**WRITE-UPS FOR Hospital –** *solve on 02/09/2024*

We start with some simple nmap

22/tcp open ssh OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2.0)

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-02-08 23:57:30Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)

443/tcp open ssl/http Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ldapssl?

1801/tcp open msmq?

2103/tcp open msrpc Microsoft Windows RPC

2105/tcp open msrpc Microsoft Windows RPC

2107/tcp open msrpc Microsoft Windows RPC

2179/tcp open vmrdp?

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)

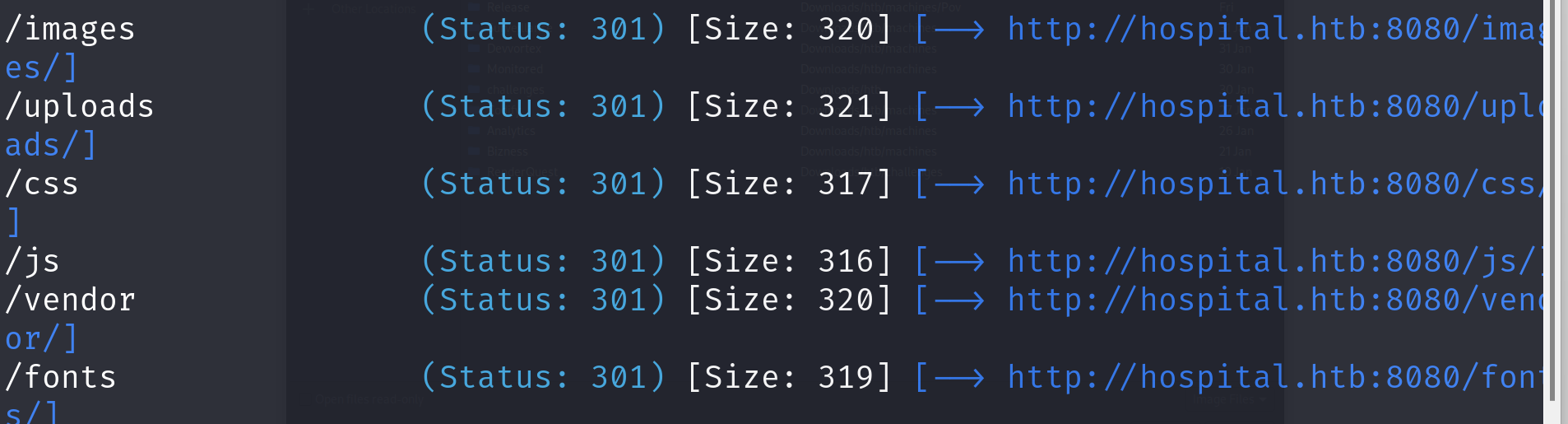
3269/tcp open globalcatLDAPssl?

3389/tcp open ms-wbt-server Microsoft Terminal Services

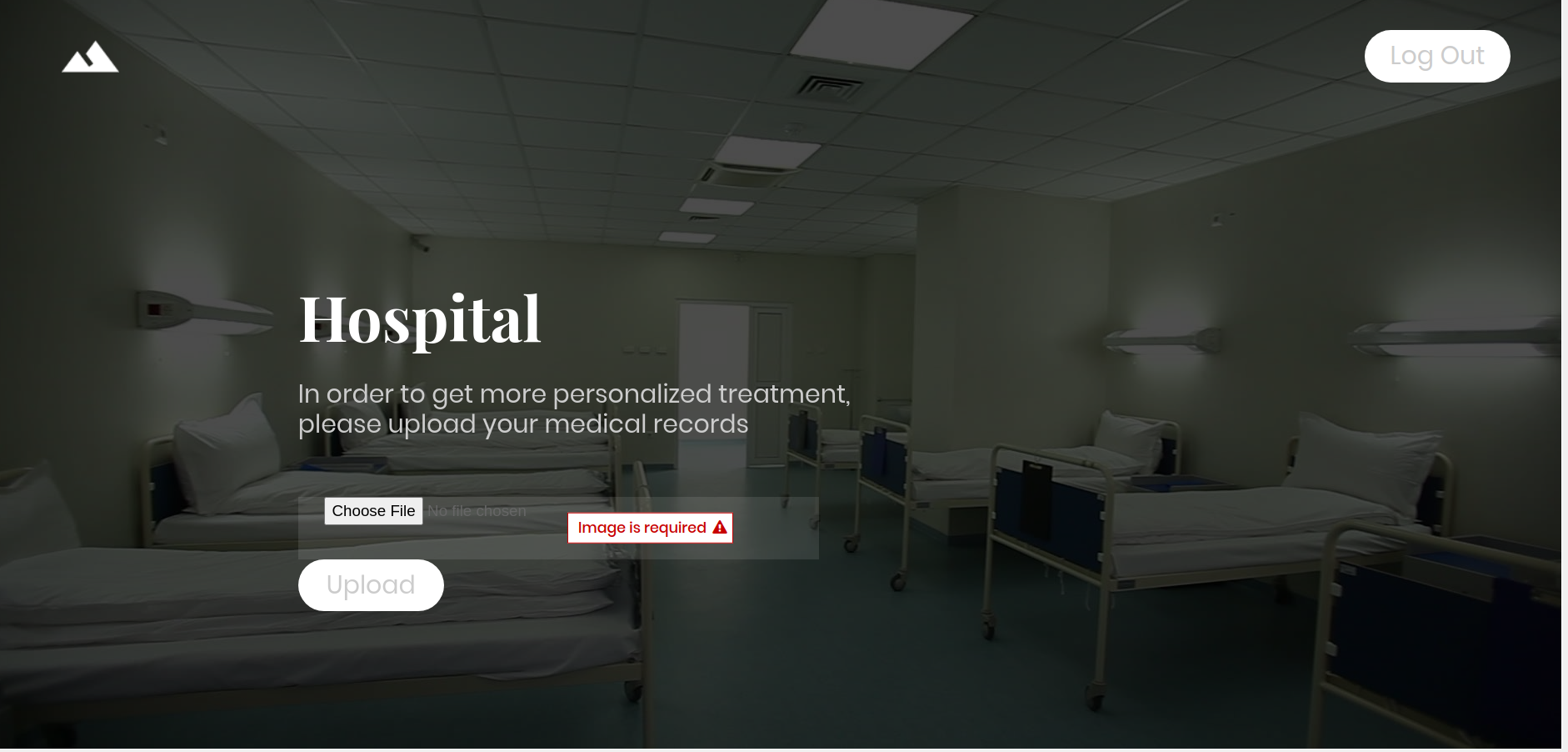
8080/tcp open http Apache httpd 2.4.55 ((Ubuntu))

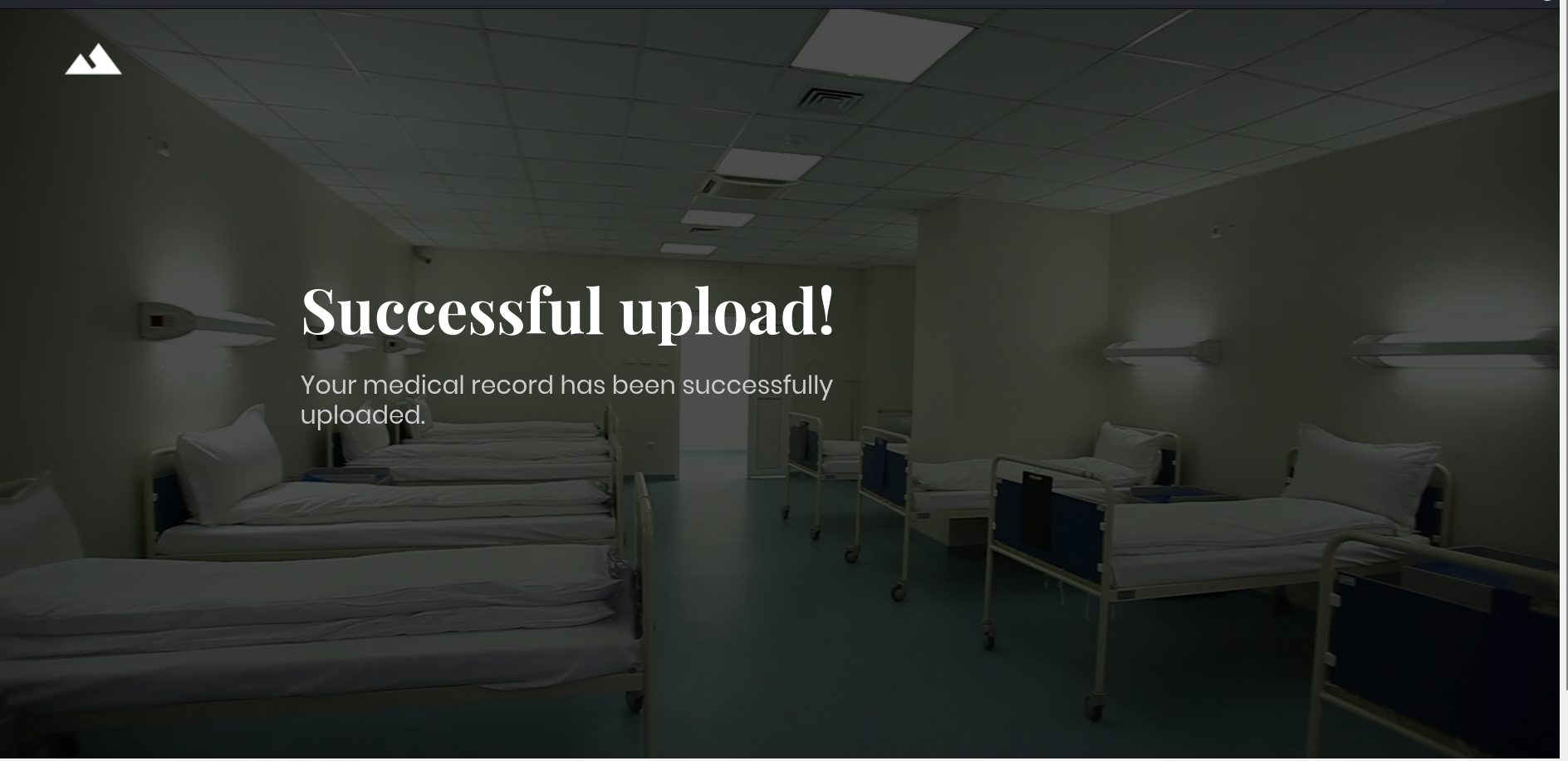
I tried to dirbuster but no luck come





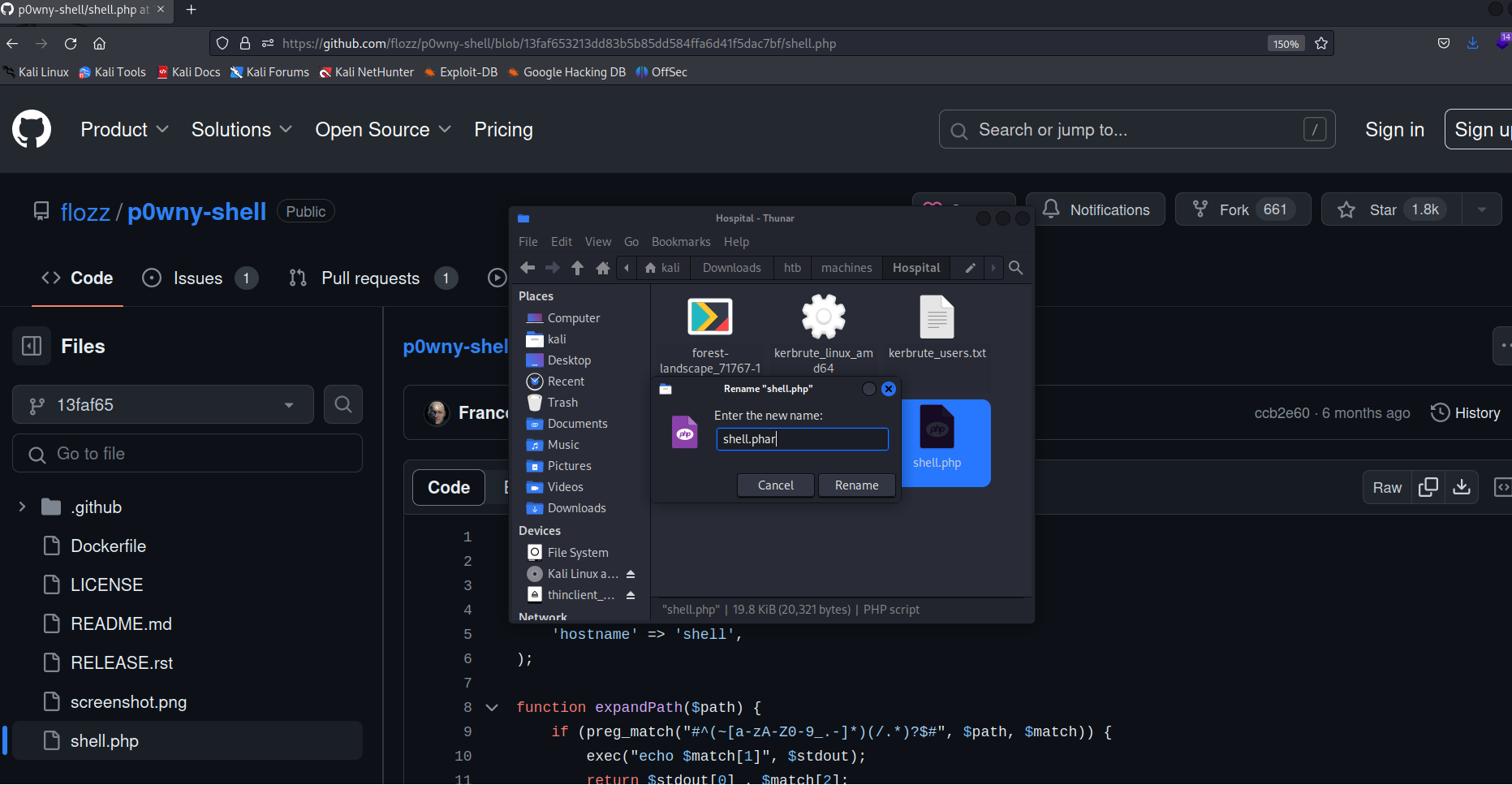
First I tried access the web on port 8080. I found a upload function seems interesting. I hoped that I can upload reverse shell to the server. Unfortunately, the system only accepts IMAGE FILE. So I searched the Internet to see if I can insert malicious code into the picture. Actually not!!! But by changing the file name to *.phar*, it could bypass the authentication.

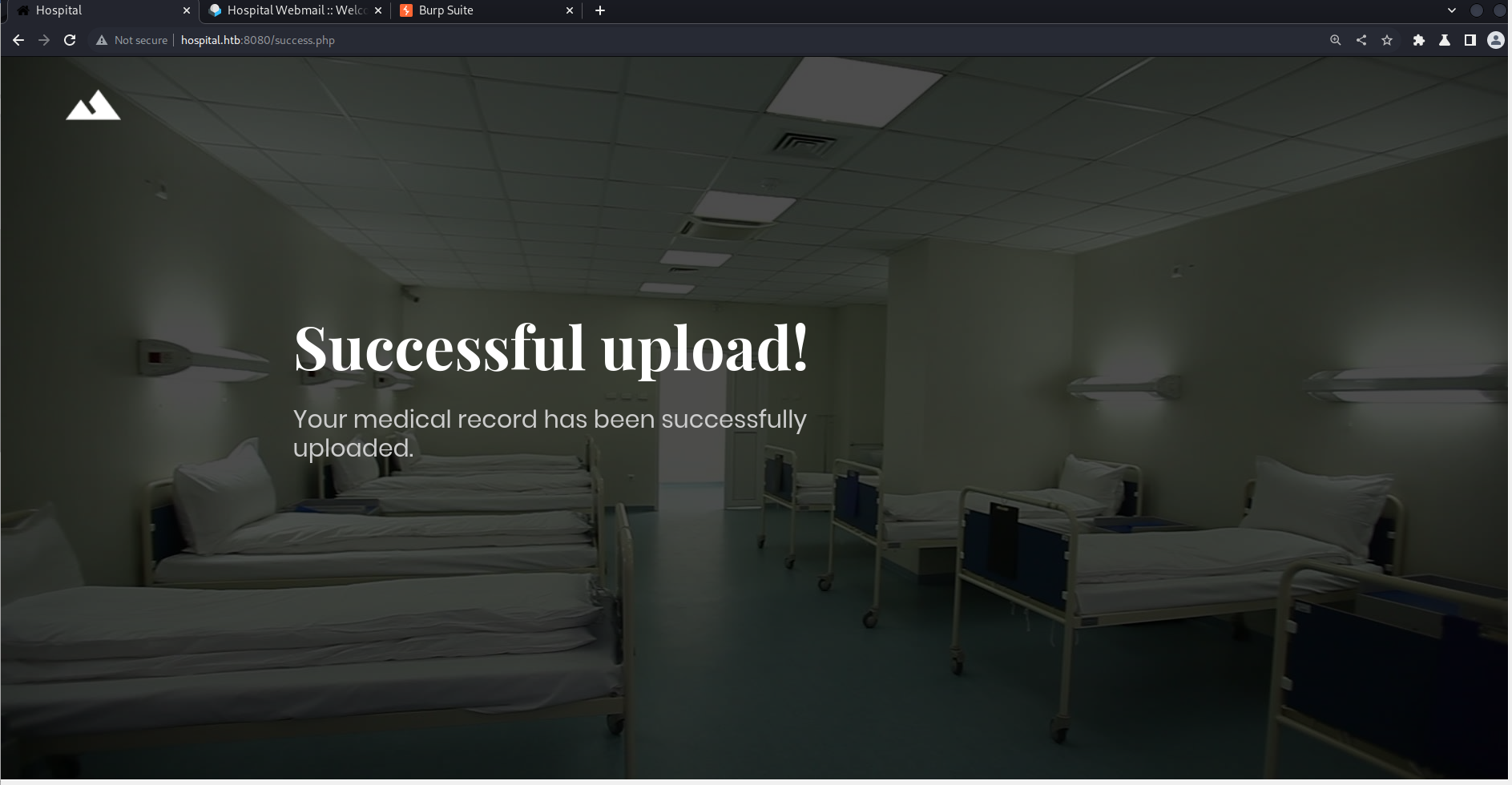




Look more at this article

<https://rcenetsec.com/hide-malicious-shell-in-image-file/#:~:text=Just%20rename%20the%20malicious%20file%20extension%3A.asp.jpg%2C.aspx%2C.jsp.jpg%2C.jspx%2C.pl%2C%20etc%E2%80%A6.%20Try,than%20the%20limit%20allowed%20by%20the%20web%20server>.





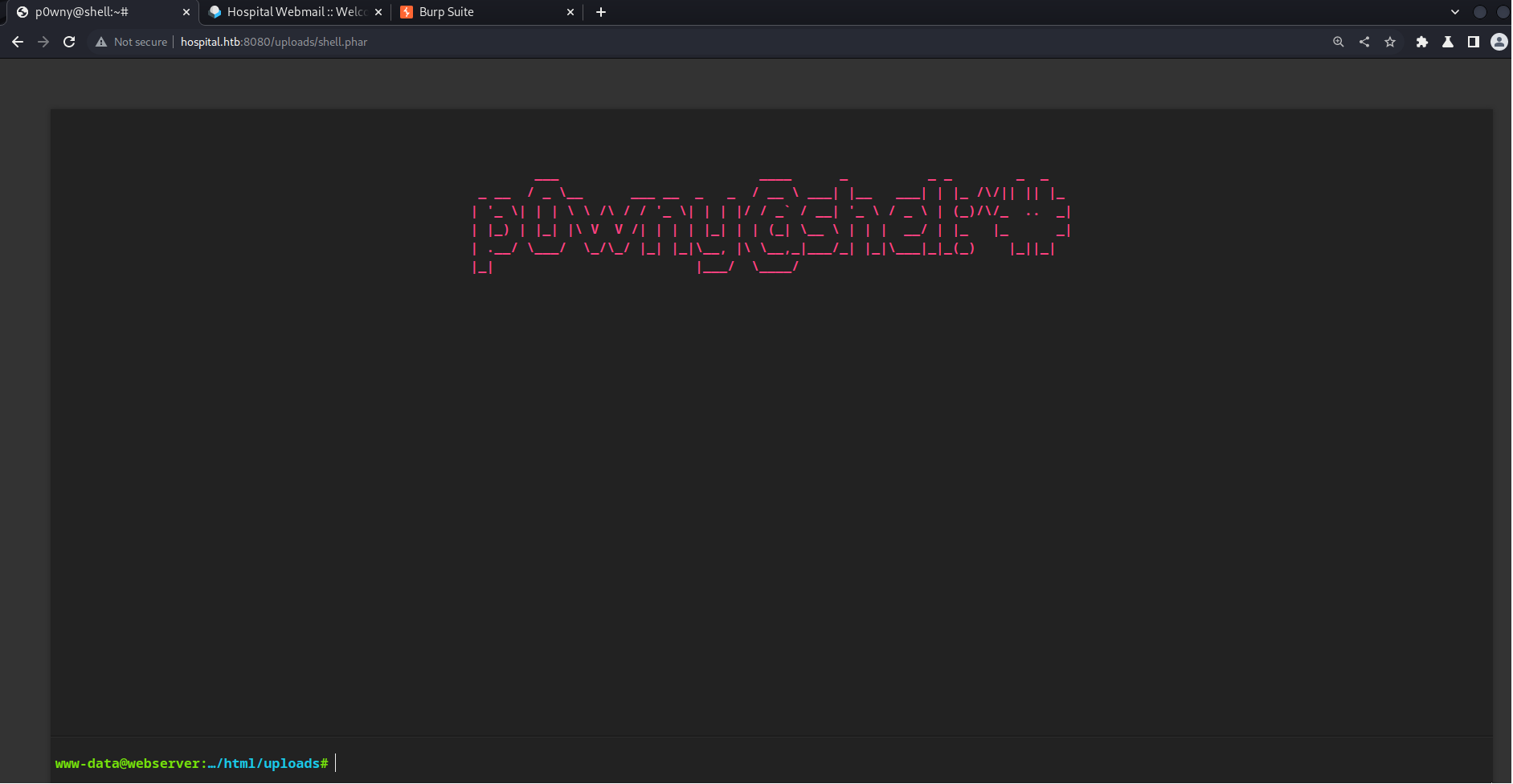
The normal reverse shell I tried below:

<https://pentestmonkey.net/tools/web-shells/php-reverse-shell>

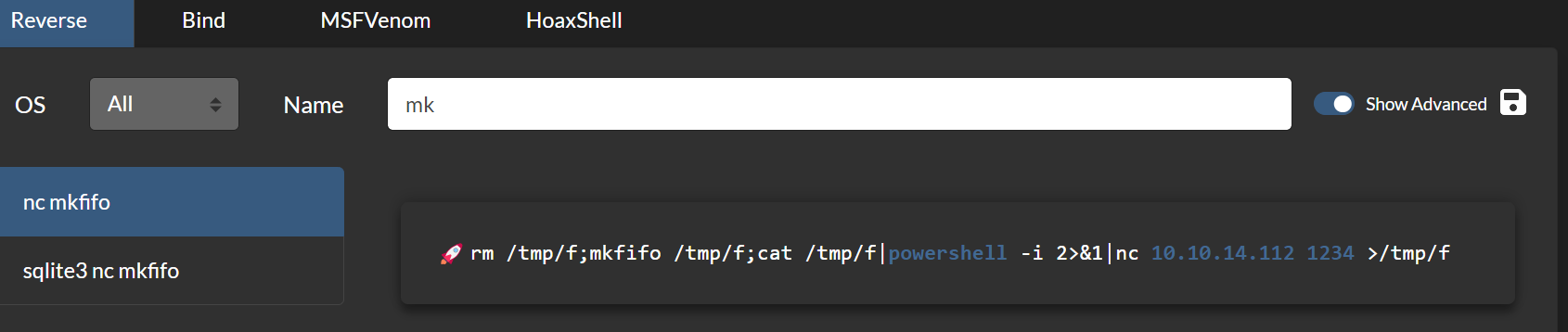
The shell not alive for along though it successfully connection.

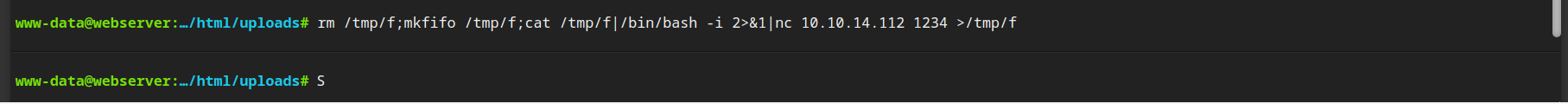
So I tried this shell, GREAT

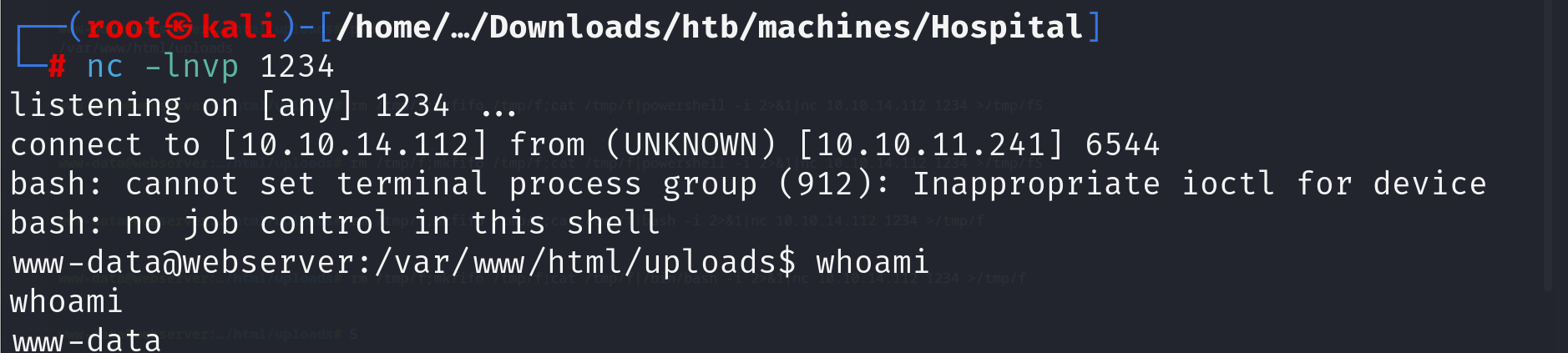
<https://github.com/flozz/p0wny-shell/blob/master/shell.php>



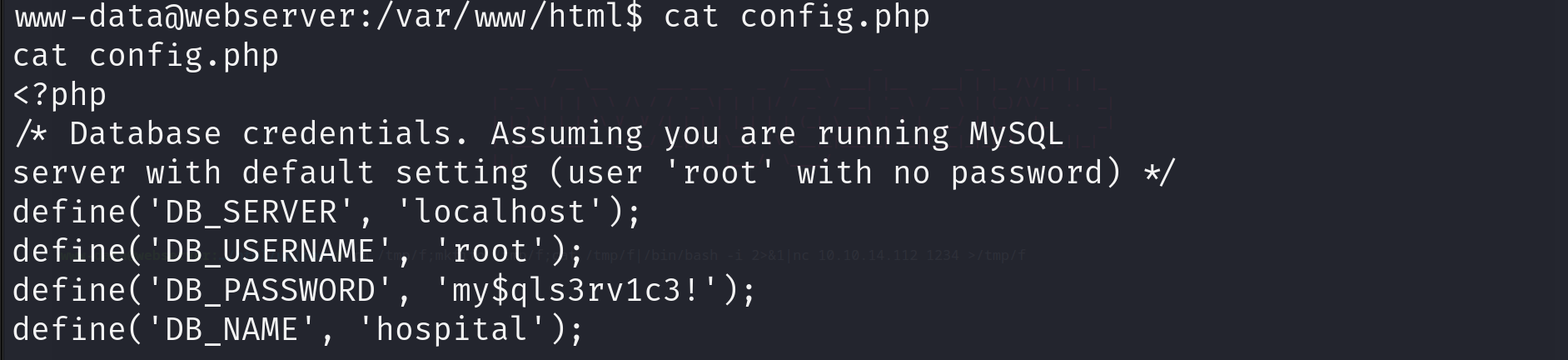
After we got the reverse shell on the web interface, I connect back to my CLI for convenience



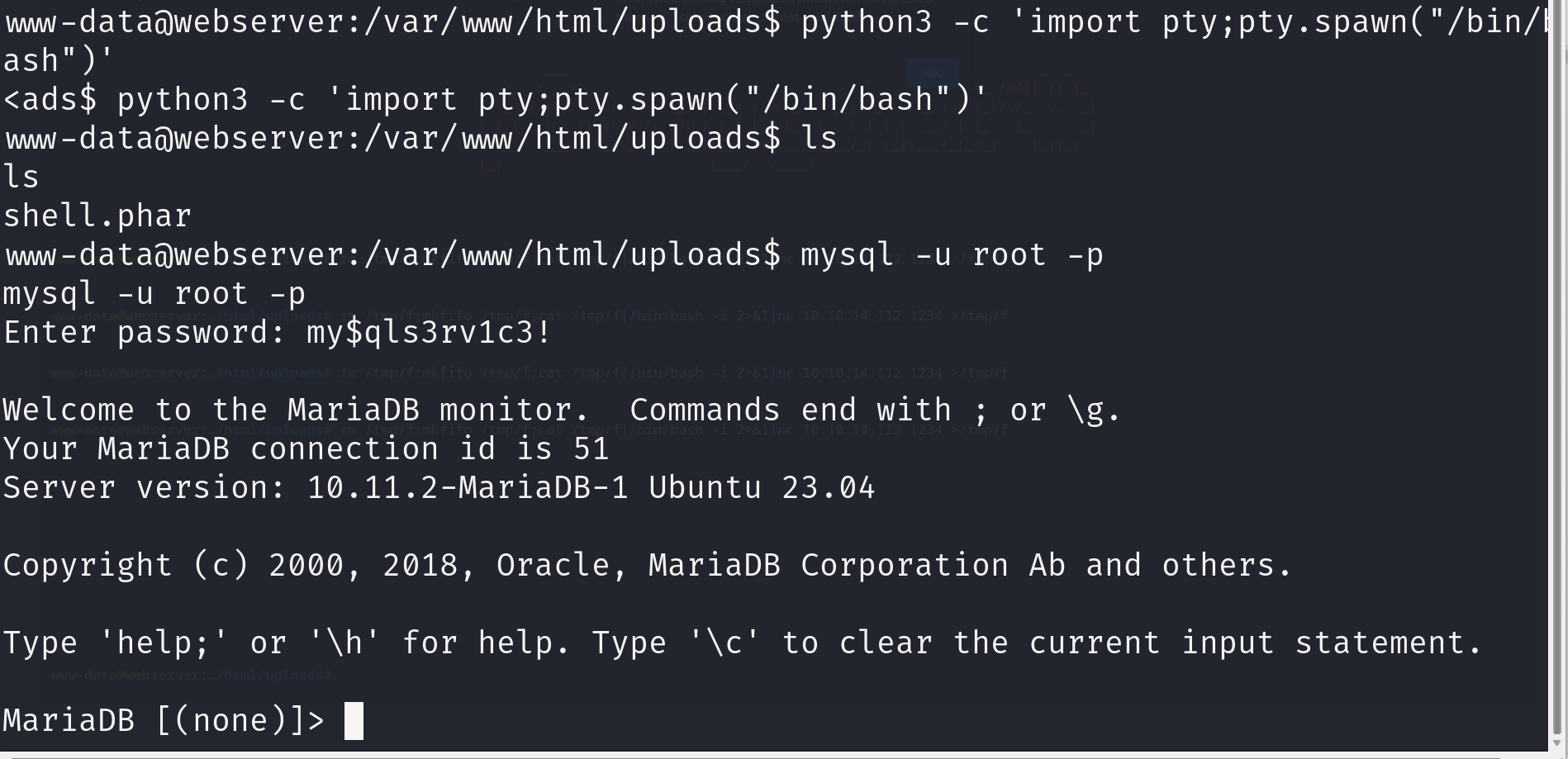




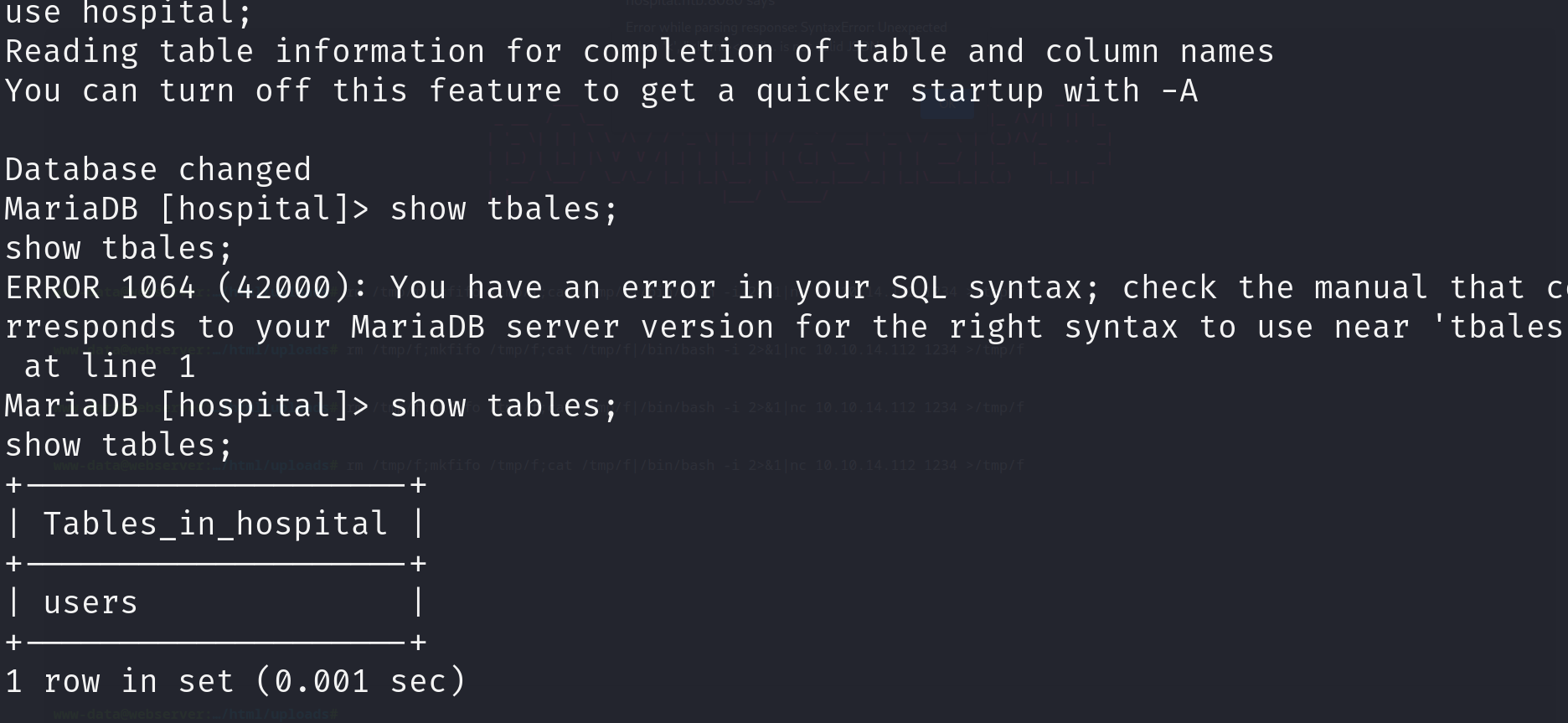
Looking around at *config.php*, I found some credential. I used that to connect to the database

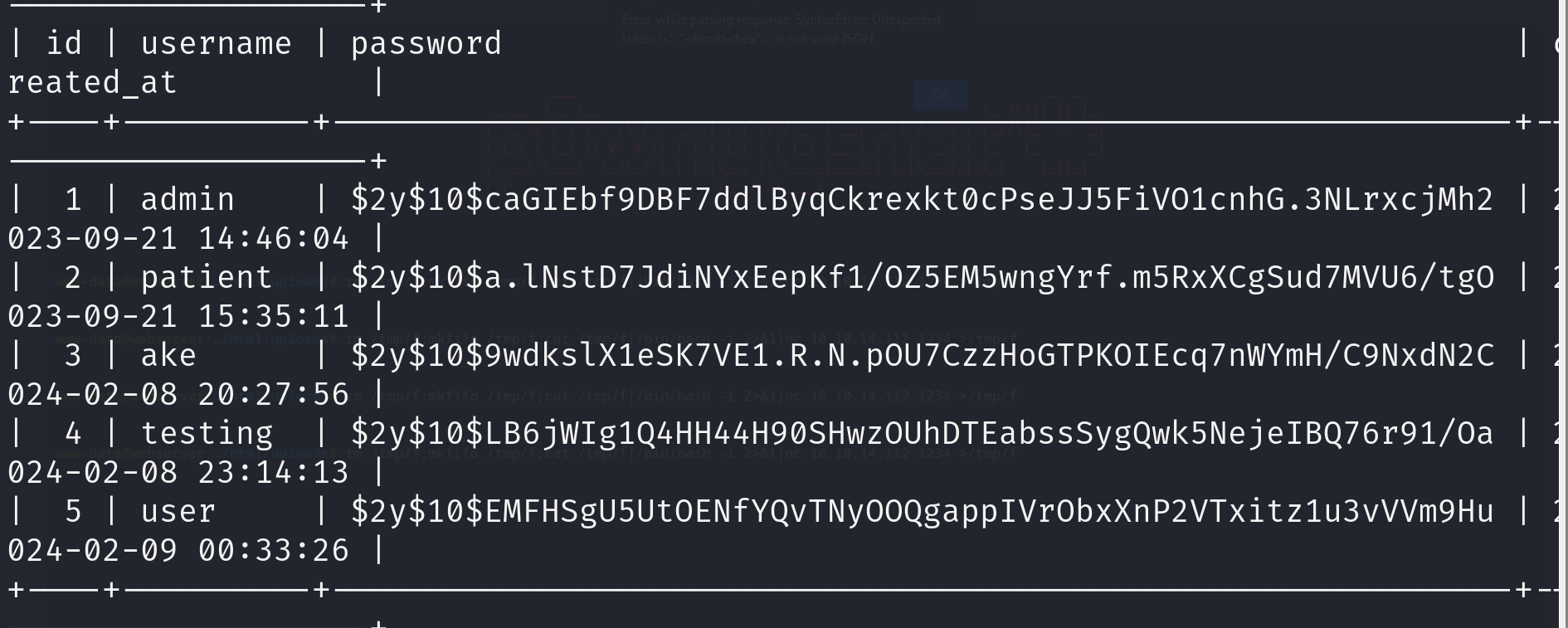


But before that, I must update the bash shell

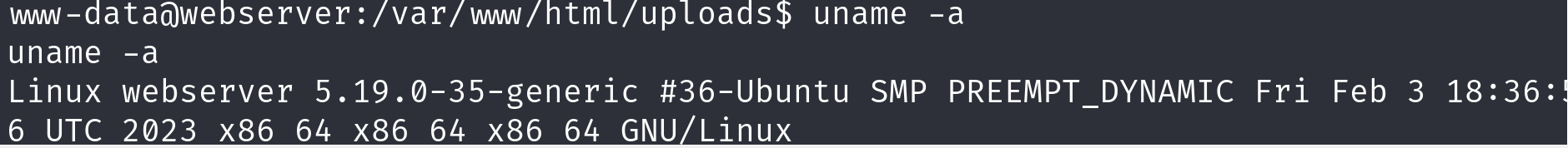








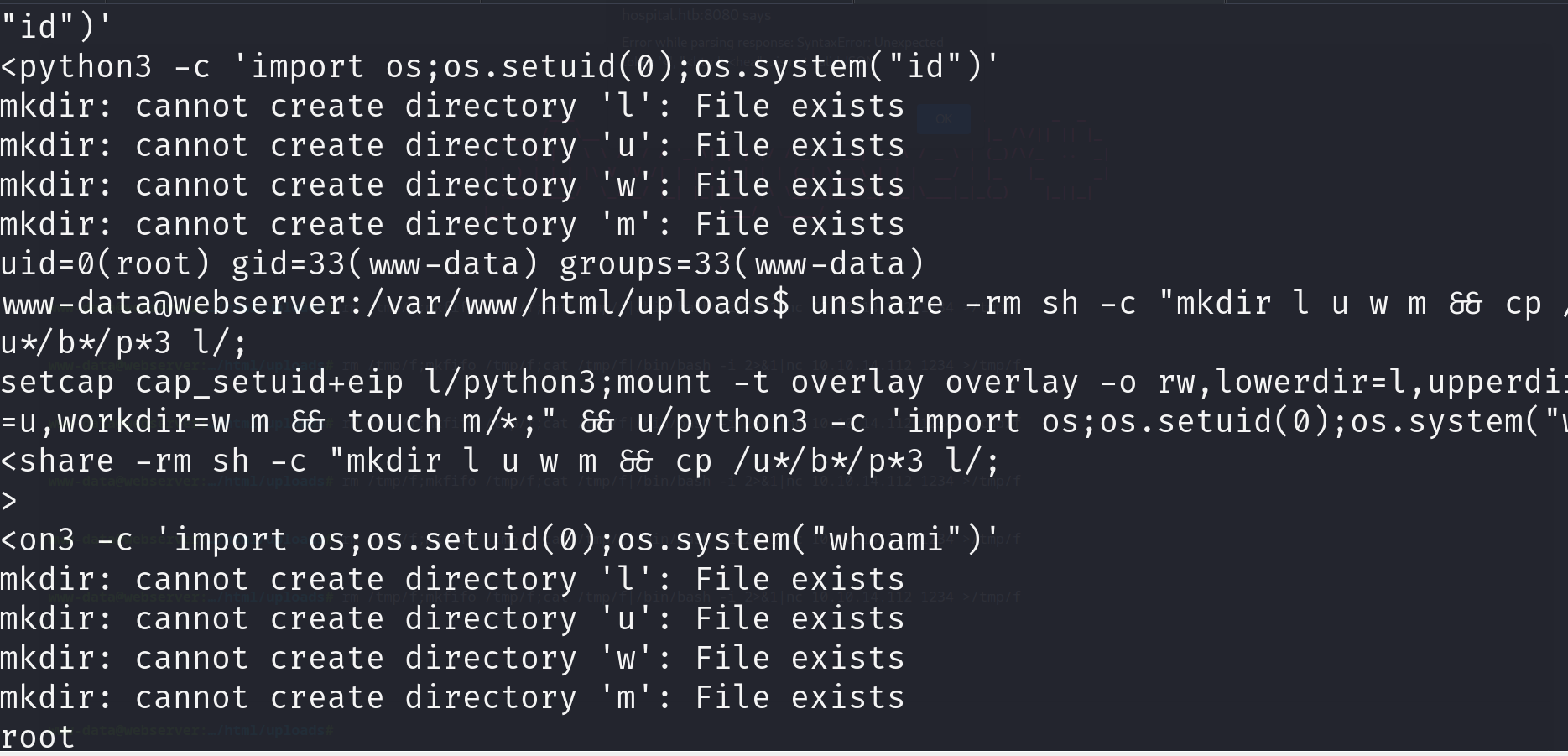
Great now we have the many hash values. But unfortunately, after a while of paying effort, I concluded that these hash are uncrackable. So I found another way to exploit the target. Started by searching the version of the machine.

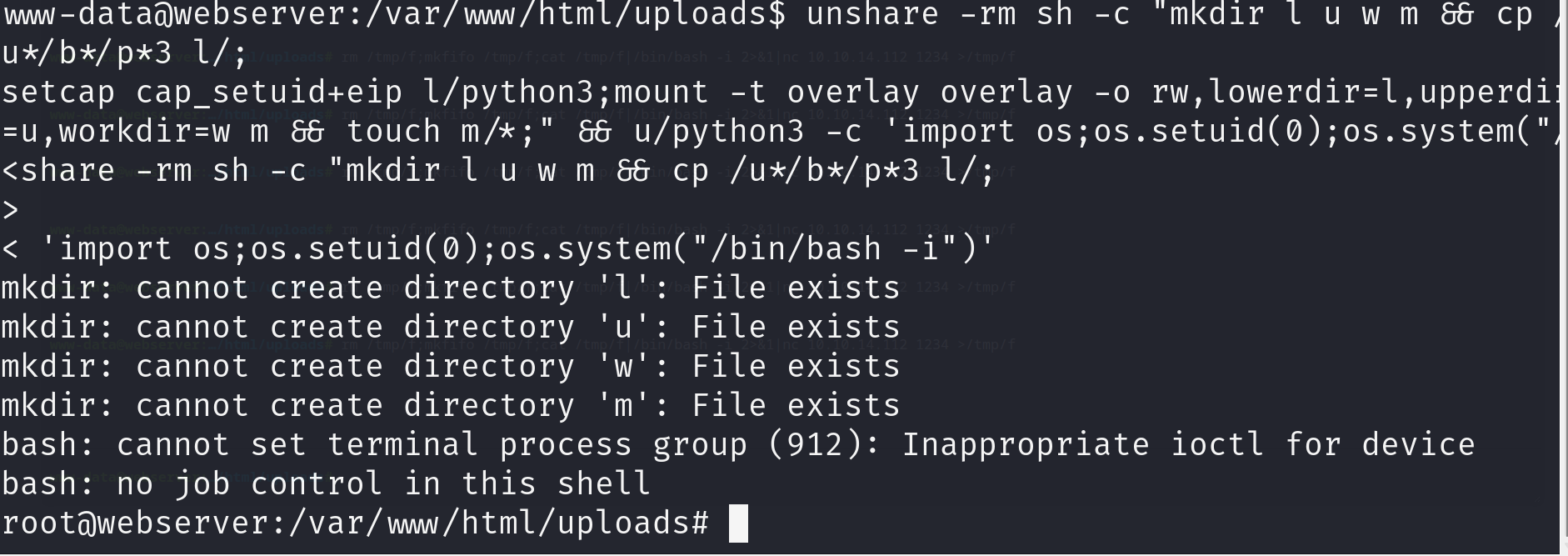


That can helps me looking for its vulnerablity

<https://www.reddit.com/r/selfhosted/comments/15ecpck/ubuntu_local_privilege_escalation_cve20232640/>

I did as in the reddit post above and got the root priviledge

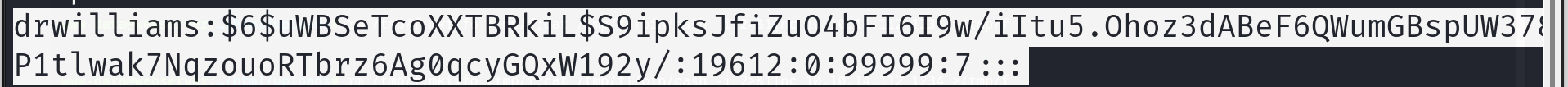




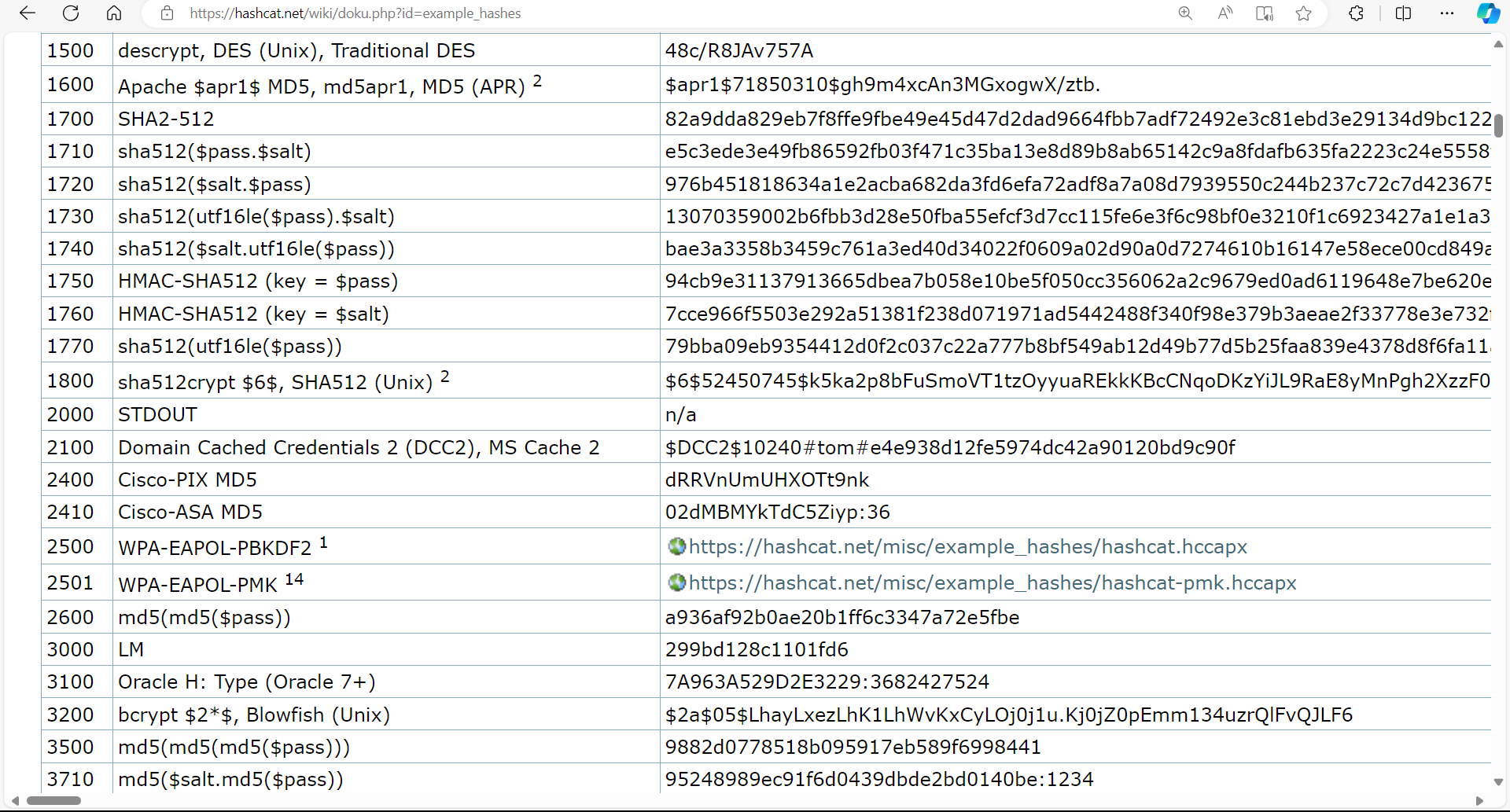
But from this root in this target, no luck or flag came ☹

It’s alright, not too easy. I look at /etc/shadow and found credential of Doctor Williams 😊





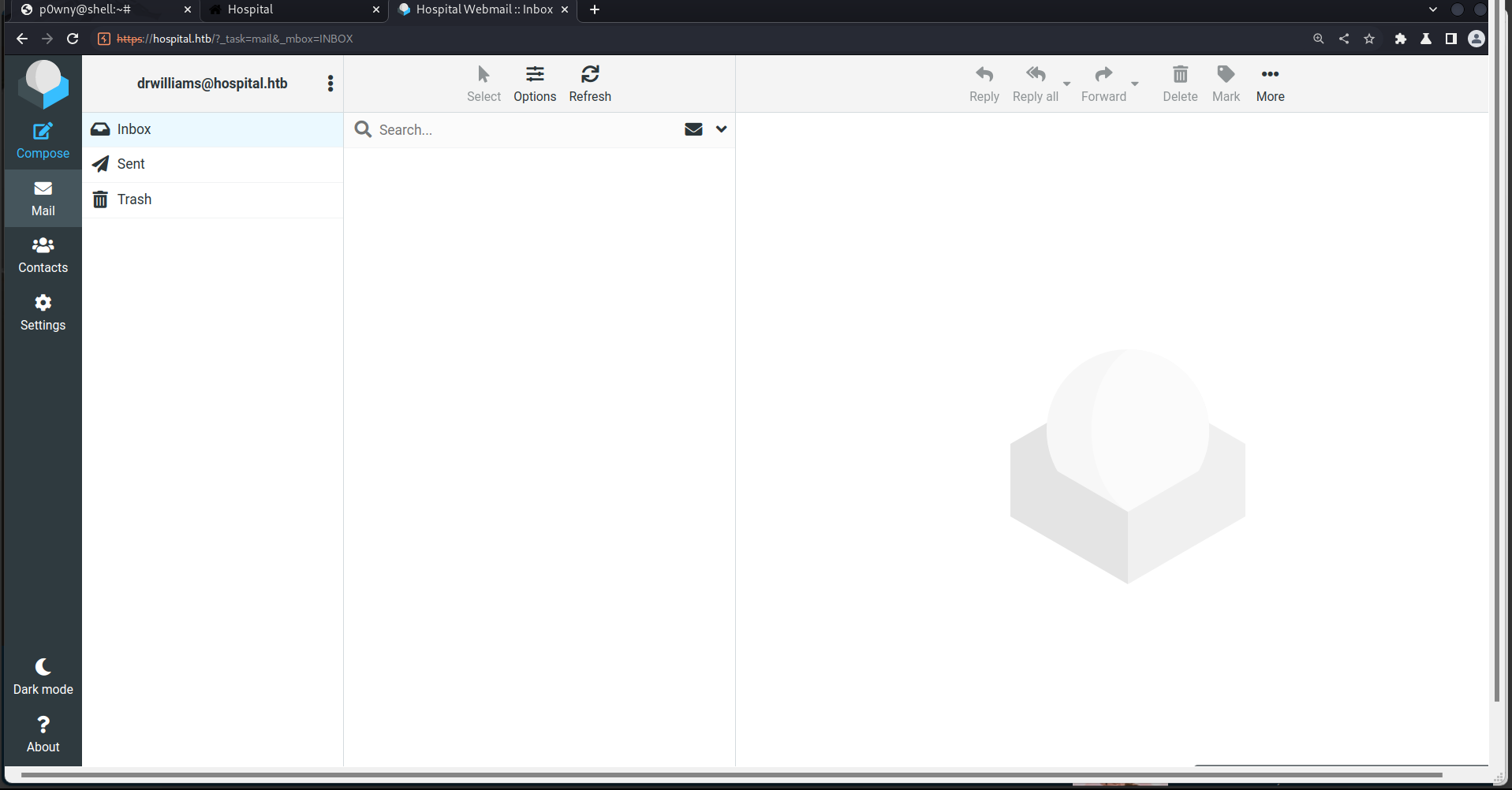
And it seems to be the *sha512crypt*



Use john to crack it in a few seconds



Now I got into the Dr. Williams’ account. And by looking at his inbox. =>> ???





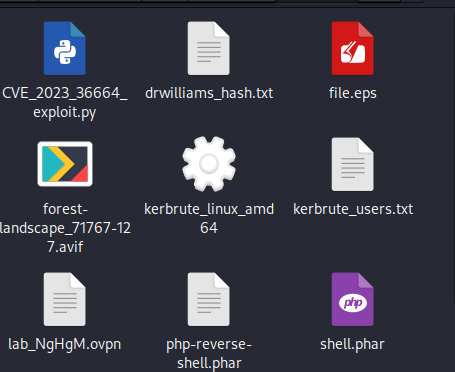
Some thing happened with *GhostScript* and *.eps* file. Just Gooooogling

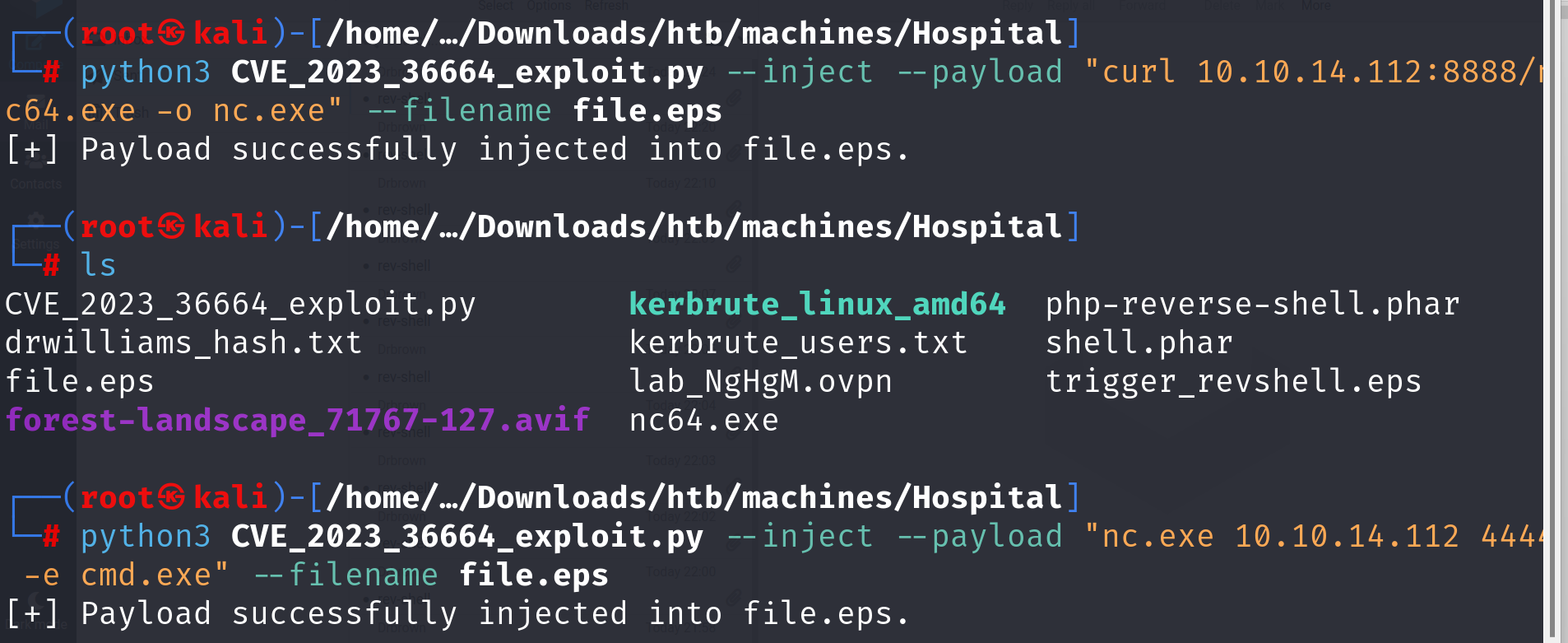
*CVE-2023-36664*

Did as the instruction

* First I set up a http server for the target to download nc64.exe from my machine, as I guested it didn’t have.
* After that I inserted payload to the target to get back the reverse shell

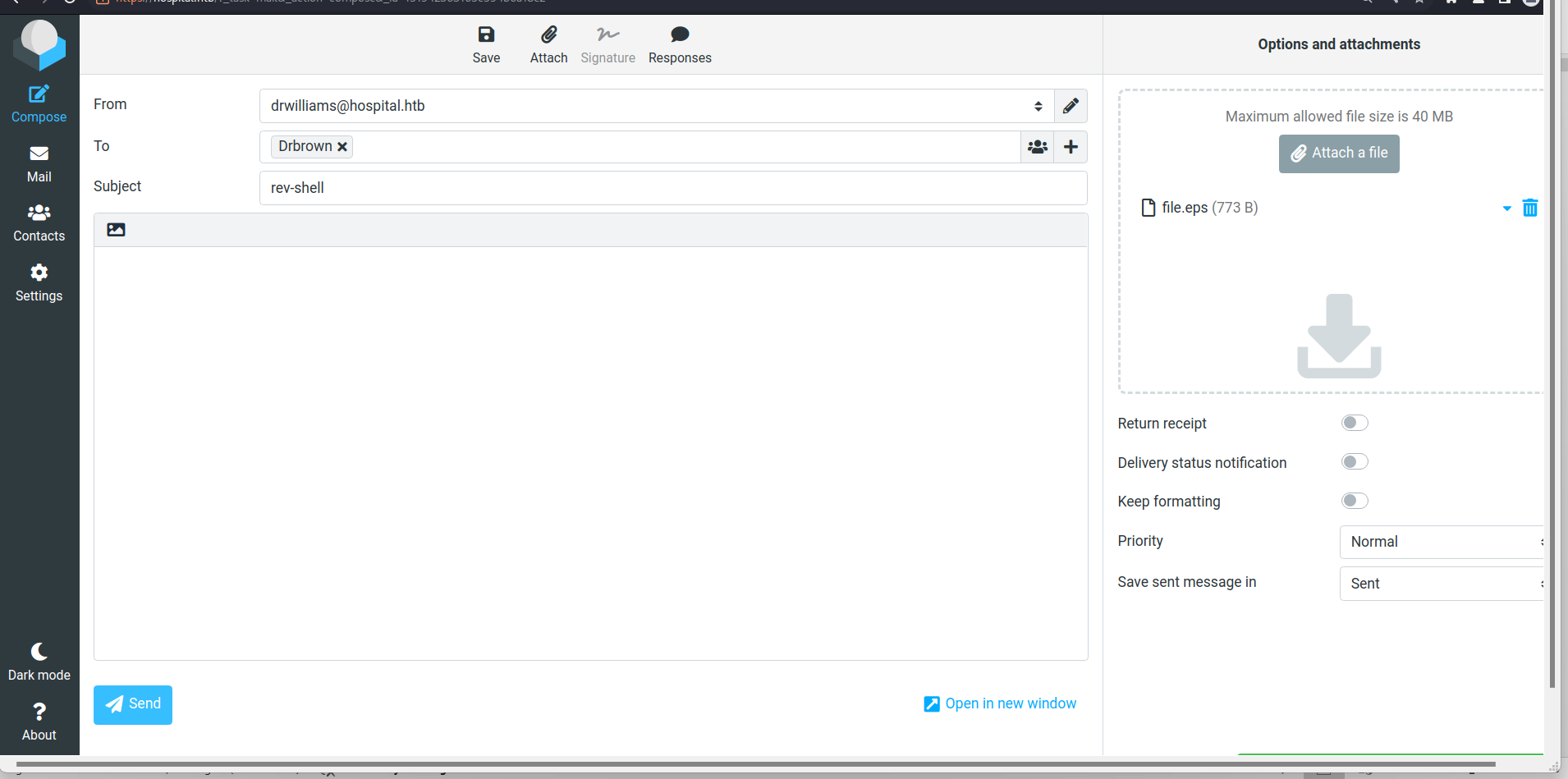
Download file.eps from github dir



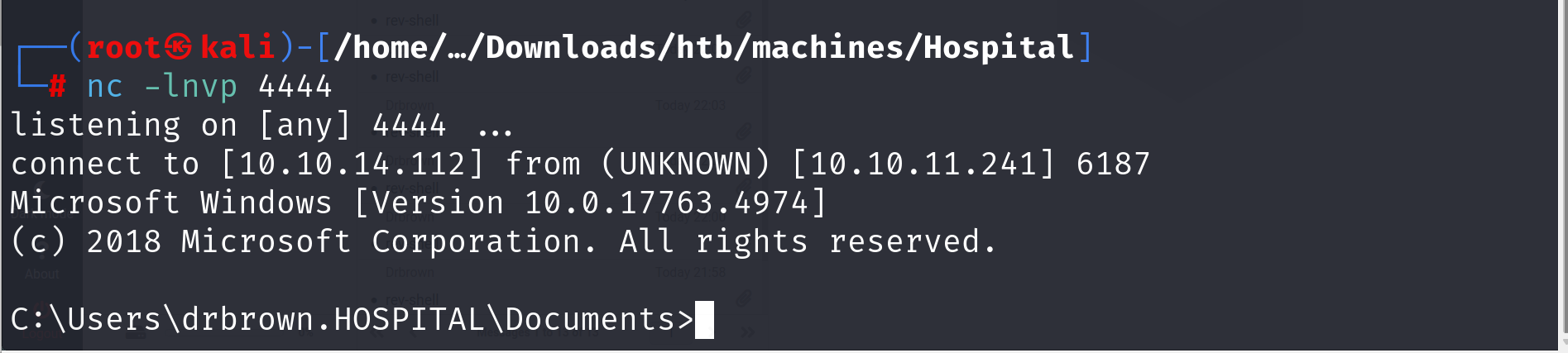




Lastly, send the file to reply DrBrown



Now I got the reverse shell

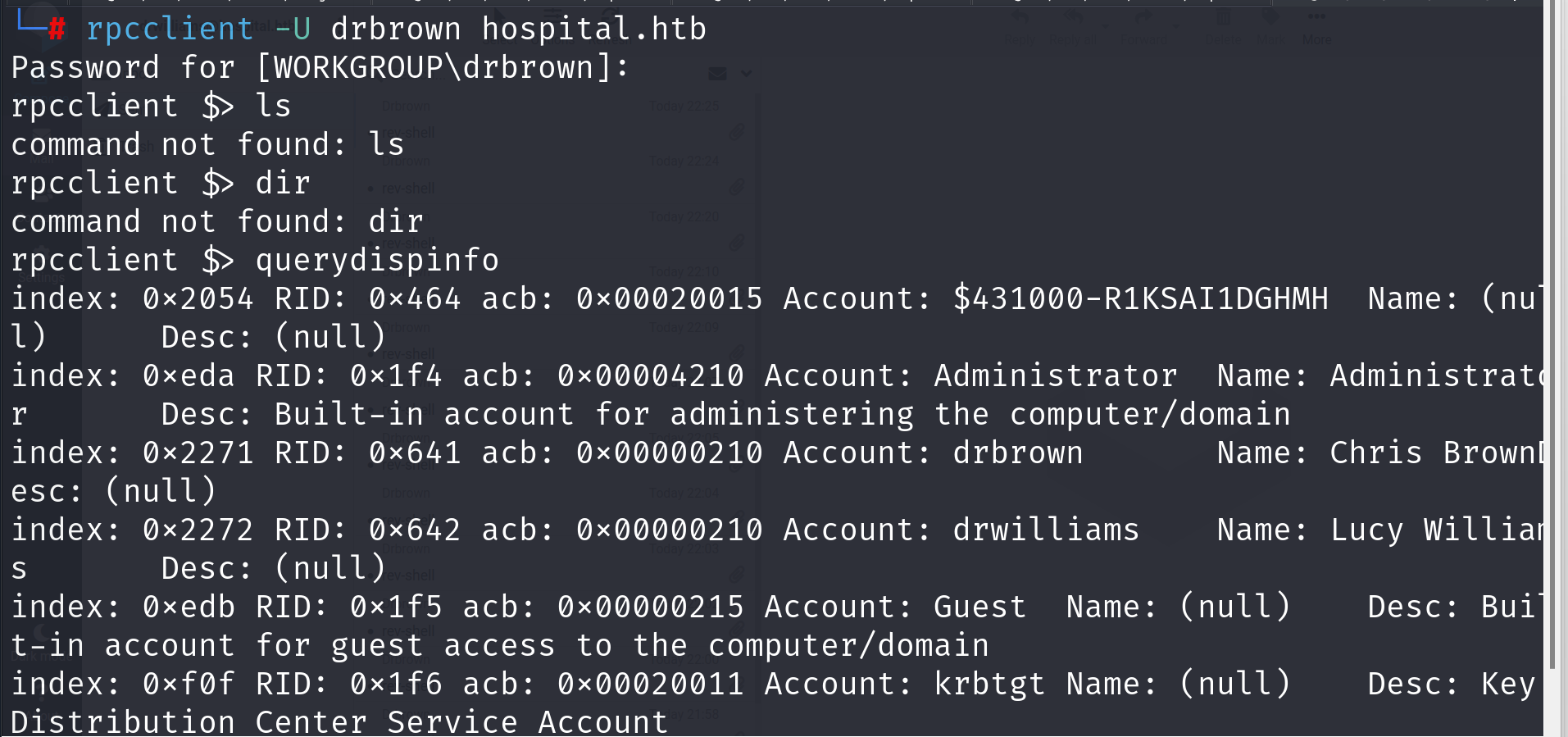


NOW USER FLAG IS DONE !@!!##@@

I also find out password of drbrown

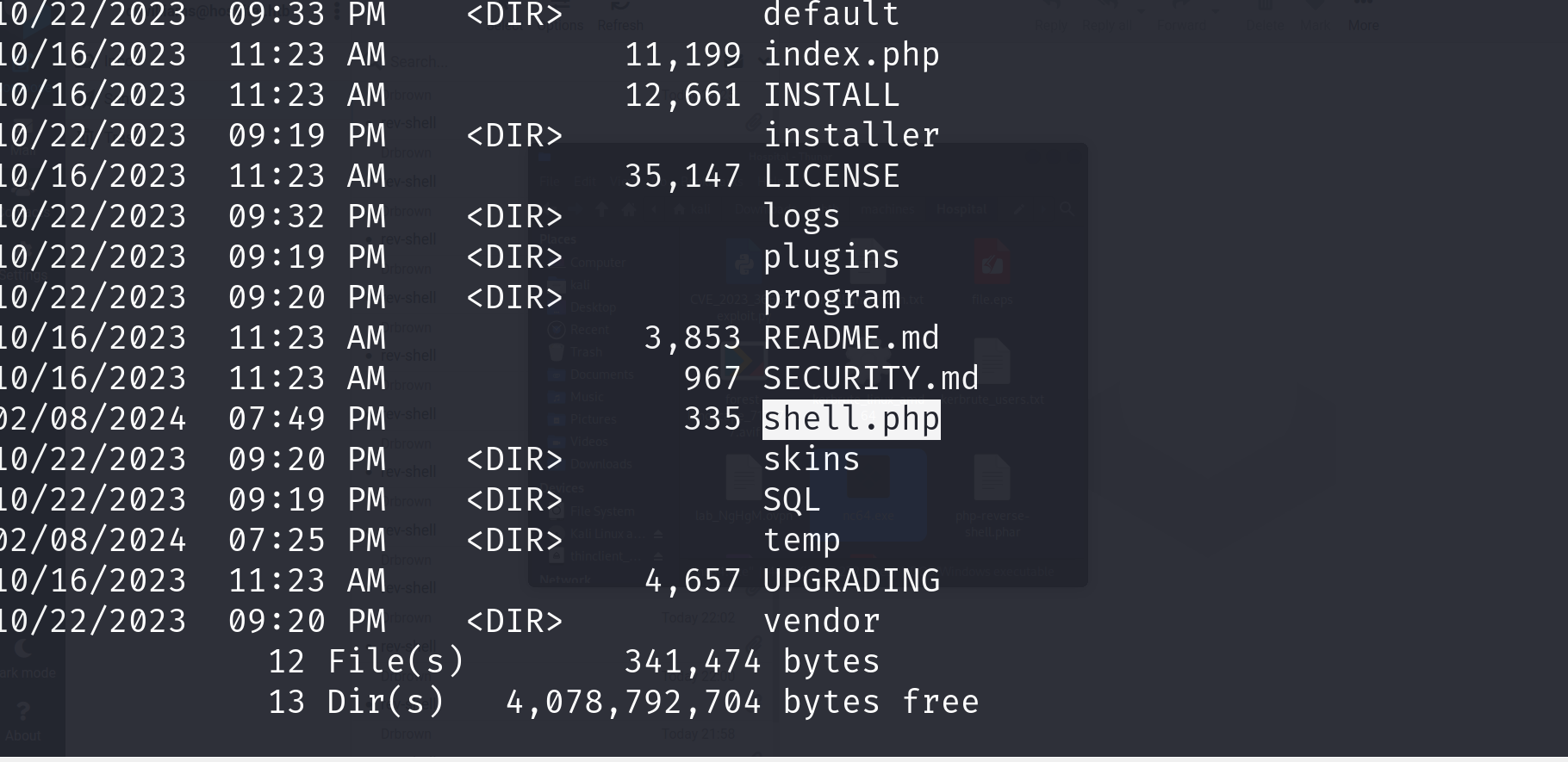


Connect using rpcclient. I found that Administrator and Guest share the same computer/domain

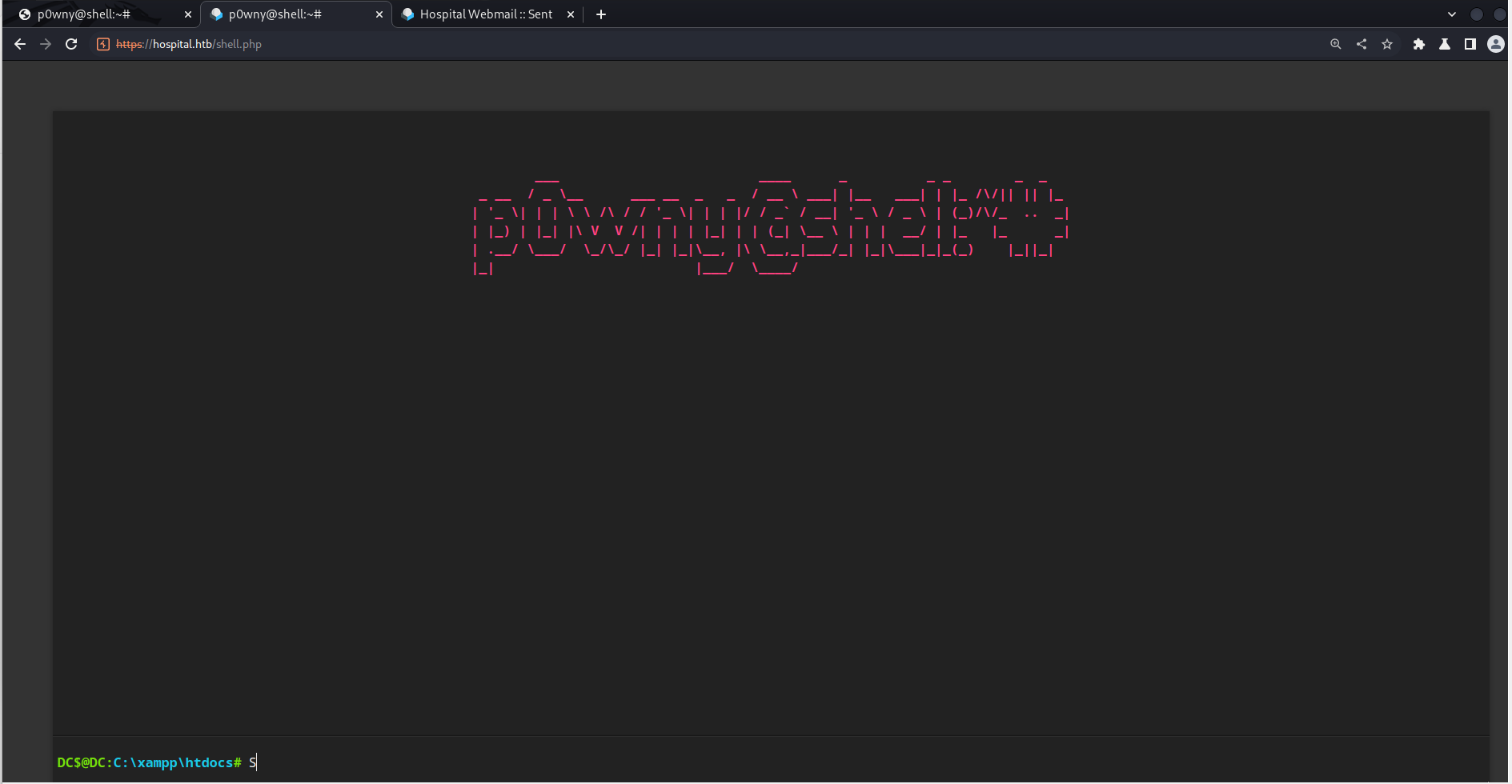


Now, navigate to \xampp\htdocs where the webserver read file from. Download shell.php (reverse shell) from my http server in my local Kali.





Use URL to directly execute the file and get another reverse shell on the web interface



THE ROOT IS ONLY A TRIVIAL FINDING PROBLEM. All things done.!!