广东工业大学

时间	单位	作者	等级	Rank
2023-11-22 16:01:35	广东工业大学 (/list/firm/4948)		中危	1

广东工业大学存在未授权访问漏洞

URL---http://nxlcth.site:809/

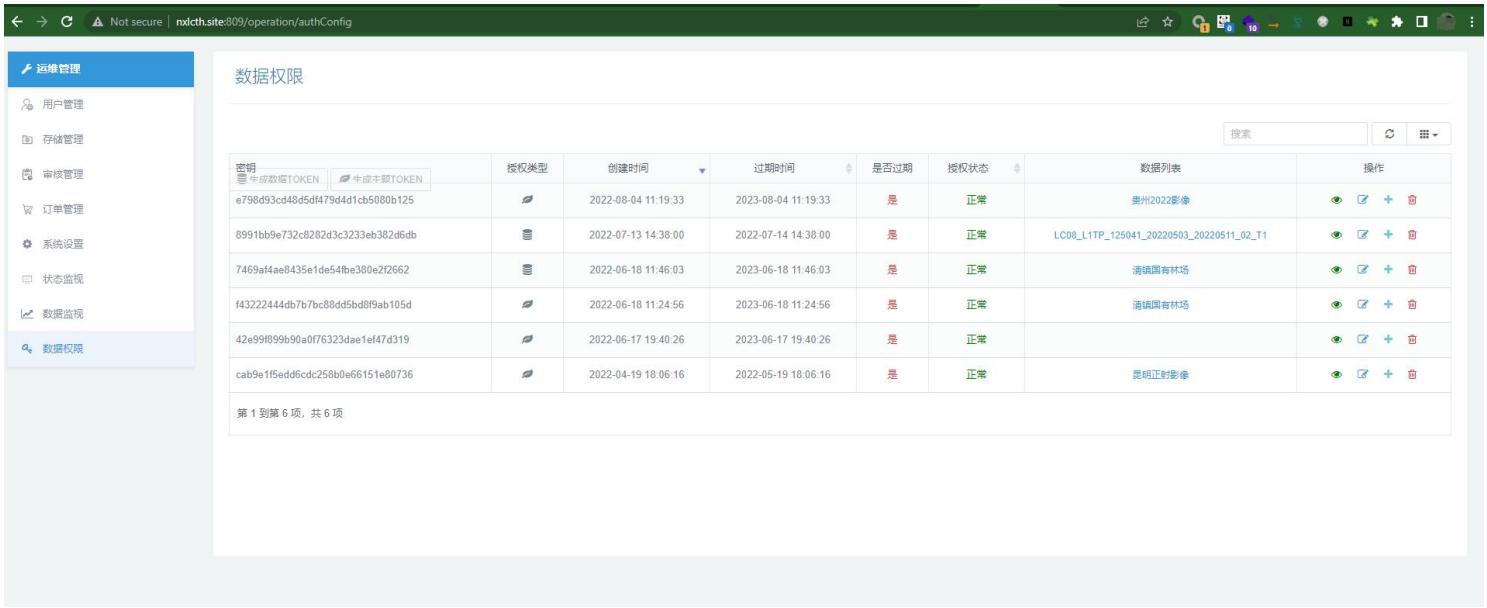
登录账号密码

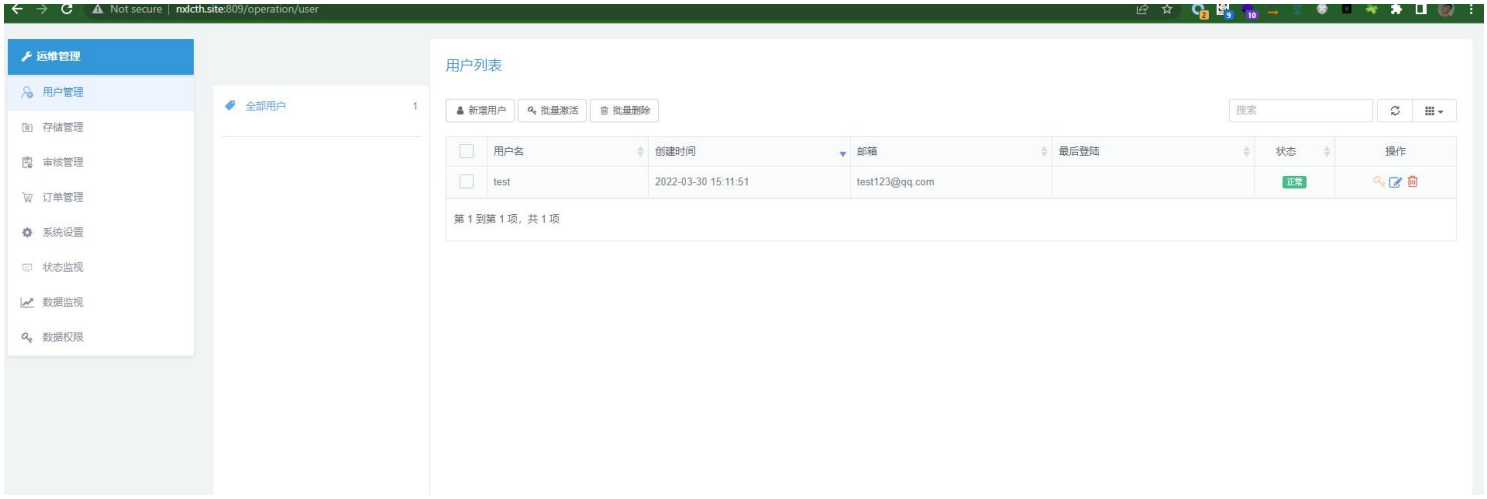
"password":"admin@zhhy2021","user":"admin"

首先确认广东工业大学站点使用的服务

IP	域名	端口/服务	站点标题	状态码	ICP备案企业	应用/组件	资产标签	地理位置	更新时间
58.22.5.40	nxlcth.site	800 http	福建智慧海洋大数据...	200	-	jQuery/3.2.1 共4条	-	福州市	2023-11-21
58.22.5.40	www.nxlcth.site	800 http	福建智慧海洋大数据...	200	-	jQuery/3.2.1 共4条	-	福州市	2023-11-21
58.22.5.40	58.22.5.40	800 http	福建智慧海洋大数据...	200	-	Font Awesome 共4条	-	福州市	2023-11-21
58.22.5.40	www.nxlcth.site	801 http	智慧海洋大数据中心	200	-	Windows Server 共6条	-	福州市	2023-11-20
58.22.5.40	nxlcth.site	801 http	智慧海洋大数据中心	200	-	Microsoft ASP.NET 共6条	-	福州市	2023-11-20
58.22.5.40	58.22.5.40	801 http	智慧海洋大数据中心	200	-	Font Awesome 共6条	-	福州市	2023-11-20
58.22.5.40	58.22.5.40	6080 http	ArcGIS	200	-	ArcGIS	-	福州市	2023-11-20
58.22.5.40	nxlcth.site	6080 http	ArcGIS	200	-	ArcGIS	-	福州市	2023-11-20
58.22.5.40	www.nxlcth.site	6080 http	ArcGIS	200	-	ArcGIS	-	福州市	2023-11-20
58.22.5.40	nxlcth.site	808 http	养殖一张图	200	-	-	-	福州市	2023-11-19

登录后台之后可以通过findsomething找到后台接口，发现是未授权访问，无需登录直接访问即可。





查看get传参包 nxlcth.site:809/operation/user

发现没有cookie 校验，可以直接访问

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