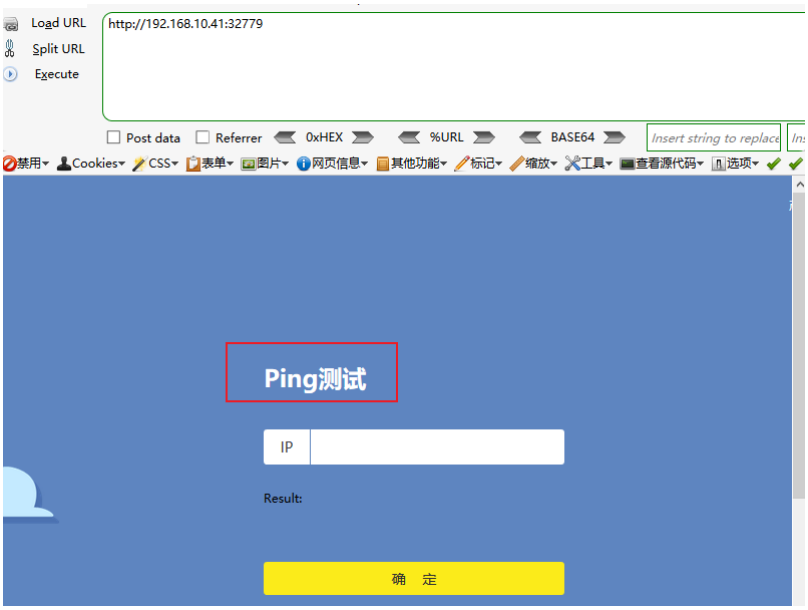
命令注入-基础注入

访问环境

1. URL为：`http://192.168.10.41`，端口为默认`80`端口，请勿访问图片中端口。
2. 页面提示一个大大的`Ping`测试。



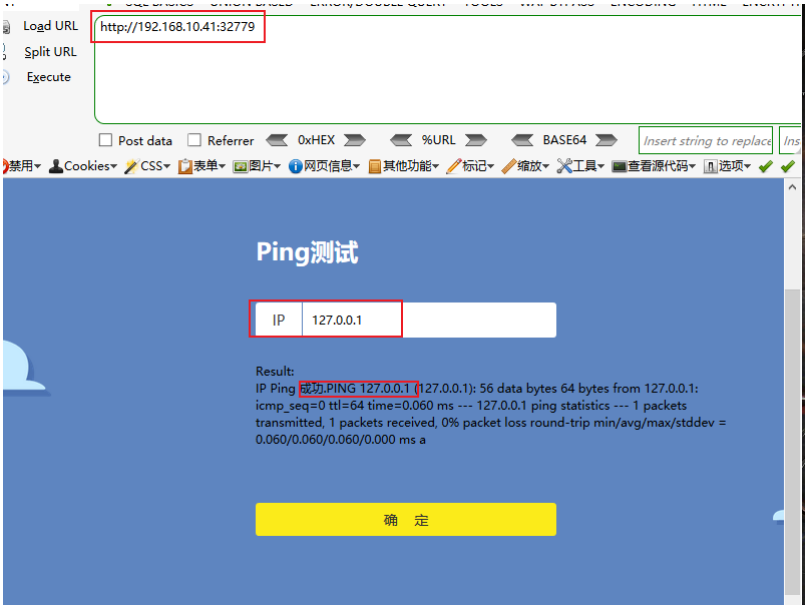
命令介绍

```
; 前面和后面命令都要执行，无论前面真假
& 前面和后面命令都要执行，无论前面真假
| 直接执行后面的语句
|| 如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句
&& 如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令
```

尝试ping127.0.0.1

步骤一：尝试ping127.0.0.1

1. 在输入框输入`127.0.0.1`查看返回结果，成功并有回显。根据返回的`TLL值，判断目标是台linux系统`。



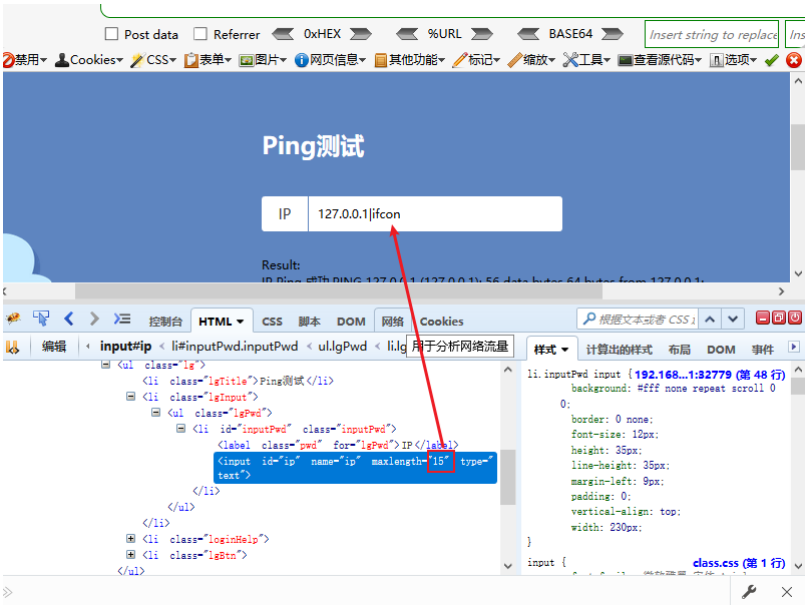
尝试执行ifconfig及ls命令

步骤一：尝试执行ifconfig命令

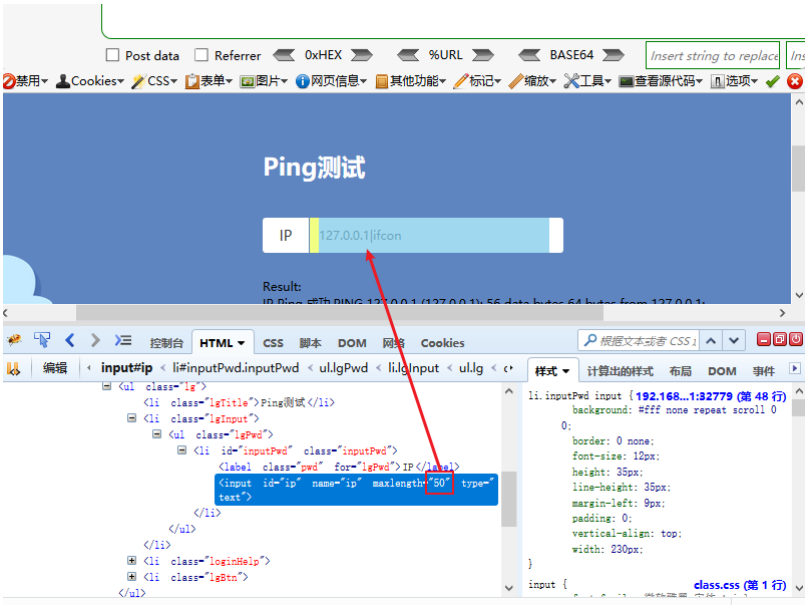
1. 在`127.0.0.1`后加入`|ifconfig`，当输入到`n`的时候，无法输入了。

2. 这个时候需要修改前端限制，按下`F12`，点击`小箭头`选中输入框。

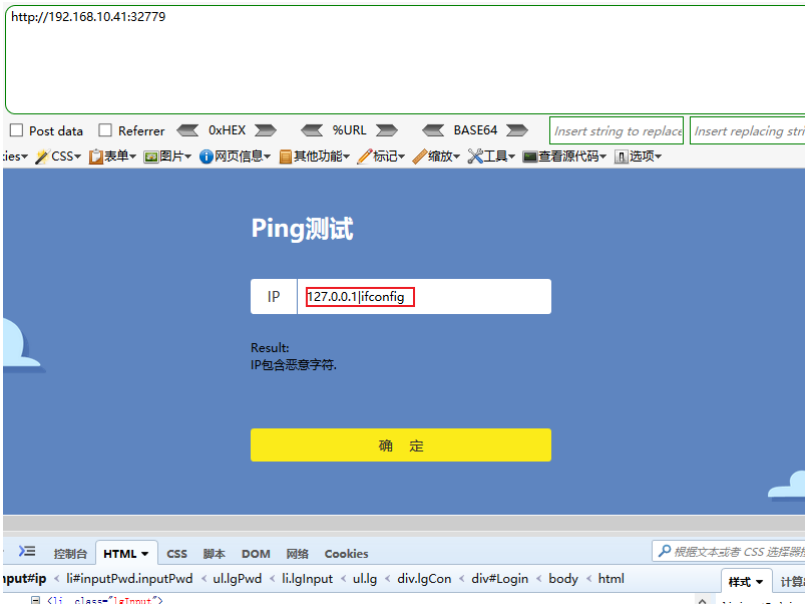
3. 可以看到长度最大到 `15`。



4. 我们修改到50，然后按 `ENTER`



5. 输入 `127.0.0.1|ifconfig` 提示恶意字符。



6. 输入 `127.0.0.1 | ls` 提示恶意字符。初步确定 `|` 被过滤了。

测试被限制的字符

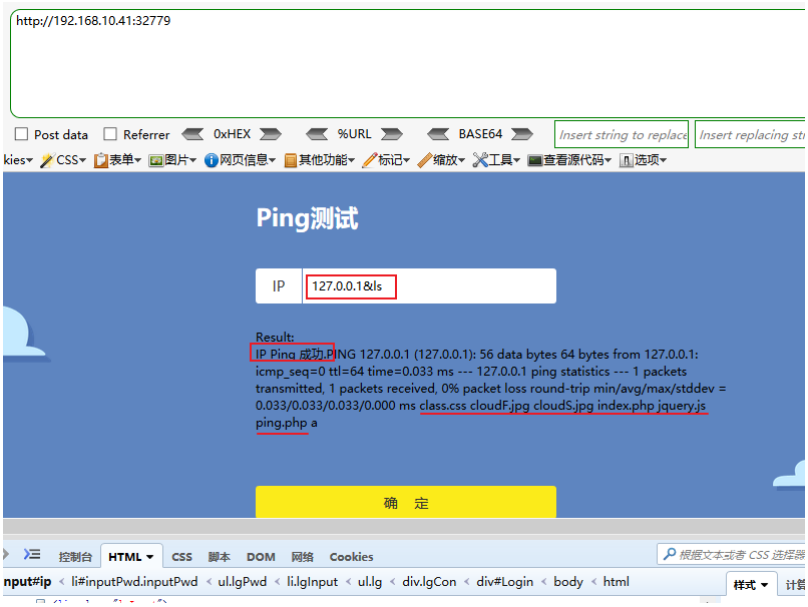
步骤一：测试有哪些字符被限制了。

1. 经过fuzz发现过滤了很多字符如下：`["$", "{", "}", "``", ";", "\"", "~", "!", "@", "#", "%", "^", "\\", ":", "_","|"];`
2. 经过测试只有`&`符合没用被过滤。

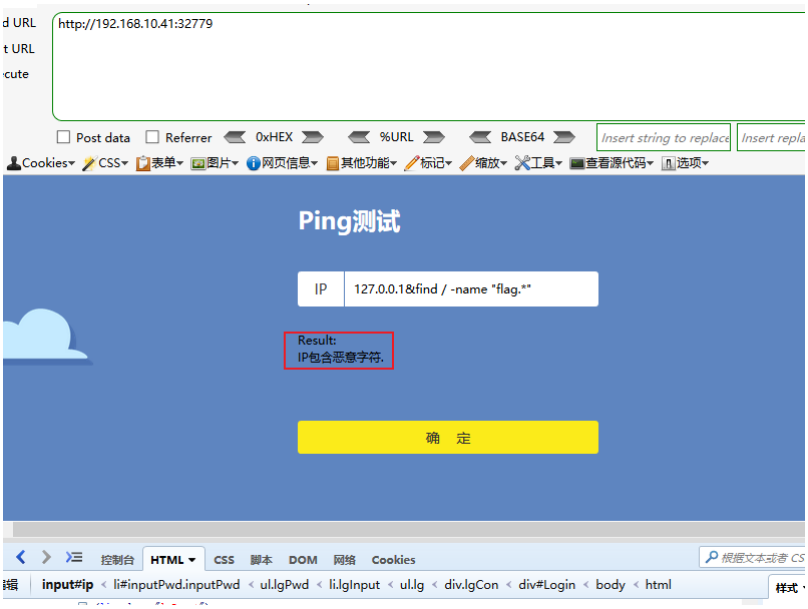
&符合命令执行测试

步骤一：使用&符合进行测试。

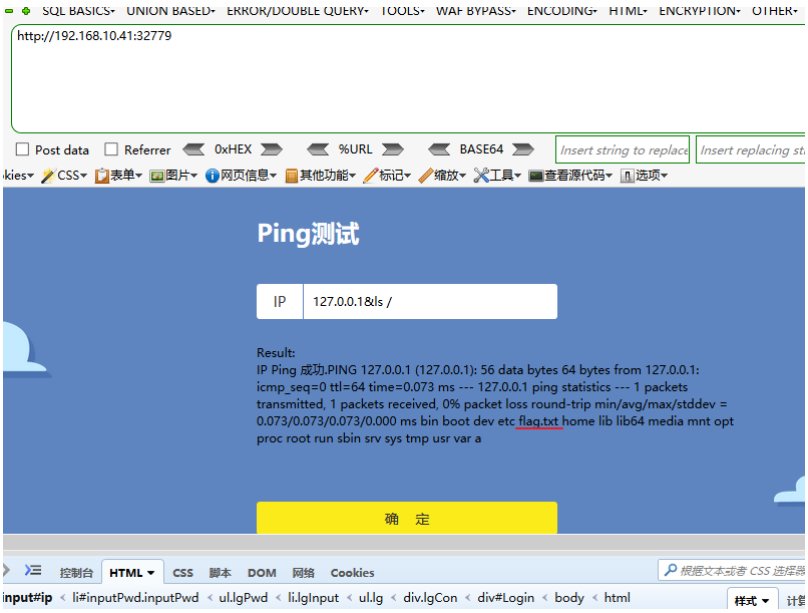
1. 接下来输入`127.0.0.1 & ls`执行成功，并看到了`ping.php`文件



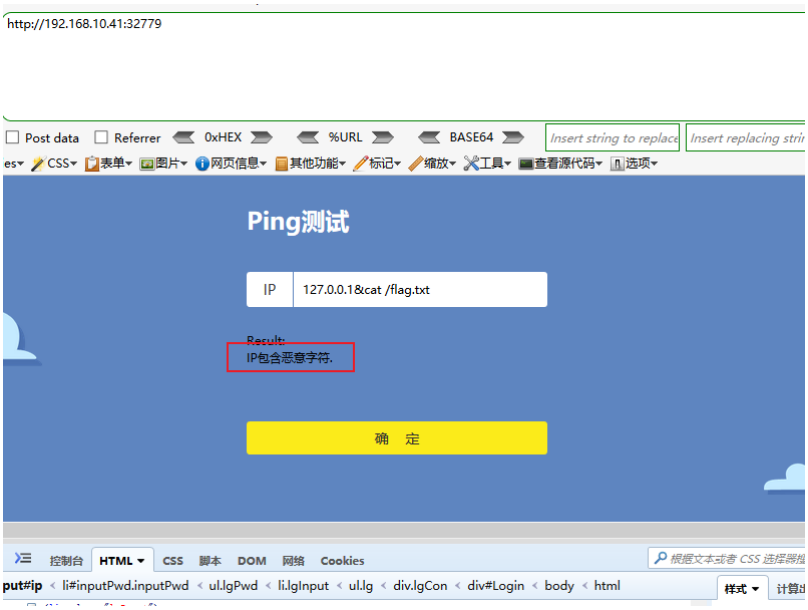
2. 接下来就可以使用`127.0.0.1&find / -name "flag.*"`进行查找`flag`，页面显示恶意字符。很有可能`fidn / - . * name`都被过滤。



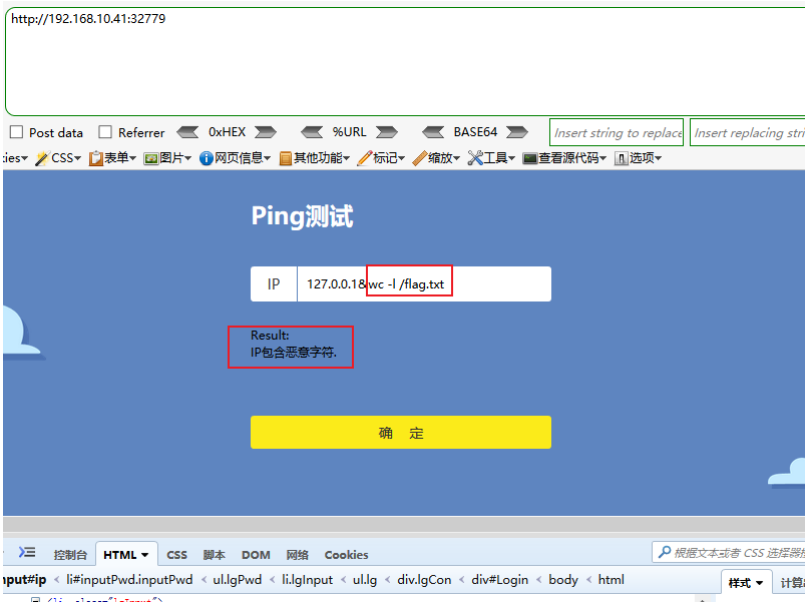
3. 只能使用复杂的方法，从根目录找起。`127.0.0.1 & ls \`，在根目录发现 `flag.txt` 文件。



4. 使用 `127.0.0.1&cat /flag.txt` 文件。又显示危险字符。再次判断 `cat` 被过滤。



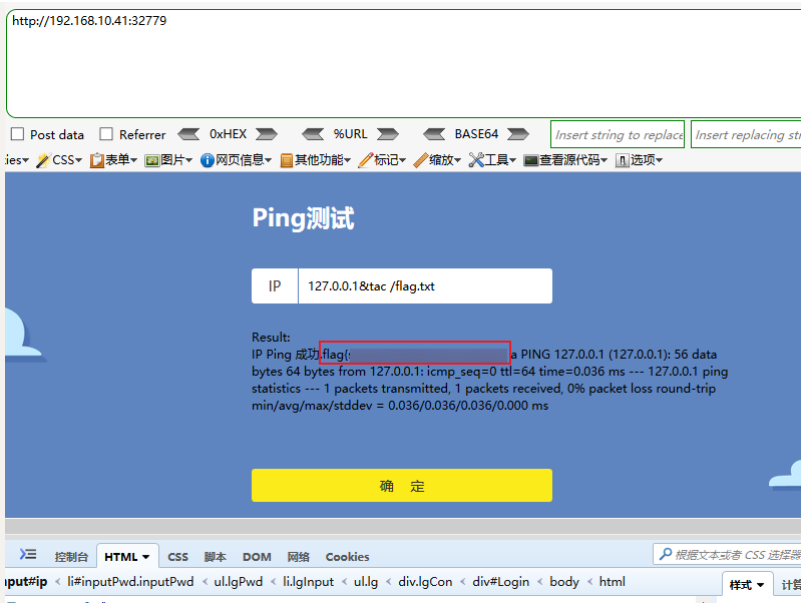
5. 使用 `wc -l` 查看flag.txt，也被过滤。



查看Flag

步骤一：经过测试，最用发现tac命令是可以用的。

1. 使用 `tac` 命令查看flag.txt文件



2. 获取到 `flag{xxxxx}`