

# 2021-XUPT-CTF-WP

--By Biscuit

**前言：** 首先感谢这次比赛的举办者，在这此比赛中我算是入门了 CTF，了解了 CTF 这种比赛，在这次比赛中我学到了很多，在这份 WP 中，我将会把我会做且需要学习的题的解析写下来，如果有错误或者有改进的地方请各位学长多多指教。

**项目：** WEB

MISC

\*没有 CRYPTO, PWN 和 Reverse 是因为我的这几个个项做的题都无太多学习价值

**目录：** ezsy\_request,一起来玩呀，争分夺秒的黑客，扫黑行动，

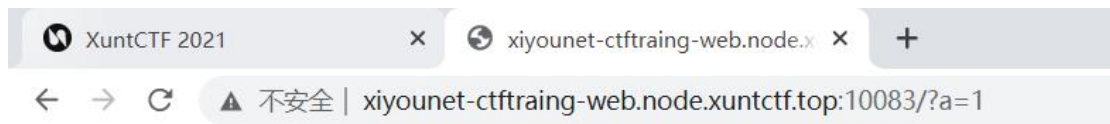
8 寻物启事，小姐姐快来学 HTTP

图片有四种格式，我的 flag 裂开了，这就是个 EXCEL，Megumin,Serize 的秘密，puzzle，Zip 加密，月光之下

# PART1:\*\*\*\*\*WEB\*\*\*\*\*

## 1.ezsy\_request

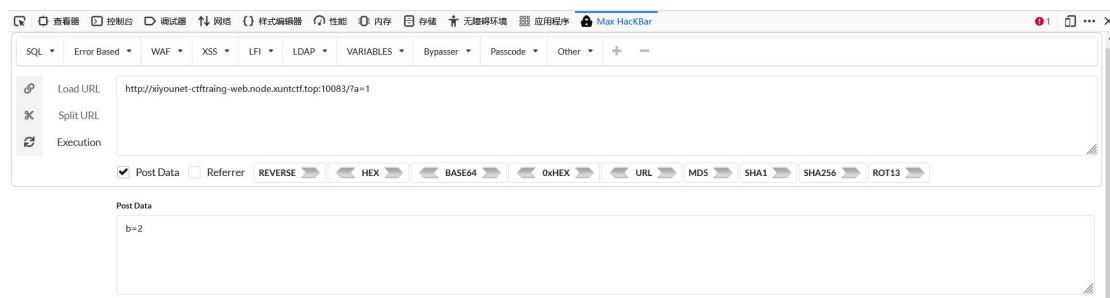
打开题目发现要用 get 方式提交一个名为 a, 值为 1 的变量, 在网址后面加上 a=1 即可, 这样我们就提交了名为 a, 值为 1 的变量。



**请用GET方式提交一个名为a,值为1的变量**

**请再以POST方式随便提交一个名为b,值为2的变量**

接着, 我们要请再以 POST 方式随便提交一个名为 b, 值为 2 的变量, 使用 HackBar 提交该值。选中 Post Data, 输入网址, 变量和参数, 提交。得到 Flag.



## 2.一起来玩呀

打开题目, 发现是一个游戏, 要分数达到十分高的时候才会出现 Flag, 于是怀疑可通过修改参数来通关。打开开发者面板, 发现游戏使用 js 写的, 在代码中找到分数的参数并修改即可。

```
req.open("GET", "f1Ag.php?score=" + score);
```

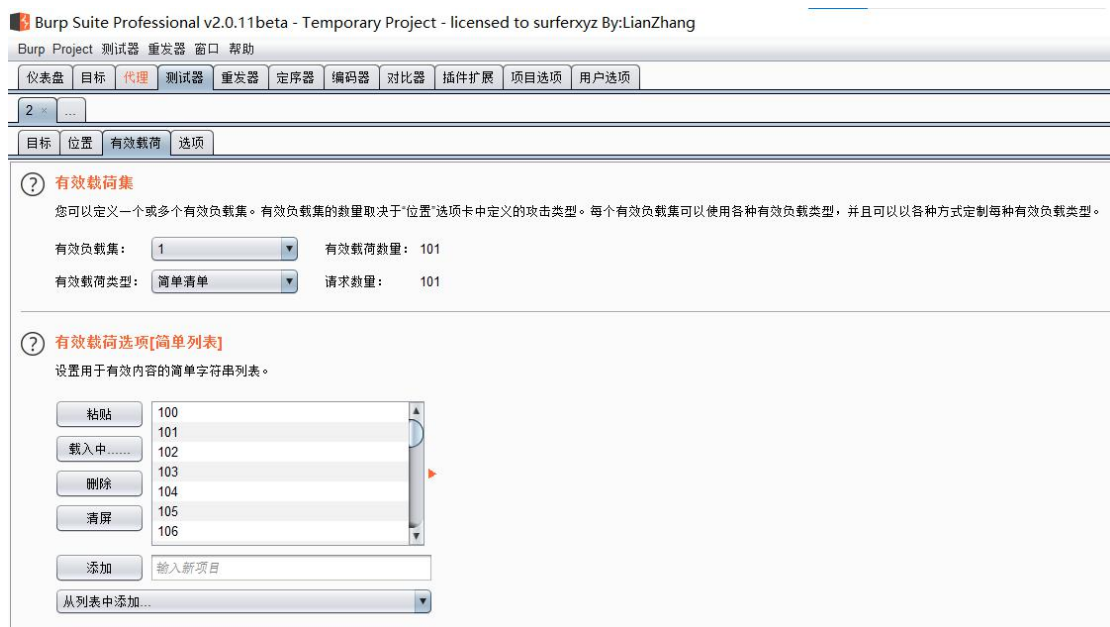
发现这句，意思是用 get 方式把 score 的值传给 f1Ag.php 文件，于是我们可以在网址后加上：`//f1Ag.php?score=999999999`

这样我们就得到了 Flag。

### 3. 争分夺秒的黑客

打开题目，打开开发者面板发现题目要求：密码是 100-200 中的某一个数，于是我们想到用 Burp 加字典的方式得到 Flag。

拦截请求后，导入字典：



跑完字典后发现异常字长，在响应中可发现 Flag。

Intruder attack 6

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器: 显示所有项目

请求	有效载荷	状态	错误	超时	长	评论
0		200	<input type="checkbox"/>	<input type="checkbox"/>	859	
1	100	200	<input type="checkbox"/>	<input type="checkbox"/>	831	
2	101	200	<input type="checkbox"/>	<input type="checkbox"/>	831	
3	102	200	<input type="checkbox"/>	<input type="checkbox"/>	831	
4	103	200	<input type="checkbox"/>	<input type="checkbox"/>	831	

请求 响应

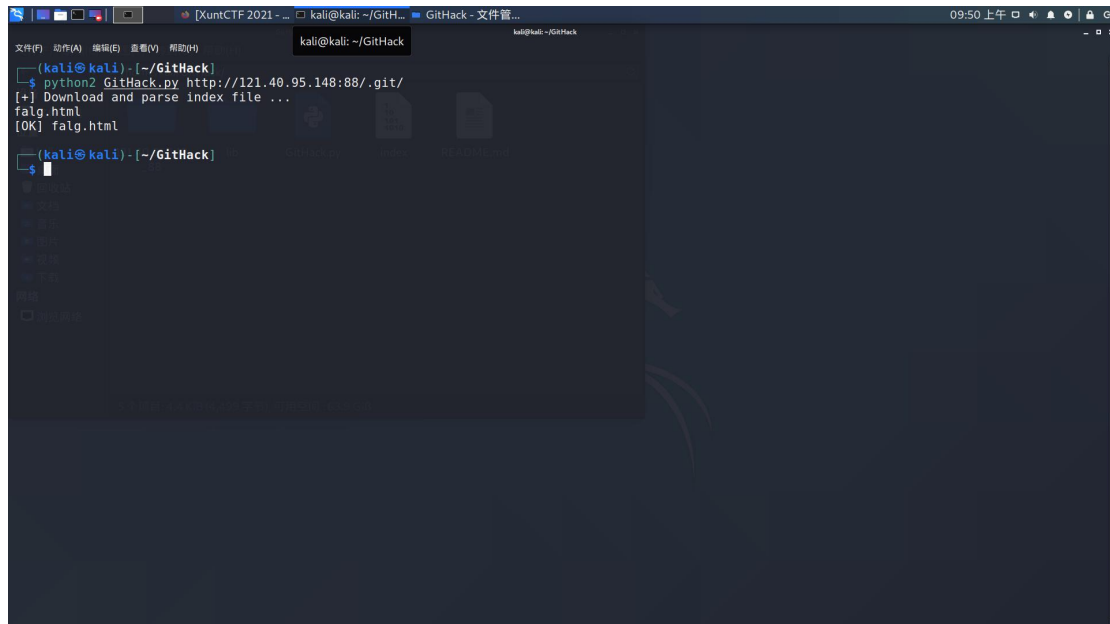
Raw 头 Hex HTML Render

HTTP/1.1 200 OK  
Server: nginx  
Date: Mon, 04 Oct 2021 01:33:10 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: close  
Content-Length: 708

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>黑客帝国</title>
</head>
<body style="background:url(http://image.nbd.com.cn/uploads/articles/images/730524/___500997682_banner.jpg); text-align: center; ">
  <h1 style="font-size: 500%; color: white;">欢迎来到黑客的世界 </h1>
  <h1 style="color: red; opacity: 0.3;">每一秒都很重要 </h1>
  <div><p><h3 style="color: black; opacity: 0.05;">密码是100-200中的某一个数 </h3></p></div>
  <form action="" method="post">
    <input type="number" name="key">
    <input type="submit" value="提交">
  </form>
  flag[978badf22af155cabcd8584e4210811d1]</body>
</html>
```

## 4. 扫黑行动

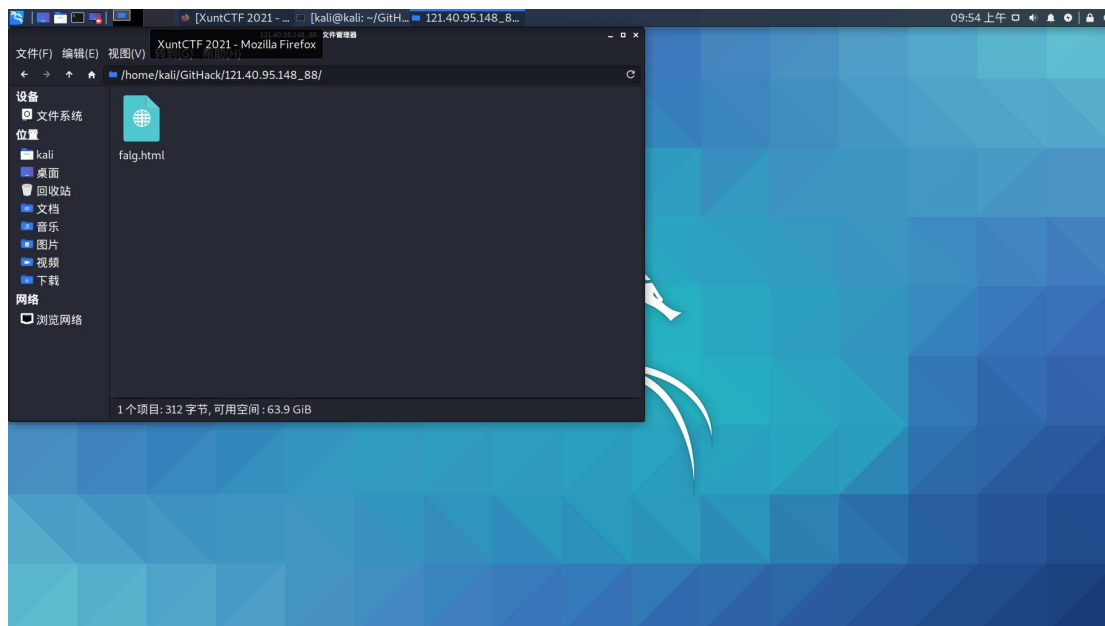
打开题目，在 HTML 中发现提示，提示 Flag 在 git 中，于是我们想到 git 泄露。在 Kali 中使用 Githack 来进行测试。



```
kali@kali: ~/GitHack
$ python2 Githack.py http://121.40.95.148:88/.git/
[+] Download and parse index file ...
flag.html
[OK] flag.html

kali@kali: ~/GitHack
$
```

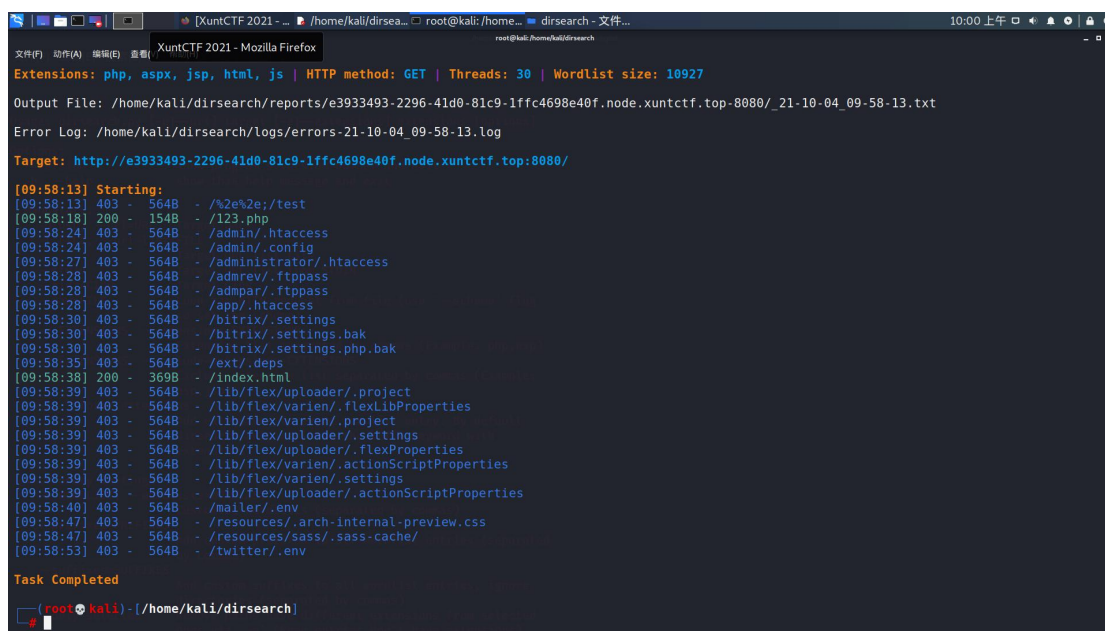
发现存在 Git 泄露。在下载的文件中发现 Flag。



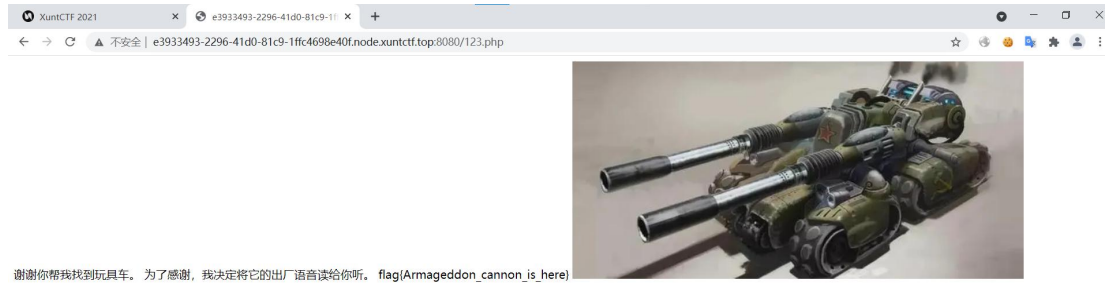
## 5. 寻物启事

在 HTML 中发现提示 Dirsearch。

于是我们在 Kali 中利用工具 Dirsearch 进行目录爆破。



进入相关文件找到 Flag。



## 6. 小姐姐快来学 HTTP

利用 Burp 抓包，发现项：Sex=1，结合网页把值改为 0：



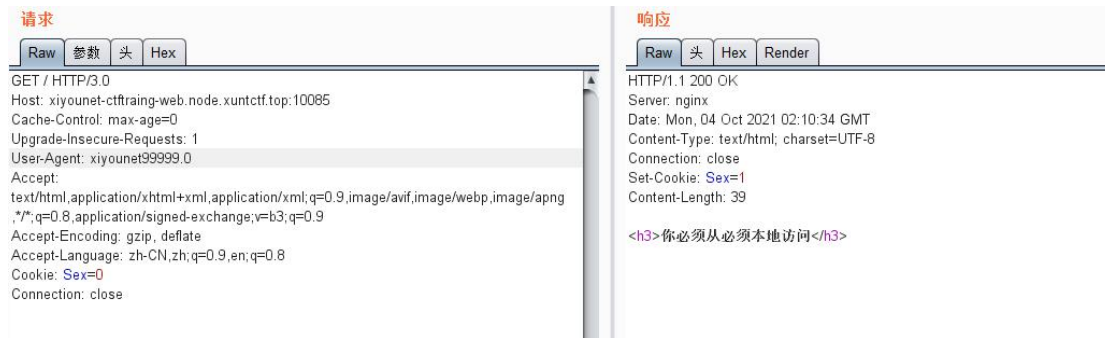
这时我们就知道这道题的考察内容了：有关 HTTP 头的知识。

根据要求更改就行了。

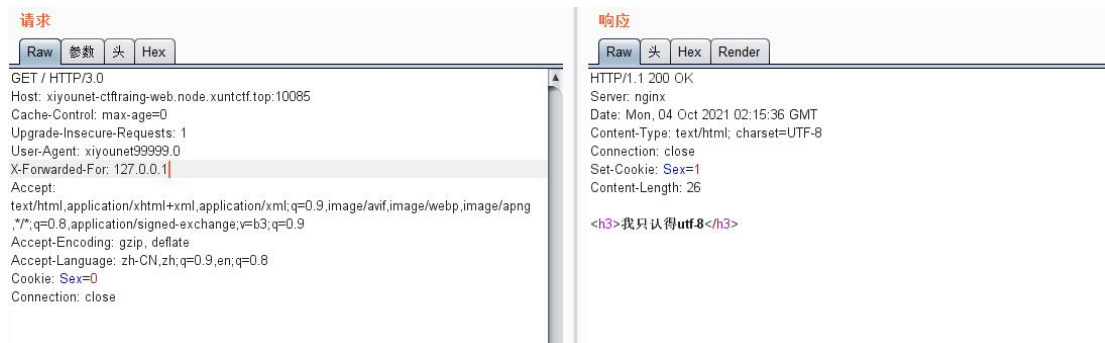
更改 HTTP 版本：



更改浏览器：



更改成本地访问：



更改编码：



在浏览器找到 md5 加密工具完成解密后得到 Flag。

## PART2:\*\*\*\*\*MISC\*\*\*\*\*

### 1.图片有四种格式

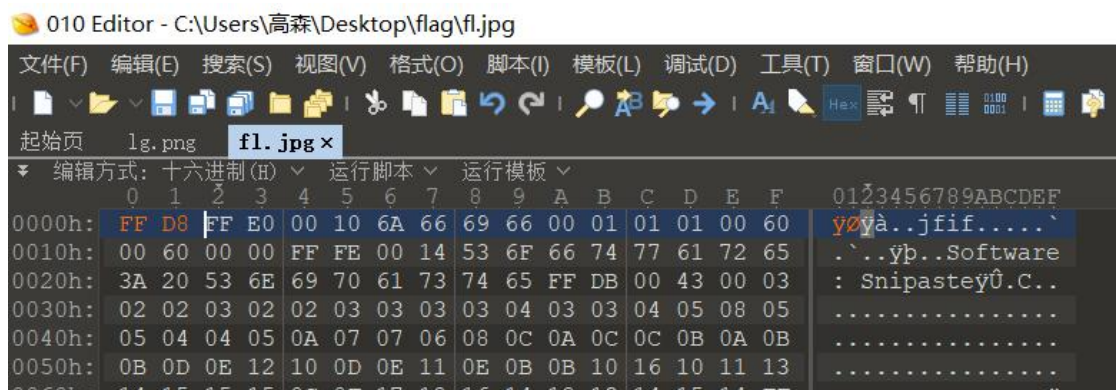
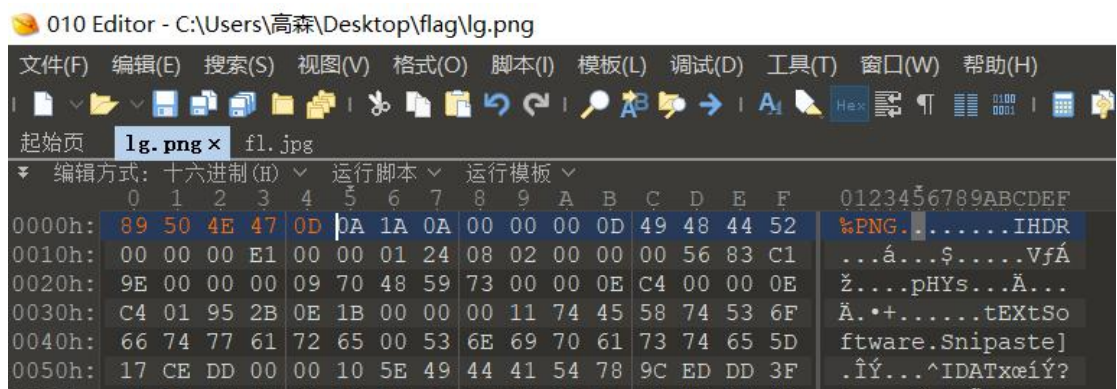
用 010Editor 打开寻找到 Flag。



1990h:	CD A4 38 18	B8 E9 87 00	62 44 F8 2C	87 65 AE 09	1a8.,e#.bDø,fe@.
19A0h:	50 DE 83 08	EC FC 44 3C	80 D0 00 EE	83 93 4B 46	Pbf.ïuD<eD.îf`KF
19B0h:	3B F0 3F A4	09 90 31 CC	17 52 C3 32	03 84 10 1B	;ð?¤..1î.RĂ2.,,..
19C0h:	05 B2 30 04	09 82 09 18	81 19 10 20	E6 49 CD 19	.²0...,... æIí.
19D0h:	A9 53 CB A9	F8 22 B0 9D	61 05 E1 C6	E5 E1 78 82	@SĖ@ø"°.a.áĖááx,
19E0h:	58 09 12 5B	26 78 F7 1B	8F 25 27 D9	89 03 BD 20	X..[&x÷...%`Û%.½
19F0h:	38 3B 10 0C	0B E1 E5 AD	88 BB 25 A2	49 24 9F 28	8;...áâ-^»%çI\$Ÿ(
1A00h:	CB 72 6D DF	D1 06 03 2C	70 F6 BC 90	5C D7 07 65	ĖrmßÑ...pö%.\x.e
1A10h:	86 02 06 01	D1 20 61 FA	A3 08 68 81	13 A3 64 88	t...Ñ aúf.h..fd^
1A20h:	05 EF 74 73	23 26 DD 11	76 03 77 9C	37 B8 C4 08	.its#&Ÿ.v.wœ7,Ă.
1A30h:	03 20 7E 7F	15 24 46 3D	2B 39 0E 2E	2E 24 93 87	. ~..\$F=+9...\$`#
1A40h:	79 F0 00 68	60 1D E7 1B	C4 41 32 77	93 96 11 95	yð.h`..ç.ĀA2w"-.*
1A50h:	70 F2 F2 43	F7 78 A6 50	7F FF D9 66	6C 61 67 7B	pòðC÷x!P.yŸflag{
1A60h:	41 5F 6C 49	4B 33 5F 4D	31 35 63 43	63 7D	A_1IK3_M15cCc}

## 2.我的 Flag 裂开了

根据题目可知图片文件头部有误，更改后：



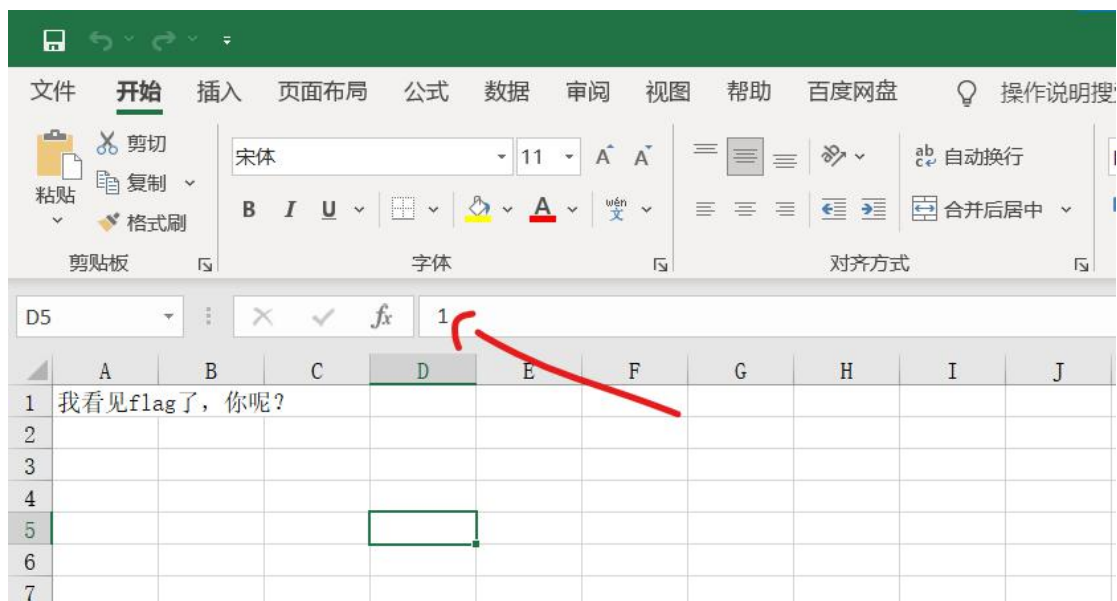
就可以在图片中发现 Flag。。





### 3. 这就是个 EXCEL

更改后缀发现是一个 EXCEL 文件，发现部分单元格有异常。



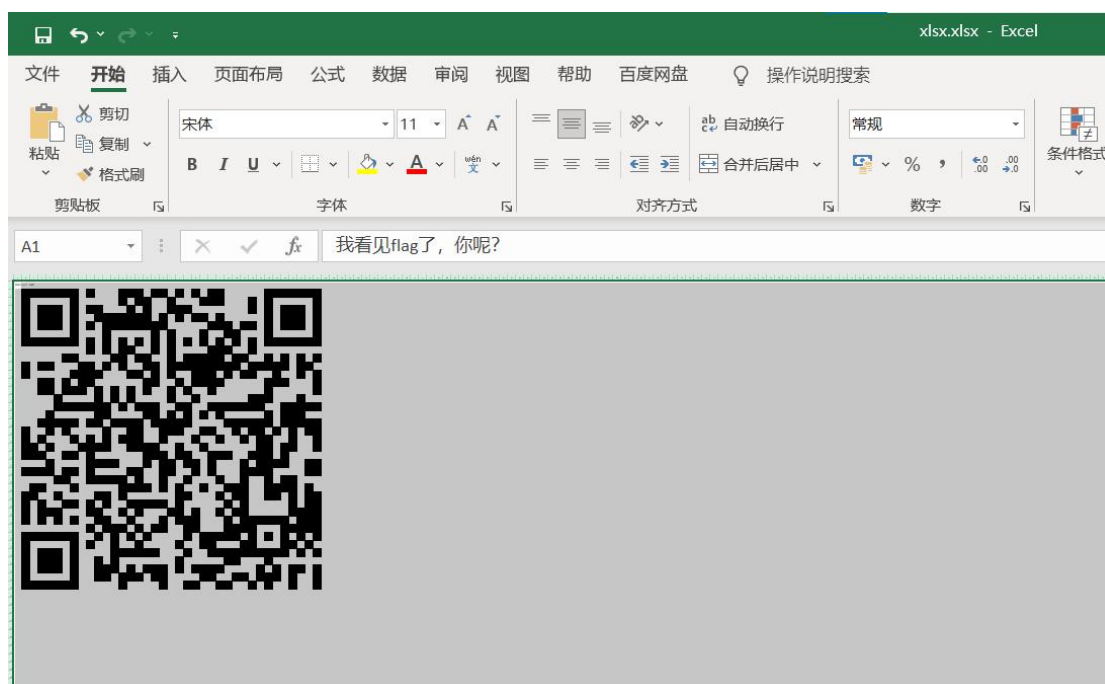
更改单元格格式为数字：

（在开始-数字选项里）

	A	B	C
1	我看见flag了，你呢？		
2		1.00	1.00

发现不规则的数字排布。

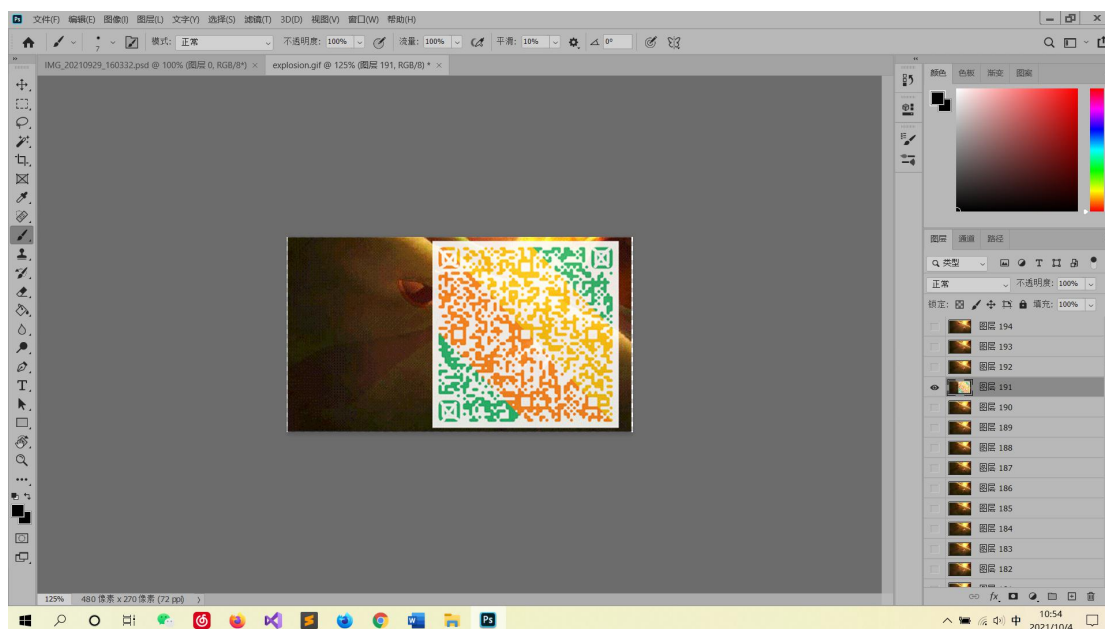
把含 1 的单元格填充黑色，调整大小：



把扫出来的结果用 BASE64 解码可得到 Flag。

#### 4. Megumin

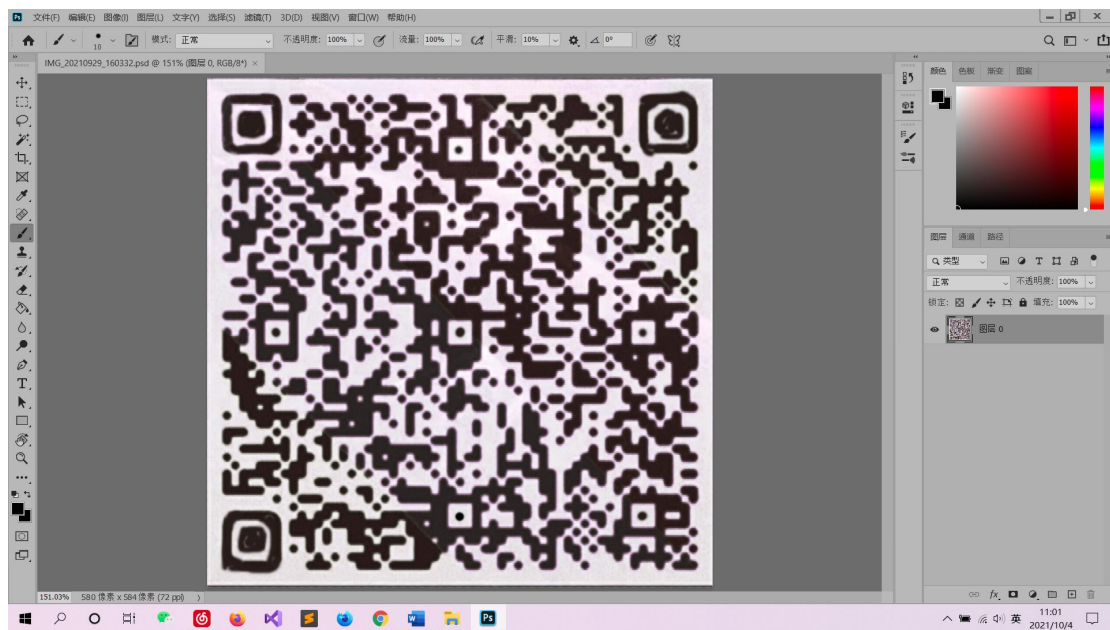
打开文件发现是一个 GIF 放到 PS 中发现关键的一帧：



对图片进行剪切。

发现是一个二维码，但是因为色彩混乱，定位图案被破坏，格式信息无法被读取而导致二维码不能被识别。

首先在 ps 中使用颜色替换指令把颜色校对，再用画笔工具把被打上叉的定位图案复原，再复原格式信息：



扫出来的数据再通过 Base64->Base32->Hex 解码就可以得到 Flag。

## 5. Serize 的秘密

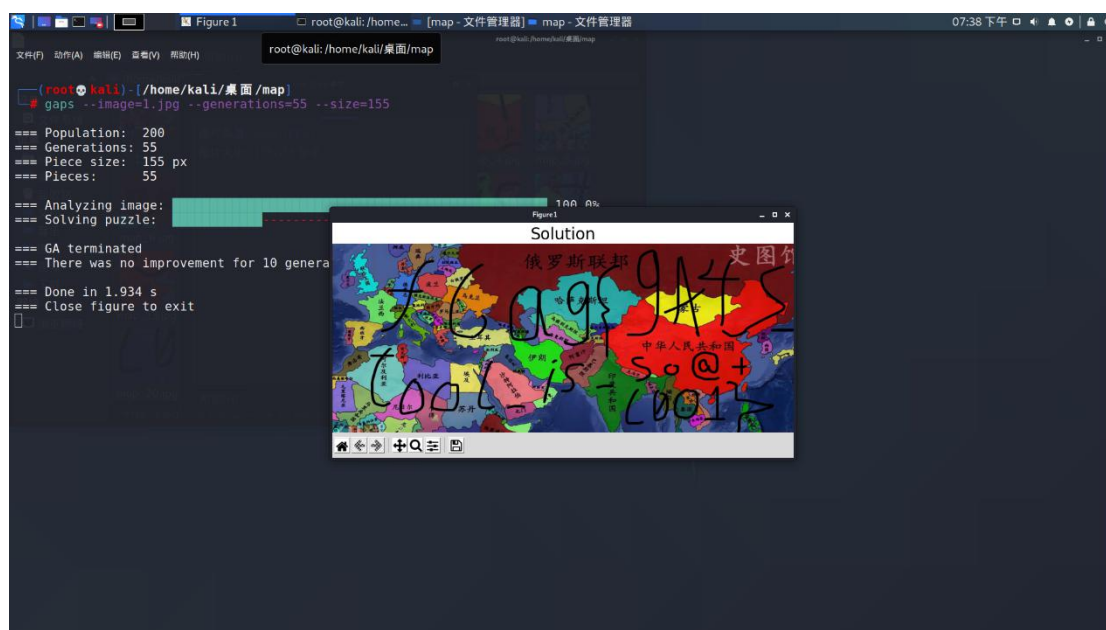
根据题目提示可知密码是 20000000 到 20021231 之间的一个数字，用 ARCHPR 暴力破解即可：



20021110 就是解压密码。

## 6. Puzzle

打开文件发现是一个拼图题，在 Kali 里用 gaps 工具进行快速拼图：

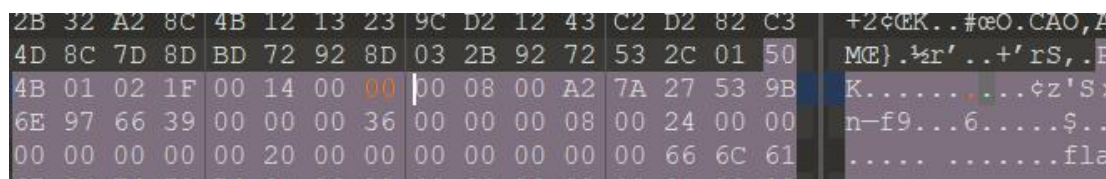


就可以得到 Flag。

\*附 Gaps 安装使用链接 <https://www.jianshu.com/p/d9e9019e8148>

## 7. Zip 加密

打开文件发现需要密码，可题目无任何密码提示，考虑伪加密，更改相应值后，发现果然是伪加密。



14 00 00 00

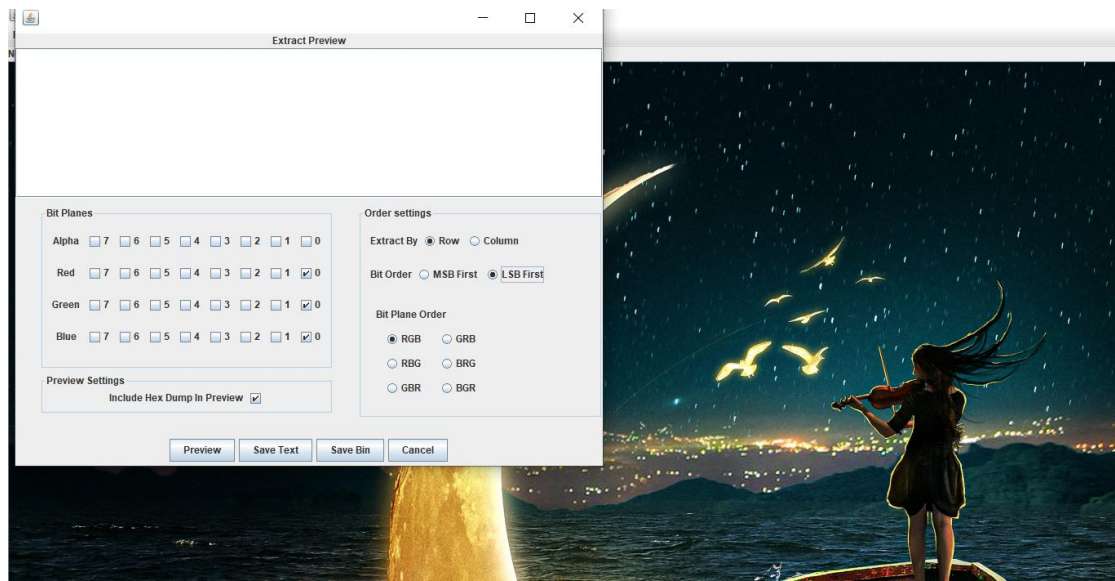
解压后找到 Flag。

## 8. 月光之下

下载文件发现是一个图片，无任何提示，放到 Stegsolve 中尝试：

尝试 LSB 隐写：





果然是：



得到新图片。

放在 010Editin:

利用查找命令成功找到 Flag。

题目来源: <https://www.xuntctf.top/>

联系 QQ: 2104925733

作者: Biscuit

网络空间安全专业 21 级 1 班 高森