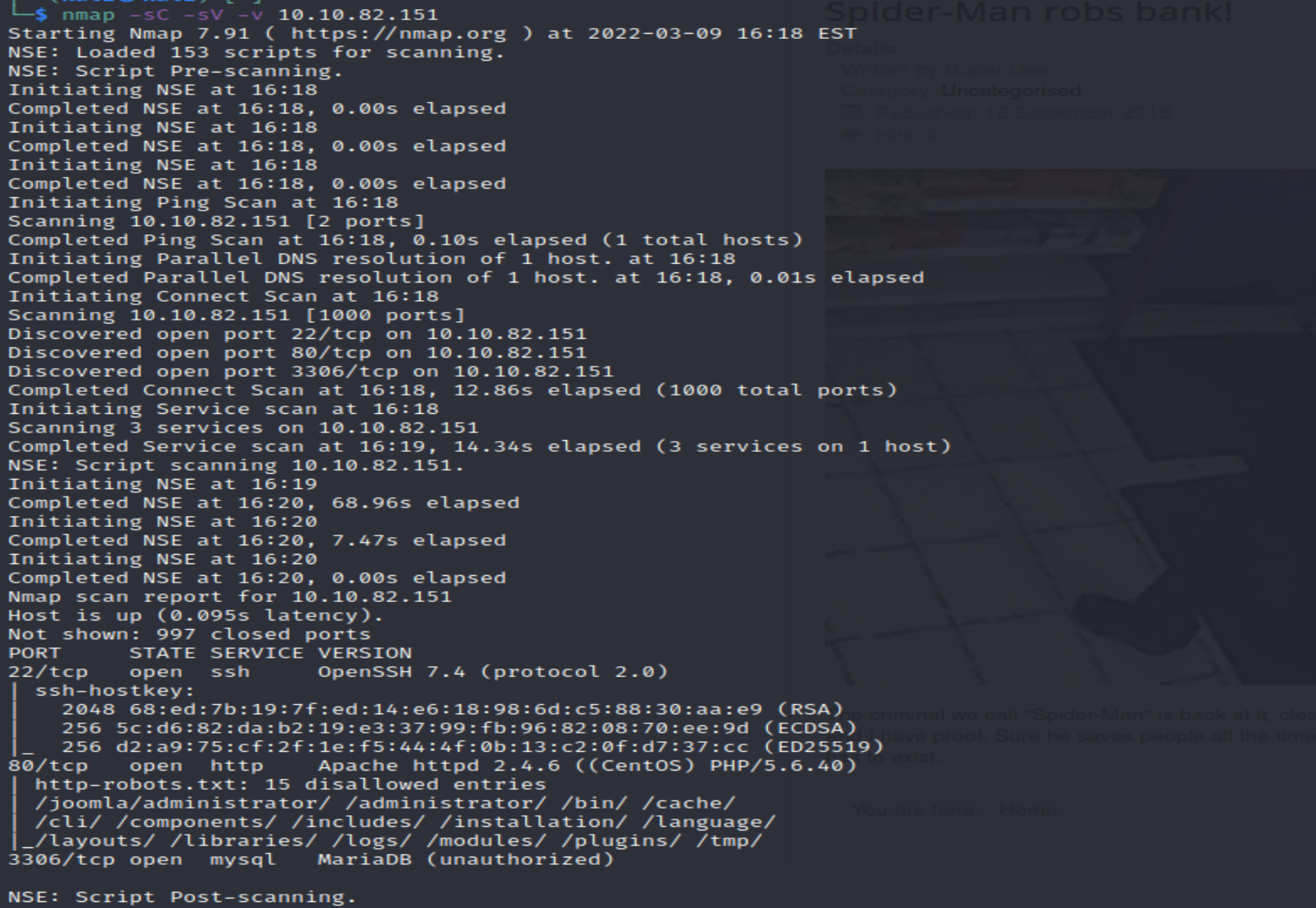
Daily bugle-hard



Deploy the machine - it may take up to 2 minutes to configure

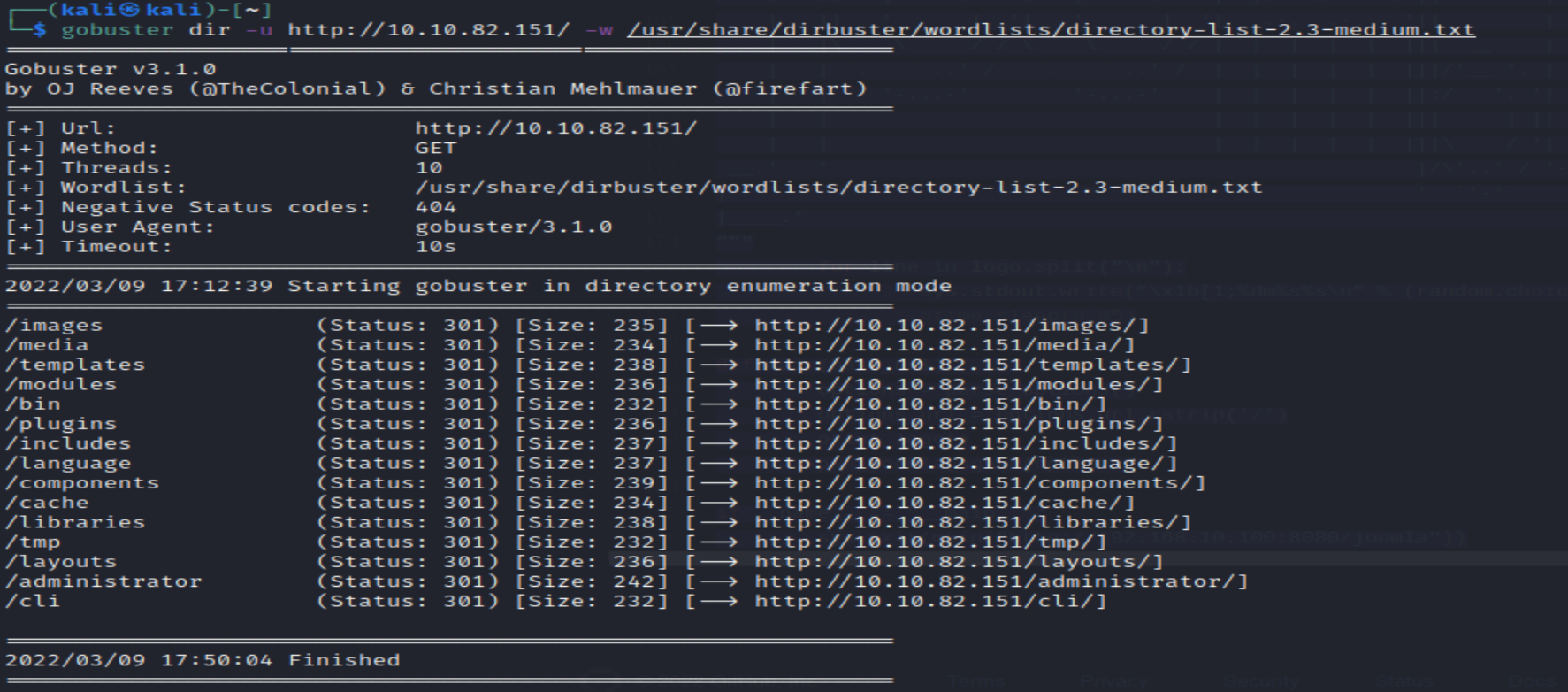
***Answer the questions below***

Access the web server, who robbed the bank?

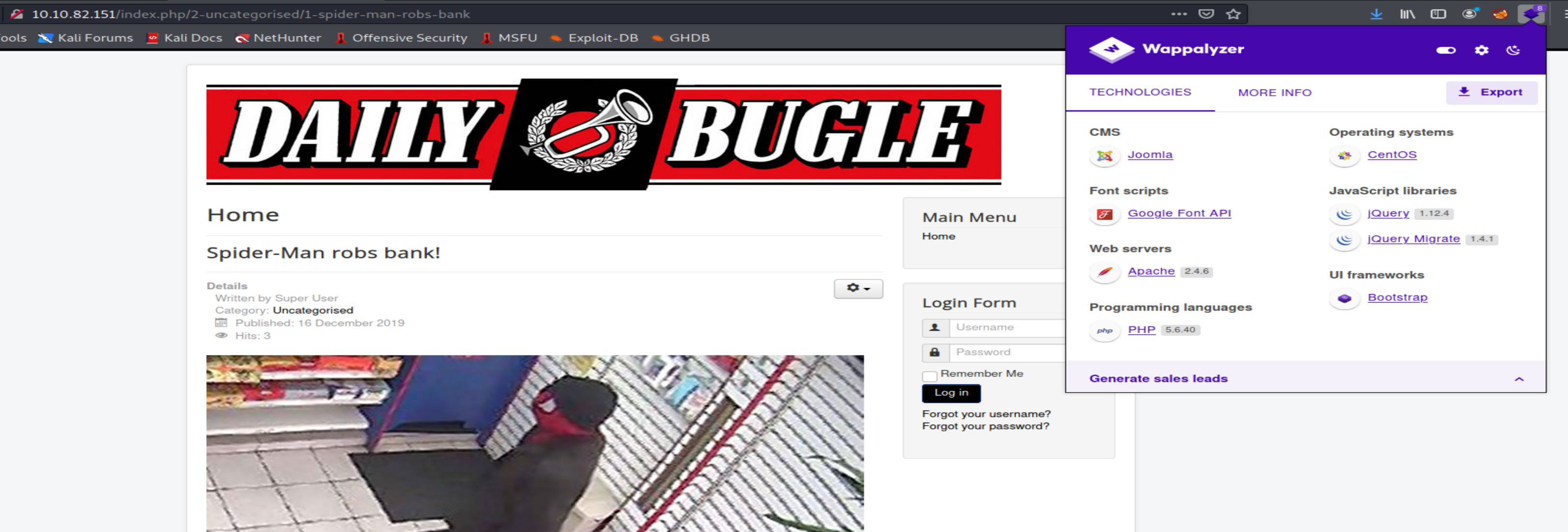


So we got three port open , SSH,HTTP,mysql. Also we got a hint that **spiderman** robs bank on the site.

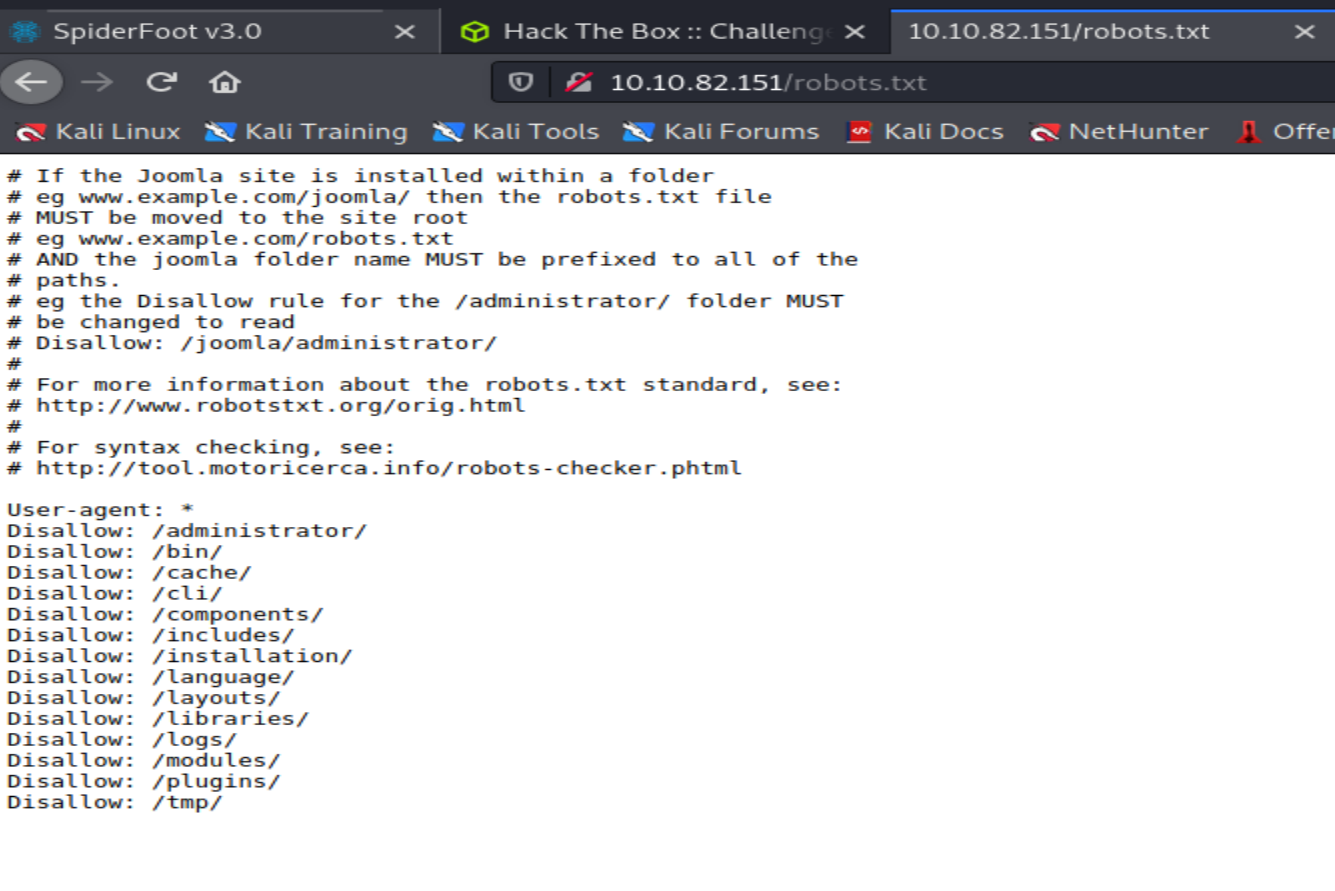
Let gobuster , running gave a lot of directories

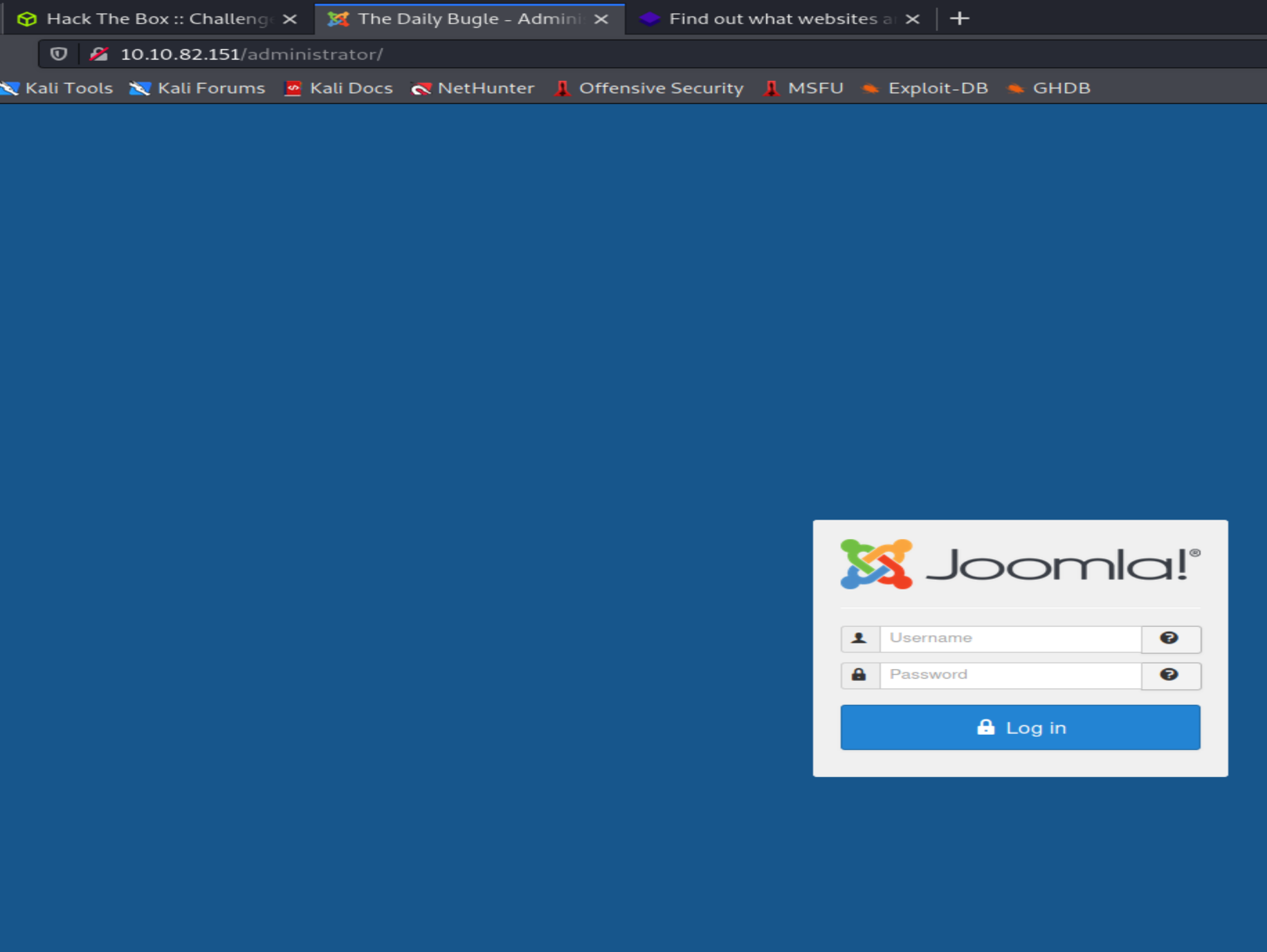


Using wappalyzer , show Joomla CMS on centoOS



Checking robots.txt



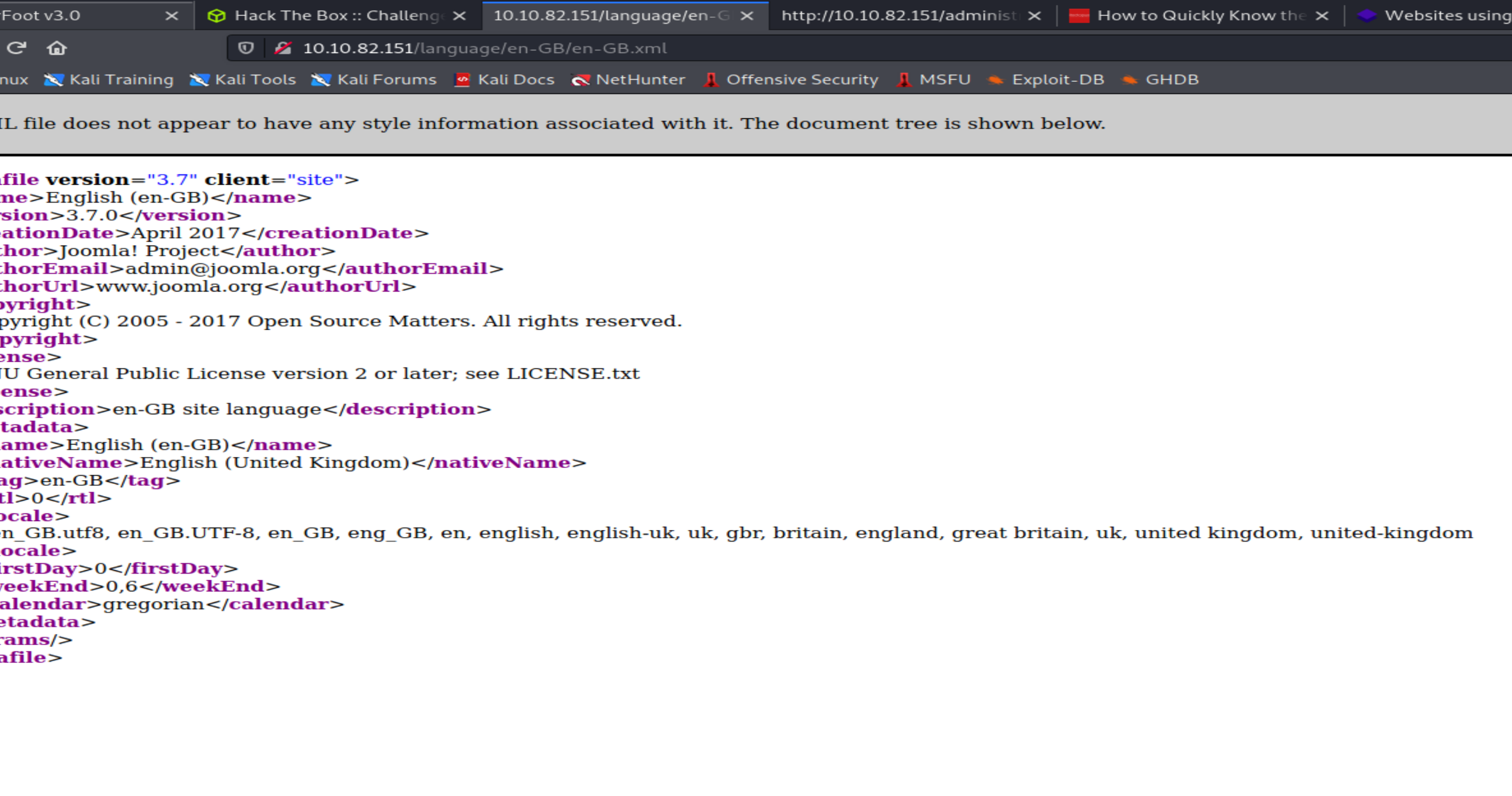


Task 2

***Answer the questions below***

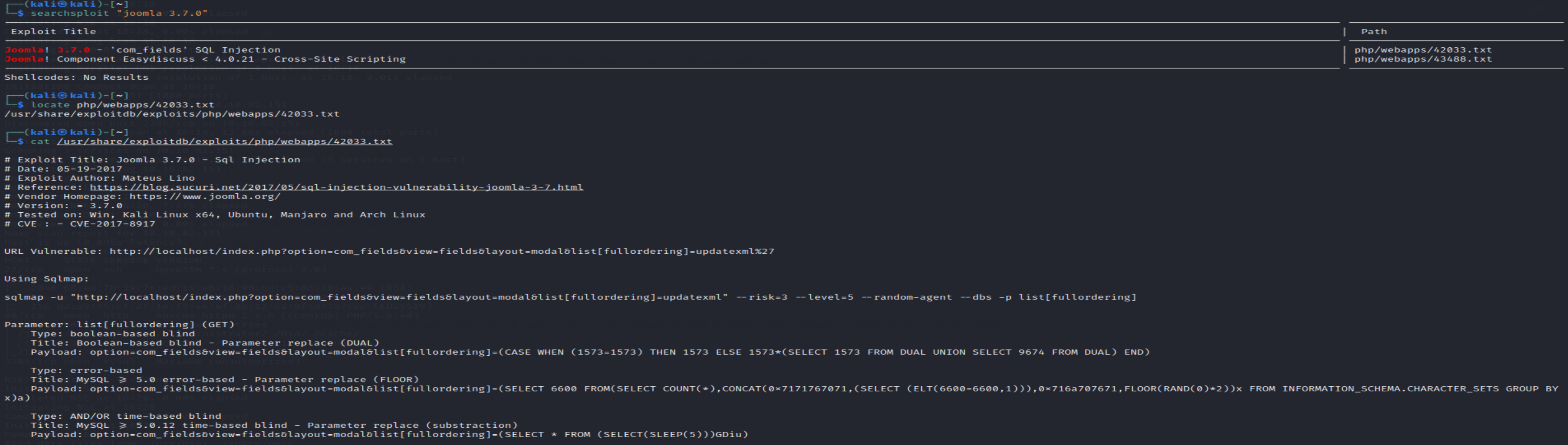
What is the Joomla version?

Incidently as we need to know joomla version before exploit it , so just traverse and look into possible directry path with xml information about version gave me:-

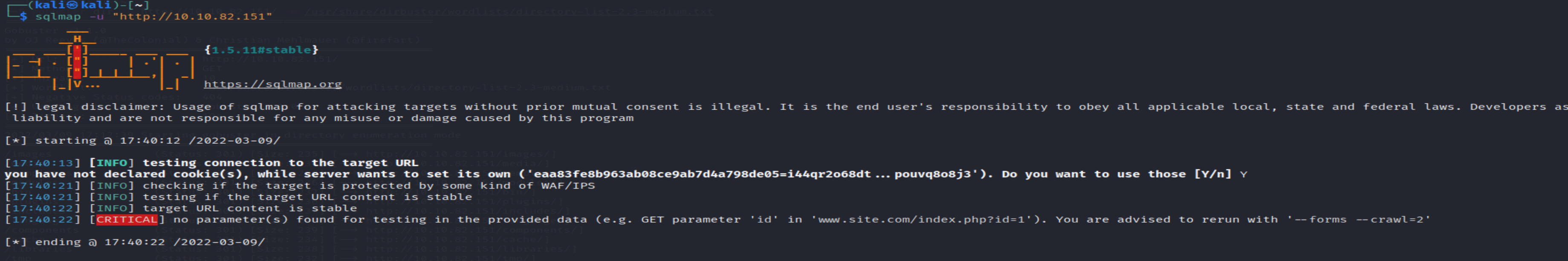


So the Joomla version is 3.7.0

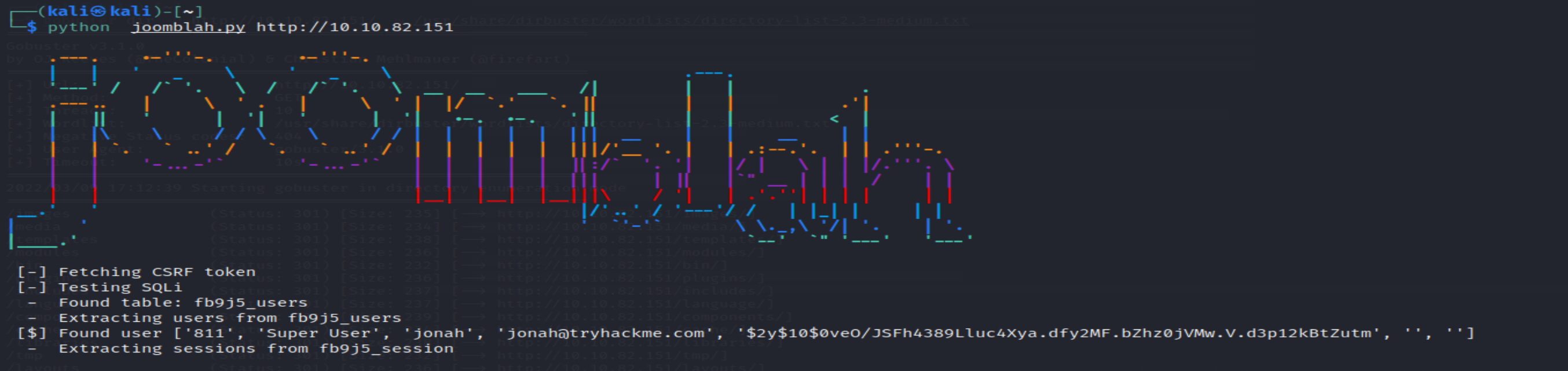
Further investigating we find relavent CVE-201708917 for our use.



We do also have option of SQLMap but joomblah.py option we can use as task 2 said . Also running SQLmap is not fruitful in this one



Running Joomblah is giving the Jonah hash passwd , as its has $2 so its bcrypt



Lets use JTR

\*Instead of using SQLMap, why not use a python script!\*

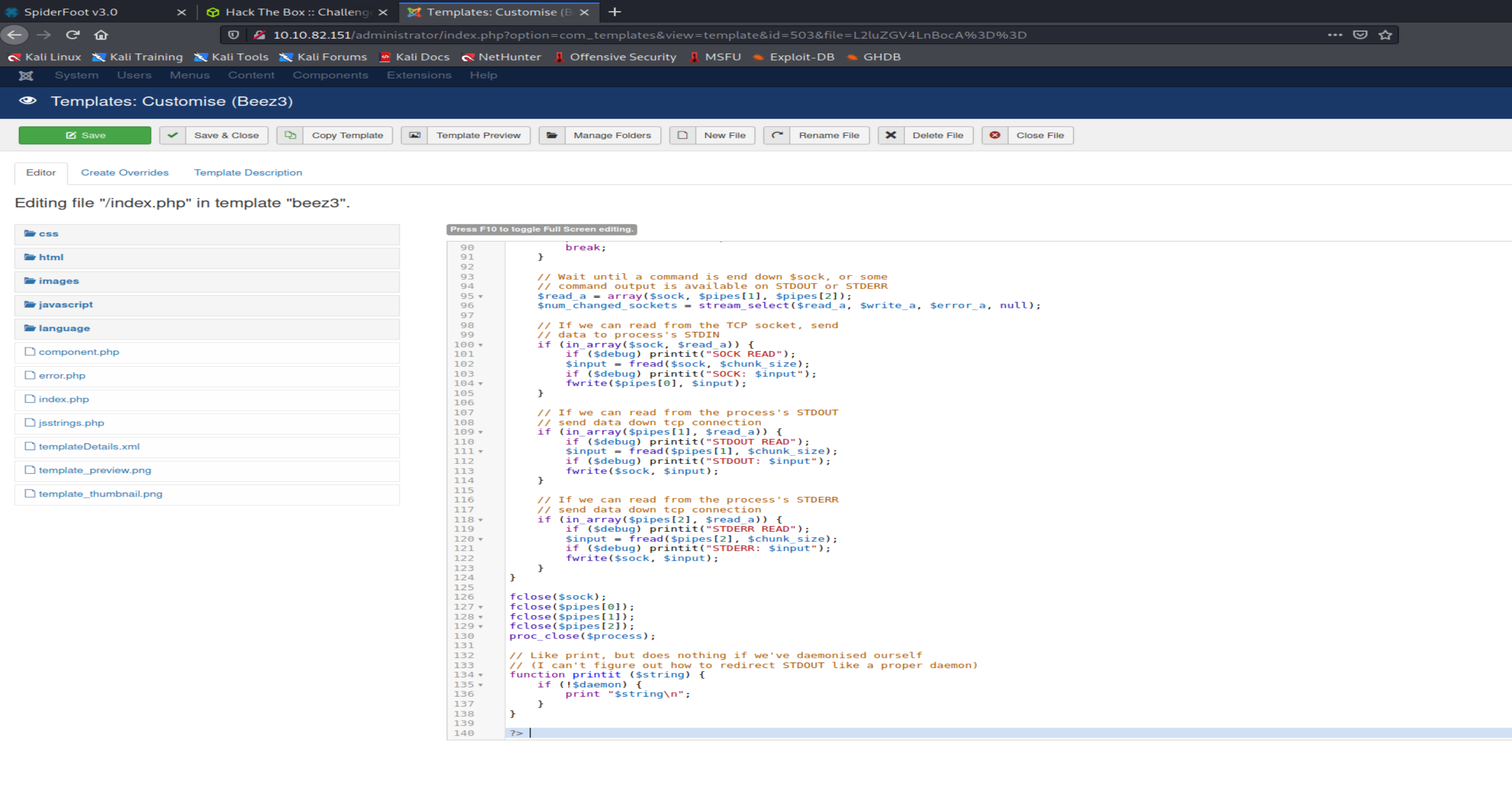
What is Jonah's cracked password?

john -format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt jonah.hash

spiderman123

What is the user flag?

Obtaining reverse shell use ip of virtual given on access of THM



The shell will give access to user jjameson but needed to sudo privileges for the user . So sudo –l and for passd cat /etc/crontab

Found nothing

So went on su jjameson with the same spiderman123 pwd nothing!!

Found configuration.php in var/www/html

And found credential of user in it

What is the root flag?

For root need to privilege escalation

Again Sudo –l

Shows (ALL ) NOPASSWD:/usr/bin/yum

Googling gives me idea of using yum with sudo i.e gtfobins . So need to generate own rpm install fpm

So added user to sudoer

Then ran fpm with payload , sudo python3 –m http.server 80

Wget rpm package , installing it then sudo su gives root flag

and root  Credits