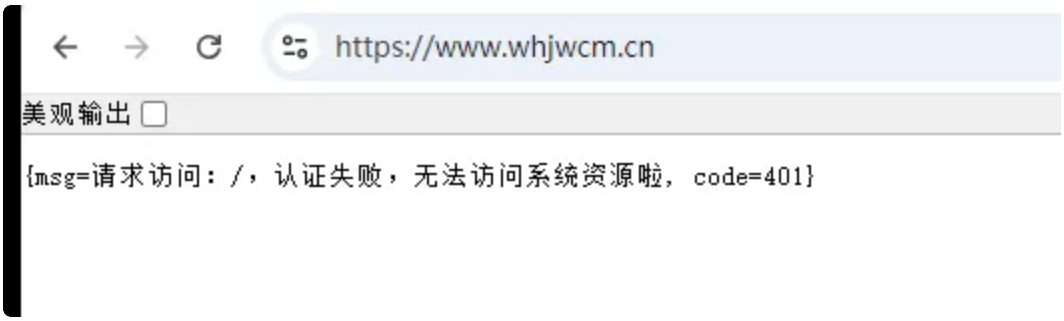
8、拿到网站怎么去挖掘漏洞

1、域名：http://whjwcm.cn/　资产比较少



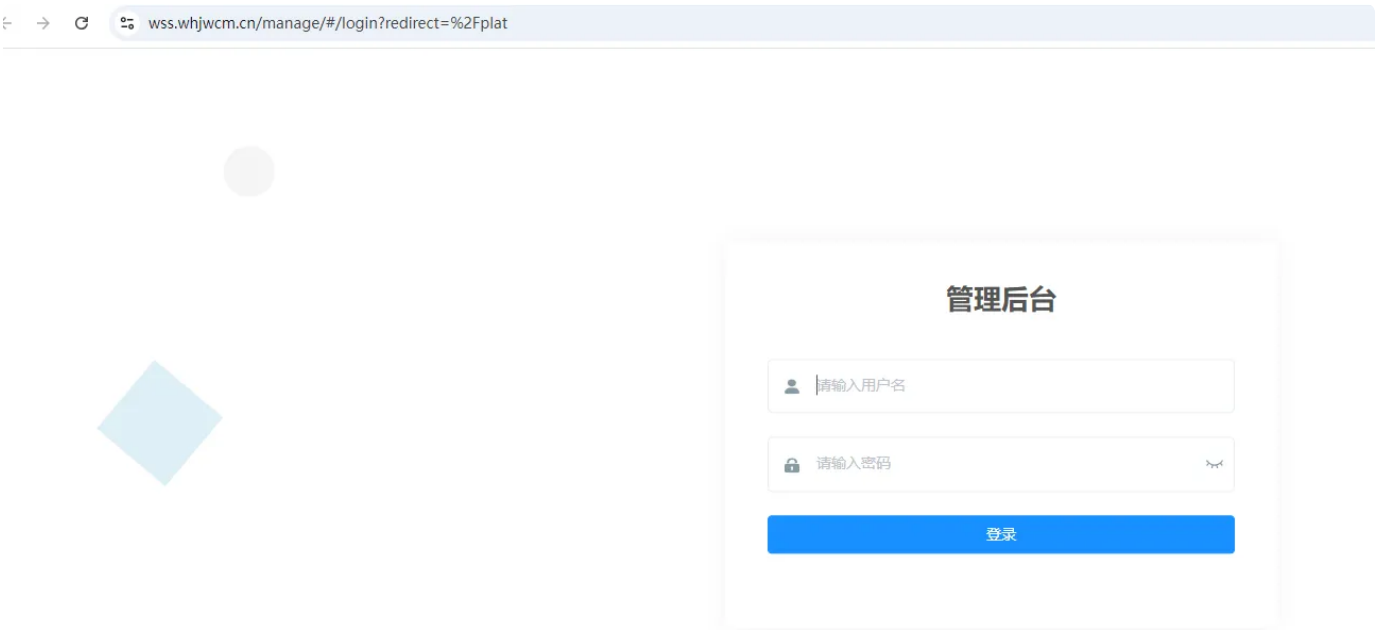
Python

```
出现这个页面，可能存在路径未拼接
去看看其他端口，不要只看web端，也要看看其他端口服务进行测试
```

Python

```
22 端口爆破基本会不成功 ， 可以忽略
3306 数据库爆破
6379 是否空密码和未授权
3389 看可能是windows系统
8081 页面也是没有东西，可以进行目录扫描，看是否存在服务
```

2、管理后台测试思路



测试思路 Python

```
1  弱口令尝试
2  看是否能用户遍历
3  看框架，是否存在可利用的漏洞
```

其他方法还不行的话，可以查看js代码，需要抓包去测试一下

请求

美化 Raw Hex U2C

```
1  POST /admin/user/login HTTP/2
2  Host: wss.whjwcm.cn
3  Content-Length: 39
4  Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24",
   "Google Chrome";v="128"
5  Accept: application/json, text/plain, */*
6  Sec-Ch-Ua-Platform: "Windows"
7  Sec-Ch-Ua-Mobile: ?0
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0
    Safari/537.36
9  Content-Type: application/json;charset=UTF-8
10 Origin: https://wss.whjwcm.cn
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh;q=0.9
16 Priority: u=1, i
17
18 {
     "username":"admin",
     "password":"12345"
   }
```

响应

美化 Raw Hex 页面渲染 U2C

```
1  HTTP/2 200 OK
2  Server: nginx
3  Date: Fri, 13 Sep 2024 07:30:10 GMT
4  Content-Type: application/json; charset=UTF-8
5  Access-Control-Allow-Origin: *
6  Access-Control-Allow-Headers: *
7  Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT,
   DELETE, HEAD
8  Strict-Transport-Security: max-age=31536000
9
10 {
     "error":1,
     "msg":
     "\u7528\u6237\u540d\u6216\u5bc6\u7801\u4e0d\u6b63\u78
     6e",
     "data":""
   }
```

1、看到数据包，我们可能会改一下返回包的数据，将error：改为0 ，试一下是否能进行绕过

2、有可能是服务器是通过校验data数据进行判断的，看是否添加data数据进行绕过

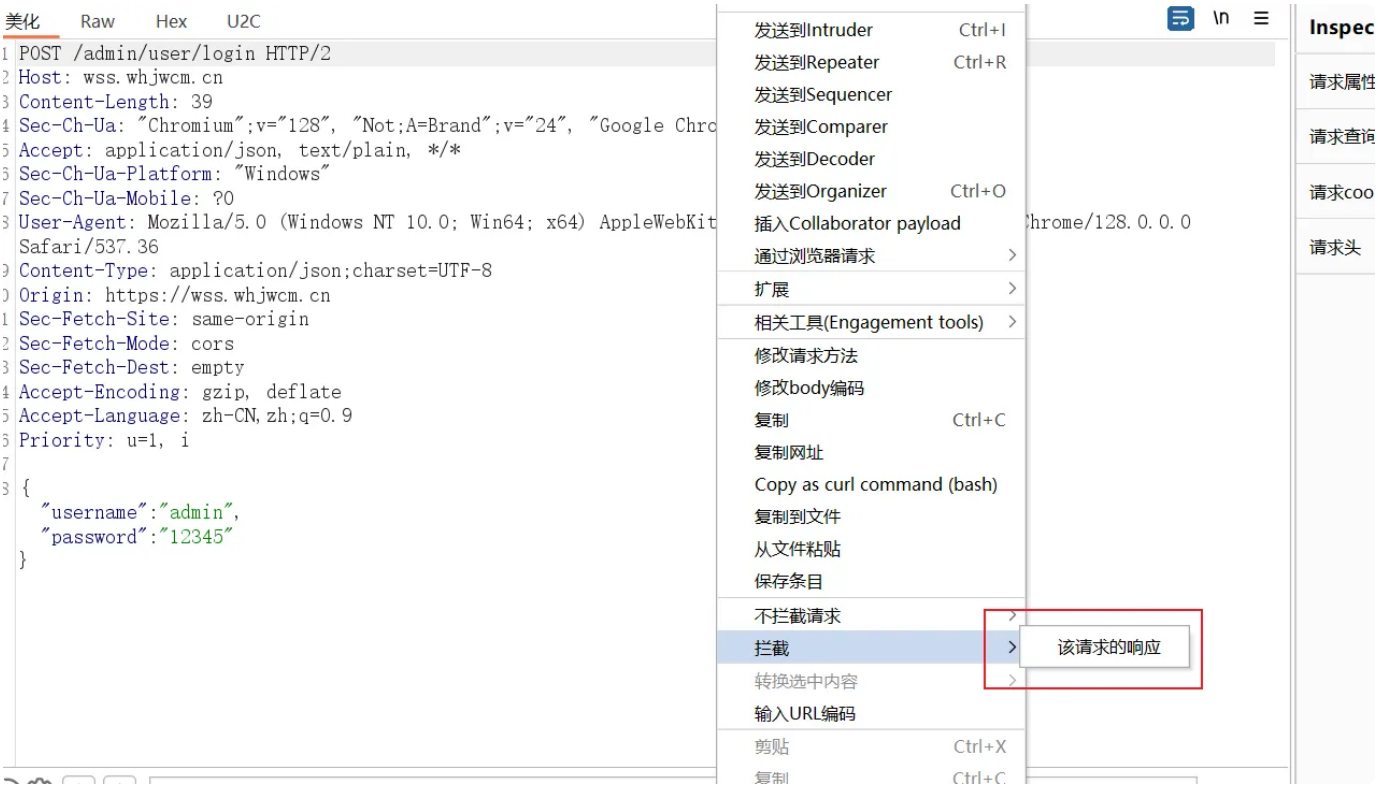
```
13          }
14      }, {
15          url: "/vue-element-admin/user/logout",
16          type: "post",
17          response: function(e) {
18              return {
19                  code: 2e4,
20                  data: "success"
21              }
22          }
23      }]
24  },
25  "39d6": function(e, t, n) {},
26  "3b07": function(e, t, n) {
27      "use strict";
28      n("92a5")
29  },
30  4360: function(e, t, n) {
```

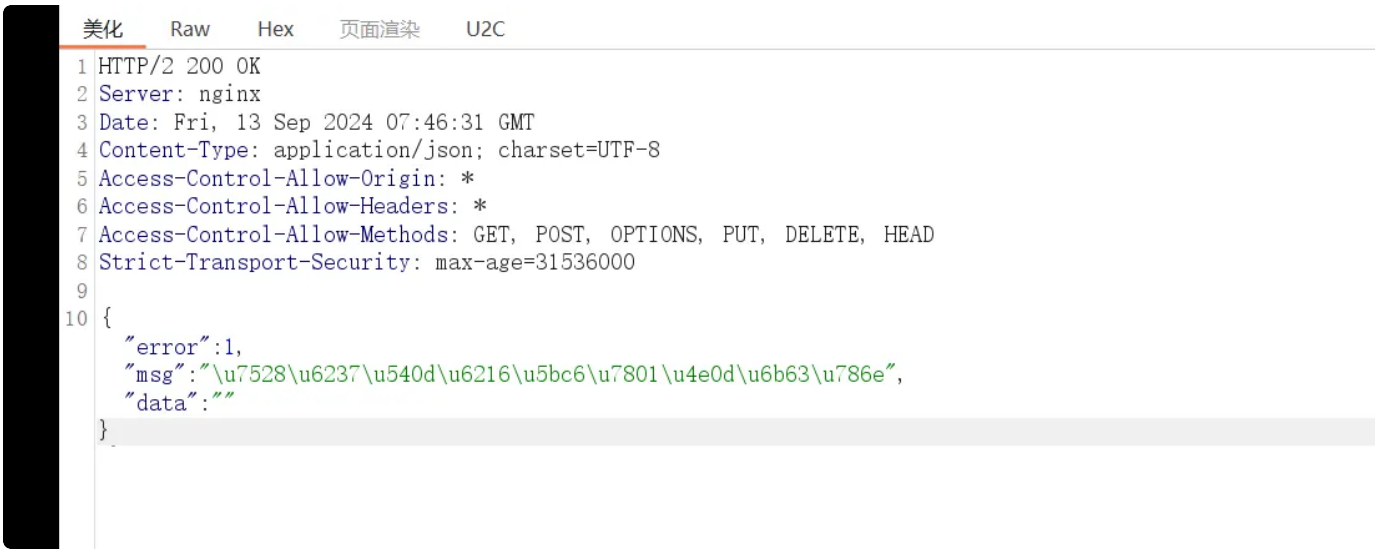
看将data添加上数据是否能进行绕过

3、像这种站点/#/ webpack 站点，更改逻辑的很不好去测试到成果

还有一个思路是，在登录的情况下，去丢包

先去抓一个包，然后拦截



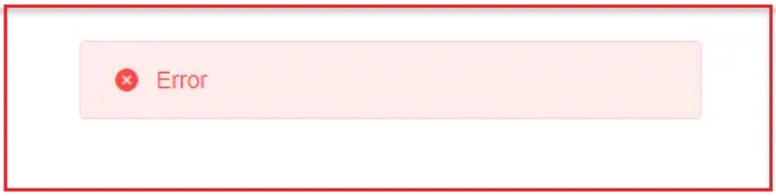


不改数据的话，返回账号密码不正确，空数据

我们修改返回包(确实改为0，会跳转到info路径)

就到了这个页面，将这个页面丢弃到，看是否能绕过（这个页面是存在的，但是存在Admin-Token的限制，未登录成功）

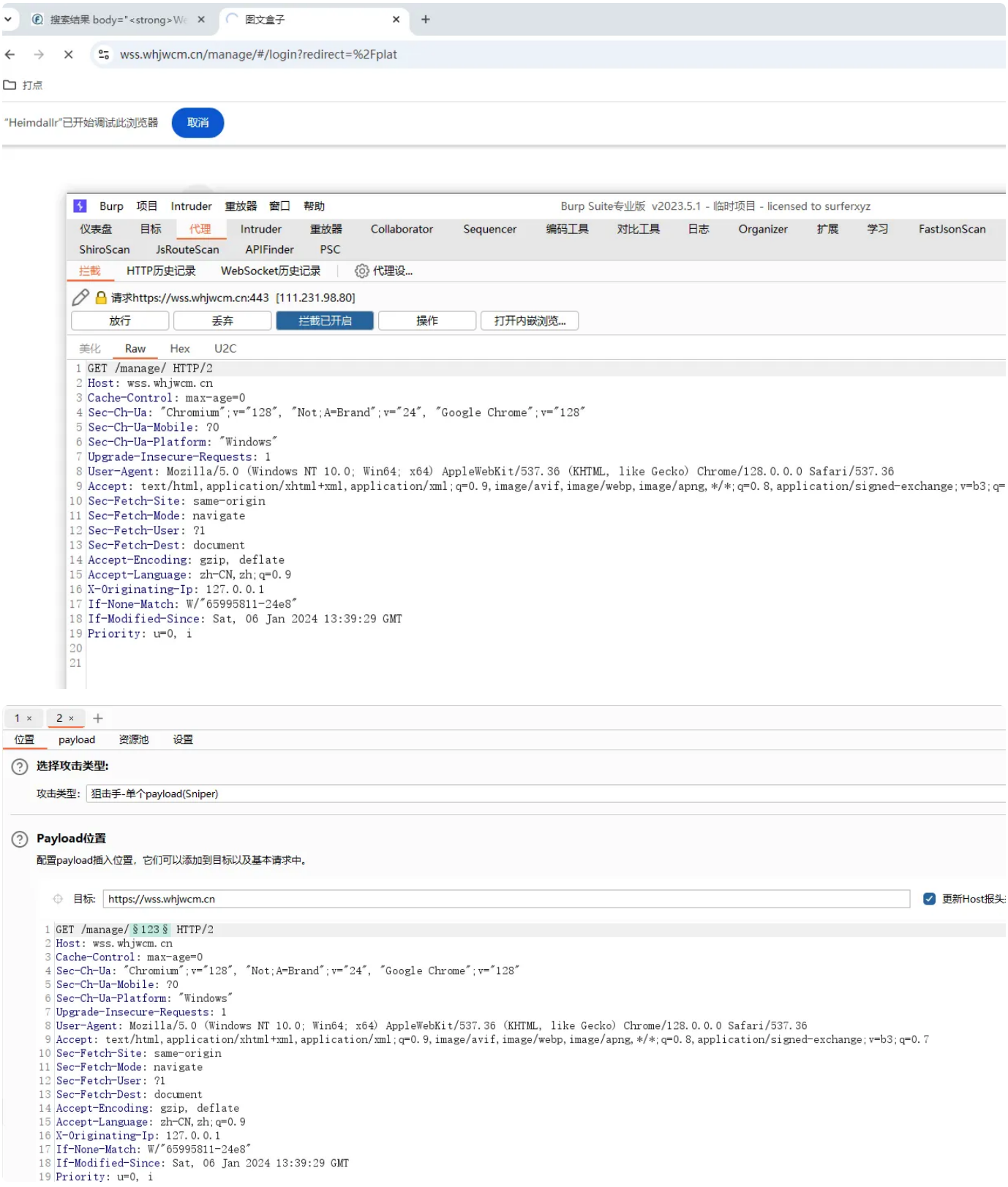
```
GET /admin/user/info HTTP/2
Host: wss.whjwcm.cn
Cookie: Admin-Token=undefined
Sec-Ch-Ua: "Chromium";v="128", "Not;A=Brand";v="24", "Google Chrome";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Priority: u=1, i
```



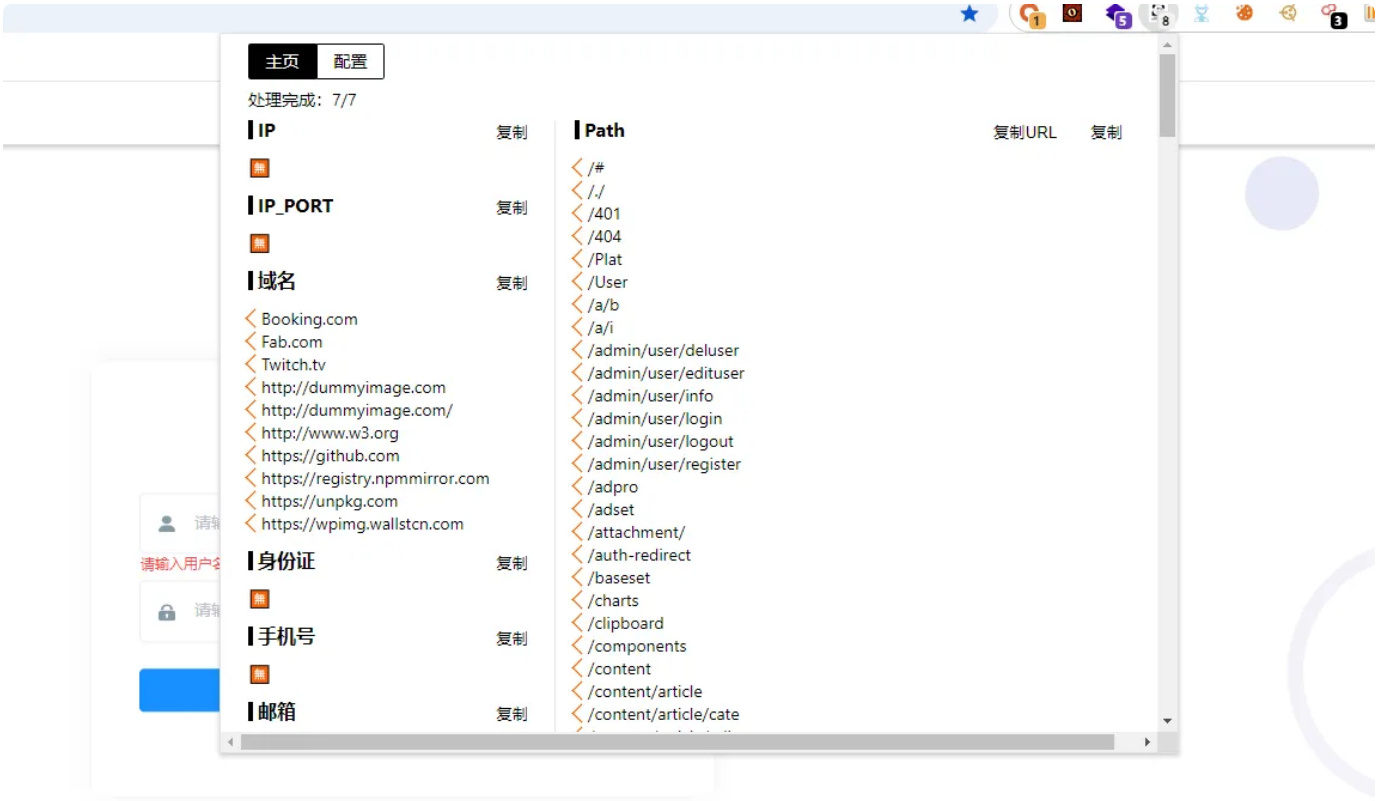
4、换个思路再测一下

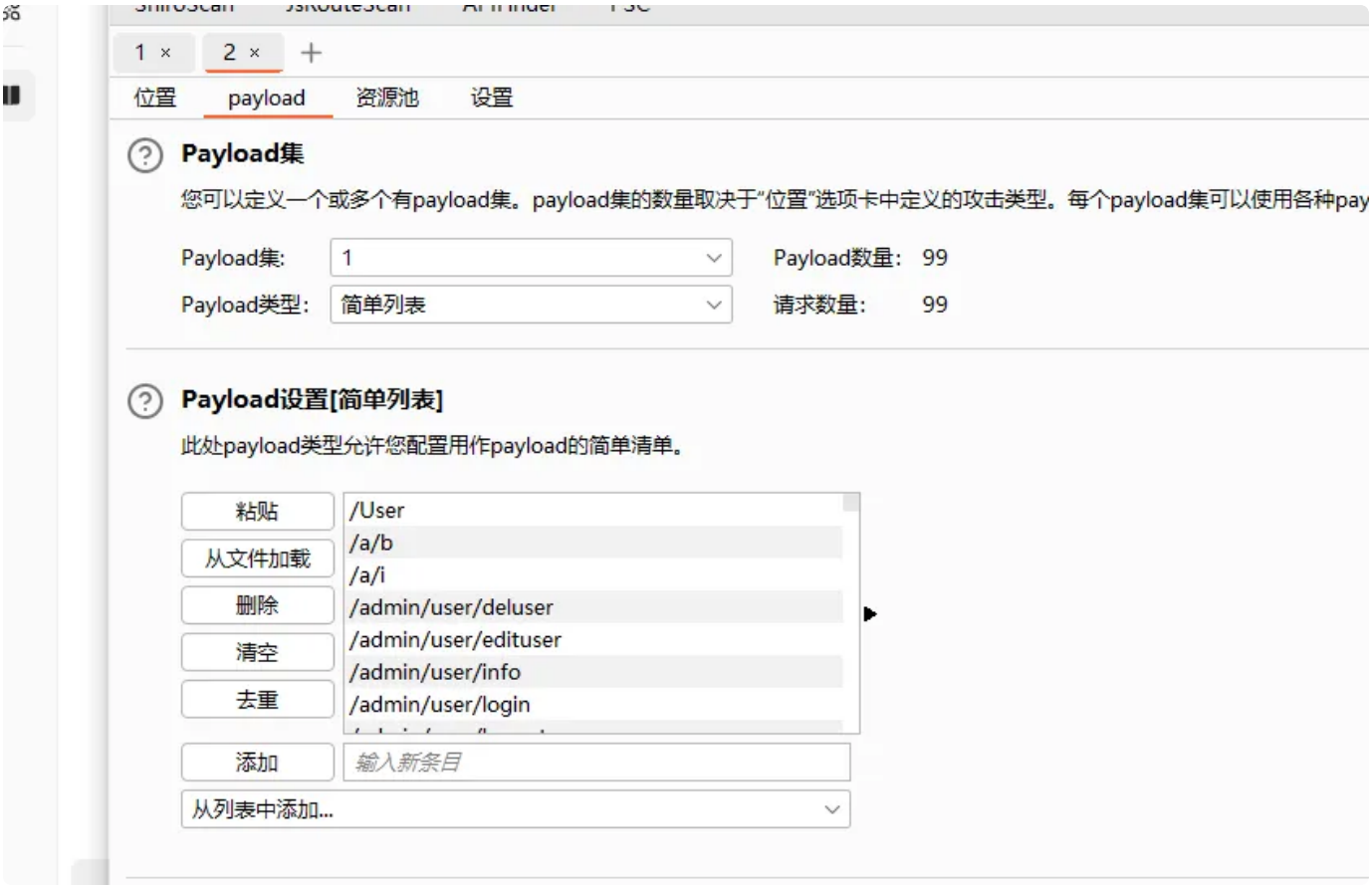
去拼接路径信息

去抓一下包



拼接findsomething中的路径信息


主页
配置
处理完成：7/7
IP
复制
IP_PORT
复制
域名
复制
Booking.com
Fab.com
Twitch.tv
http://dummyimage.com
http://dummyimage.com/
http://www.w3.org
https://github.com
https://registry.npmmirror.com
https://unpkg.com
https://wpimg.wallstcn.com
身份证
复制
手机号
复制
邮箱
复制
Path
复制URL
复制
/#
/./
/401
/404
/Plat
/User
/a/b
/a/i
/admin/user/deluser
/admin/user/edituser
/admin/user/info
/admin/user/login
/admin/user/logout
/admin/user/register
/adpro
/adset
/attachment/
/auth-redirect
/baseset
/charts
/clipboard
/components
/content
/content/article
/content/article/cate


1 ×
2 ×
位置
payload
资源池
设置
Payload集
您可以定义一个或多个有payload集。payload集的数量取决于"位置"选项卡中定义的攻击类型。每个payload集可以使用各种pay
Payload集:
1
Payload数量:
99
Payload类型:
简单列表
请求数量:
99
Payload设置[简单列表]
此处payload类型允许您配置用作payload的简单清单。
粘贴
从文件加载
删除
清空
去重
/User
/a/b
/a/i
/admin/user/deluser
/admin/user/edituser
/admin/user/info
/admin/user/login
添加
输入新条目
从列表中添加...