

XCTF(攻防世界)

原创

Assass1n- 于 2021-12-02 21:05:24 发布 196 收藏

分类专栏: [ctf](#) 文章标签: [p2p](#) [debian](#) [webview](#)

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/qq_63685461/article/details/121684356

版权



[ctf专栏收录该内容](#)

5 篇文章 0 订阅

[订阅专栏](#)

目录

[1.this_is_flag](#)

[2.pdf](#)

[3.如来十三掌](#)

[4.give you flag](#)

[5.stegano](#)

[6.坚持60s](#)

1.this_is_flag

属于是介绍flag长啥样子了

译

难度系数:  ★★ 2.0

题目来源: 暂无

题目描述: Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

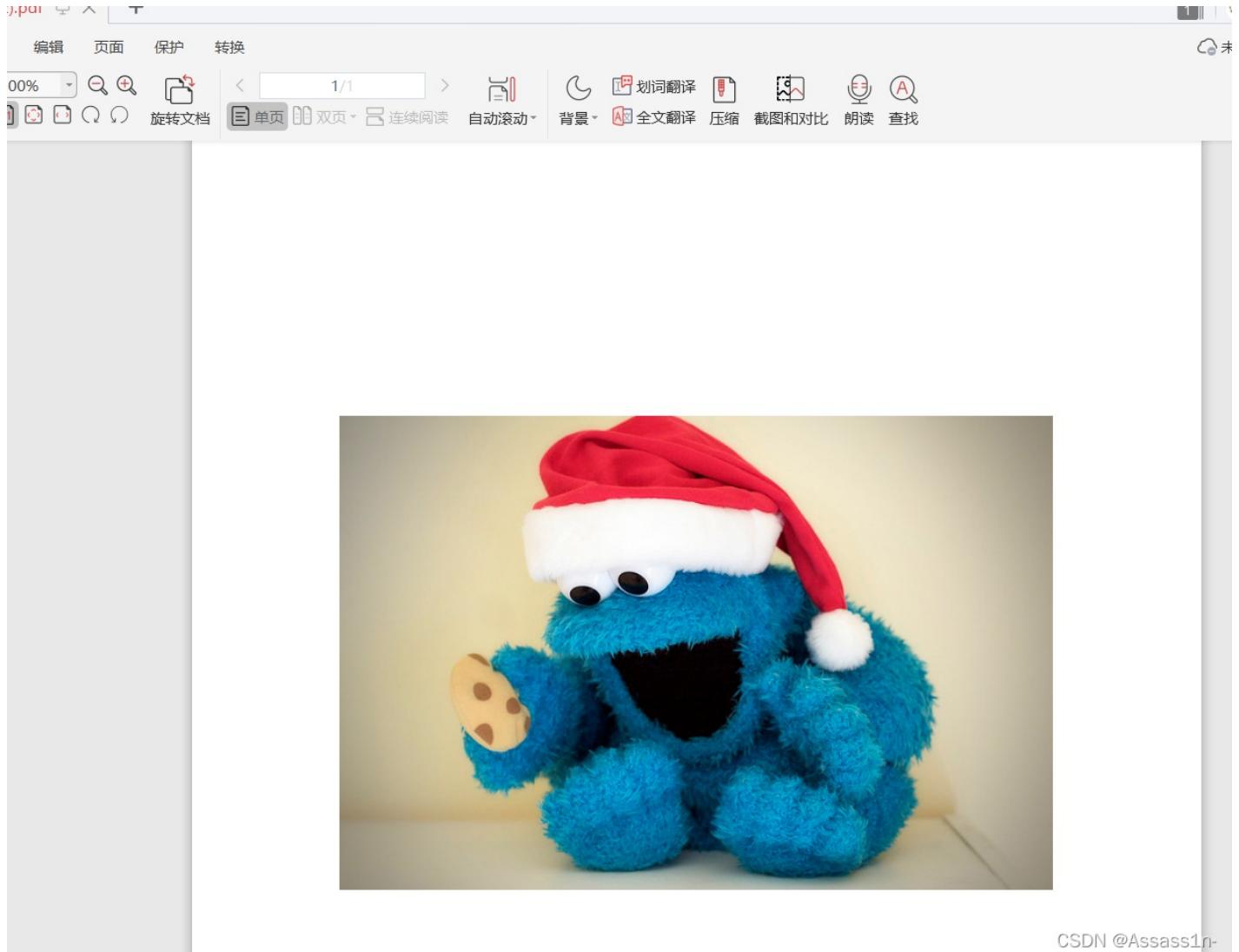
题目场景: 暂无

题目附件: 暂无

CSDN @Assass1n-

[2.pdf](#)

下载附件



CSDN @Assass1n-

啥也没有 pdf格式的尝试转为word

↑
↑
↑
↑
↑
↑
↑
↑
↑
↑
↑
↑



CSDN @Assass1n-

3.如来十三掌

下载附件一个word文档

受保护的视图 请注意 - 来自 Internet 的文件可能包含病毒。除非您需要编辑，否则保持在受保护视图中比较安全。 启用编辑(E) X

夜哆悉諸多苦奢陀奢諦冥神哆盧穆幡三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆多鉢以南哆心日姪罰蒙呐神。舍切真怯勝呐得俱沙罰婆是怯遠得呐數罰輸哆遠薩得槃漫夢盧幡亦醯呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

文档结尾 CSDN @Assass1n-

看这格式一个佛曰加密得到MzkuM3gvMU Aw zuvn3cg oz MIM T uvq zAenJch MU Aeqz Wenz Em LJW9

试了base没用，想不到了就查了一下这个是rot-13加密

字符串

MzkuM3gvMU Aw zuvn3cg oz MIM T uvq zAenJch MU Aeqz Wenz Em LJW9

计算

解码结果

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

复制

译

CSDN @Assass1n-

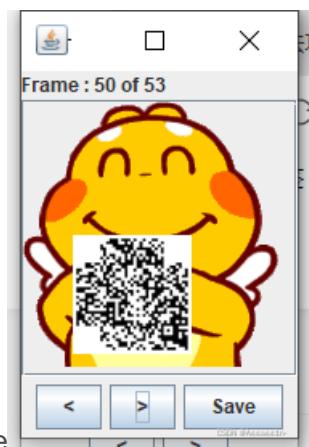
得到一串base加密字符串解密得到flag flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

4.give you flag



CSDN @Assass1n-

这里我说一下这其实是个gif表情包看完发现有一段会亮出一个二维码



果断掏出工具stegsolve





得到flag

5.stegano

一个pdf文件在网页打开

```
*index.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
NoFlagHere! NoFlagHere! NoFlagHere! XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXX
BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA BBBBB BA AAAB BBBB AAAAA BBBB BAAA A
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet magna
volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam
orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget
ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor
massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh
egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputate. Aenean quis tempor
orci. Cras placerat lectus nulla, eu bibendum metus interdum in. Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Cras faucibus odio ut metus vulputate, id laoreet magna vulputate. Integer nec enim vel arcu porttitor egestas.
Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum ut mi.
Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curabitur
scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo aliquam.
Nulla feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim lacus,
sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilisi.
Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metus
interdum in. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vulputate, id laoreet
magna vulputate. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc
diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictum sit amet at orci.
Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipiscing dui. Duis eget

```

第2行, 第169列 100% Windows (CRLF) CSDN @Assass1n

可以看到一串AB BA的字符 百度只有ab的密码查到培根密码，但是这种密码的格式都是5个5个字符一起的，这种格式让我想到摩斯密码先试着把A换成.把B换成-空格换成/

-.-/---/-. /--./-. /-. /-/- /.. /---/- /... /---/-. /-. /---/-. /.... /---/-. /.../-. /---/-. /.../-. /.... /---/-. /...

./.... 得到摩斯密码然后解密，得到flag



6.坚持60s

一个java环境的游戏你可以试着玩出来，当然只是试试反正我是不行

The screenshot shows the JD-GUI interface with the following code displayed:

```
package cn.bjsxt.plane;
import java.awt.Image;
import java.awt.Rectangle;
public class GameObject {
    int height;
    Image img;
    int speed = 10;
    int width;
    double x;
    double y;
    public Rectangle getRect() {
        return new Rectangle((int) this.x, (int) this.y, this.width, this.height);
    }
    public GameObject(Image img2, double x2, double y2, int speed2, int width2, int height2) {
        this.img = img2;
        this.x = x2;
        this.y = y2;
        this.speed = speed2;
        this.width = width2;
        this.height = height2;
    }
    public GameObject() {
    }
}
```

The code defines a `GameObject` class with fields for height, image, speed, width, and coordinates (x, y). It includes methods for getting a rectangle representation and a constructor that initializes these fields.

一个软件jdax Java反汇编

```
    ...
    case 5:
        printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
        return;
    case 6:
        printInfo(g, "flag{RGFqaURhbG1fSmlud2FuQ2hpamk}", 50, 150, 300);
        return;
    default:
        return;
    }
}
```

CSDN @Assass1n-

找到flag 里面是个base加密

The screenshot shows a web-based tool for decoding strings. At the top, there is an advertisement for a 100G SSD worth 1680 yuan. Below the ad, the input field contains the string `RGFqaURhbG1fSmlud2FuQ2hpamk=`. The output field shows the decoded text: `DajiDali JinwanChi ji`. Below the output field are buttons for clearing, encoding, decoding, and a checkbox for UTF-8 decoding. A blue button labeled "译" (translate) is also present. At the bottom, it says "Base编码系列: Base64 Base32 Base16".

最后的flag