[ACTF2020 新生赛]Exec1

原创

黑仔、 于 2020-09-15 22:11:36 发布

分类专栏： CTF--纸上谈兵 文章标签： linux

本文链接：https://blog.csdn.net/qq_42404383/article/details/108610981

[ACTF2020 新生赛]Exec

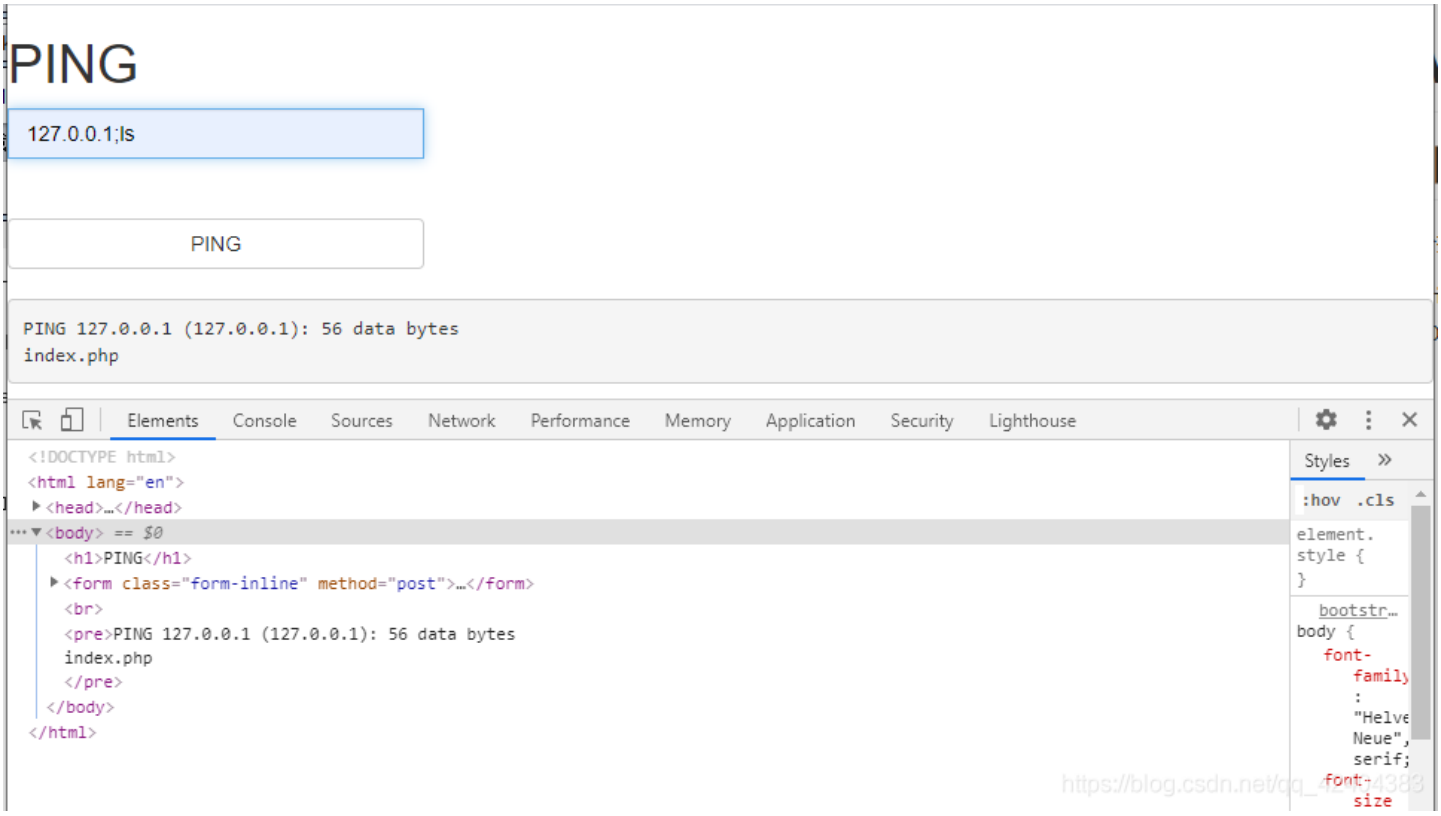
题目：

考察命令执行+绕过？

PING

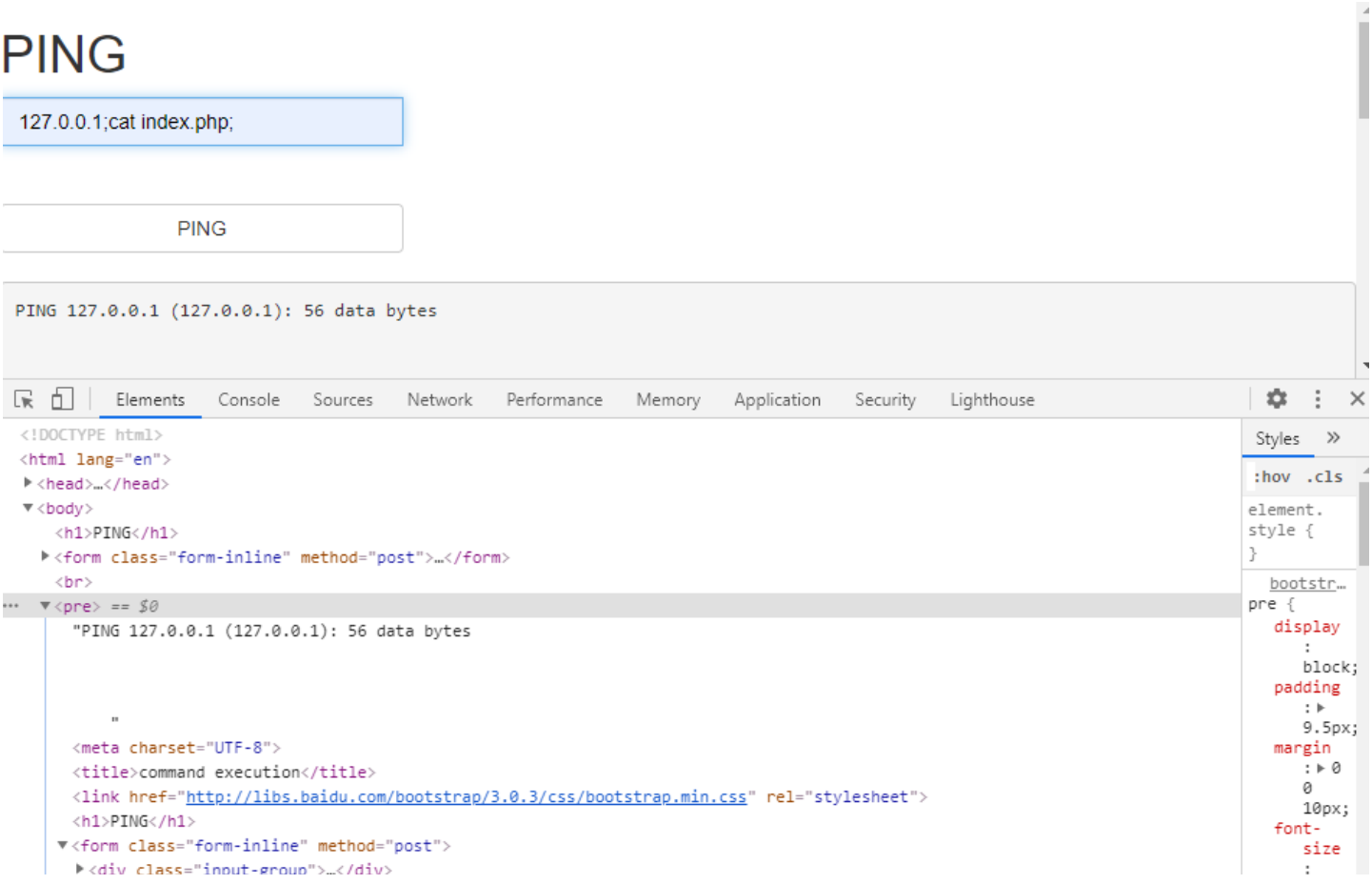
请输入需要ping的地址

PING



解题：

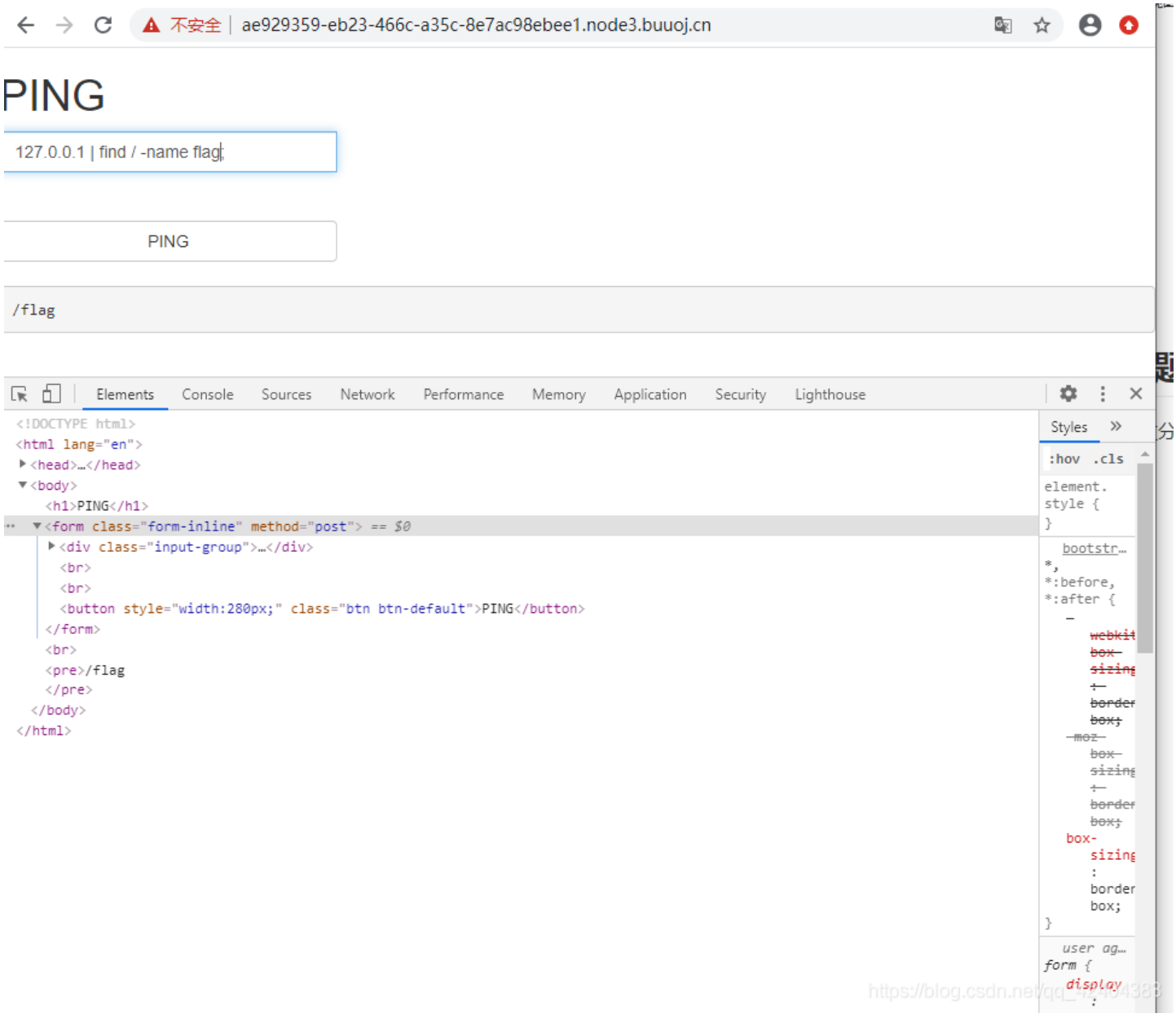
跳过分析阶段，直接解题



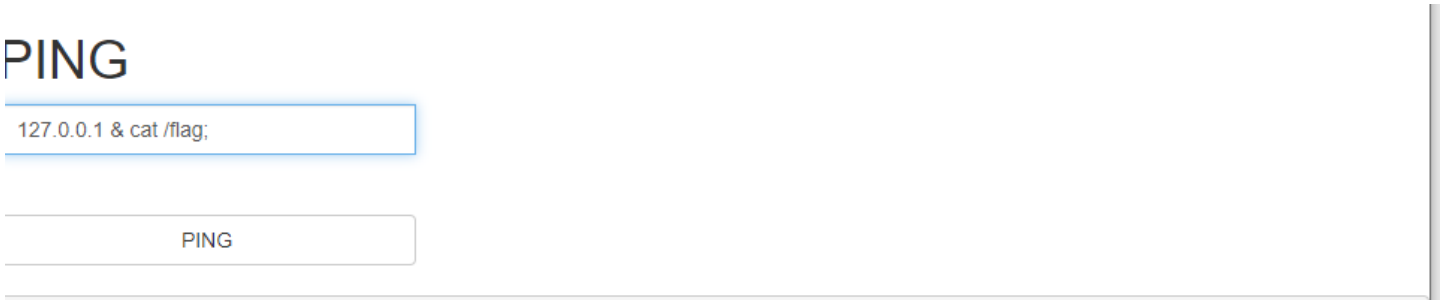
```
      <br>
      <br>
      <button style="width:280px;" class="btn btn-default">PING</button>
    </form>
    <br>
    <pre>
      <!--?php
      if (isset($_POST['target'])) {
          system("ping -c 3 ".$_POST['target']);
      }
      ?-->
    </pre>
  </pre>
 </body>
</html>
```

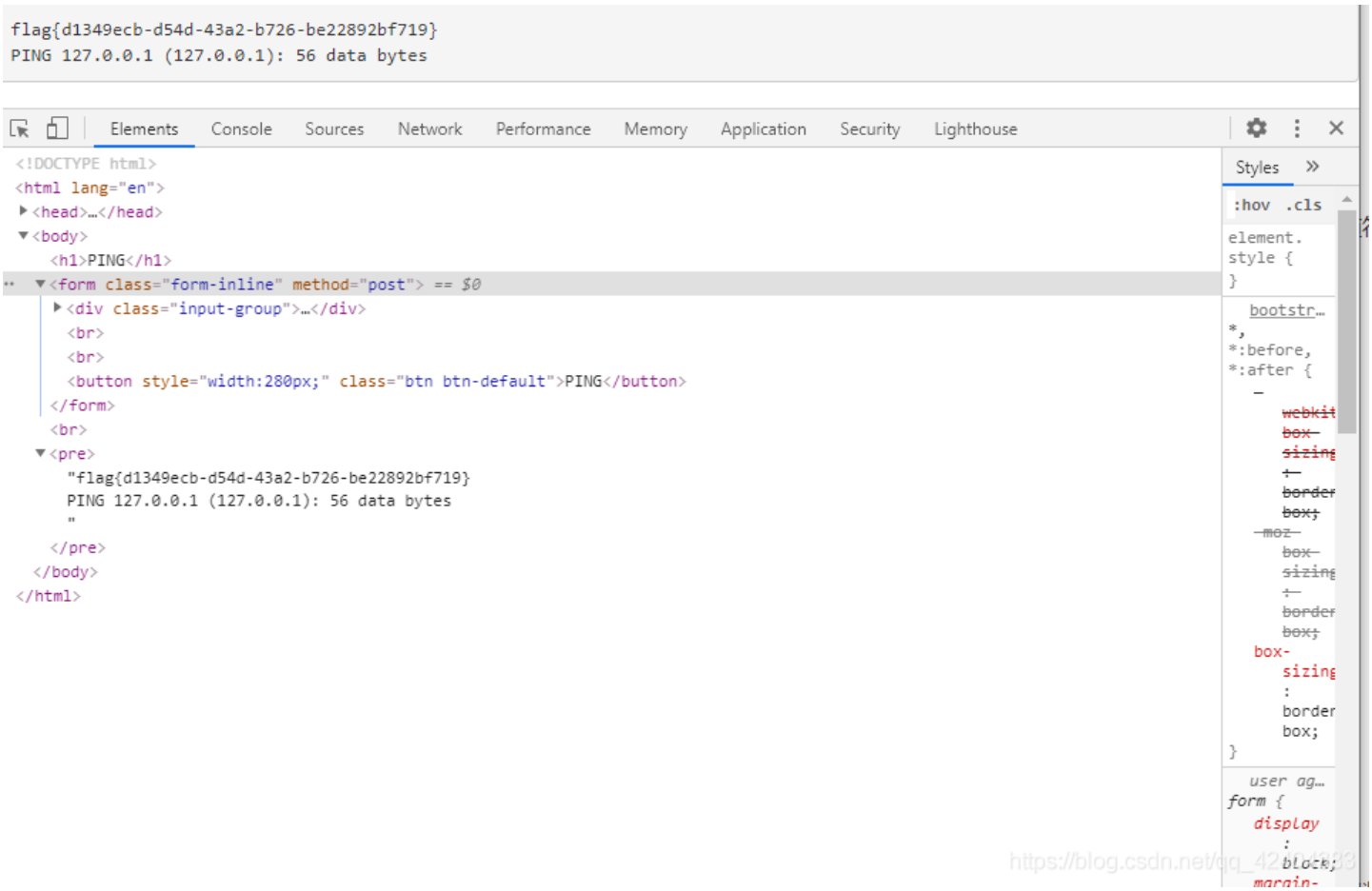
```
    13px;
  line-
    height
    :
    1.4285
  color:
    #333
  word-
    break
    :
    break-
    all;
  word-
    wrap
    :
    break-
    word;
```


管道符找到flag



读取数据





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。