ich is co 在挖掘一些业务的时候,很多系统都会放在一个统一认证中去访问,你只有登录统一认 证才能去访问某个系统,那么当我们在挖掘的时候,遇见这样的环境怎么办呢?

当然是最简单的修改返回包查看是否可以未授权查看内容,当然很多时候都是白给,但 是我们还是要尝试一下撒。

当我们扫描出 xxxx.com 存在一个子域名,我们去访问站点 http://stde.xxxx.com 发现他 要跳转到一个统一认证的页面,此时我们进行抓包对每一个数据包进行分析:

```
st:
er-Agent: Mozilla/5.0 (Windows MT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
ser_agent. Modilaty 5.0 (windows ps : 0.0; minor; ps; pr : 31.0) vector outward
compt = paince(mod) non
compt = language: thrCU, ht, q=0.0; h=TM; q=0.7; h=MX; q=0.5; en=US; q=0.3; en; q=0.2
compt = language; csp; definer
effects:
application/json; charsef=UTF=0
ontertionate in consecution of the control of the c
```

每一次放包都会自动跳转,但是发现该数据包时,我将箭头所指的{}删掉,发现就可以 进入系统卡死在功能点页面,因为页面只有功能点没有数据,我就继续点击功能点

点击任意功能点继续抓包:出现如图的数据包的时候将 401,提示我们需要先登录才能 进行访问

```
DITP/1. 200 0X
Date: Thu. 26 Aug 2021 09:28:46 GMT
Content-Type: application/json
Connection: close
tccess-Control-Allow-Origin: http://192.168.100.92:8001
tccess-Control-Allow-Wethods: POST, GET, OPTIOWS
tccess-Control-Allow-Headers: *
tccept: *
 lccept: *
lccess=Control=Allow=Credentials: true
 I-Frame-Options: SAMEORIGIN
 Jary: Cookie
 Access-Control-Allow-Origin:
 Access-Control-Allow-Methods: GET, POST, OPTIONS
 Content-Length: 117
{"code": 401, "message": "诱先册录", "data": {"type": "account", "currentAuthority": "admin", "status": "error"}}
```

常规操作,将 401 改为 200,发现居然成功访问数据:

```
HTTP/1.1 200 AB Aug 2021 09:29:00 GMT
Content-Type: application/json
Content-Earth, 5:49
Access—Control-Allow-Origin, http://192.168.100.92:8001
Access—Control-Allow-Monder: POST, GET, OPTIONS
Access—Control-Allow-Monders: *
Accept: *
A
       Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEONIGIN
Yary: Accept-Encoding
Access-Control-Allow-Origin: #
Access-Control-Allow-Methods: GET, POST, OPTIONS
                                                                                                ontrol-Allow-Credentials: true
Options: SAMEORIGIN
       ("code" 200, "massas" "memutan" data" [1st", [('st" 2021#99", "malus" 2021#99", "galus" "0021#99", "malus" 2021#99", "ma
   HTIP/1.1 200 OR
Date: Thm. 26 Aug 2021 09:29:09 GMT
Content-Type: application/json
Content-Length: 173
Connection: Close
Access=Control-Allow=Origin: http://192.168.100.92:8001
Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Control-Allow=Access=Access=Control-Allow=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=Access=
```

可以发现整个站点功能点都可以用这个方法查看数据:

