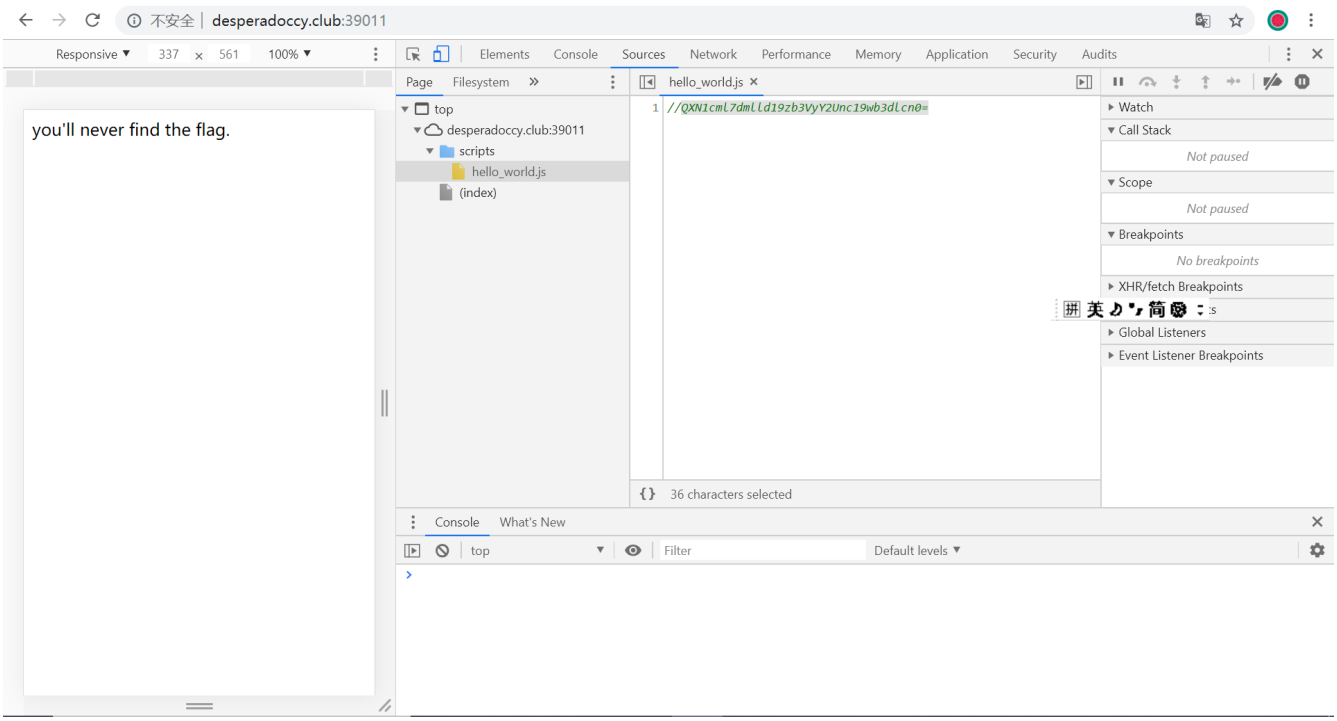
Writeup

1.签到题目：

解压成.jpg格式，用010 editor打开：

最后有一串用base64编码过后的字符串，用base64在线解码即可。

2.baby_web:



隐藏在scripts文件夹下的.js文件中，用base64解码即可。

3.web第二题：

应该是隐藏在网页的中，查看网页源代码：

没有注释，没有网页跳转和导航，也没有隐藏在网页的各种信息里面

想法是用burpsuit截包破解密码，但是不知道密码长度和范围，失败

另一个想法是用burpsuit截包伪造IP，但是也失败了..

4.pwn的第一题：

用IDA打开，并在虚拟机终端连接到网页

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // [sp+Ch] [bp-64h]@1
  char buf; // [sp+10h] [bp-60h]@4
  size_t nbytes; // [sp+6Ch] [bp-4h]@4

  setvbuf(stdin, 0LL, 2, 0LL);
  setvbuf(_bss_start, 0LL, 2, 0LL);
  setvbuf(stderr, 0LL, 2, 0LL);
  puts("I have a door.Could you open it?");
  puts("Please input your passworld size");
  __isoc99_scanf(4196649LL, (__int64)&v4);
  if ( v4 > 19 || v4 < 0 )
    exit(0);
  puts("Please input your password");
  LODWORD(nbytes) = v4 - 1;
  read(0, &buf, (unsigned int)(v4 - 1));
  return 0;
}
```

第一个输入的数肯定是0~19，第二个输入的密码是第一个输入的数减去一的unsigned int的形式，但是不知道具体怎么做...

5.web快速计算：

应该是写python的脚本，然后运行：

```
import re #正则模块
import requests

s = requests.Session()
url = '139.9.212.218:39009'
r = s.get(url)
r.encoding = 'utf-8'    #修改编码
print(r.text)
num = re.findall(re.compile(r'<br/>\s+.*?='), r.text)[0]  #正则表达式找到算术式

print ('result:\n\n%s=%d\n' % (num, eval(num)))  #输出算术式计算结果
r = s.post(url, data={'v': eval(num)})  #将结果提交  抓包可看出要用v提交
print (r.text)  #输出返回结果
```

findall函数返回的总是正则表达式在字符串中所有匹配结果的列表list

但是匹配算术表达式错了...