VUE framework system has logical defects and vulnerabilities

Vulnerability description:

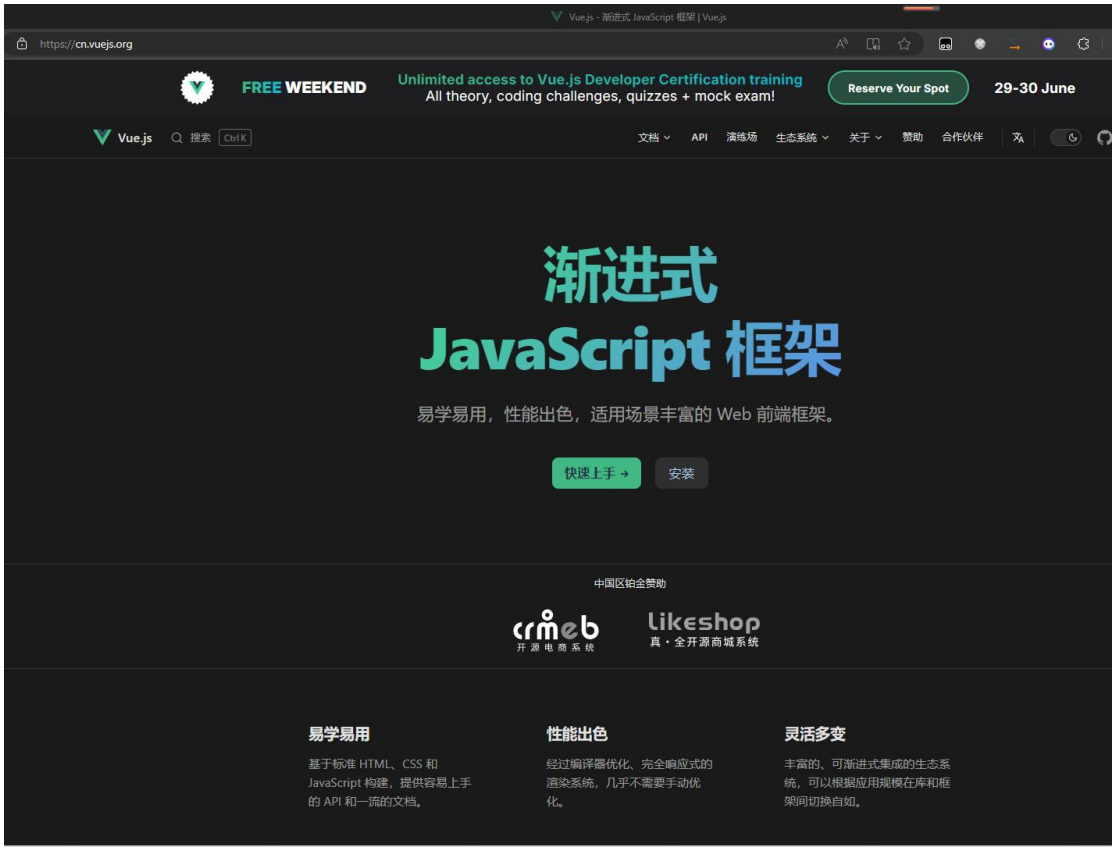
Vue.js is a progressive framework for building user interfaces A JavaScript framework used to build user interfaces. As one of the three dominant front-end frameworks (Vue, React, Angular), it is built on standard HTML, CSS, and JavaScript, and provides a declarative, component-based programming model to help you efficiently develop user interfaces.

The VUE framework system has a logical vulnerability that attackers can exploit to bypass system authentication and log in to any account.

It can be seen that the versions involved are both 2.6. x and 2.7. x

VUE official website:

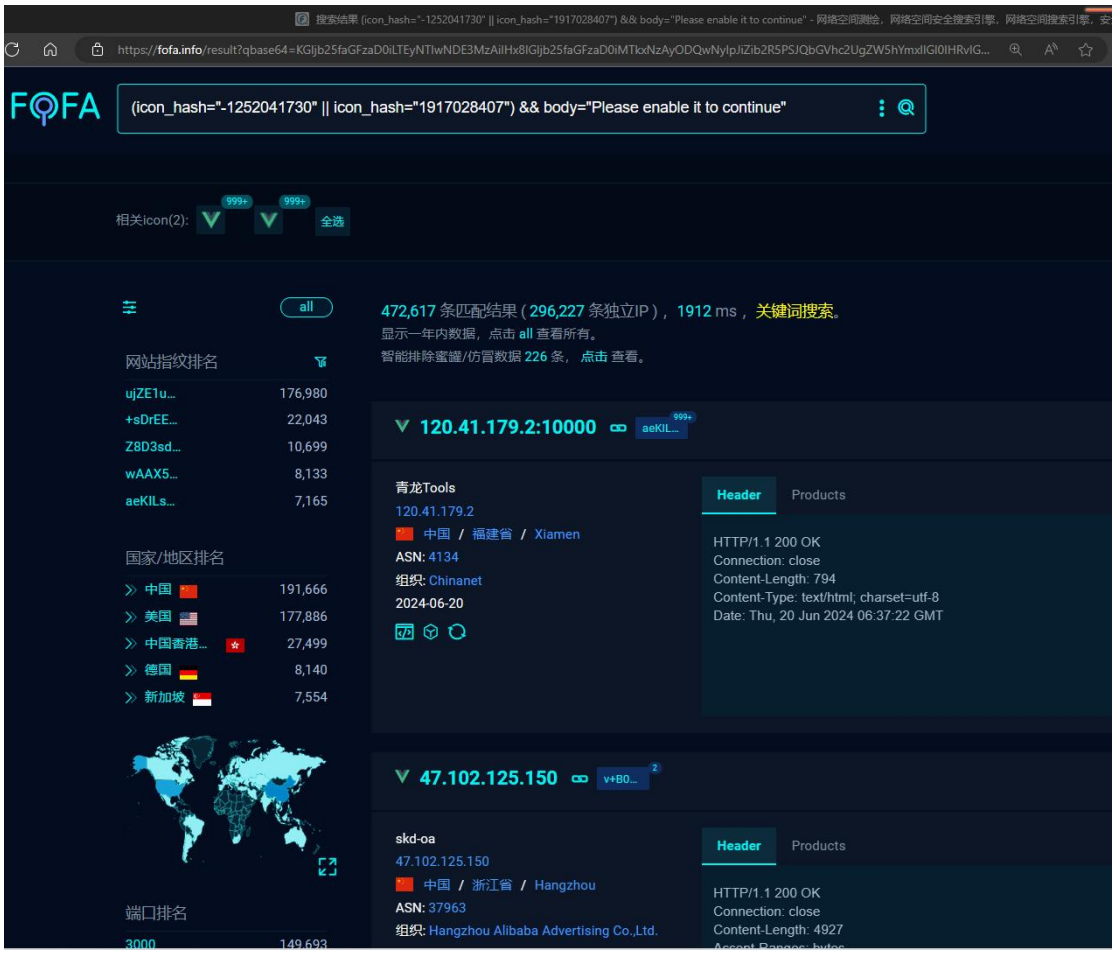
https://cn.vuejs.org/



Fofa syntax: JS page prompts for filtering VUE framework icons and VUE framework BODY attributes

(icon_hash="-1252041730" || icon_hash="1917028407") && body="Please enable it to

continue"

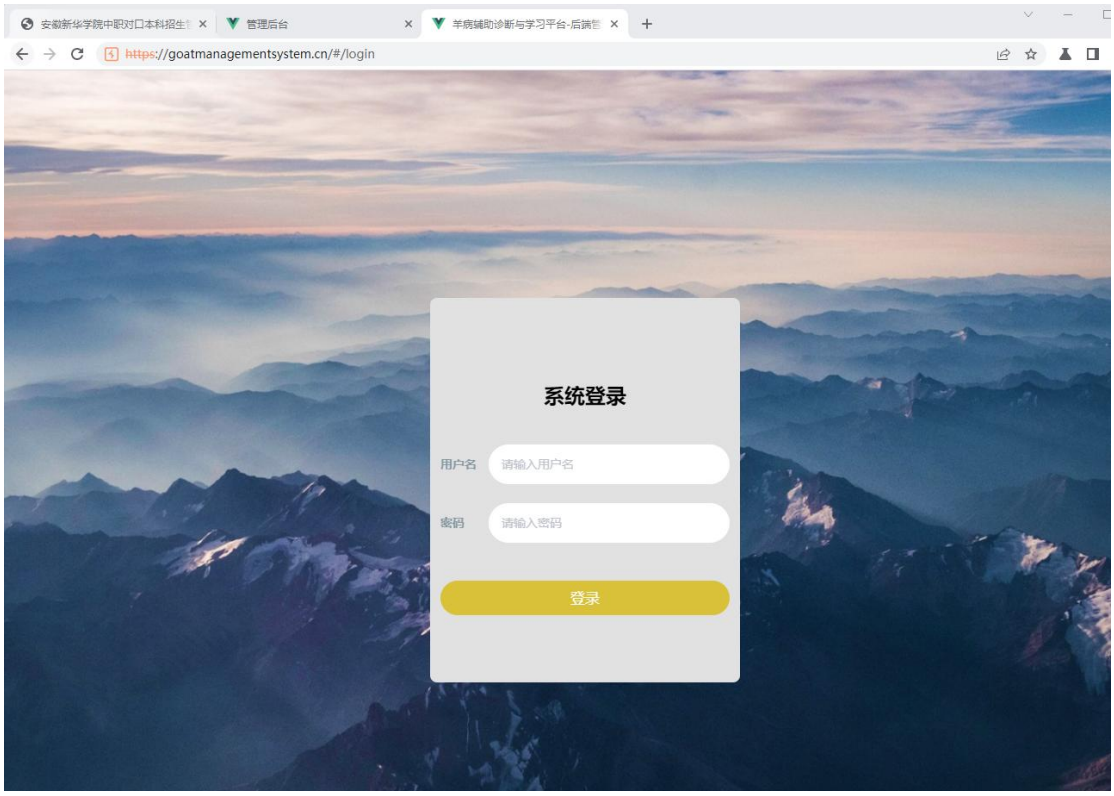


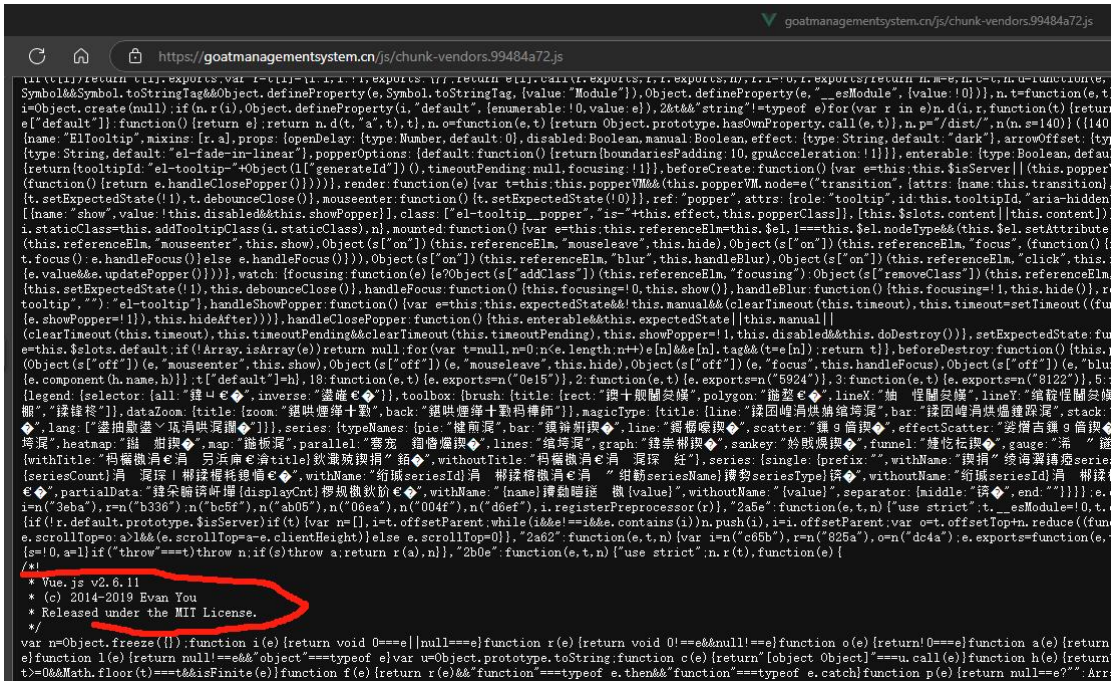
2. Reproduce the process

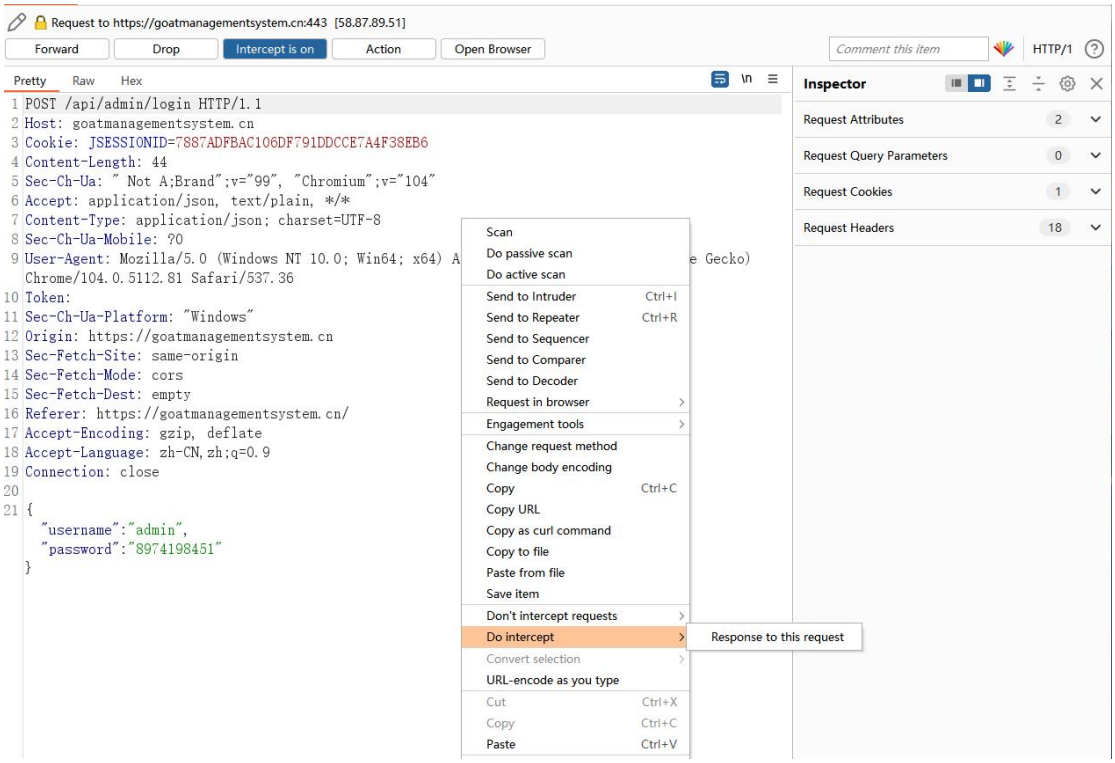
Reproduce IP1: https://goatmanagementsystem.cn/#/login

You can use the shortcut key: ctrl+u to view the page source code, and check the/js/chunk vendors. xxxxxx. js file to see the Vue framework version.

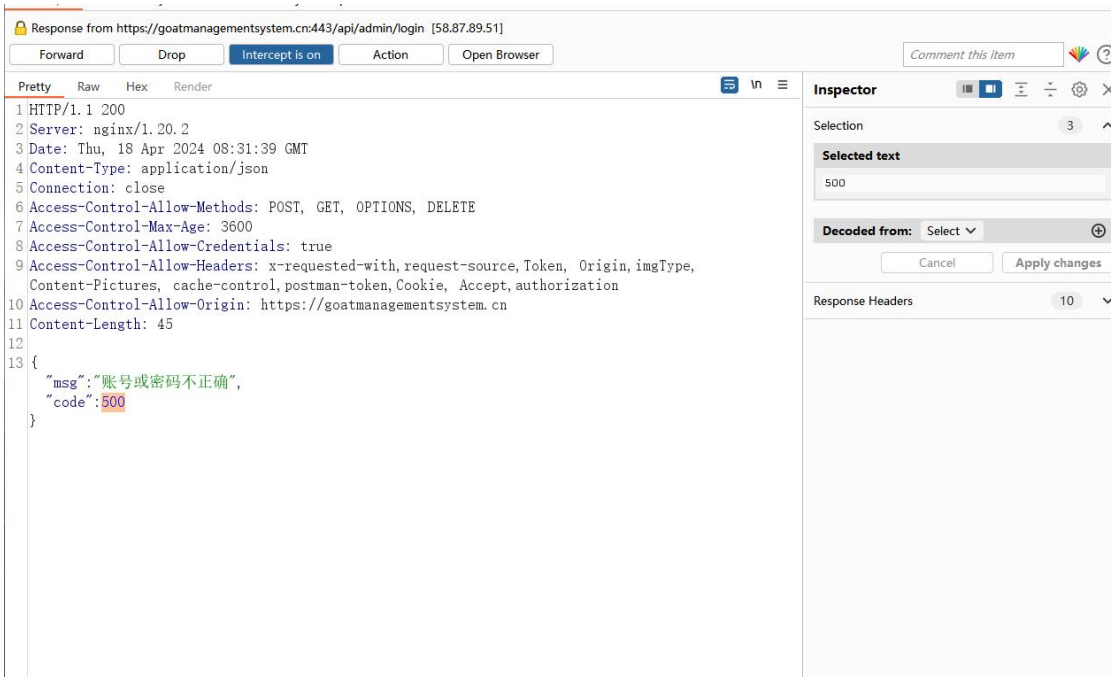
Use BURP to capture login packages, right-click on the burst and select the DO intercept option.

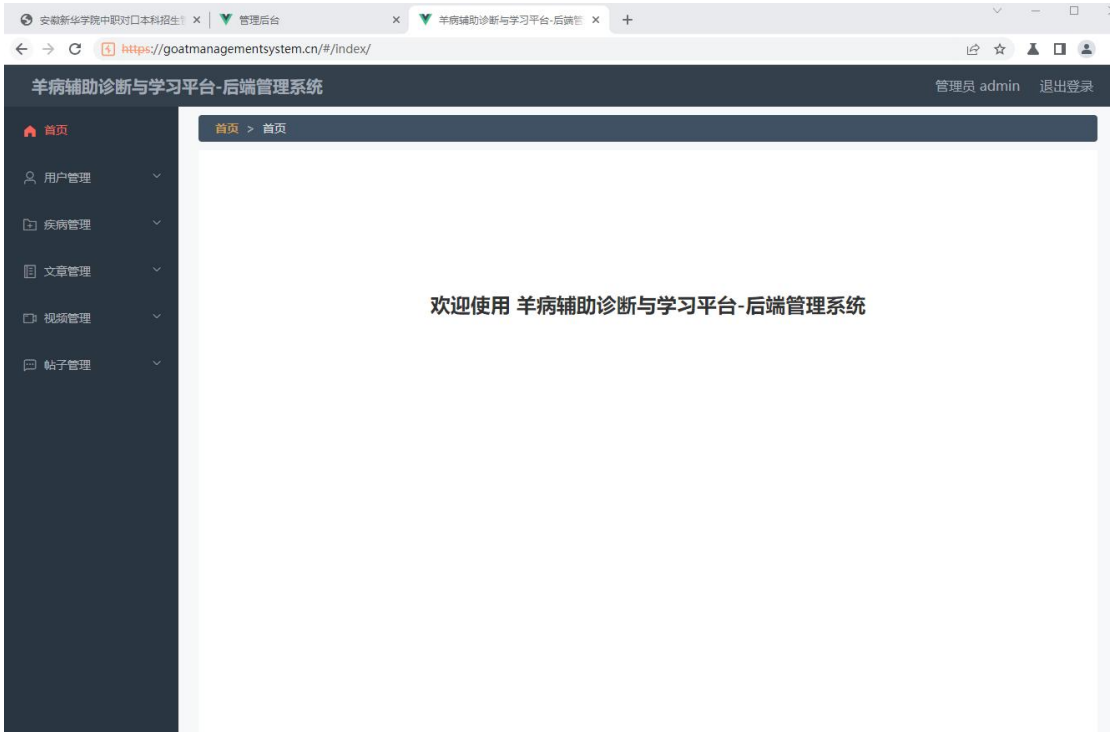

安徽新华学院中职对口本科招生
管理后台
羊病辅助诊断与学习平台-后端
https://goatmanagementsystem.cn/#/login
系统登录
用户名
请输入用户名
密码
请输入密码
登录


goatmanagementsystem.cn/js/chunk-vendors.99484a72.js
https://goatmanagementsystem.cn/js/chunk-vendors.99484a72.js
/*!
* Vue.js v2.6.11
* (c) 2014-2019 Evan You
* Released under the MIT License.
*/

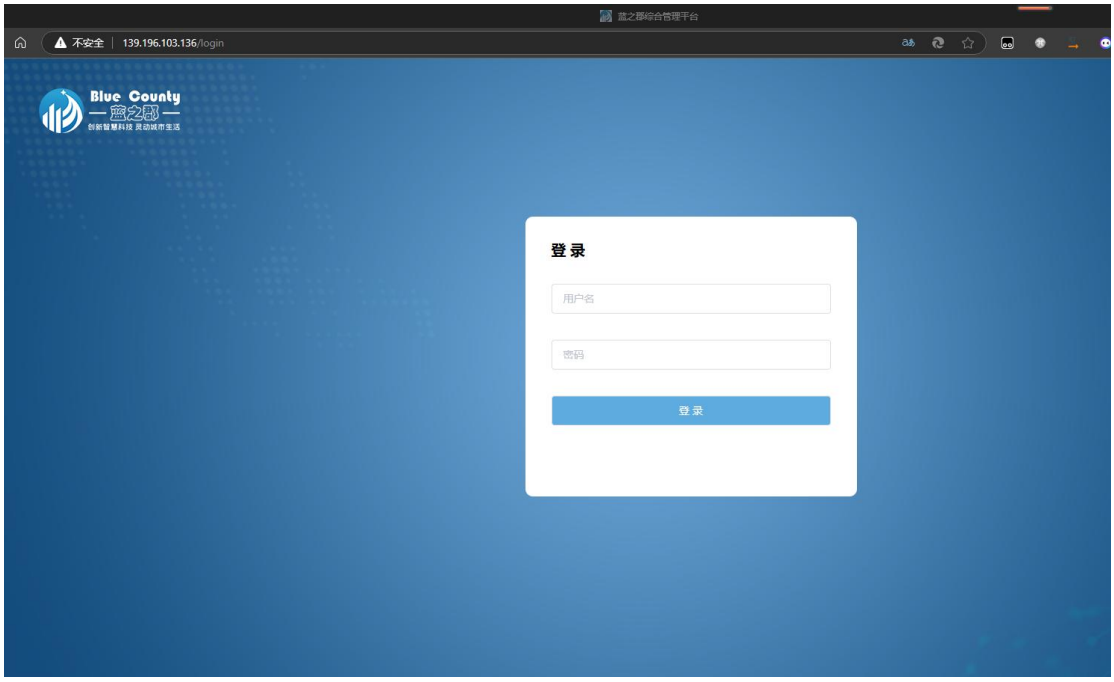


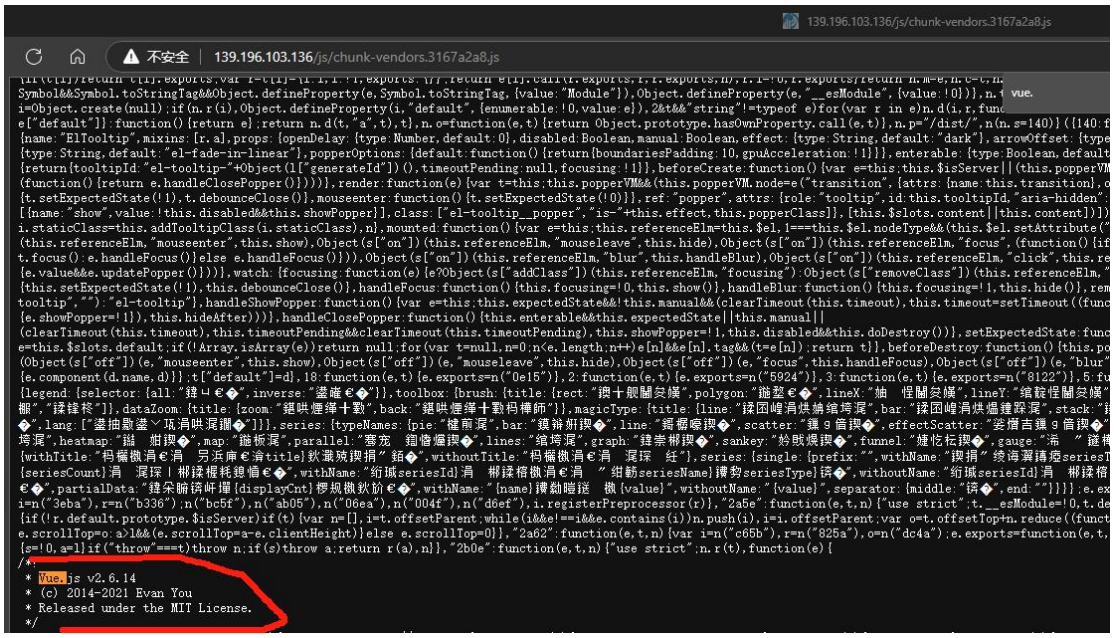
Change the code to 200.

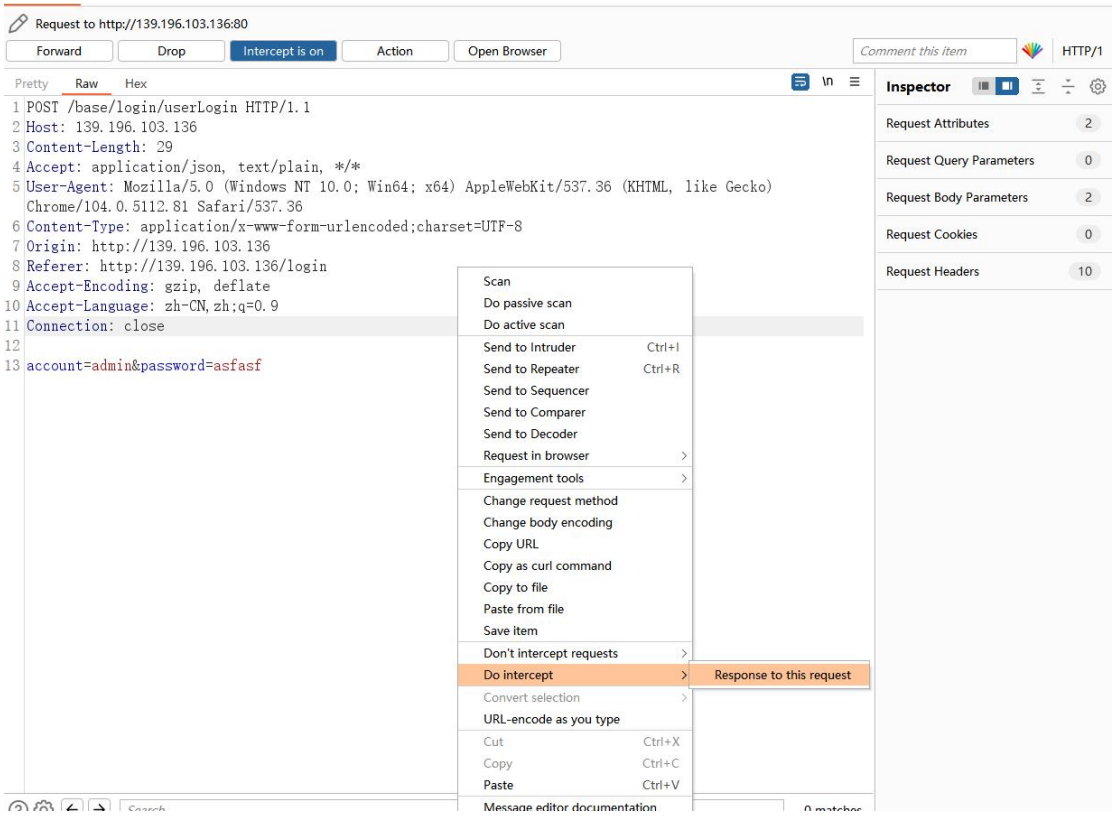


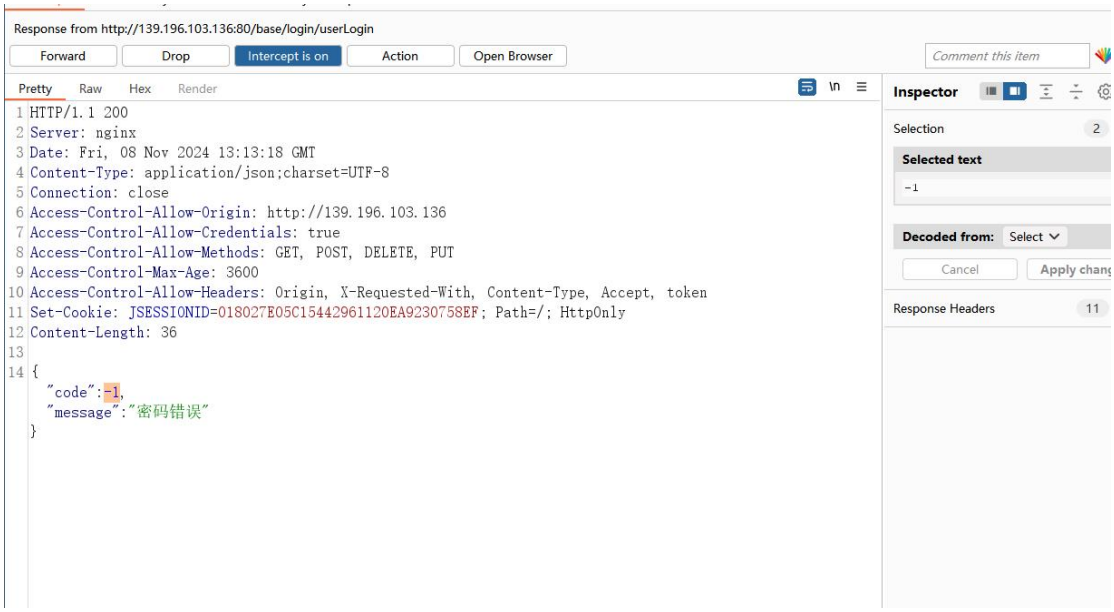


IP2：http://139.196.103.136/

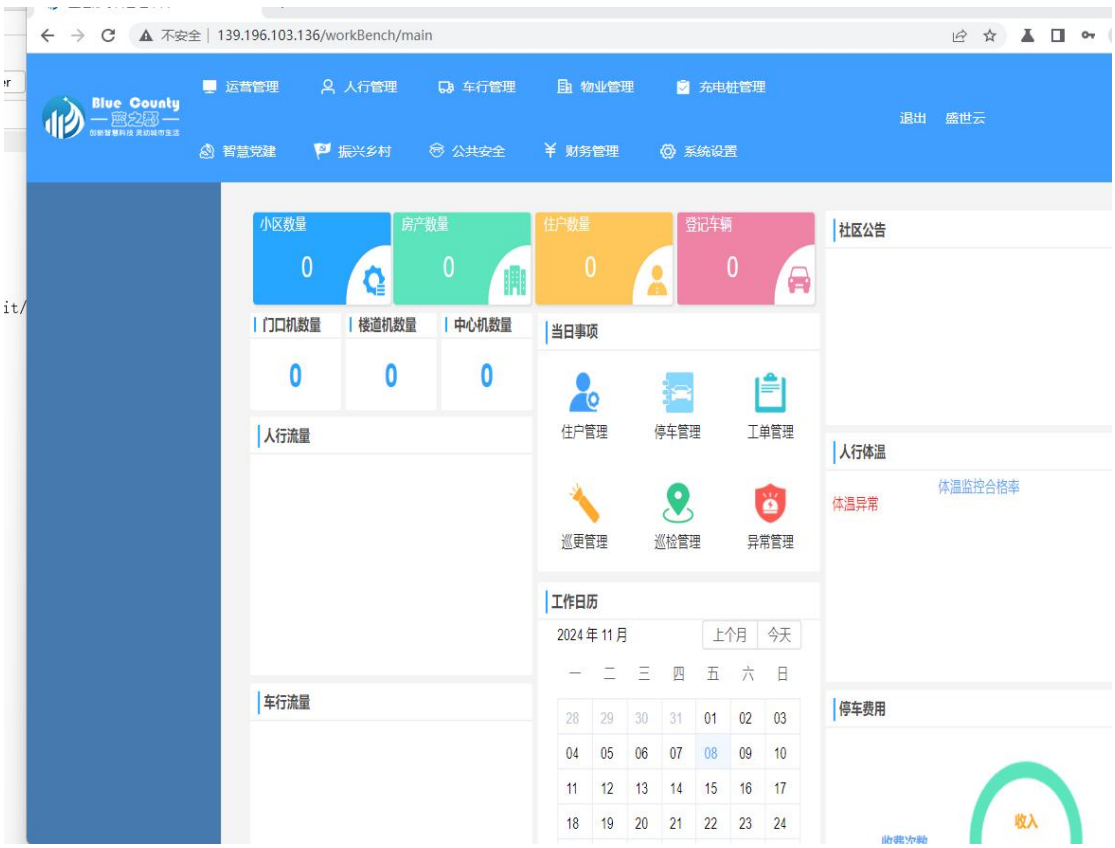



139.196.103.136/js/chunk-vendors.3167a2a8.js
不安全
139.196.103.136/js/chunk-vendors.3167a2a8.js
vue.
* Vue.js v2.6.14
* (c) 2014-2021 Evan You
* Released under the MIT License.


Request to http://139.196.103.136:80
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
HTTP/1
Pretty
Raw
Hex
1 POST /base/login/userLogin HTTP/1.1
2 Host: 139.196.103.136
3 Content-Length: 29
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36
6 Content-Type: application/x-www-form-urlencoded;charset=UTF-8
7 Origin: http://139.196.103.136
8 Referer: http://139.196.103.136/login
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13 account=admin&password=asfasf
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 0
Request Headers 10
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Response to this request
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation

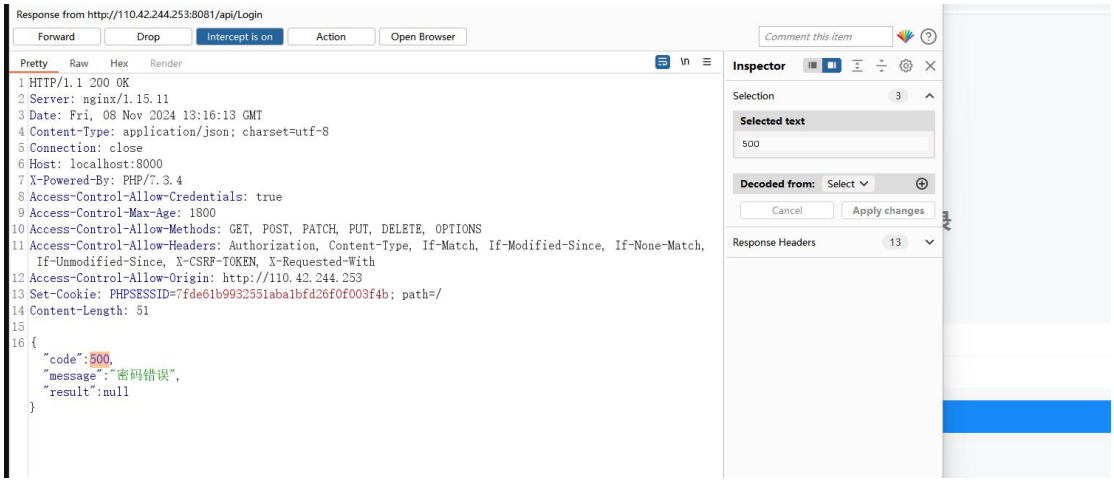


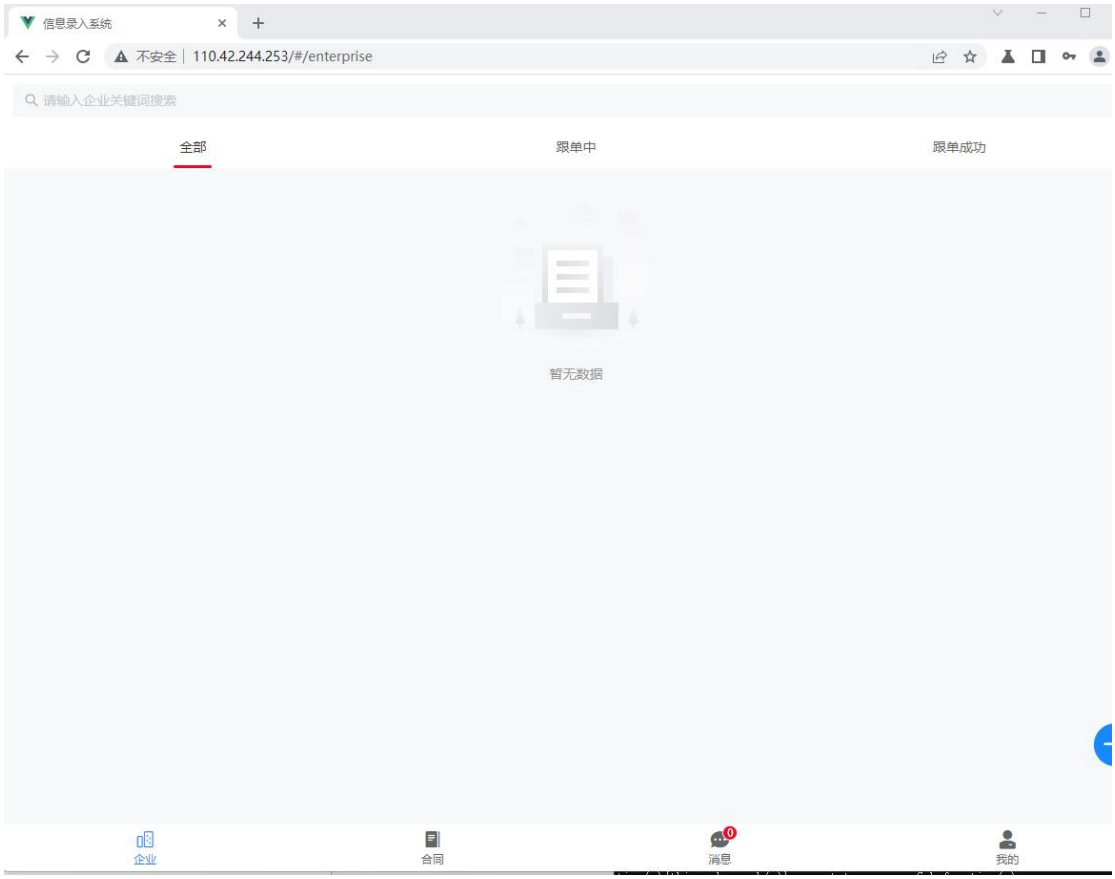
Capture the request packet and intercept the return packet to modify the code to 200.



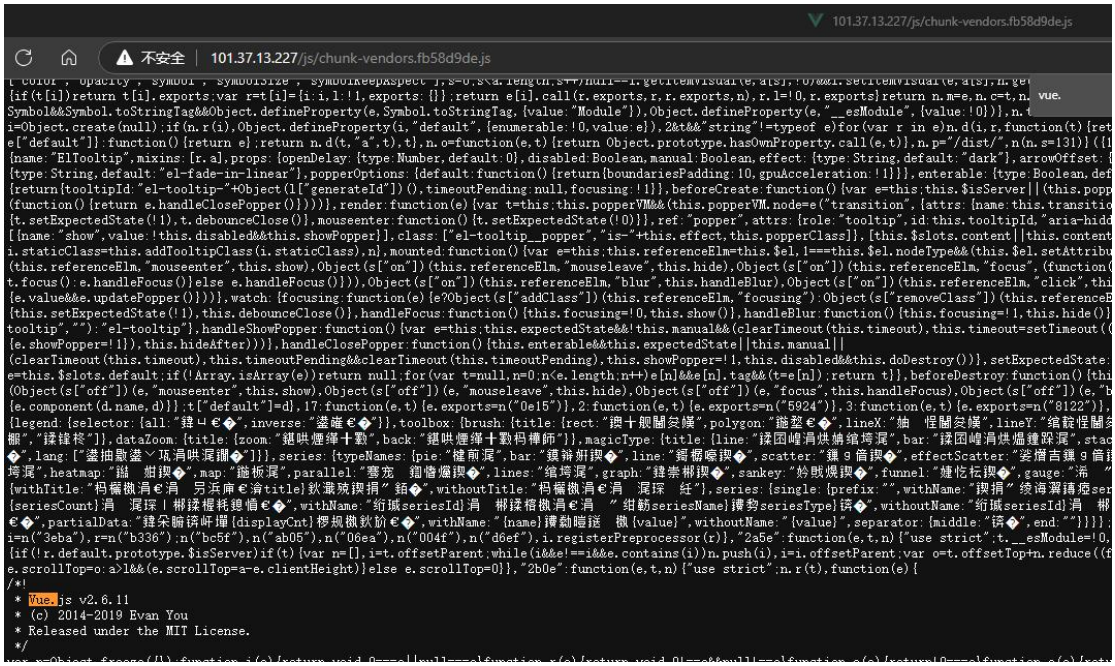
IP3：http://110.42.244.253/

Capture the request packet and intercept the return packet to modify the code to 200.

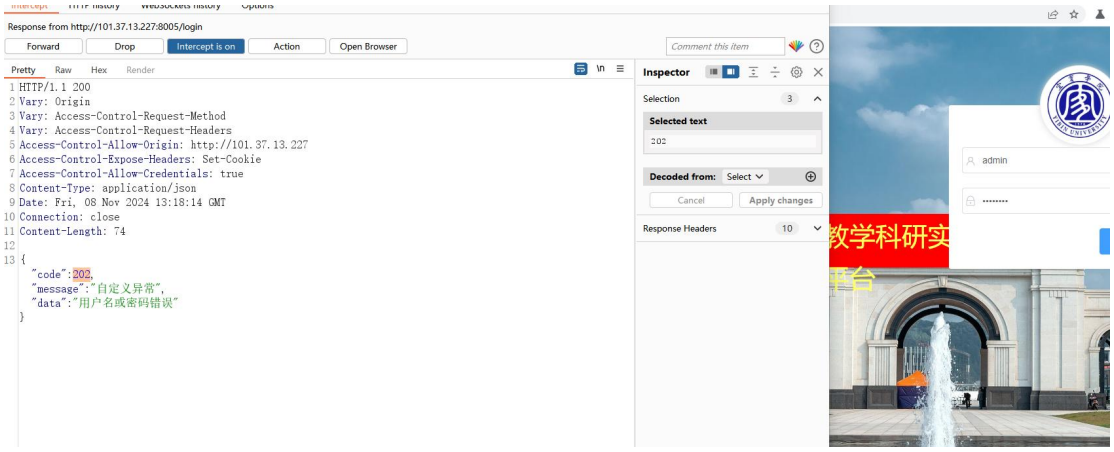


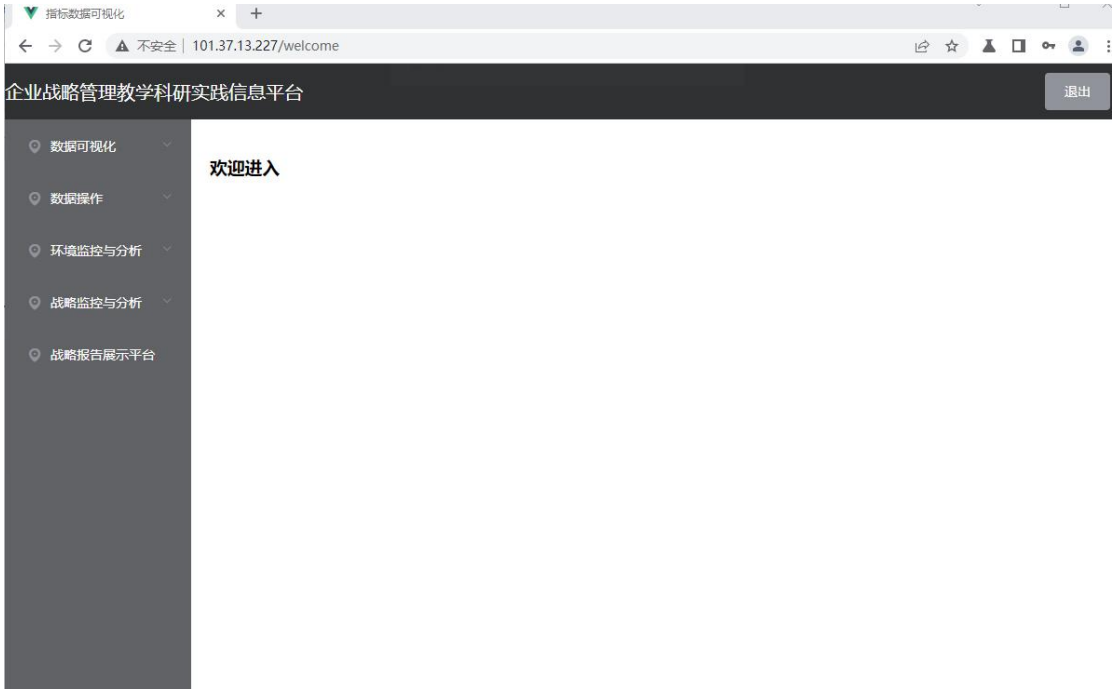


IP4：http://101.37.13.227

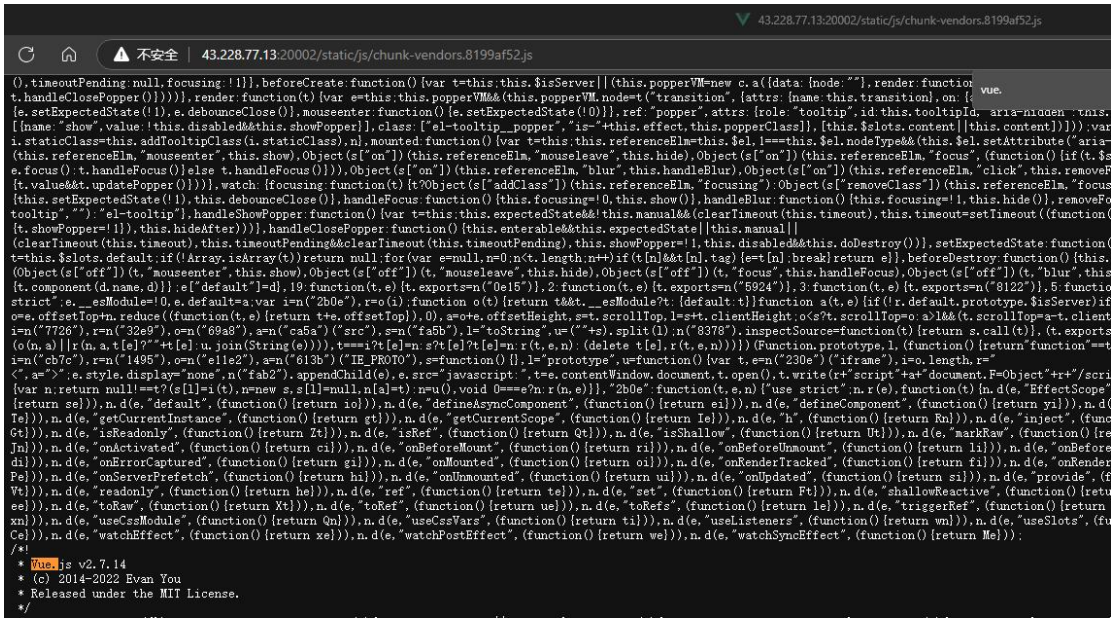


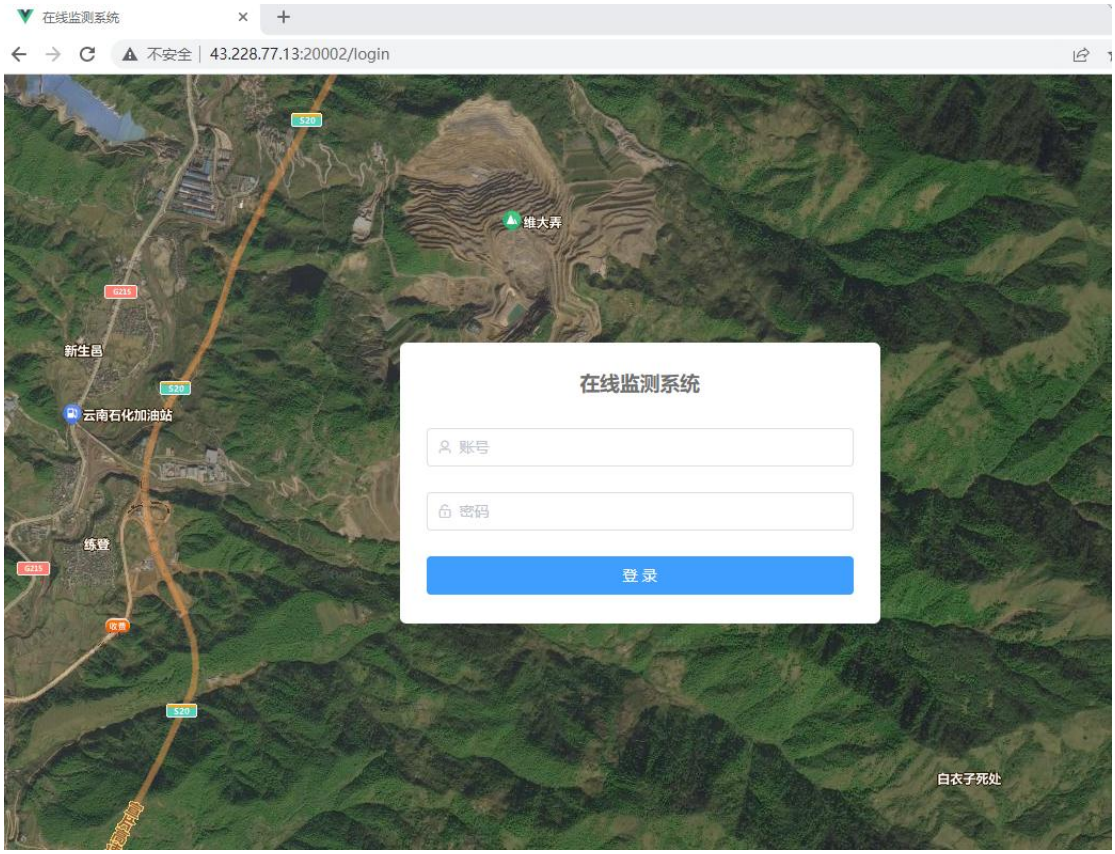
Capture the request packet and intercept the return packet to modify the code to 200.



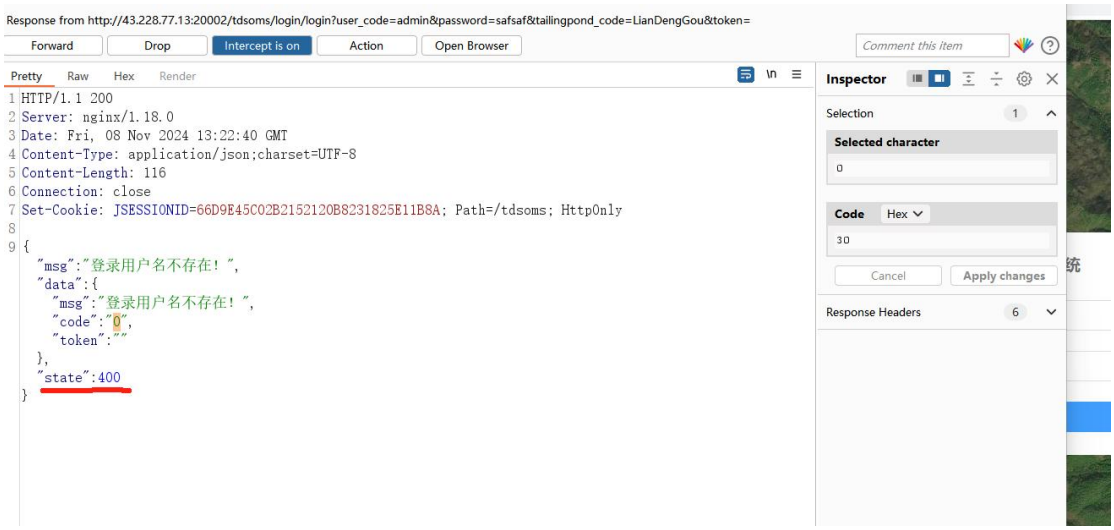


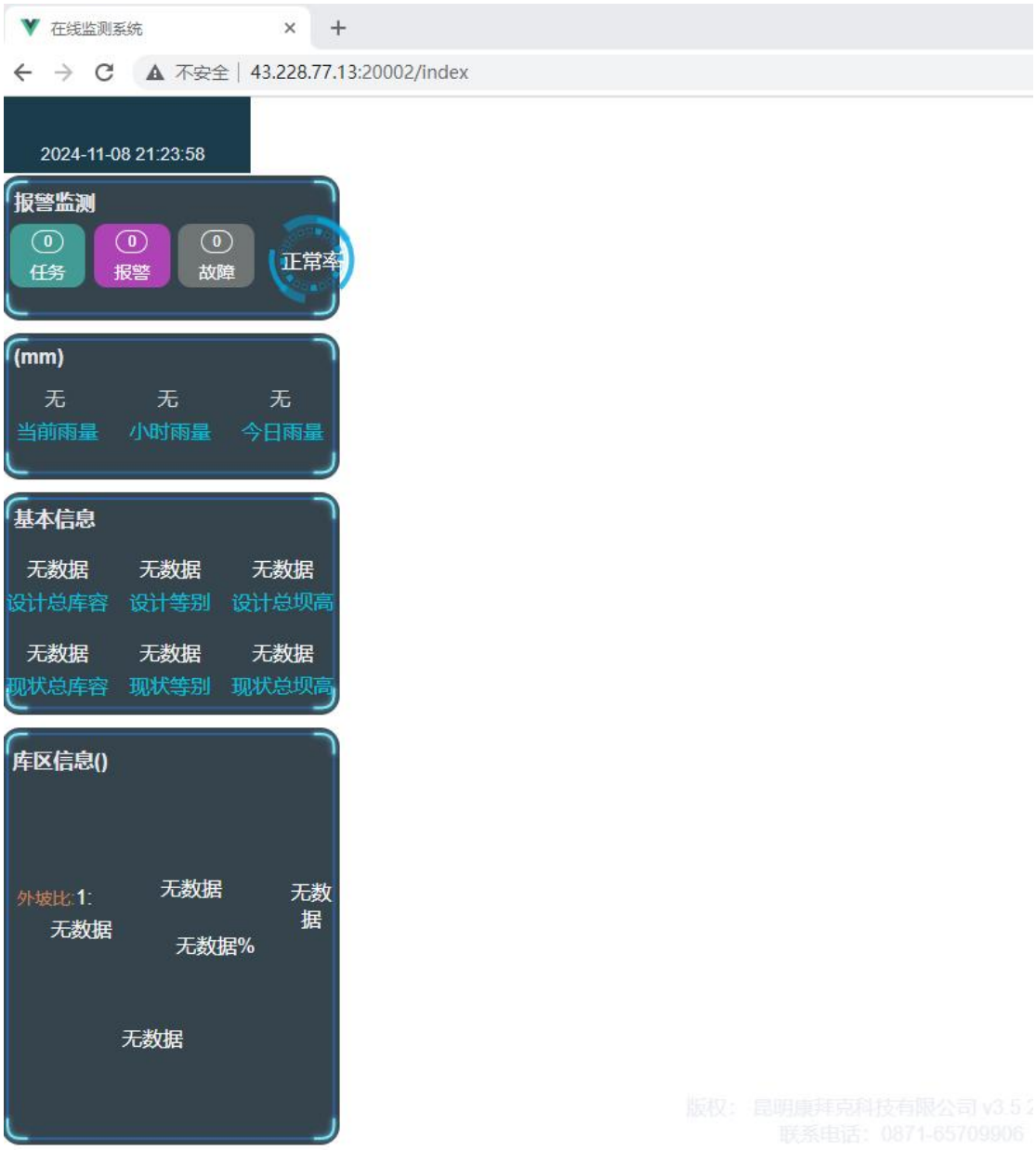
IP5:http://43.228.77.13:20002



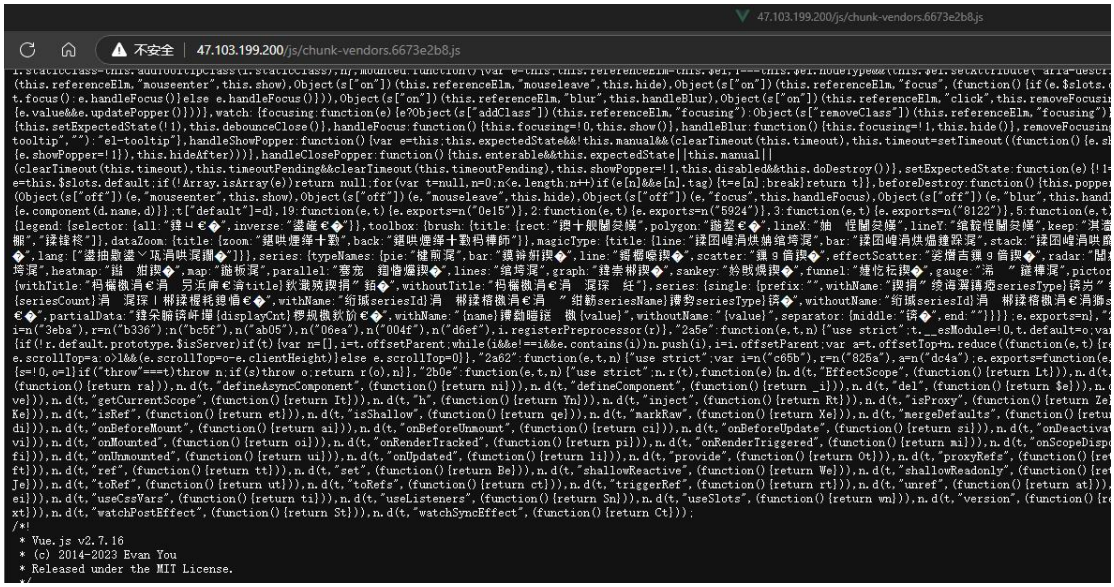


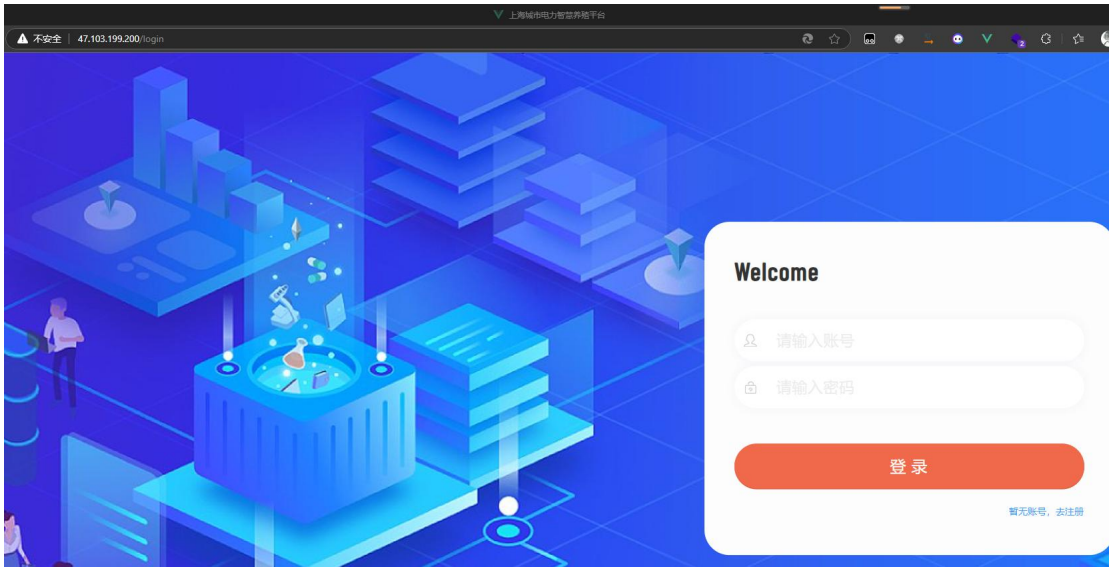
We need to change both the code and state to 200 here.



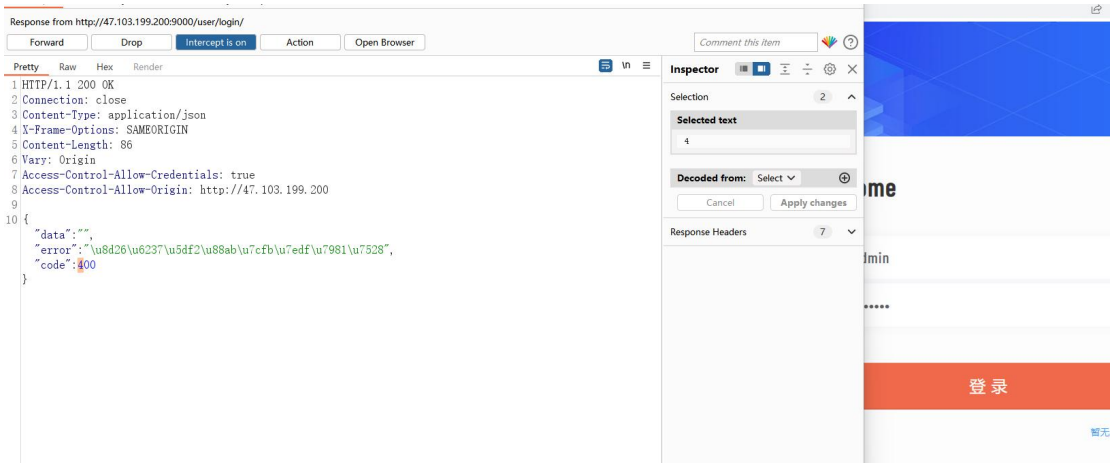


IP6：http://47.103.199.200/





Capture the request packet and intercept the return packet to modify the code to 200.




上海城市电力智慧养殖平台
不安全 | 47.103.199.200/home
上海城市电力智慧养殖平台
2024-11-08 21:26:43
退出登录
企业介绍
上海城市电力发展有限公司是一家集水产养殖、新能源、农业种植、农业休闲旅游观光的综合性开发公司。公司以发展绿色能源、生态养殖为使命，严格按照绿色、环保、生态的总体定位和
温度℃
湿度
风向
风力
光照
降雨量
大气压
报警统计
基地列表
报警信息