

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。

运营维护

用户管理

存储管理

审核管理

订单管理

系统设置

状态监视

数据监视

数据权限

数据权限

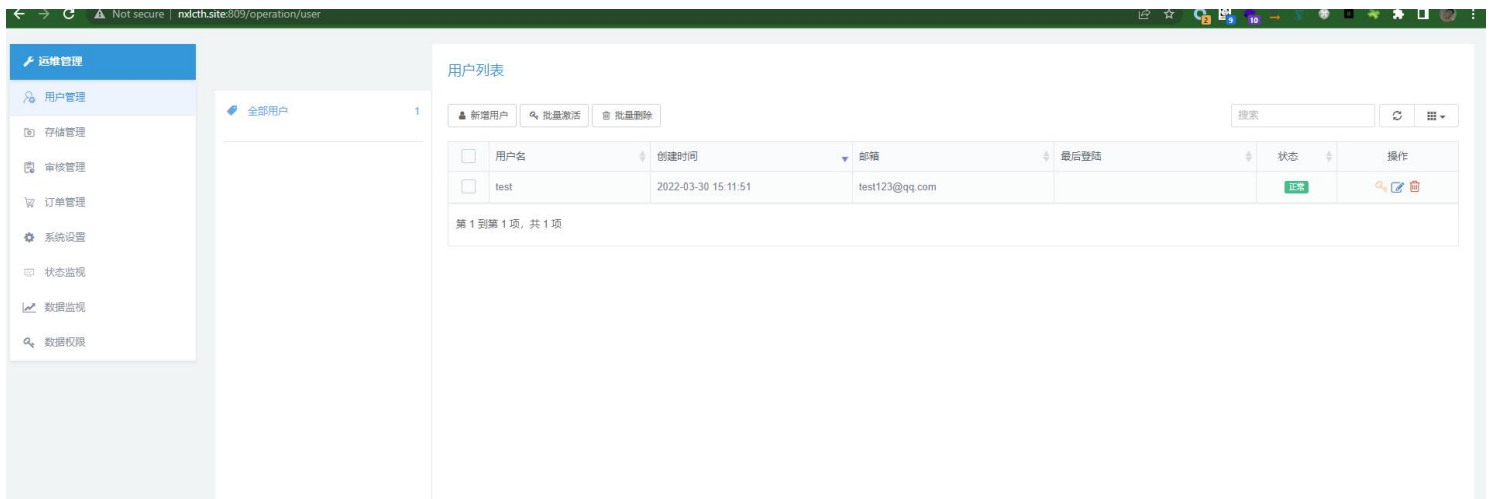
搜索

刷新

更多

密钥	授权类型	创建时间	过期时间	是否过期	授权状态	数据列表	操作
<div>生成数据TOKEN</div> <div>生成主密钥TOKEN</div> <div>e798d93cd48d5df479d4d1cb5080b125</div>	数据	2022-08-04 11:19:33	2023-08-04 11:19:33	是	正常	贵州2022影像	<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>
8991bb9e732c8282d3c3233eb382d6db	数据	2022-07-13 14:38:00	2022-07-14 14:38:00	是	正常	LC08_L1TP_125041_20220503_20220511_02_T1	<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>
7469ef4ae8435e1de54fba380e2f2662	数据	2022-06-18 11:46:03	2023-06-18 11:46:03	是	正常	清镇国有林场	<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>
f43222444db7b7bc88dd5bd89ab105d	数据	2022-06-18 11:24:56	2023-06-18 11:24:56	是	正常	清镇国有林场	<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>
42e99f899b90a0f76323daae1ef47d319	数据	2022-06-17 19:40:26	2023-06-17 19:40:26	是	正常		<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>
cab9e1f5edd65cdc258b0e66151e80736	数据	2022-04-19 18:06:16	2022-05-19 18:06:16	是	正常	昆明正时影像	<div>查看</div> <div>编辑</div> <div>新增</div> <div>删除</div>

第 1 到第 6 项, 共 6 项



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

发现没有cookie 校验，可以直接访问

