

# 第四届“蓝帽杯”全国大学生网络安全 技能大赛 Writeup

原创

你们这样一点都不可耐  于 2020-08-08 20:54:06 发布  4020  收藏 8

分类专栏: [CTF](#) 文章标签: [python](#) [CTF](#) [网络安全](#) [安全](#) [经验分享](#)

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/vanarrow/article/details/107884660>

版权



[CTF 专栏收录该内容](#)

13 篇文章 10 订阅

订阅专栏

## 第四届“蓝帽杯”全国大学生网络安全 技能大赛 Writeup

### Misc

[签到](#)

[sudo](#)

[熟悉的解密](#)

### Web

[文件包含绕过](#)

[easiestSQLi](#)

[Soitgoes](#)

## Misc

### 签到

观色

010editor查看, 发现文件头是GIF89a, 是gif文件

Stegsolve 调色道, 出现前半flag

ps打开, 分离两个图层

Stegsolve分析, 得到后半flag, 即可得到完整flag

### sudo

喜欢玩数独吗, 一起来玩吧。

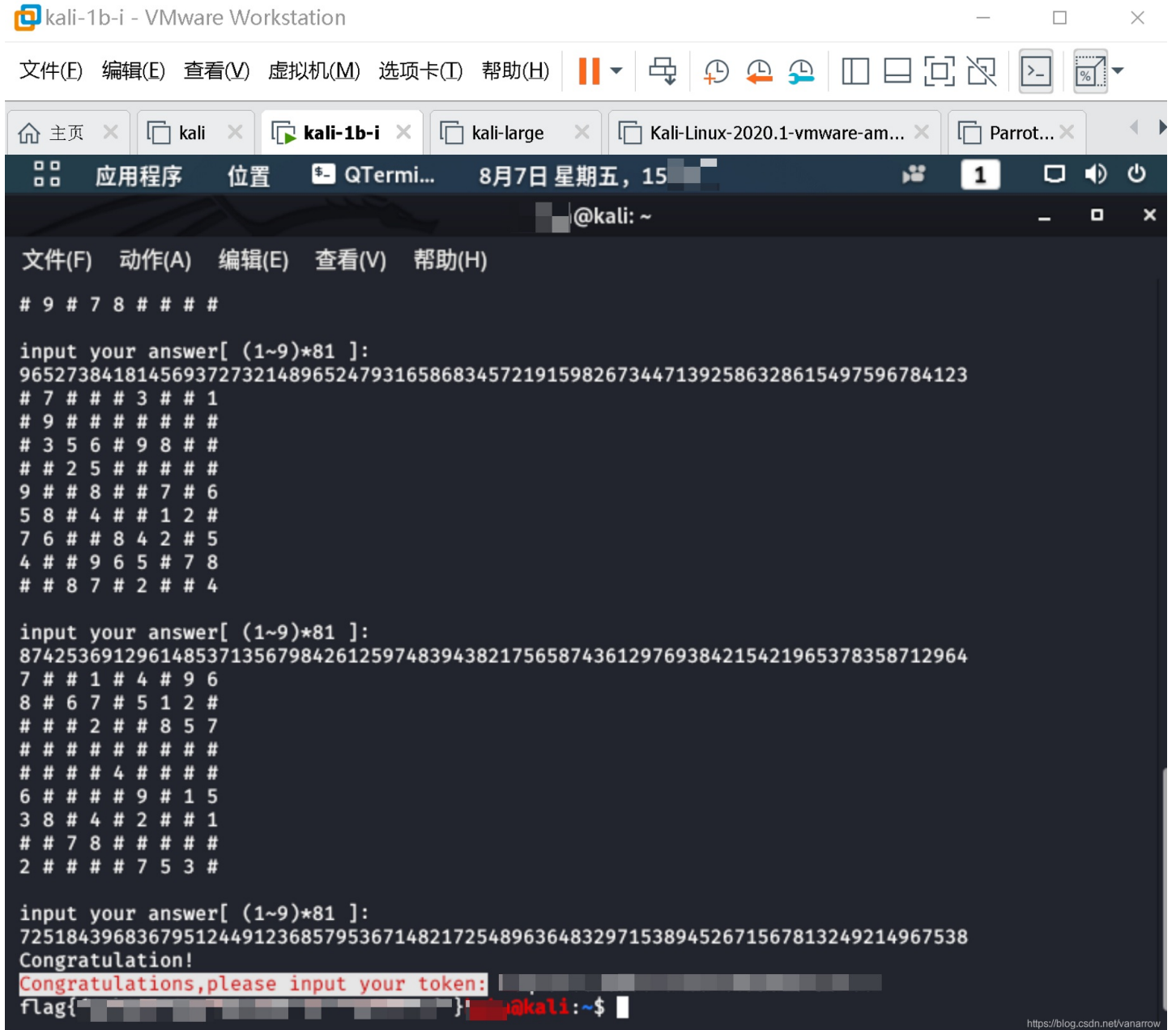
```
nc 47.93.204.245 12000
```

1-9数字玩9981数独

复制选区到Notepad++正则表达式

编写脚本计算，输入答案

整个过程务必快速输入，超过时间就断开连接



The screenshot shows a terminal window titled "kali-1b-i - VMware Workstation". The terminal displays a 9x9 number puzzle and its solution. The puzzle is as follows:

```
# 9 # 7 8 # # # #  
input your answer[ (1~9)*81 ]:  
965273841814569372732148965247931658683457219159826734471392586328615497596784123  
# 7 # # # 3 # # 1  
# 9 # # # # # # #  
# 3 5 6 # 9 8 # #  
# # 2 5 # # # # #  
9 # # 8 # # 7 # 6  
5 8 # 4 # # 1 2 #  
7 6 # # 8 4 2 # 5  
4 # # 9 6 5 # 7 8  
# # 8 7 # 2 # # 4
```

The solution is as follows:

```
input your answer[ (1~9)*81 ]:  
874253691296148537135679842612597483943821756587436129769384215421965378358712964  
7 # # 1 # 4 # 9 6  
8 # 6 7 # 5 1 2 #  
# # # 2 # # 8 5 7  
# # # # # # # #  
# # # # 4 # # # #  
6 # # # # 9 # 1 5  
3 8 # 4 # 2 # # 1  
# # 7 8 # # # # #  
2 # # # # 7 5 3 #
```

After the solution, the terminal displays "input your answer[ (1~9)\*81 ]:" followed by "725184396836795124491236857953671482172548963648329715389452671567813249214967538". Below this, it says "Congratulation!" and "Congratulations, please input your token:". The token is a long string of characters, and the terminal prompt "flag{" is followed by the token. The terminal prompt is "@kali: ~\$".

## 熟悉的解密

逐行base64解密得到py脚本

```
#!/usr/bin/env python
#-*- coding: utf-8 -*-
import sys
from ctypes import *
def encipher(v, k):
    y = c_uint32(v[0])
    z = c_uint32(v[1])
    sum = c_uint32(0)
    delta = 0x9e3779b9
    n = 32
    w = [0,0]
    while(n>0):
        sum.value += delta
        y.value += ( z.value << 4 ) + k[0] ^ z.value + sum.value ^ ( z.value >> 5 ) + k[1]
        z.value += ( y.value << 4 ) + k[2] ^ y.value + sum.value ^ ( y.value >> 5 ) + k[3]
        n -= 1
    w[0] = y.value
    w[1] = z.value
    return w
def encodestr(text, key):
    cipherList = []
    text += (8 - len(text) % 8) * chr(0)
    for i in range(len(text)/8):
        v1 = 0
        v2 = 0
        for j in range(4):
            v1+= ord(text[i*8+j]) << (4-j-1)*8
            v2+= ord(text[i*8+j+4]) << (4-j-1)*8
        cipherList.append(encipher([v1,v2],key))
    return cipherList
if __name__ == "__main__":
    key = [11,22,33,44]
    flag = ?
    cipher = encodestr(flag1,key)
    #cipher = [[4018289233L, 2950320151L], [1771827478L, 493980876L], [1863284879L, 1137797599L], [2759701525L,
3957885055L], [2600866805L, 78850724L]]
```

Tea算法解出前一半flag

base64隐写解出后一半flag

## Web

### 文件包含绕过

```
<?php
highlight_file(__FILE__);
include("../check.php");
if(isset($_GET['filename'])){
    $filename = $_GET['filename'];
    include($filename);
}
?>
```

curl 命令+bzip2.compress协议绕过

## easiestSQLi

他们说这年头黑客很多，所以我的SQL就过滤了一大堆的东西！这下谁也 别想拿到我的flag了哈哈哈哈哈

给flag 表，列

布尔盲注，用pyhon脚本

## Soitgoes

find the flag.

使用php伪协议读取源码

?file=php://filter/read=convert.base64-encode/resource=try.php

反序列化

小范围爆破

```
<?php
class Seri{
    public $alize;
    public function __construct($alize) {
        $this->alize = $alize;
    }
    public function __destruct(){
        $this->alize->getFlag();
    }
}

class Flag{
    public $f;
    public $t1;
    public $t2;

    function __construct($file){
        echo "Another construction!!";
        $this->f = $file;
        $this->t1 = $this->t2 = md5(rand(1,10000));
    }

    public function getFlag(){
        $this->t2 = md5(rand(1,10000));
        echo $this->t1;
        echo $this->t2;
        if($this->t1 === $this->t2)
        {
            if(isset($this->f)){
                echo @highlight_file($this->f,true);
            }
        }
    }
}
?>
```

```
<?php
error_reporting(0);
$file = $_GET["file"];
$p = $_GET["p"];
if (isset($file)) {
    echo 'NONONO' . '<br>';

    if (preg_match("/flag/", $file)) {
        die('HACKER GOGOGO!!!');
    }
    @include($file);

    if (isset($p)) {
        $p = unserialize($p);
    } else {
        echo "NONONO";
    }
}
?>
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)