二向箔-百日打卡writeup16-20

原创

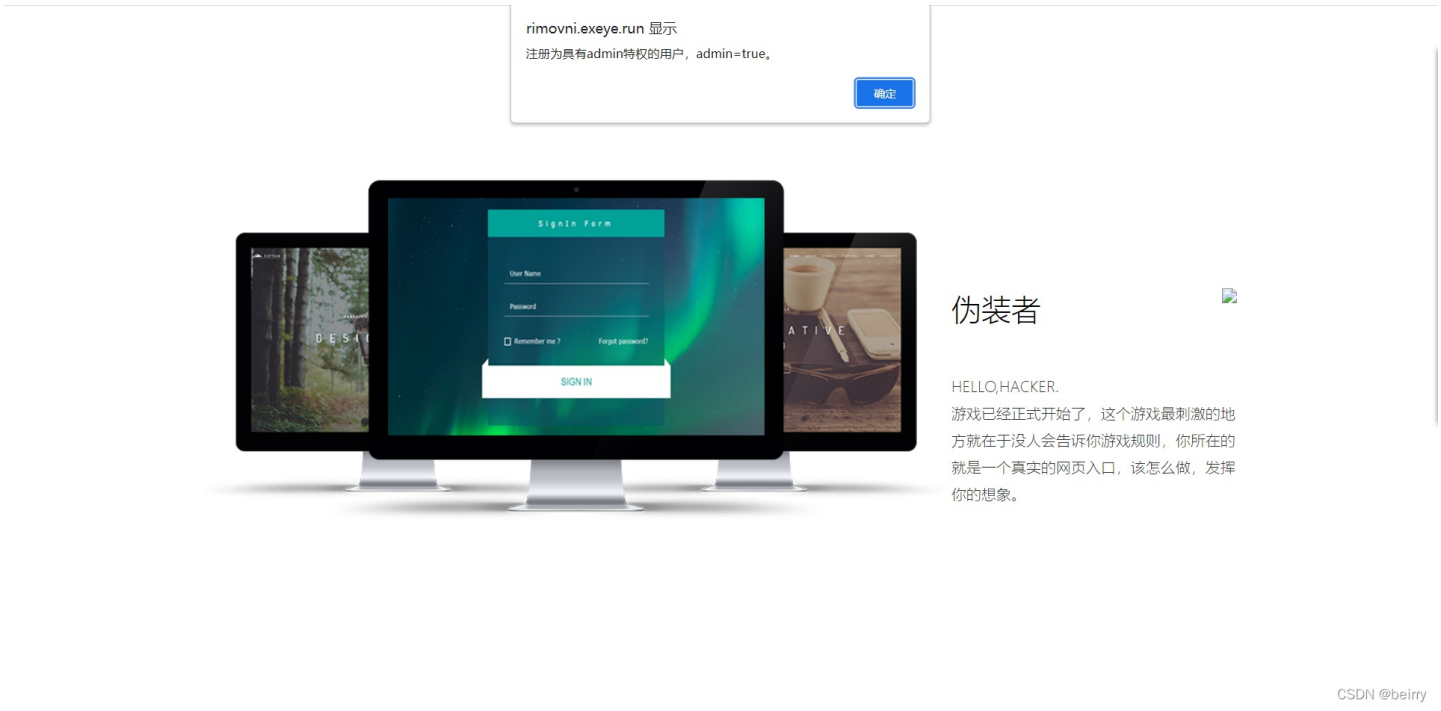
beirry 于 2021-12-08 16:19:17 发布 140 收藏

分类专栏： 二向箔安全-百日打卡 文章标签： web安全

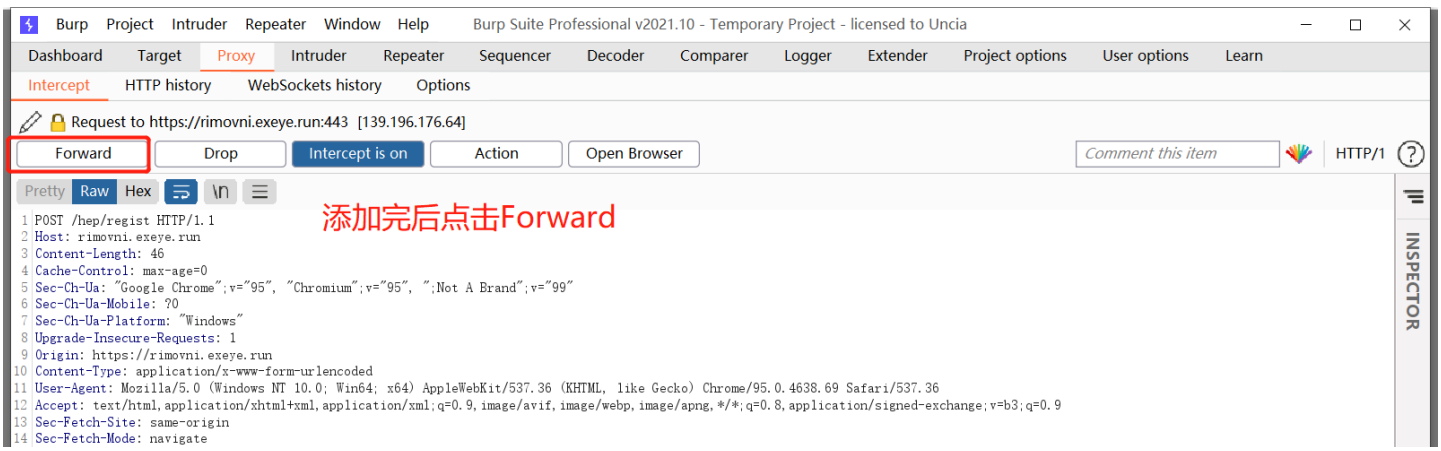
本文链接：https://blog.csdn.net/beirry/article/details/121793488

NO.16

还是登陆页面



提示也很明显了，首先要注册一个admin账户，将admin=true一同发往服务端进行注册admin用户。

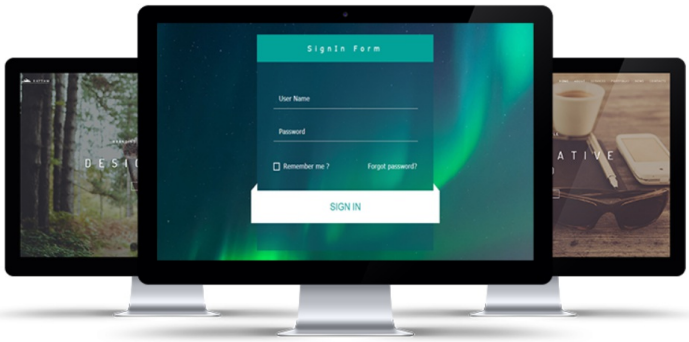


```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://rimovni.exeye.run/hep/index
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

username=admin&password=123&password_again=123&admin=true
```

添加&admin=true

得到flag

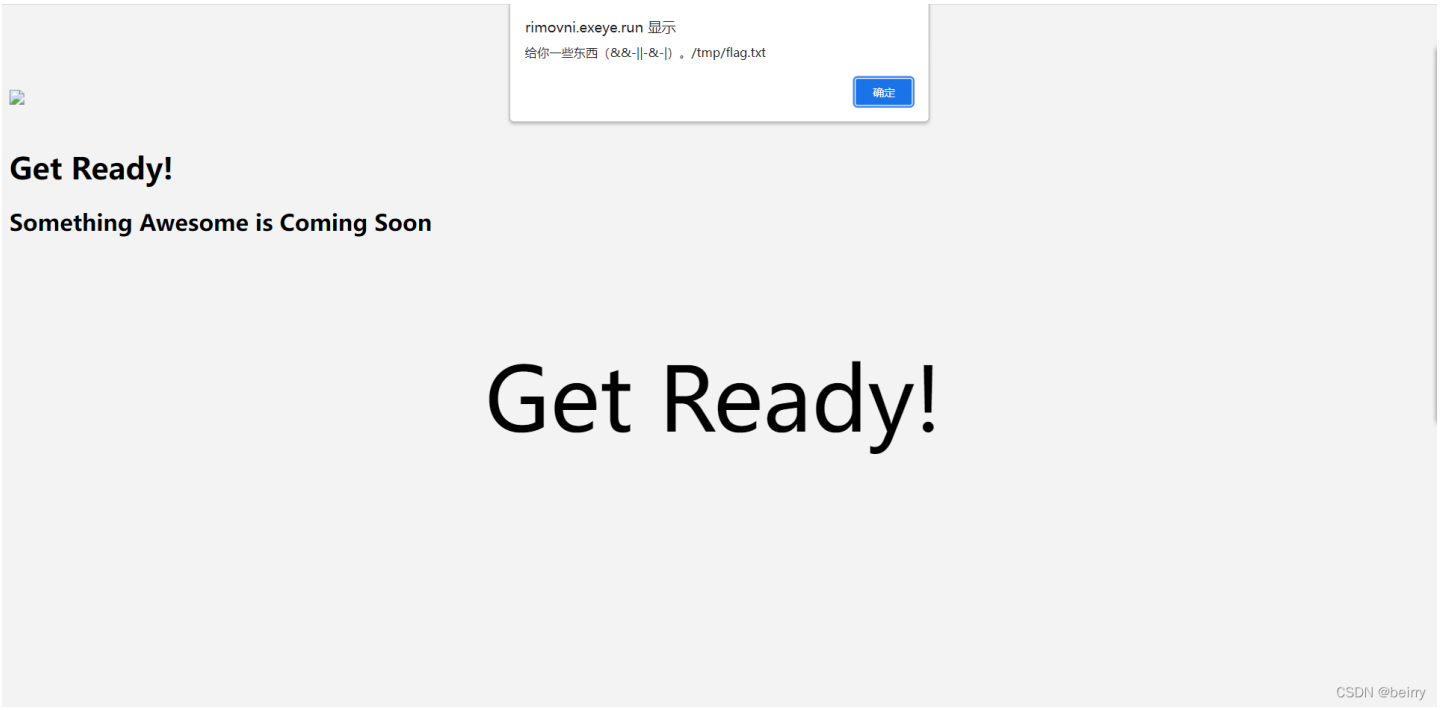


伪装者

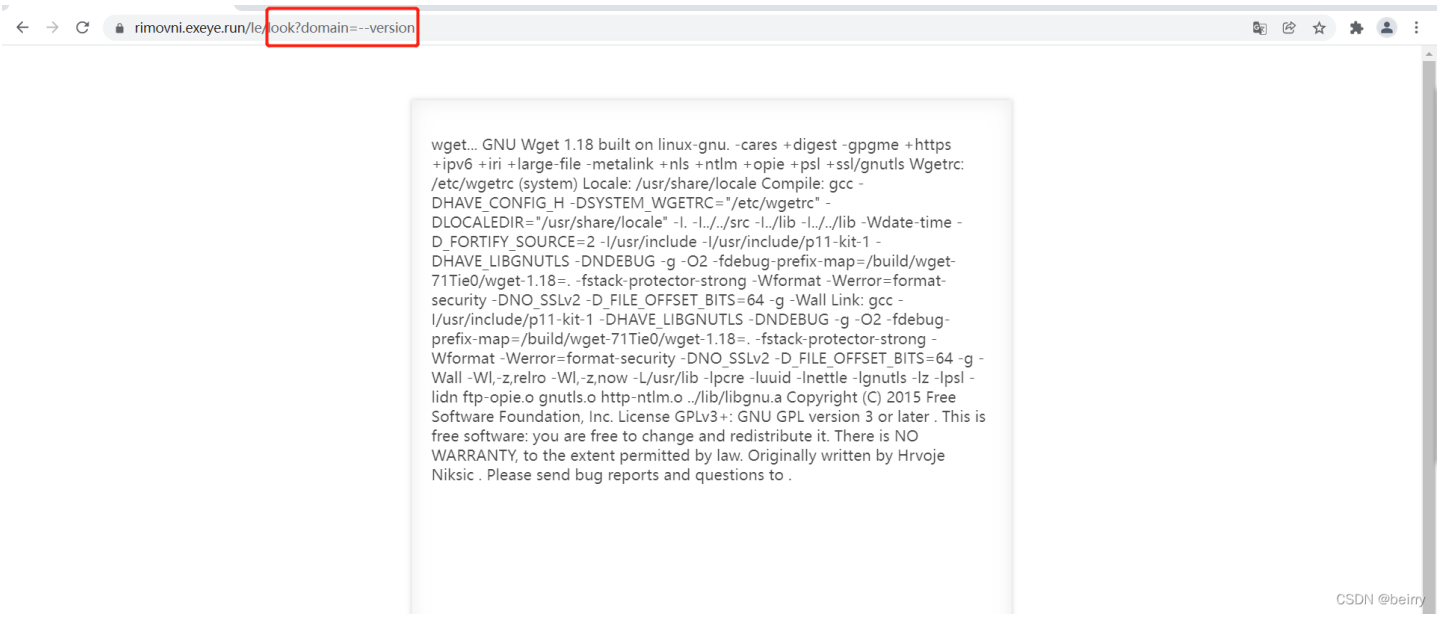
恭喜你two{I_havE_AdmiN}。退出

NO.17

看到`&& ||`很明显这道题是要命令执行了



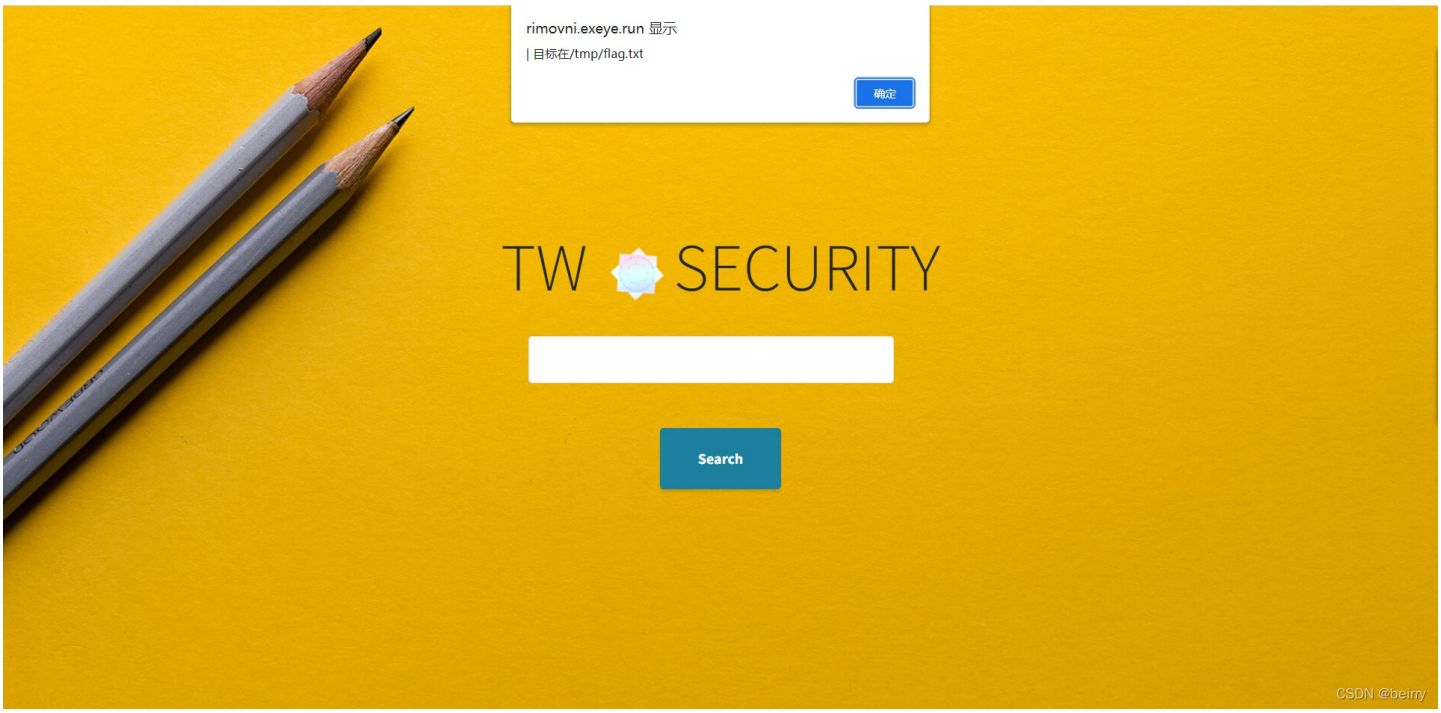
点击Get Ready,看到这个是利用GET传值方式传值



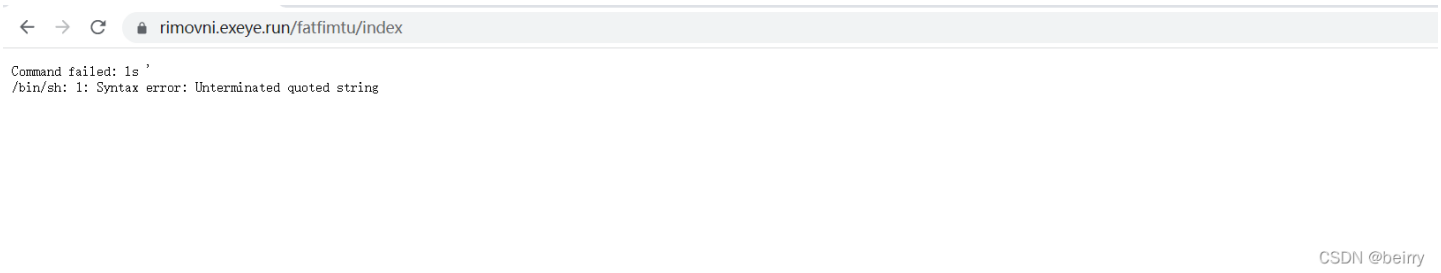
那我们直接构造`?domain=--version|cat /tmp/flag.txt`
得到flag

NO18

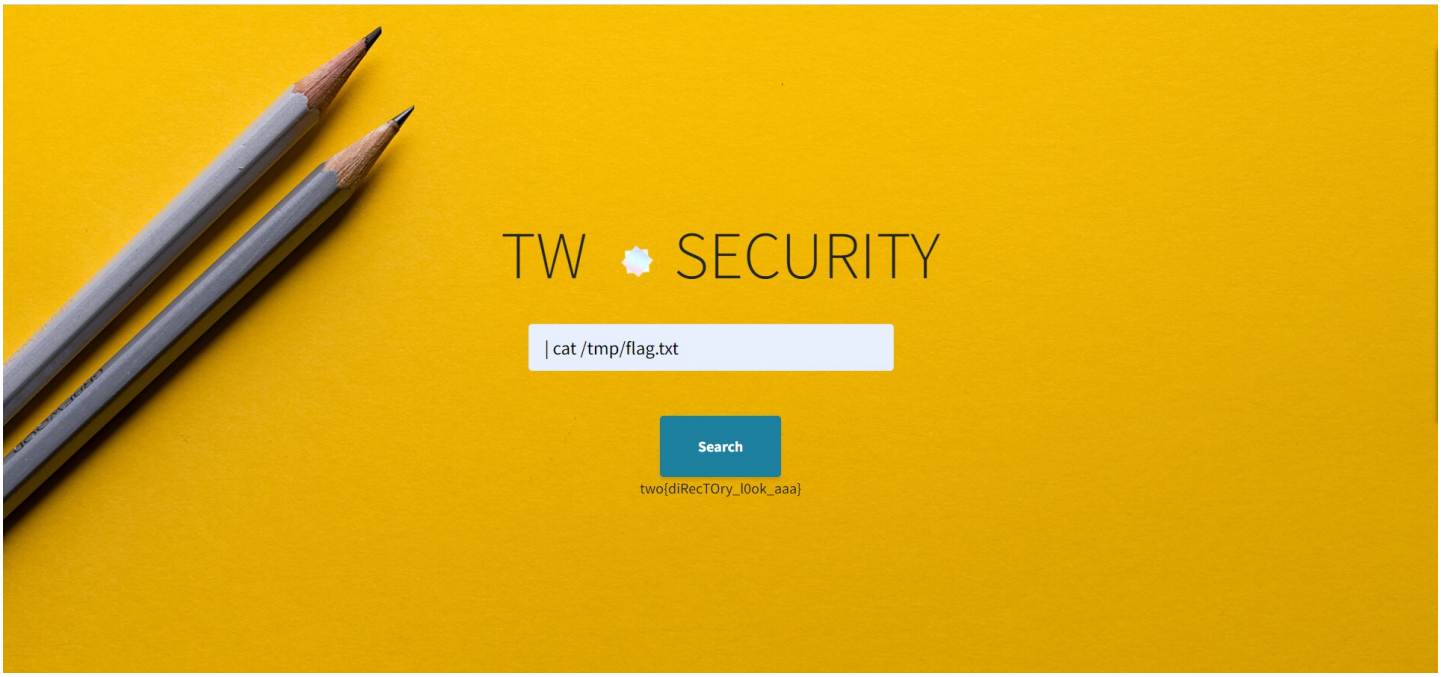
一开始以为是关于sql读取文件来获取内容



结果尝试输入单引号，并不是报关于sql的错误

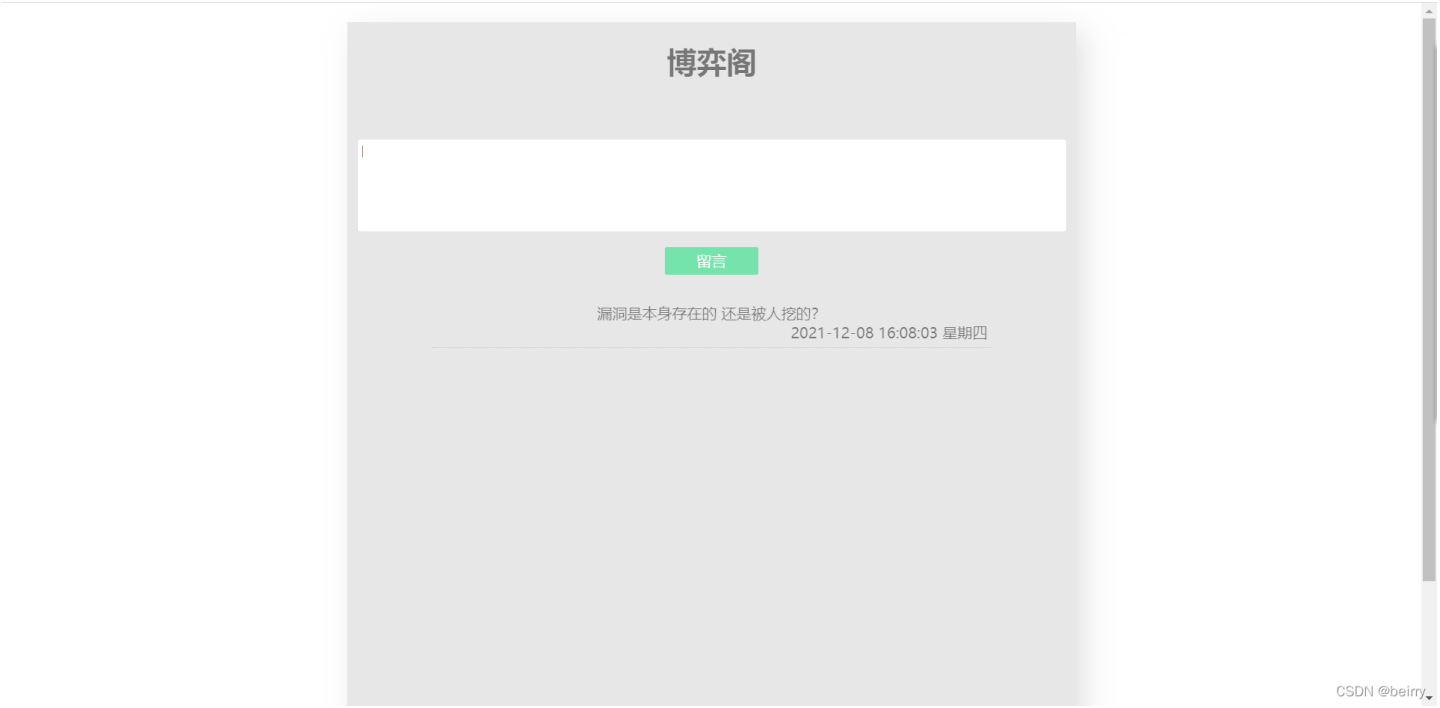


那又很明显是命令执行了，输入`| cat /tmp/flag.txt`
得到flag

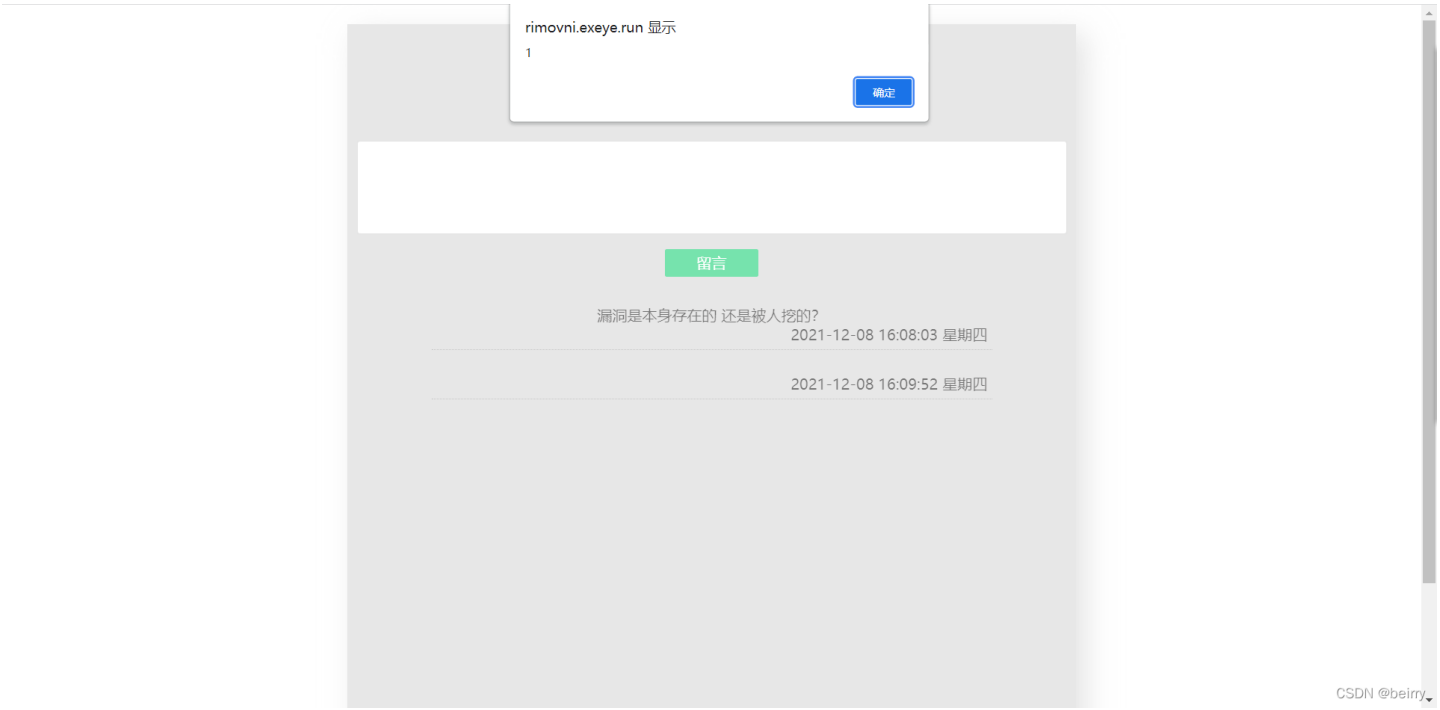


NO19

虽然这道题没有提示，但是看到留言框就已经是很明显的提示了，我之前在做xss题目时也讲过，<a>和<img>标签被过滤的可能性是很小的，所以一般我会从这两个标签来尝试

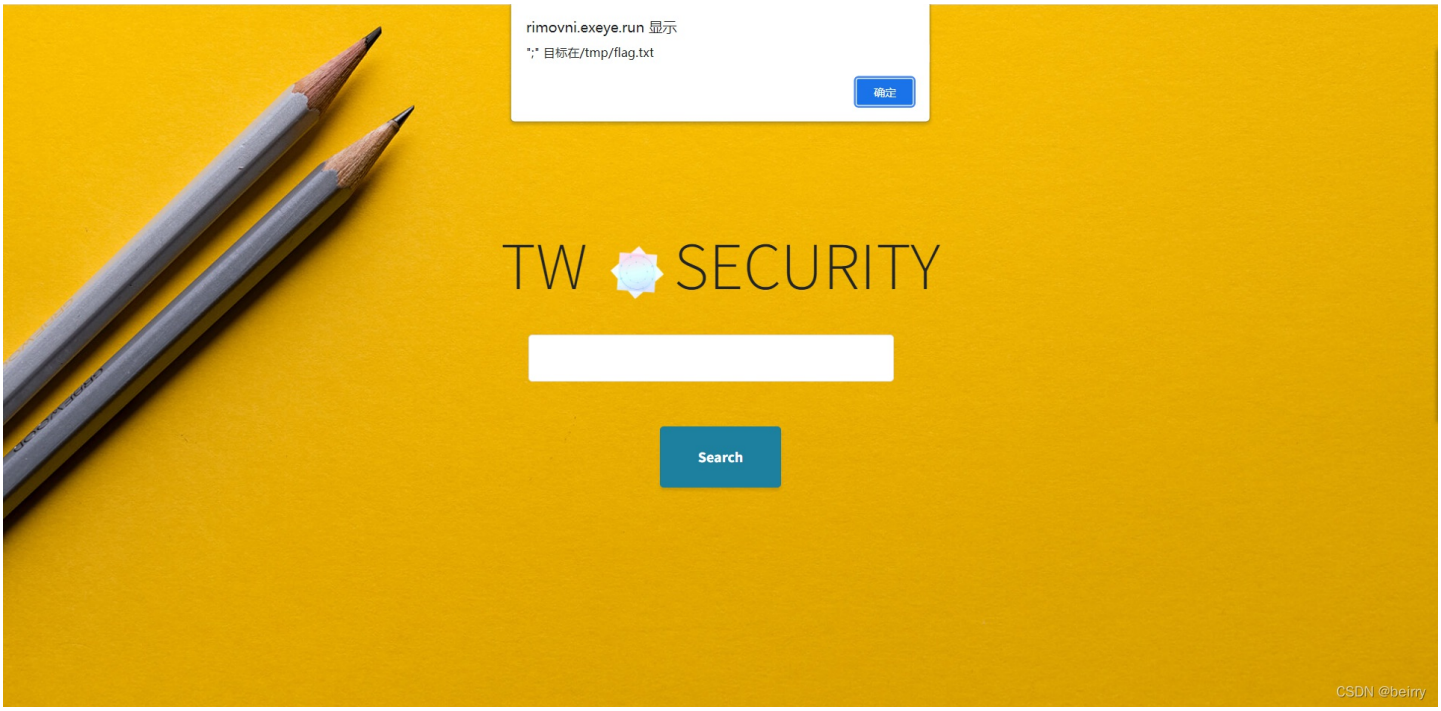


输入`<img src=x onerror=alert(1)>`

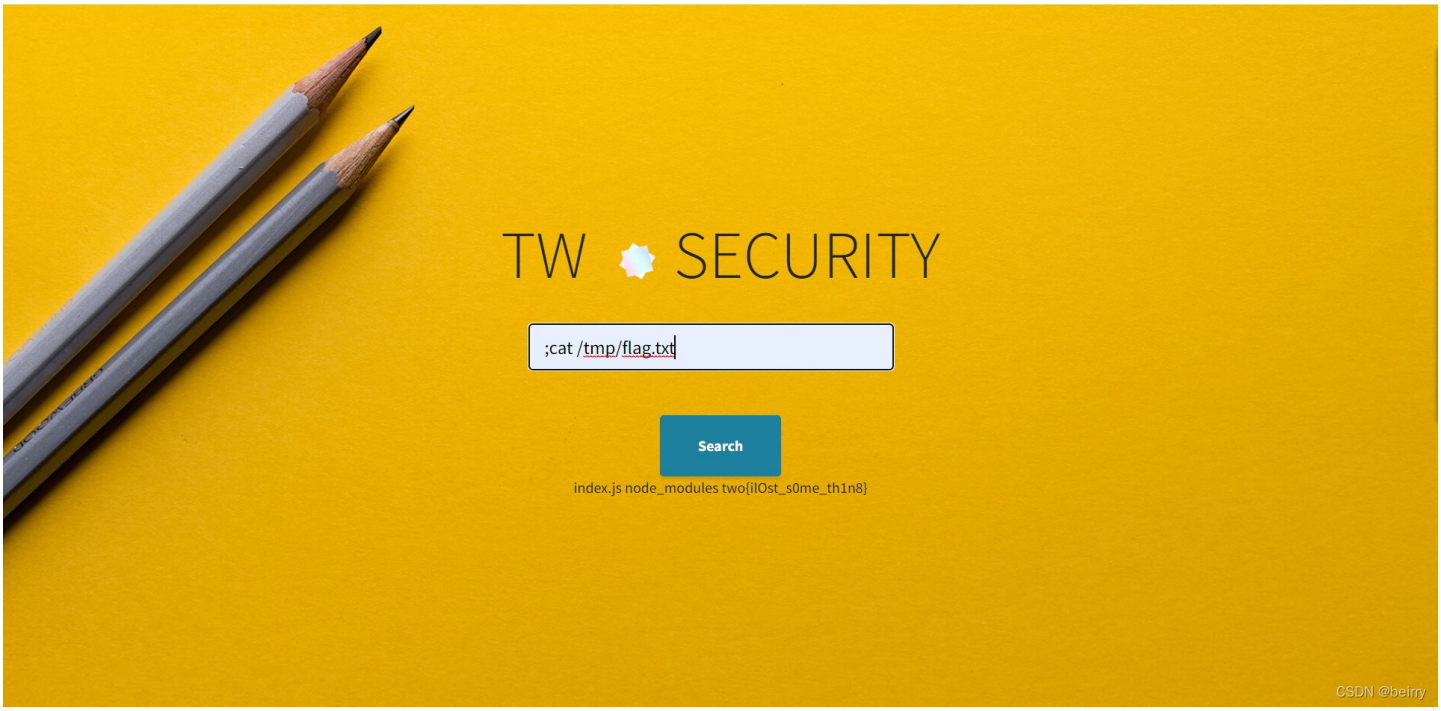


NO.20

提示又是命令注入了



输入`;cat /tmp/flag.txt`
得到flag



16-20题至少有3道是命令注入，这些题更加偏向于基础，告诉我们有哪些手段去执行我们输入的命令，并没有什么需要绕过的手段。