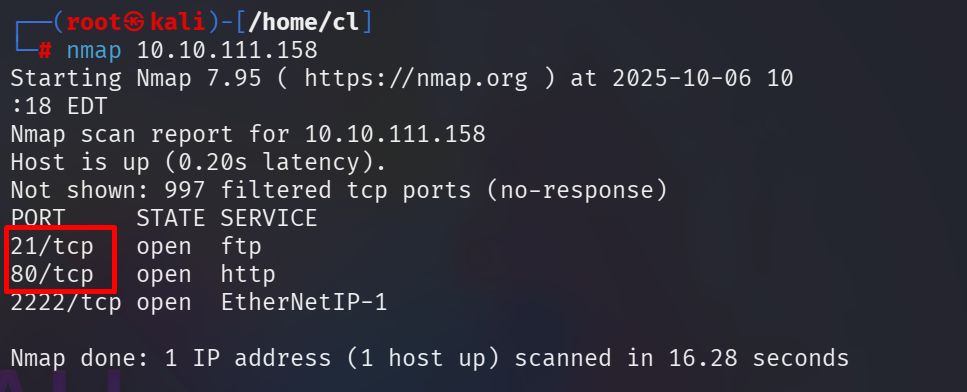
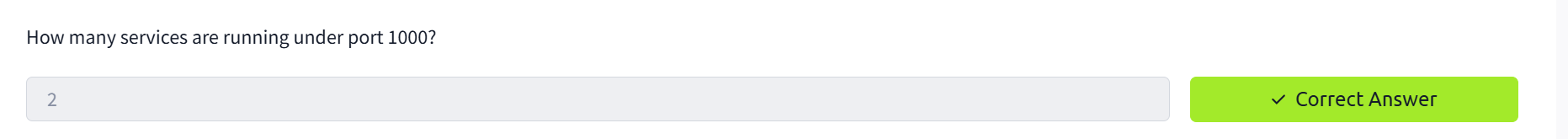
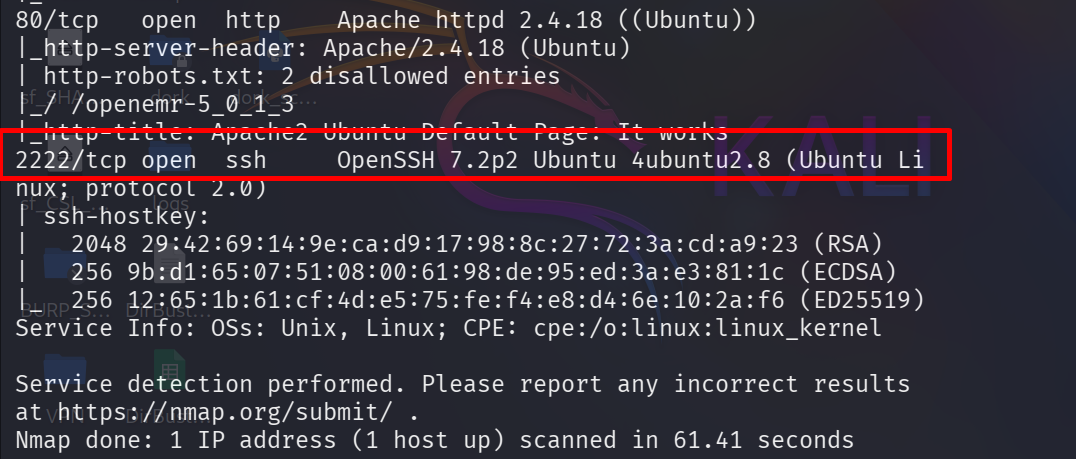
**Simple CTF**

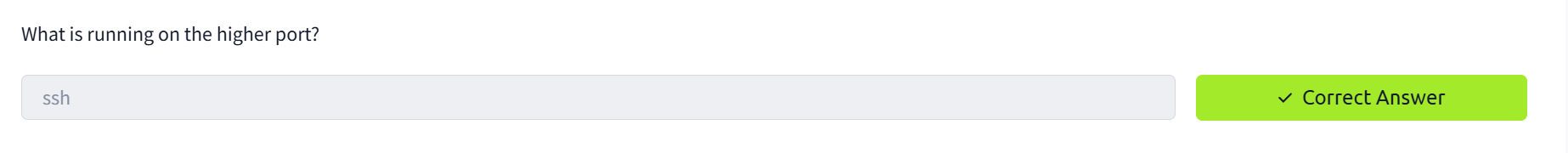
**Step 1: Run nmap, To find how many services are running, just perform a port scan. Here we found 3 open ports and 2 ports are bellow 1000.**

****

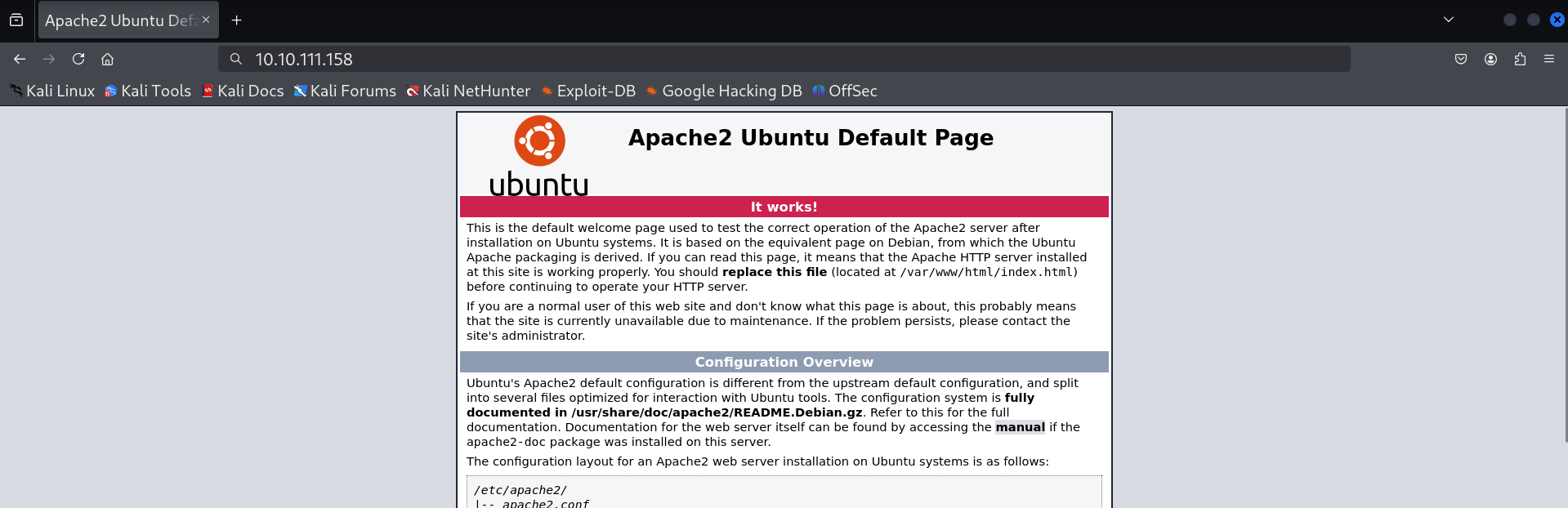
****

**Step 2: Found the height port 2222 is running SSH service. Here perform a port with service scan. Nmap -sCV 10.10.111.158**

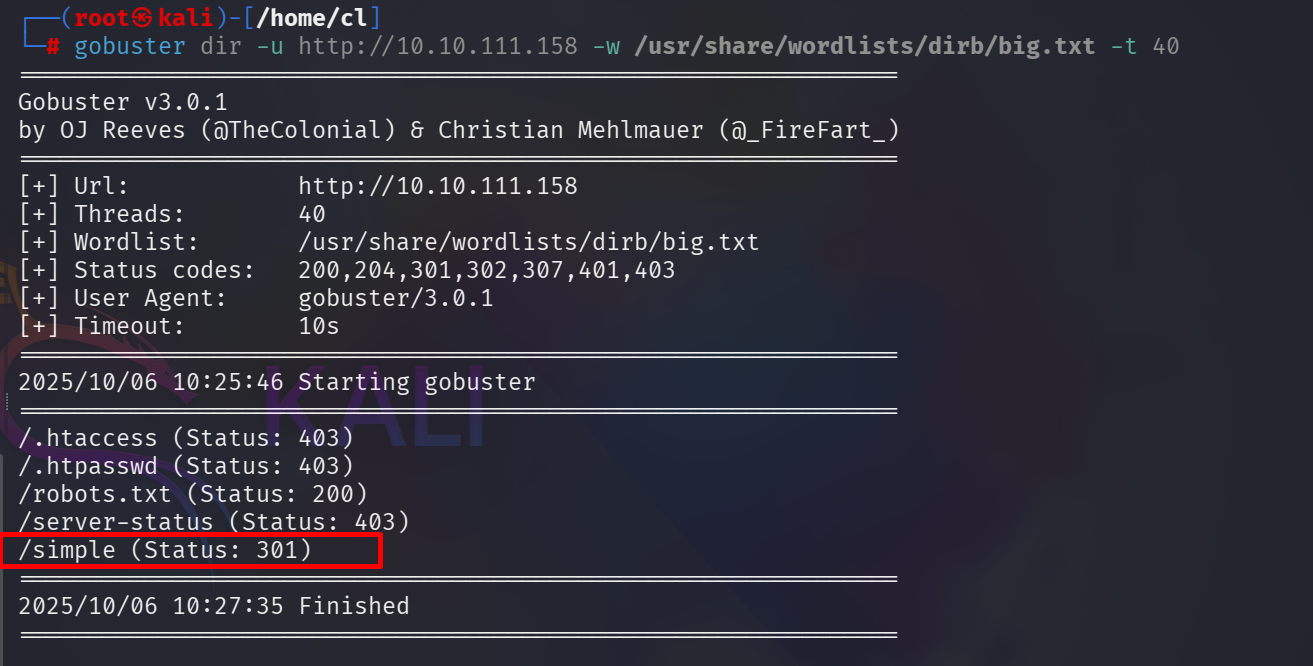
****

****

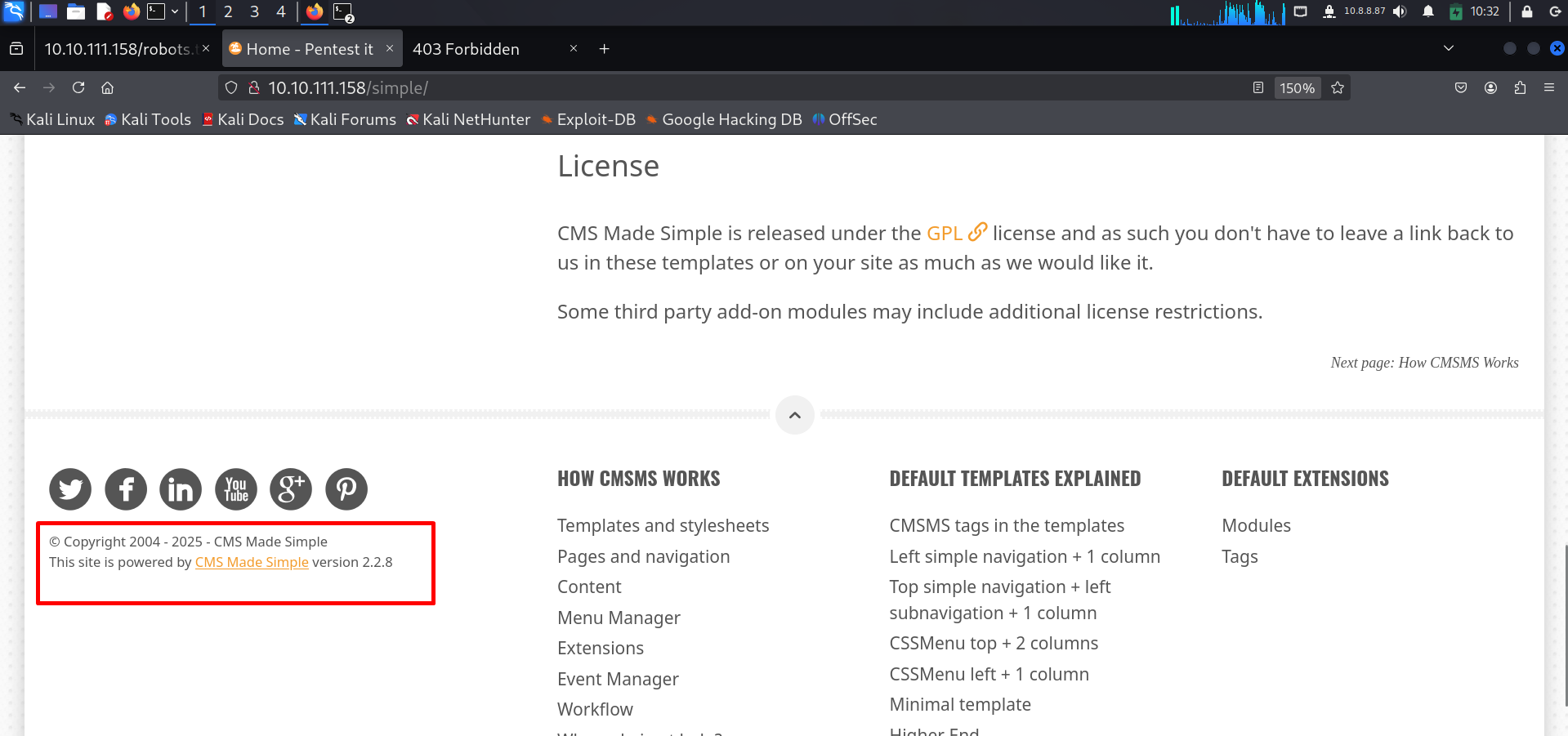
**Step 3: Next question asked us to find a CVE To exploit the system. We know that a web server is running on port 80 so let's see. Here apache server is running on port 80.**

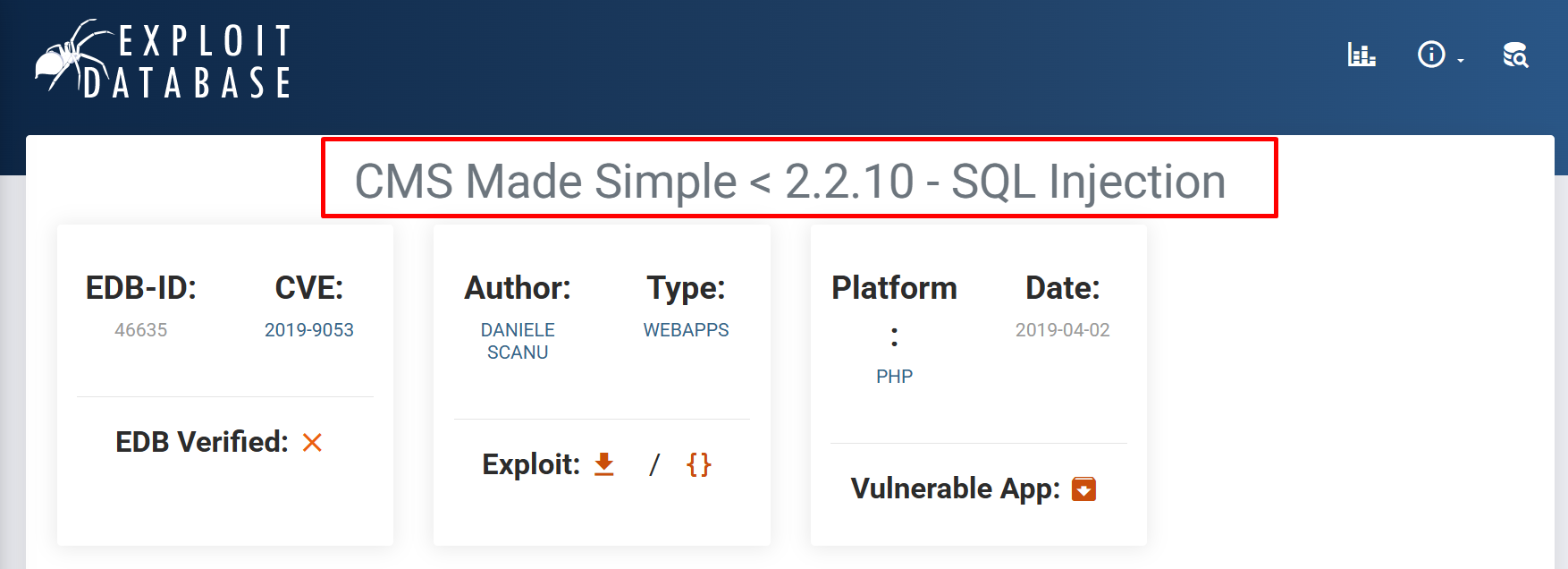
****

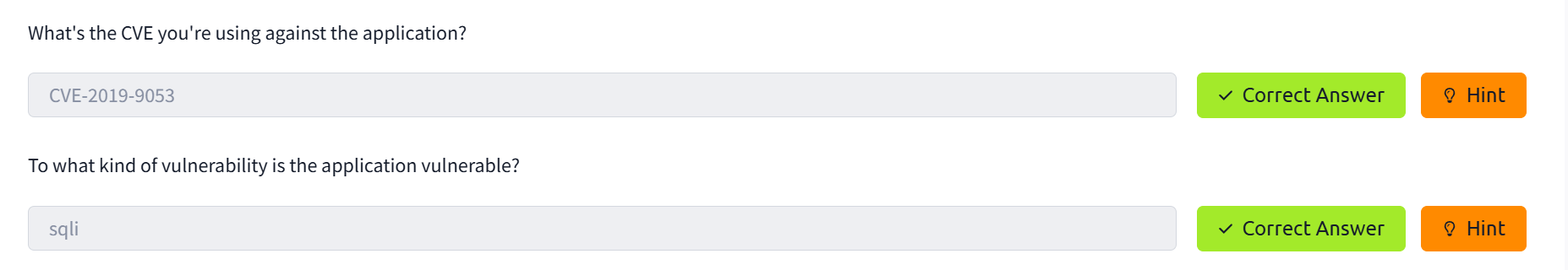
**We need to find out the hidden directory. Here using gobuster for that directory enumeration. And found a directory named /simple. So we visit that directory.**

****

**At the bottom of that page we found the version of this CMS site and it is 2.2.8. So, we search on the internet to find out is there any exploit of that version is available or not.**

****

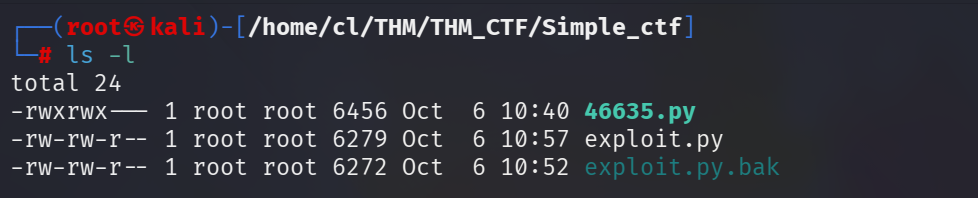
****

****

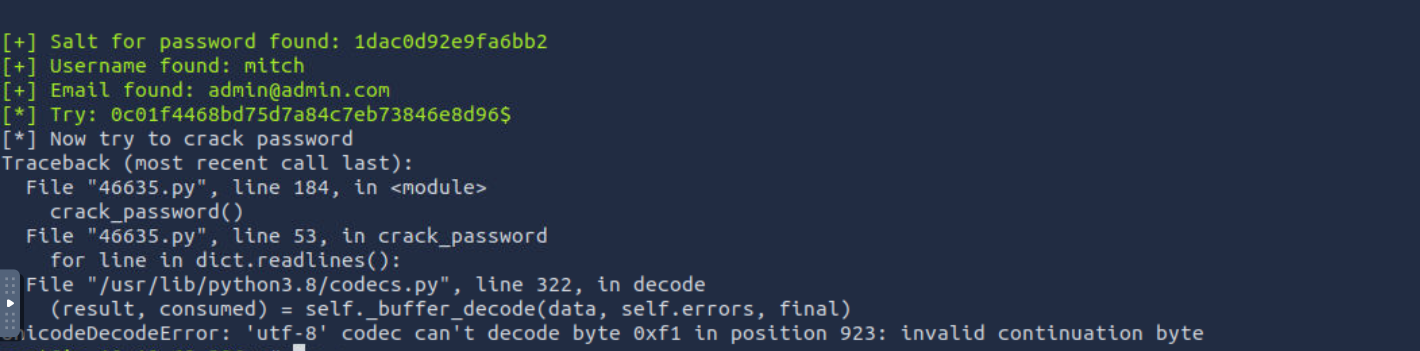
**Step 4: Download that file and run it (as follow steps)**

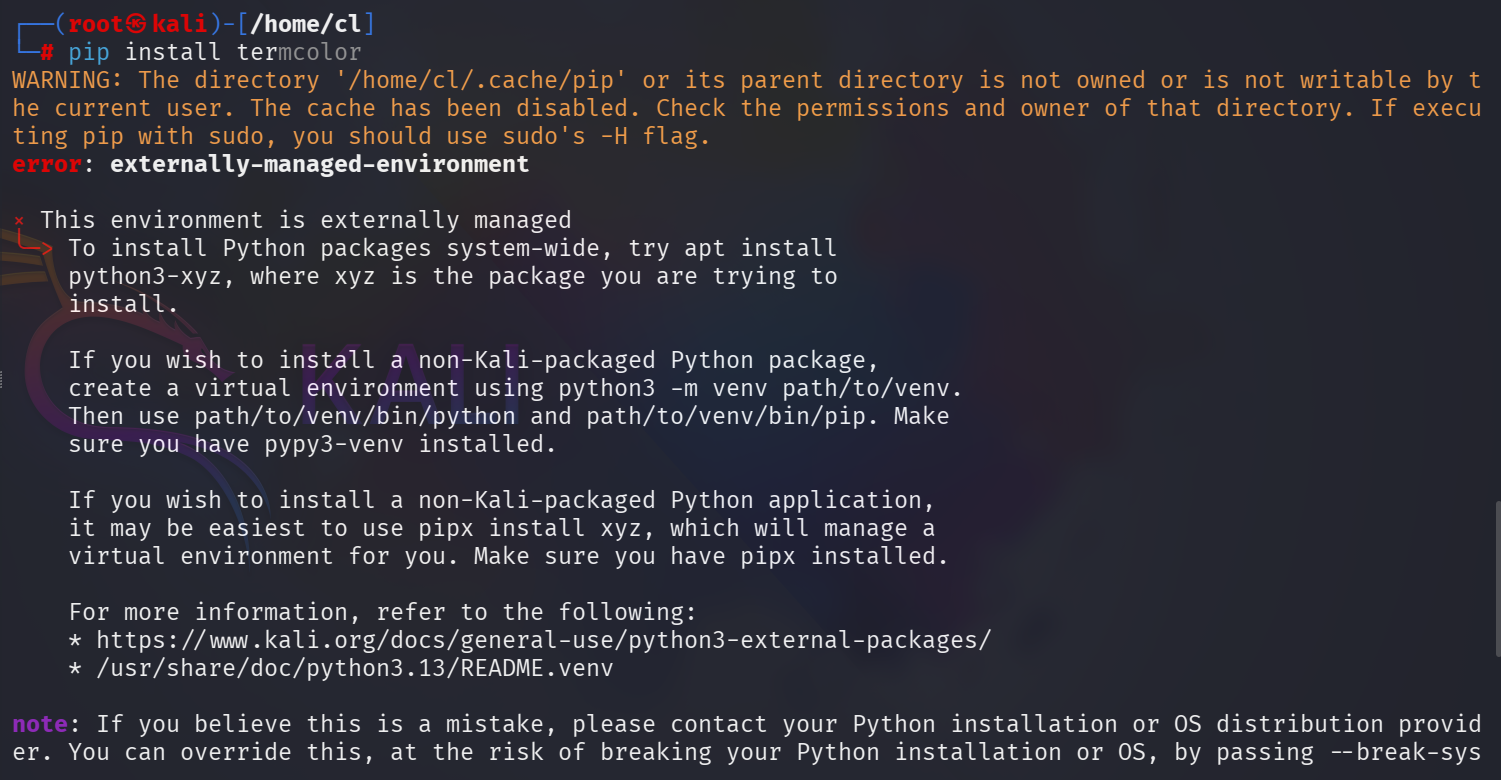
****

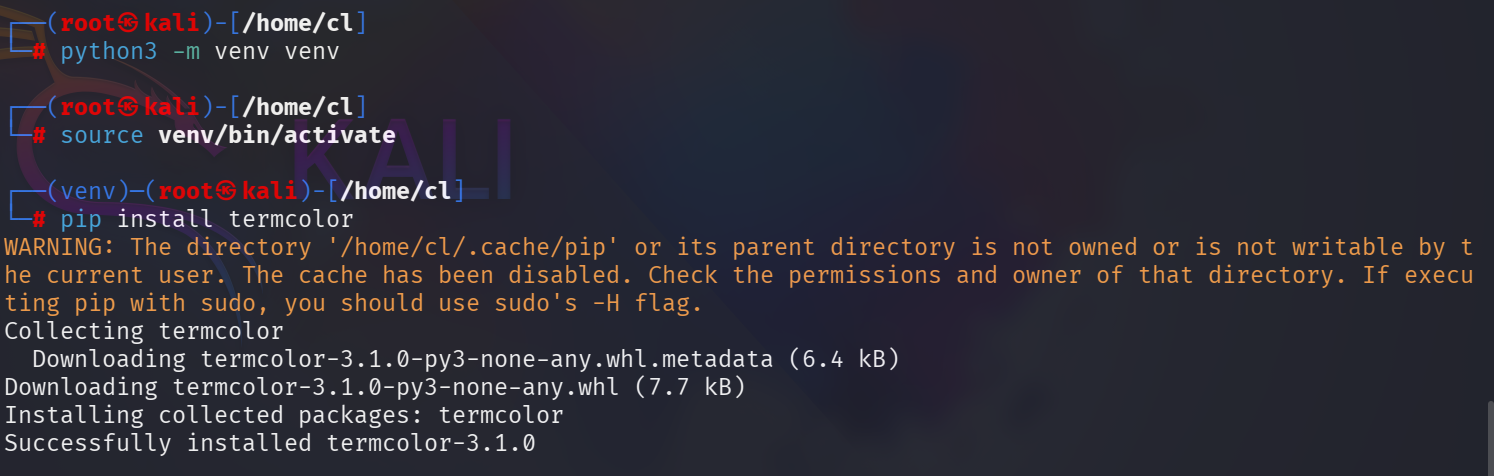
****

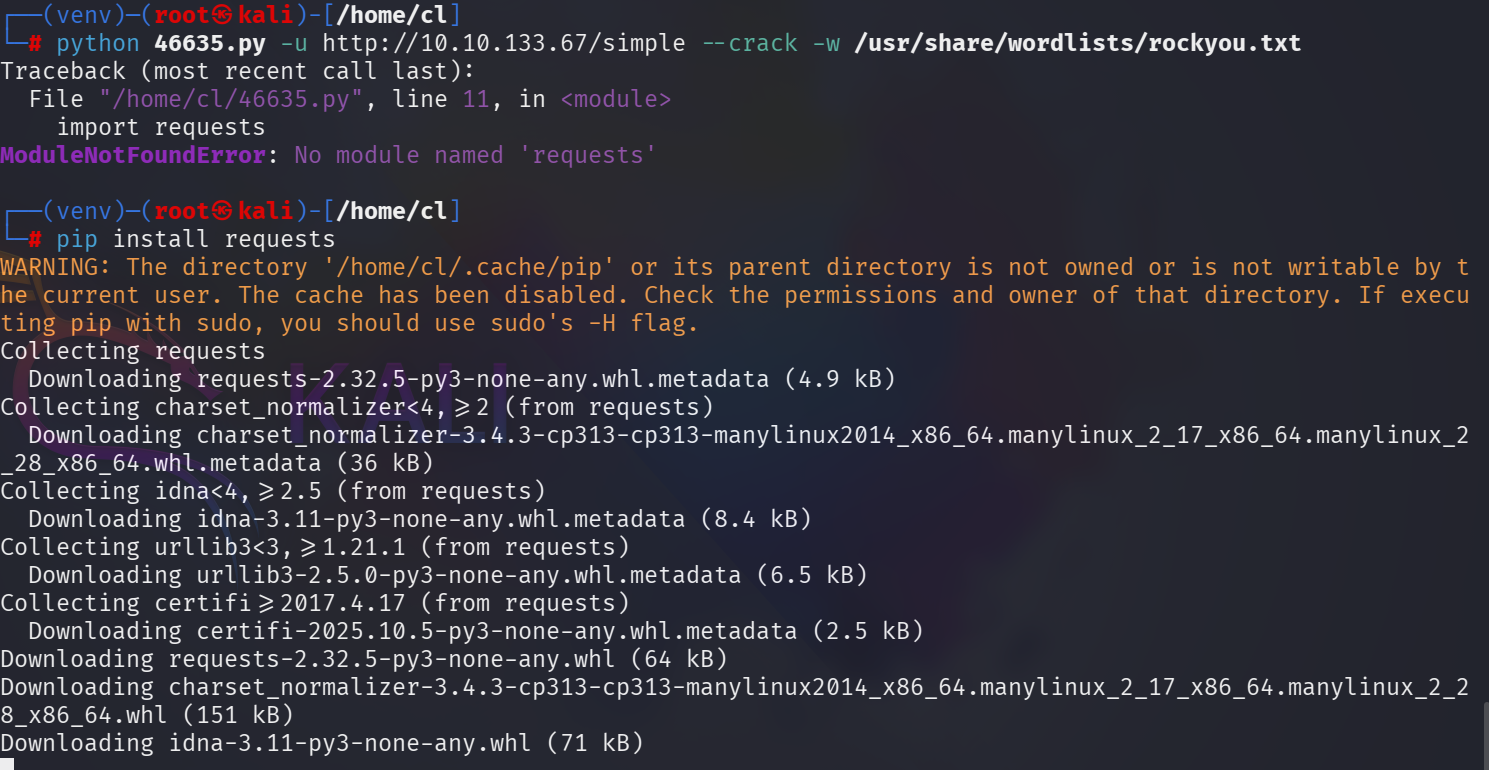
****

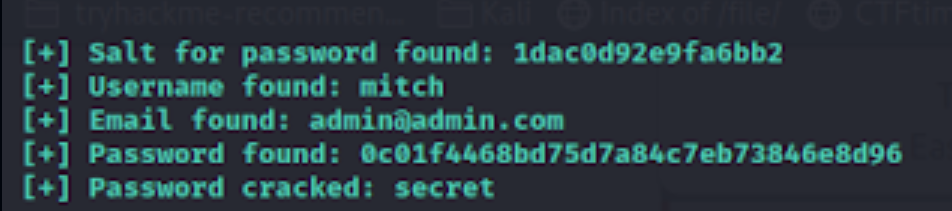
****

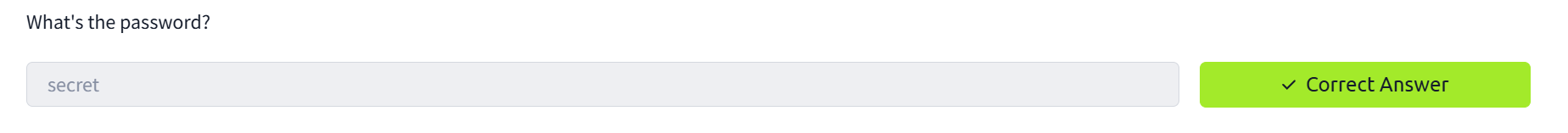
****

****

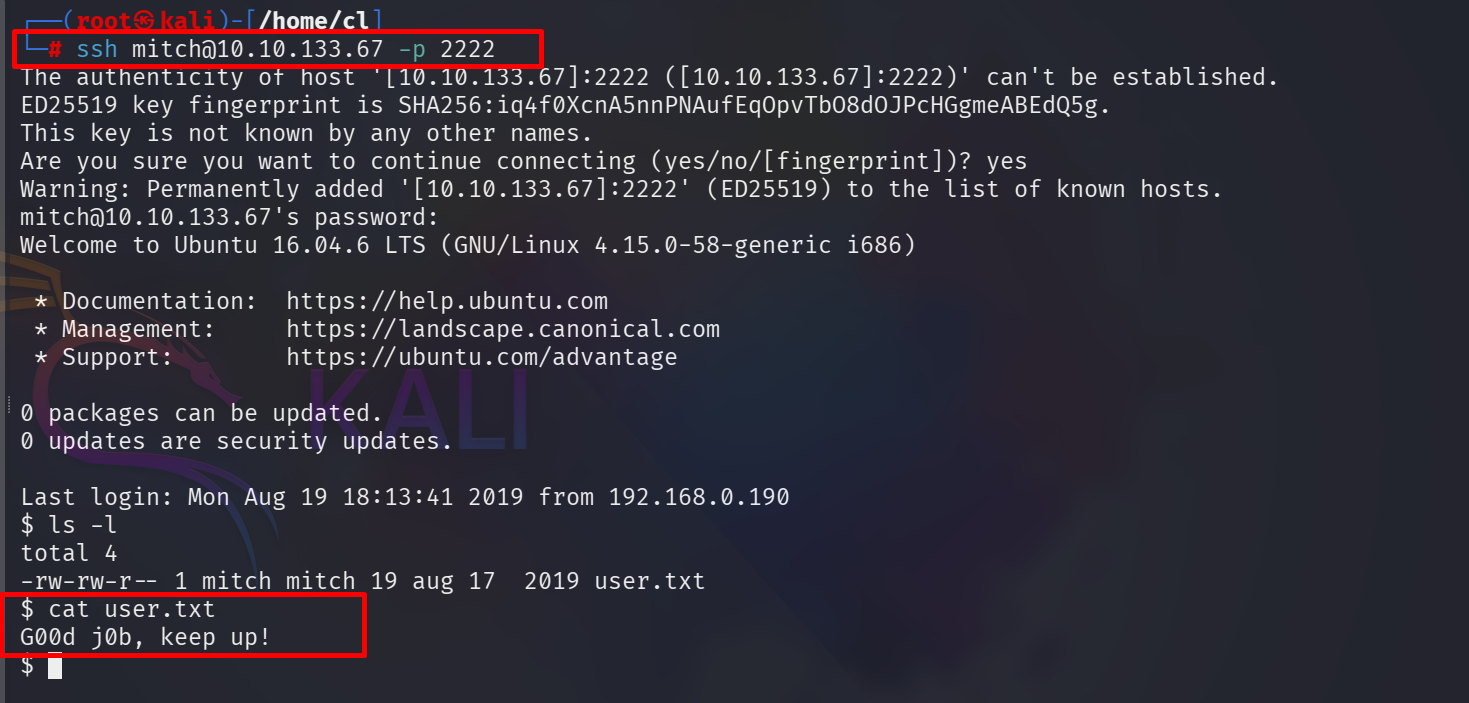
****

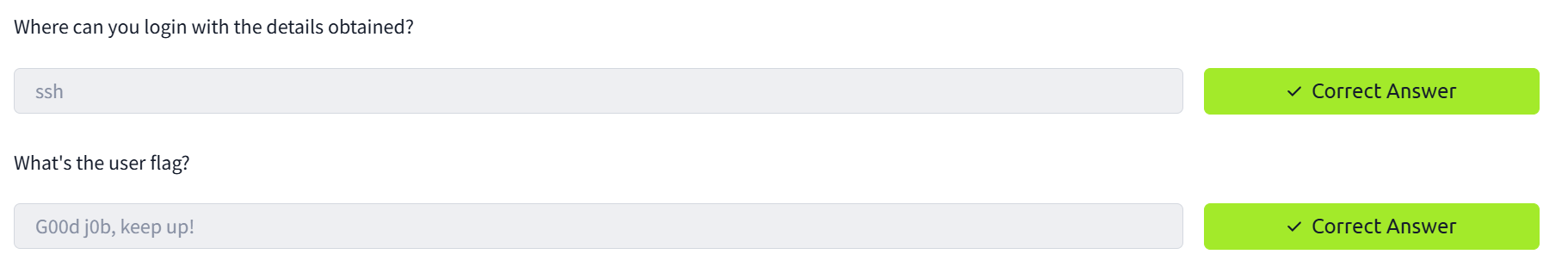
****

****

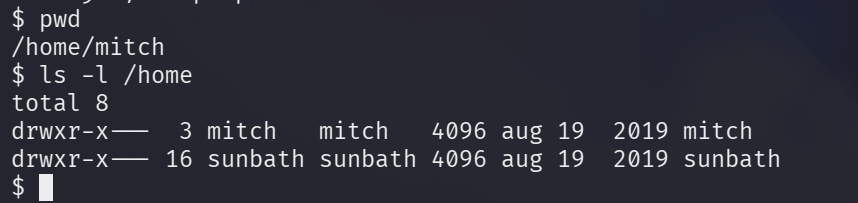
****

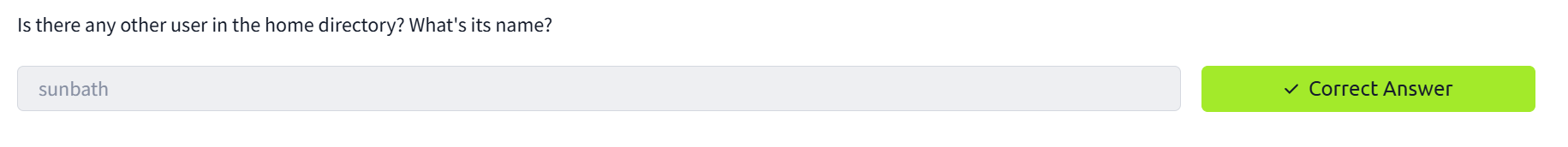
**Step 5: Now we have the username and password, try to login into that machine via ssh service with the port 2222.**

****

****

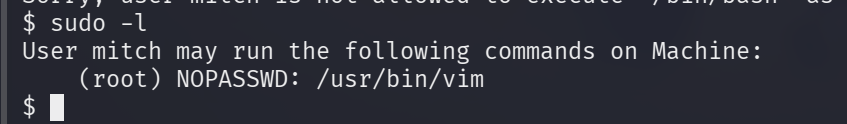
**Step 6: Now Under Linux each user has a directory with his name in the "/home" folder.**

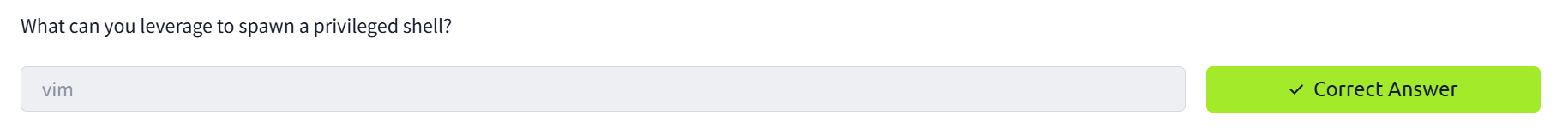
****

****

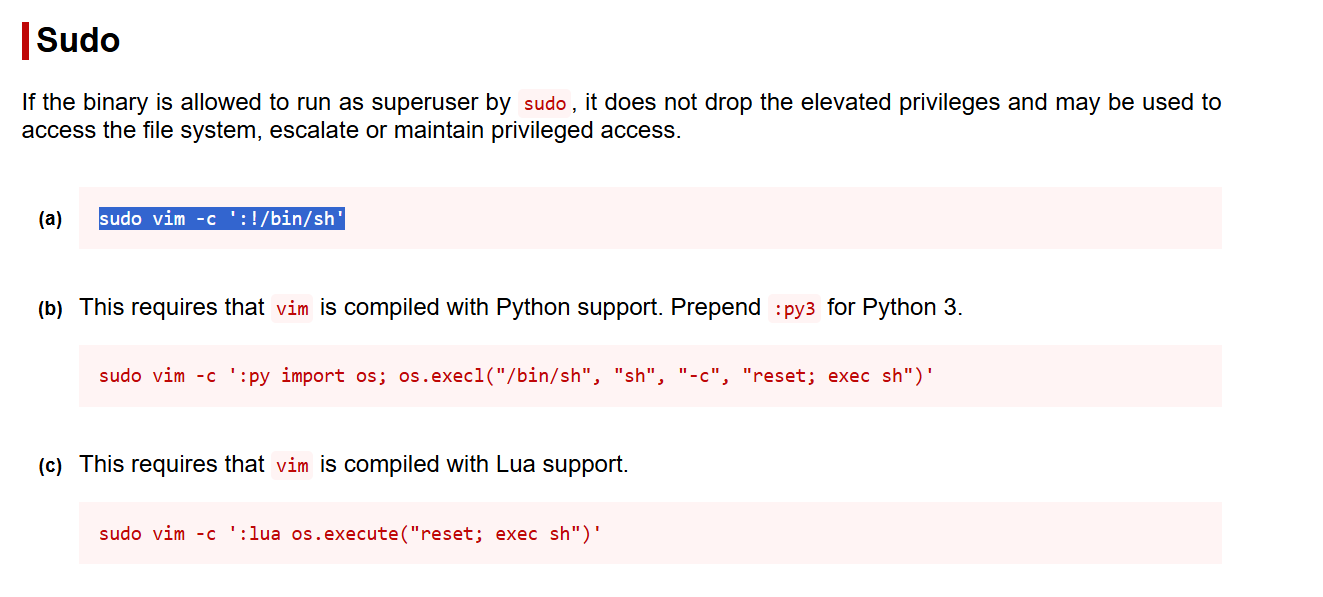
**Step 7: Privilege Escalatio**

**On to privileged escalation! First I like to start off with running “sudo -l” to see what my current user can run.**

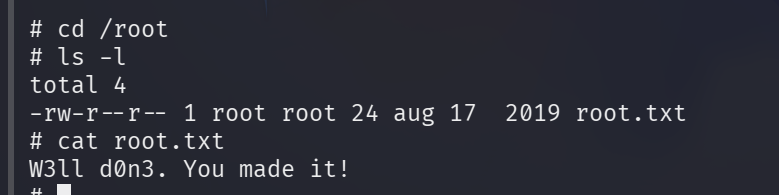
****

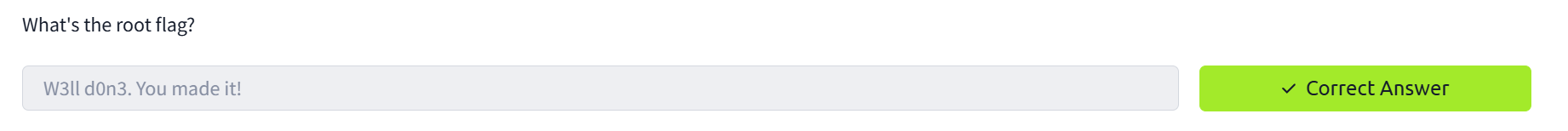
****

**We can see the user “mitch” can run /usr/bin/vim without a password. With that information, let’s check out GTFOBins and see if we can use that for privesc.**

****

**Step 8: Under the root user home directory there is a file, open it and got the flag.**

****

****