BUUCTF Web pingpingping

原创

维多利亚蜜汁鱼 于 2021-07-03 14:03:39 发布 151 收藏 3

分类专栏： Web CTF

本文链接：https://blog.csdn.net/CrotZZ/article/details/118439287

Web 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏

CTF

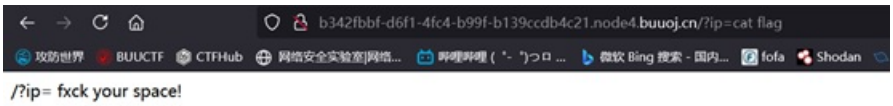
18 篇文章 0 订阅

订阅专栏

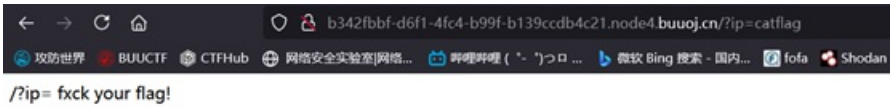
打开后

/?ip=

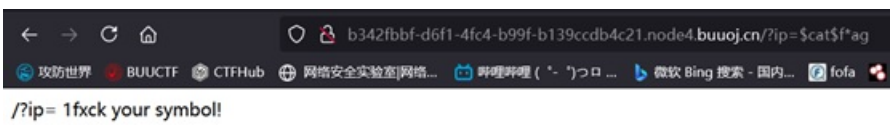
没什么提示



试了下cat flag，空格好像是被过滤了

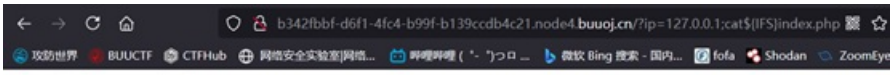


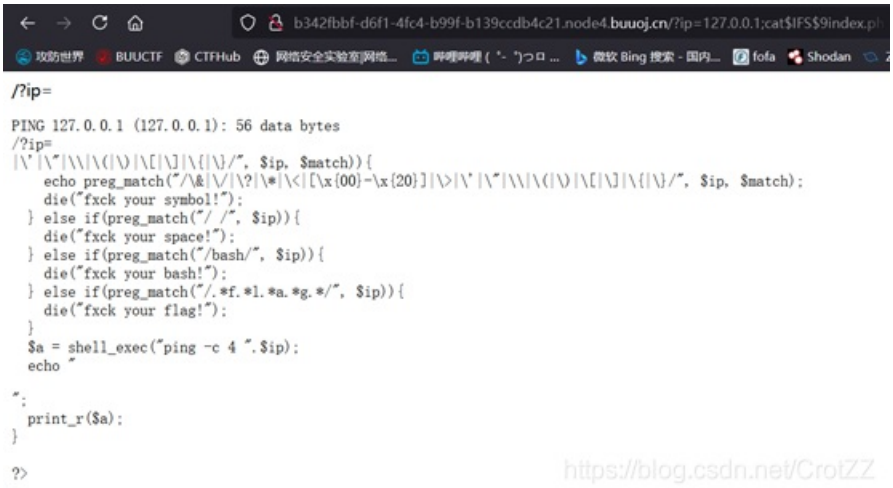
去空格，flag也被过滤



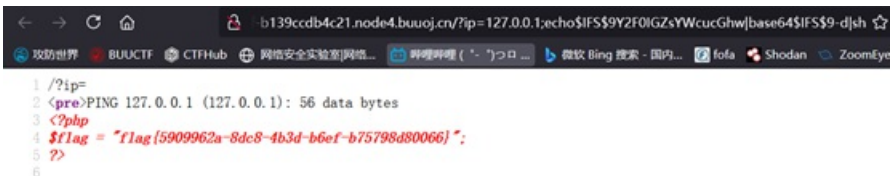
根据题目是ping 所以得先ip=127.0.0.1返回结果是上面这样的

ls看有什么文件，flag是已经被过滤的，需要想其他办法得到里面内容



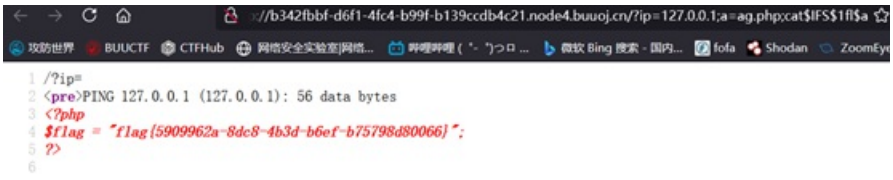


试了下一些绕过空格的方法，得到index.php里面的内容，虽然有些看不懂但大致意思还是明白，空格、bash、命令里是否有flag都被过滤



这里是用了echoIFS9Y2F0IGZsYWcucGhw|base64IFS9-d|sh，用base64编码绕过，空格用ifs代替，起先一直没出结果后来才发现用的是flag的base64编码，这里要flag.php

```
echo$IFS$9Y2F0IGZsYWcucGhw|base64$IFS$9-d|sh
```



**a=ag.php;catIFS9fla**这样类型的拼接构造也能绕过得到结果，如果是a=fla b=g.php 然后catIFS9a$b好像是不行的。

```
a=ag.php;cat$IFS$9fl$a
```