




[ACTF2020 新生赛]Exec1

原创

黑仔丶  于 2020-09-15 22:11:36 发布  615  收藏 1

分类专栏: [CTF--纸上谈兵](#) 文章标签: [linux](#)

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/qq_42404383/article/details/108610981

版权



[CTF--纸上谈兵](#) 专栏收录该内容

16 篇文章 1 订阅

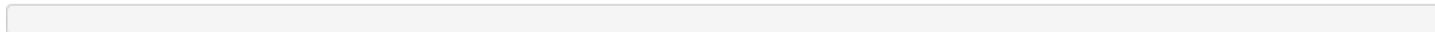
订阅专栏

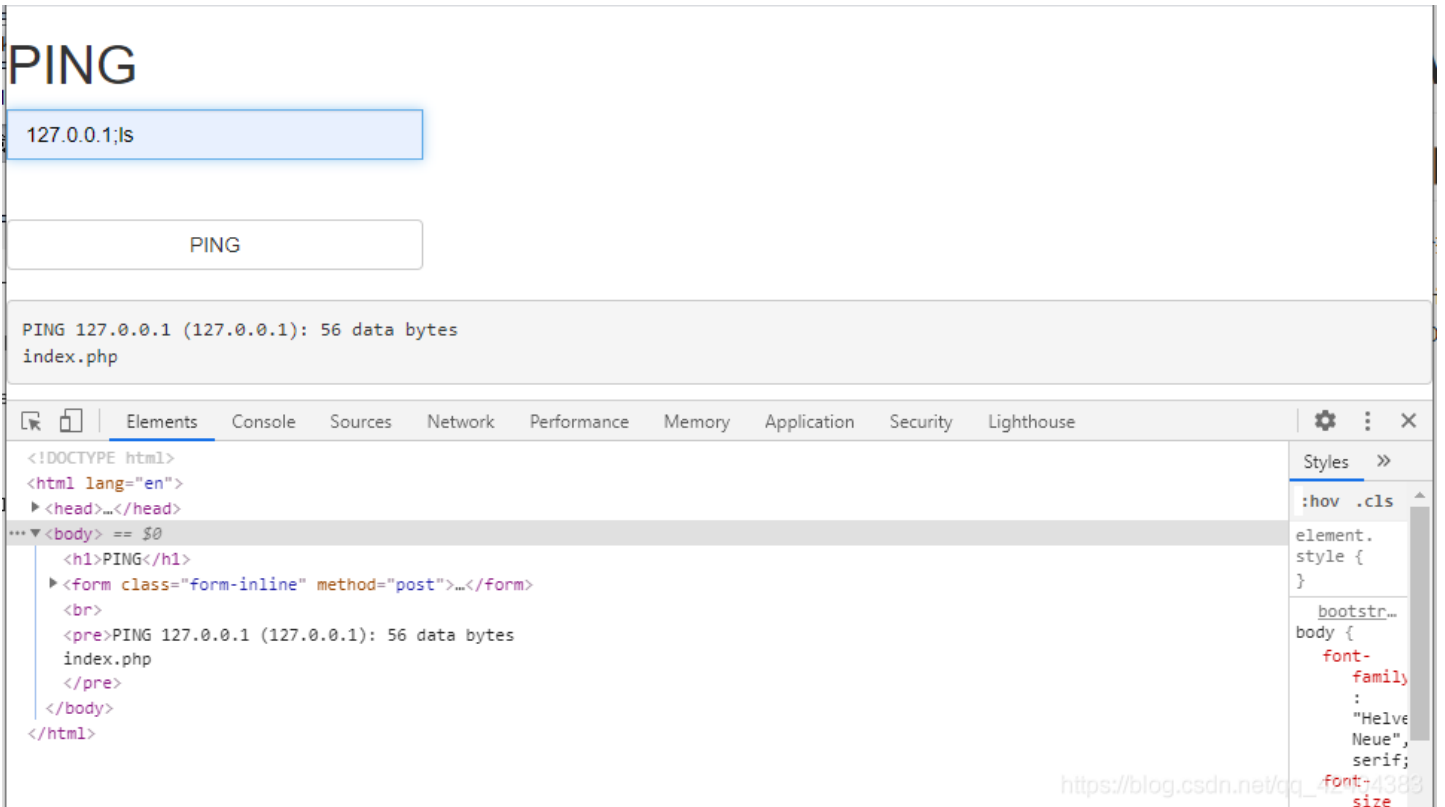
[ACTF2020 新生赛]Exec

题目:

考察命令执行+绕过?

PING

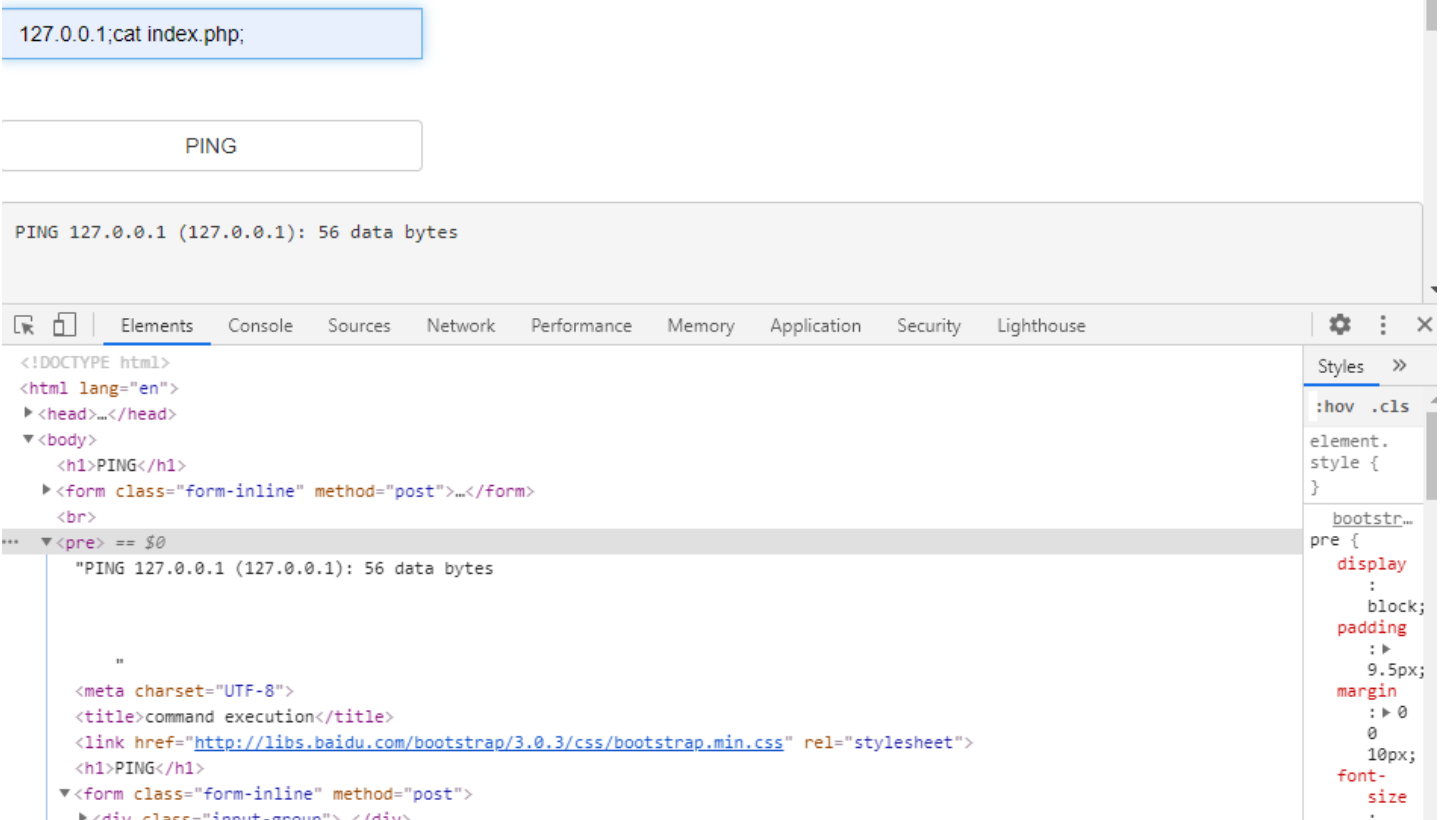




解题:

跳过分析阶段，直接解题

PING

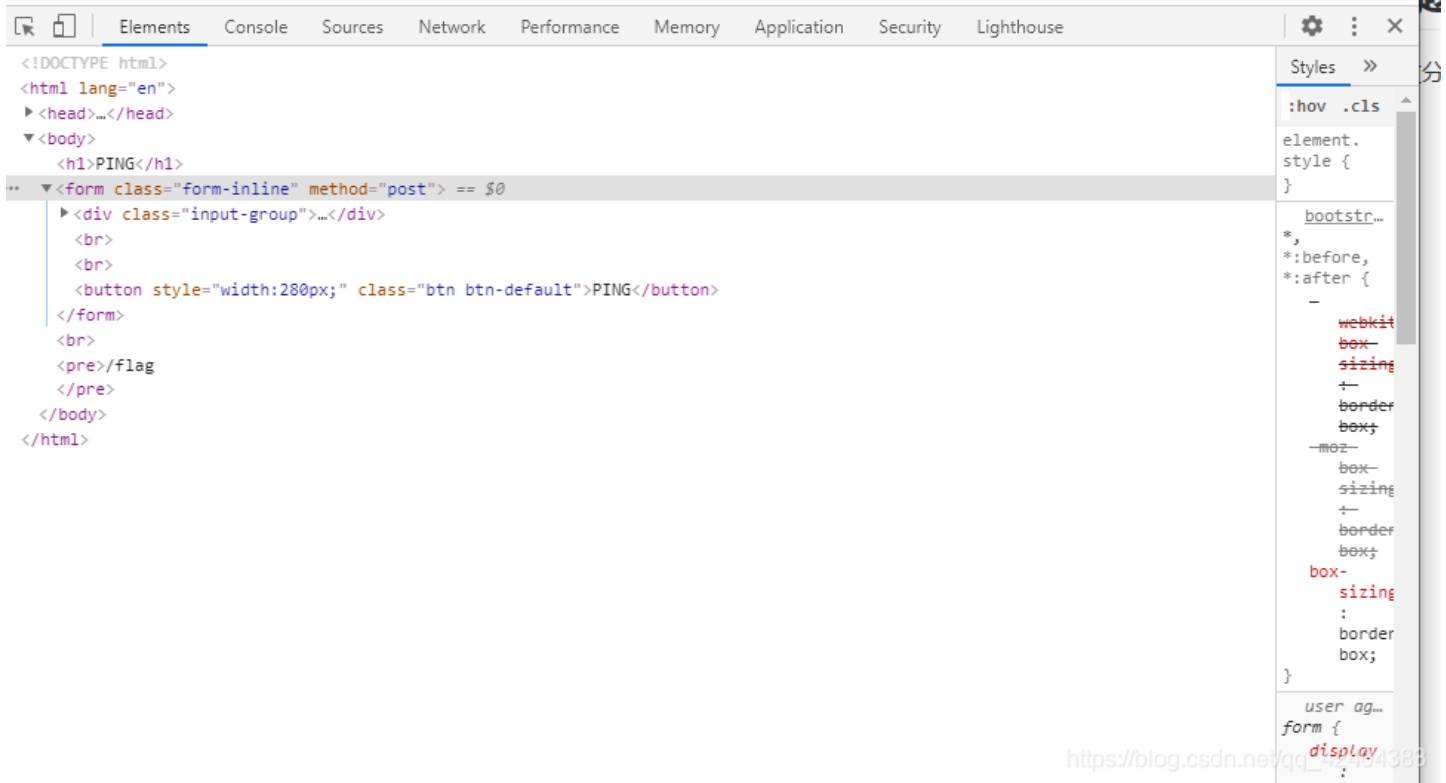
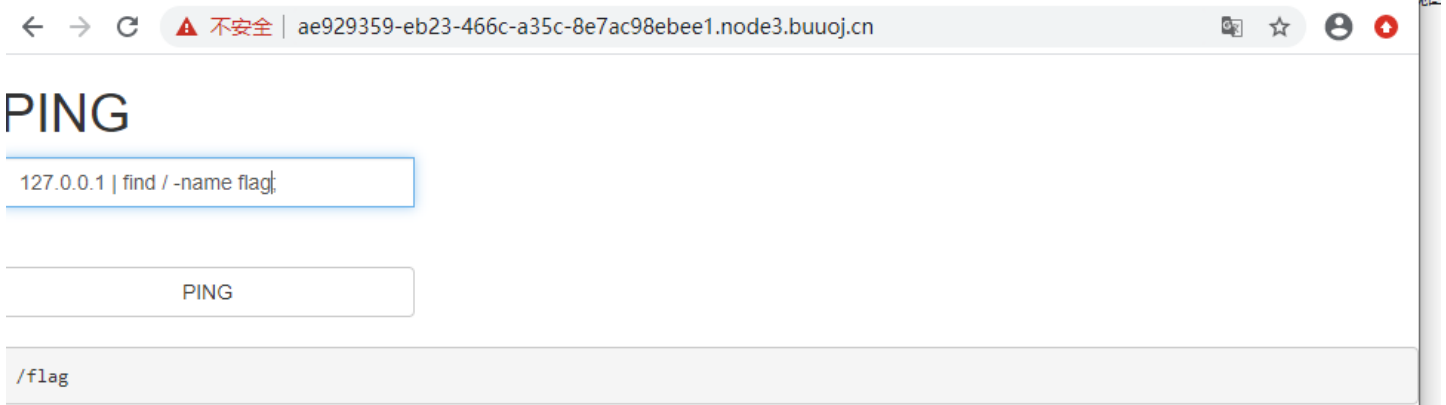


```
<pre>
<!--?php
if (isset($_POST['target'])) {
    system("ping -c 3 ".$_POST['target']);
}
?-->
</pre>
</body>
</html>
```

```
13px;
line-
height
:
1.4285
color:
#333
word-
break
:
break-
all;
word-
wrap
+
break-
word;
```

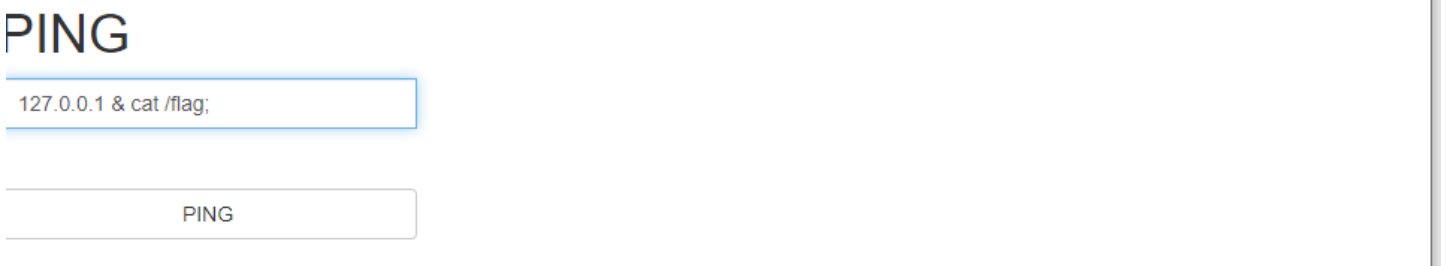
https://blog.csdn.net/qq_42404383

管道符找到flag

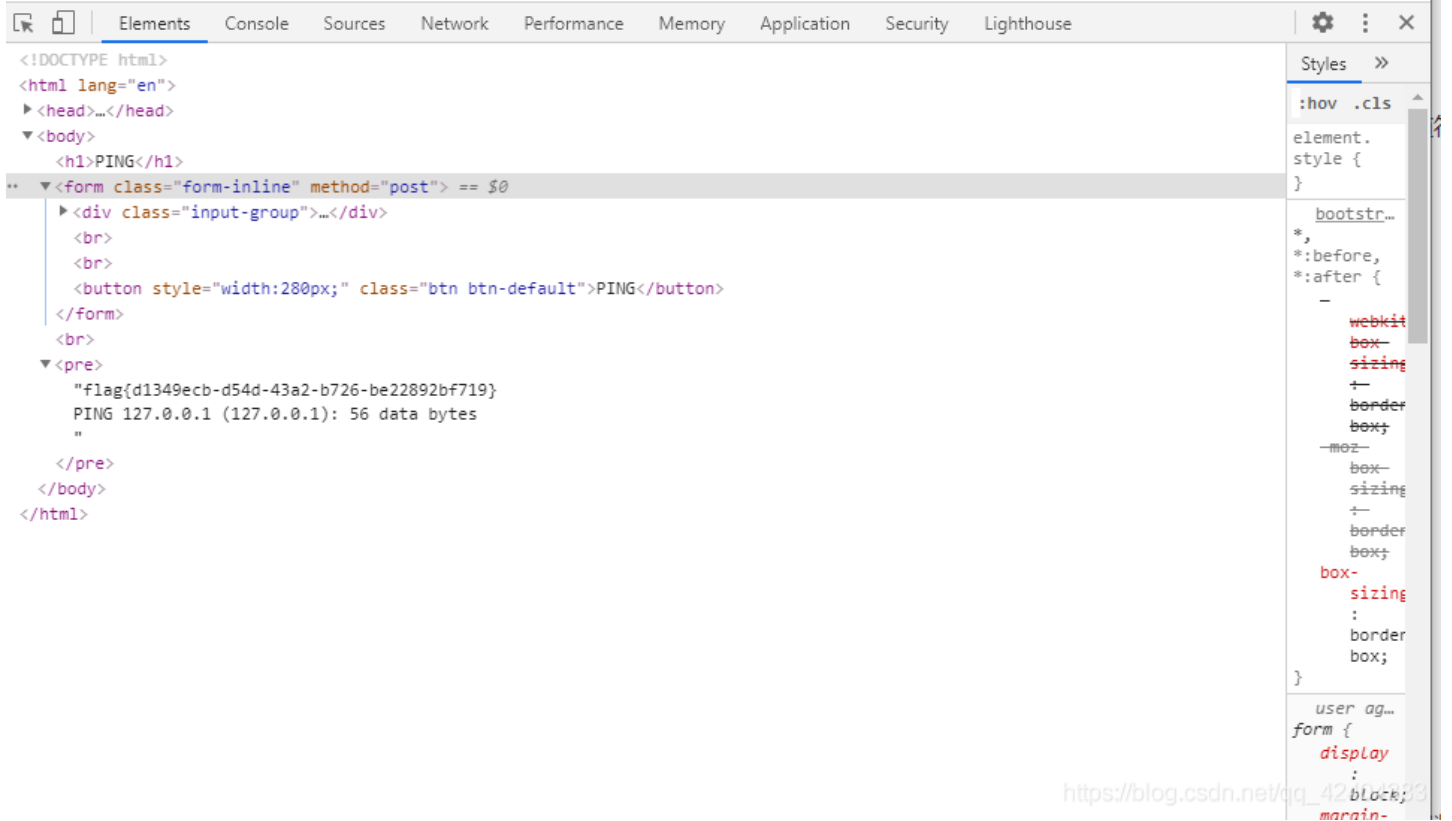


https://blog.csdn.net/qq_42404383

读取数据



```
flag{d1349ecb-d54d-43a2-b726-be22892bf719}
PING 127.0.0.1 (127.0.0.1): 56 data bytes
```



The screenshot shows a web browser's developer tools interface. The top bar includes tabs for Elements, Console, Sources, Network, Performance, Memory, Application, Security, and Lighthouse. The Elements panel is active, displaying the DOM tree. The root element is `<html lang="en">`, which contains a `<head>` and a `<body>`. The `<body>` contains an `<h1>PING</h1>` and a `<form class="form-inline" method="post">` element. The form contains a `<div class="input-group">` and a `<button style="width:280px;" class="btn btn-default">PING</button>`. Below the form is a `<pre>` tag containing the output of a ping command: `"flag{d1349ecb-d54d-43a2-b726-be22892bf719}"`, `PING 127.0.0.1 (127.0.0.1): 56 data bytes`, and `"`. The Styles panel on the right shows the default browser styles for the button, including `border: 1px solid #ccc;`, `border-radius: 4px;`, and `padding: 5px 10px;`. A URL is visible at the bottom right: `https://blog.csdn.net/qq_42138333`.

总结:

纯老套路，没有增加任何过滤远程命令执行漏洞。熟悉Linux命令即可。